



ESTUDOS SOBRE A LGPD

LEI GERAL DE PROTEÇÃO DE DADOS

DOCTRINA E APLICABILIDADE NO ÂMBITO LABORAL

Artigos, Decisões & Glossário

Organizadores:

Luciane Cardoso Barzotto e Ricardo H. Martins Costa

Apoio:



**ESTUDOS SOBRE LGPD – LEI
GERAL DE PROTEÇÃO DE
DADOS – LEI Nº 13.709/2018:
DOCTRINA E APLICABILIDADE
NO ÂMBITO LABORAL**

ORGANIZADORES

LUCIANE CARDOSO BARZOTTO

**Desembargadora do TRT da 4ª Região, Doutora em Direito pela UFPR
e professora do Programa de Pós-graduação em Direito da UFRGS**

RICARDO HOFMEISTER DE ALMEIDA MARTINS COSTA

Desembargador do TRT da 4ª Região, Especialista em Direito pela FGV

© Tribunal Regional do Trabalho da 4ª Região, 2022

Presidente do Tribunal Regional do Trabalho da 4ª Região
Desembargador Francisco Rossal de Araújo
Diretor da Escola Judicial do Tribunal Regional da 4ª Região
Desembargador João Paulo Lucena
Realização administrativa
TRT4 e EJUD4

Edição e editoração: Diadorim Editora
Capa: Rosana de Souza Kim Jobim
Revisão: Cris Gutkoski
Projeto gráfico: Flávio Ilha

CONSELHO CIENTÍFICO-EDITORIAL

Fabiano Menke UFRGS-CNPd (Conselho Nacional de
Proteção de Dados e Privacidade)
Luiz Eduardo Gunther Unicuitiba – TRT9
Denise Maria SchelleMBERGER Fernandes MPT
Regina Linden Ruaro PUCRS
Gabrielle Bezerra Sales Sarlet PUCRS
Giovanni Olsson Unochapecó-CNJ
Tereza Aparecida Asta Gemignani TRT15 – Comitê Científico Enamat
Leandro Krebs Gonçalves EJUD 4

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD

E82 Estudos sobre LGPD – Lei Geral de Proteção de Dados – lei nº 13.709/2018:
doutrina e aplicabilidade no âmbito laboral [recurso eletrônico] / organizado por Luciane
Cardoso Barzotto, Ricardo Hofmeister de Almeida Martins Costa - Porto Alegre : Escola Judicial
do Tribunal Regional do Trabalho da 4ª Região. Diadorim Editora, 2022.

690 p. ; PDF ; 7MB.

ISBN: 978-65-995463-8-9 (Ebook)

1. Direito. 2. Direito digital. 3. Lei Geral de Proteção de Dados. I. Barzotto, Luciane
Cardoso. II. Costa, Ricardo Hofmeister de Almeida Martins. II. Título. III. Brasil. Tribunal
Regional do Trabalho (4ª Região) Escola Judicial do Tribunal Regional do Trabalho da 4ª Região

2022-936

CDD 340.0285

CDU 34:004

Tribunal Regional do Trabalho da 4ª Região
Avenida Praia de Belas, 1432. Prédio III. 2º andar
CEP 90110-904 - Porto Alegre - RS
Telefone: (51) 3255.2683

Qualquer parte desta publicação pode ser reproduzida, desde que citadas a fonte e a respectiva autoria. O teor dos textos publicados é de total responsabilidade dos autores, não expressando necessariamente a posição da Escola Judicial do Tribunal Regional do Trabalho da 4ª Região

APRESENTAÇÃO

A Emenda Constitucional nº 115, de 10 de fevereiro de 2022, alterou a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. O caput do artigo 5º da Constituição passa a vigorar acrescido do seguinte inciso LXXIX: “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”.

Com isso, temos uma nova percepção da LGPD – Lei Geral de Proteção de Dados, entrada em vigor em 2020. Portanto, a presente obra coletiva pretende estudar as transformações trazidas pela LGPD. Trata-se da primeira publicação sobre a LGPD no âmbito do Tribunal Regional do Trabalho da 4ª Região, com o propósito de divulgar a produção jurisprudencial sobre o tema, fomentar a produção intelectual sobre o assunto e propiciar à comunidade jurídica a elucidação acerca de conceitos correlatos à proteção de dados.

O chamamento para participação deste e-book foi direcionado a autores, estudiosos do tema, integrantes tanto dos quadros da Justiça do Trabalho, como de fora da instituição, alunos e professores de Programas de Pós-graduação (PPGD da UFRGS, PUCRS, CDeA, entre outros tantos), oriundos de outras unidades federativas e de outros países. A condução dos trabalhos se deu sob a responsabilidade do Grupo de Estudos LGPD e Trabalho, assim constituído: Ana Paula Kotlinski Severino, Bárbara Fagundes, Fernanda Juliane Brum Corrêa, Gilberto Destro, Jaqueline Maria Menta, Jorge Alberto Araújo, Luciane Cardoso Barzotto, Marcela Casanova Viana Arena, Max Carrion Brueckner, Rita Volpato. Somando-se ao grupo de estudos, na organização dos verbetes, trabalhou, especialmente, a Estagiária do TRT4, Aline Dal Bó Correa.

É importante salientar que temos no TRT4, a Portaria 2036 de 2 de agosto de 2021 a qual institui a Política de Privacidade e Proteção de Dados no âmbito do Tribunal Regional da 4ª Região.

O e-book está composto por três partes:

1. Artigos sobre LGPD sobre aspectos gerais e vinculações trabalhistas;
2. Decisões aplicando a LGPD;
3. Glossário de verbetes comentado de palavras, temas ou tópicos da LGPD.

Como um serviço à comunidade jurídica, o grupo de estudos selecionou cursos e palestras gratuitas no YouTube, em planilha organizada pelo juiz Gilberto Destro, documento que pode ser acessado por este link: <https://docs.google.com/spreadsheets/d/1d1XmsLqZOGdLyTsez0l8Pi7wkypGEufLWZwgQI6-NgQ/edit?usp=sharing>.

Divulga-se ainda o Painel LGPD nos Tribunais, contendo uma seleção de decisões judiciais envolvendo a Lei Geral de Proteção de dados, com acesso disponível em <https://www.jusbrasil.com.br/static/pages/lgpd-nos-tribunais.html>.

Na condição de organizadora espero que a obra sirva para divulgar nova cultura de privacidade nas nossas instituições, tão necessária para um tempo de proteção de dados como direito fundamental. Agradeço a todos que se esforçaram e participaram neste projeto coletivo!

LUCIANE CARDOSO BARZOTTO

Coordenadora do GT da Lei 13.709/18 do TRT4, Doutora em Direito, Desembargadora Federal do Trabalho do TRT4 e professora do PPGD da UFRGS

PREFÁCIO

O tema da proteção de dados pessoais exige um olhar atento no tocante a toda a disciplina que rege a garantia dos direitos humanos. Por isso, é um dos assuntos de maior importância dos últimos anos do ponto de vista de impacto nas relações entre indivíduos e instituições, visto que a sociedade digital é extremamente dependente do uso dos dados como principal recurso para viabilizar as trocas econômicas e sociais.

Vivemos um momento em que passa a ser essencial praticar a “Ética de Dados”, que traz consigo os pilares de transparência, segurança e privacidade, como desdobramento natural da Ética corporativa em um contexto de transformação digital.

Devido à novidade da matéria e sua complexidade, há uma grande necessidade de se aprofundar os estudos da interdisciplinaridade da proteção de dados com demais direitos para a construção de um modelo sustentável.

É dentro desse contexto, que *Estudos sobre LGPD, Lei Geral de Proteção de Dados, Lei n. 13.709/2018: doutrina e aplicabilidade no âmbito laboral* é extremamente atual e completa.

Organizada pelos excelentíssimos Desembargadores Dra. Luciane Cardoso Barzotto, que é coordenadora do Grupo de Estudos de LGPD da Escola Judicial do TRT da 4ª Região, e Dr. Ricardo Hofmeister de Almeida Martins Costa, Desembargador ex-diretor da Escola Judicial do TRT da 4ª Região, traz uma abordagem rica e aprofundada sobre a problemática da nova regulamentação e a necessidade de sua harmonização com as questões relacionadas ao direito do trabalho.

O livro é resultado de um trabalho primoroso do grupo de estudos composto por vários estudiosos do tema: Ana Paula Kotlinski Severino, Bárbara Fagundes, Gilberto Destro, Jaqueline Maria Menta, Jorge Alberto Araújo, Marcela Casanova Viana Arena, Max Carrion Brueckner, Rita Volpato.

Ademais, há ainda muitas questões relacionadas a como serão interpretados os conceitos novos trazidos pela legislação, que vão desde a aplicação das bases legais que legitimam o tratamento dos dados pessoais até os limites de responsabilidade entre controlador e operador. E é por isso que este livro traz, de forma exemplar, um conjunto de decisões relacionadas de maneira a contribuir na análise de casos, permitindo a formação doutrinária e também jurisprudencial.

A abordagem através de artigos facilita a leitura que faz perpassar pelos principais assuntos que desafiam aqueles que estão na jornada do conhecimento da proteção de dados. Os capítulos trazem os principais desafios e discussões em torno da problemática relacionada aos direitos fundamentais, à própria privacidade, às relações de trabalho, aos agentes de tratamento, ao consentimento, ao tratamento dos dados de saúde, ao direito ao esquecimento, aos dados de criança e adolescente, ao teletrabalho, à responsabilidade civil, ao meio ambiente, no uso de tecnologias disruptivas como o reconhecimento facial, entre outros.

Além de uma leitura muito agradável, instigante e convidativa, a obra contou com o cuidado especial de seus organizadores nesta curadoria atenciosa e muito bem seleta de conteúdos e autores. Convido a todos a enriquecer ainda mais seus conhecimentos e desejar uma boa leitura.

PATRICIA PECK PINHEIRO, PhD

Doutora em Direito Internacional pela Universidade de São Paulo
Conselheira Titular do Conselho Nacional de Proteção de Dados – CNPD

SUMÁRIO

PRIMEIRA PARTE – ARTIGOS JURÍDICOS

1 PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL AUTÔNOMO NA CONSTITUIÇÃO BRASILEIRA DE 1988	20
--	-----------

INGO WOLFGANG SARLET

2 A LEI GERAL DE PROTEÇÃO DE DADOS E SEUS IMPACTOS NAS RELAÇÕES DE TRABALHO	35
--	-----------

IURI PINHEIRO VÓLIA BOMFIM

3 RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS DOS TRABALHADORES: DILEMAS EM TORNO DA ANÁLISE DE RISCO	57
---	-----------

CLAUDIA LIMA MARQUES E CÍNTIA ROSA PEREIRA DE LIMA

4 RUMO AO DIREITO FUNDAMENTAL DE PROTEÇÃO DE DADOS PESSOAIS: ALGUMAS APROXIMAÇÕES NA SEARA TRABALHISTA	67
---	-----------

EDUARDO K. ZAFFARI E TÊMIS LIMBERGER

5 DESCOMPLICANDO OS AGENTES DE TRATAMENTO, COM BASE NA LEI GERAL DE PROTEÇÃO DE DADOS	82
--	-----------

SELMA CARLOTO

6 O CONSENTIMENTO DO TRABALHADOR E O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS PESSOAIS	91
---	-----------

TERESA COELHO MOREIRA

7 PROTECCIÓN DE DATOS DE SALUD EN EL ÁMBITO LABORAL: UNA PERSPECTIVA ESPAÑOLA	99
--	-----------

FRANCISCA RAMÓN FERNÁNDEZ

**8 PROTEÇÃO DE DADOS E O SISTEMA JUDICIAL PORTUGUÊS
- UMA SÍNTESE 112**

JOSÉ JOAQUIM FERNANDES OLIVEIRA MARTINS

**9 O DIREITO AO ESQUECIMENTO, A LEI GERAL DE PROTEÇÃO
DE DADOS PESSOAIS (LGPD) E AS RELAÇÕES DE TRABALHO:
BREVES REFLEXÕES 128**

GUILHERME GUIMARÃES FELICIANO E CLAUDIRENE ANDRADE RIBEIRO

**10 ADAPTAÇÕES NECESSÁRIAS DAS RELAÇÕES DE TRABALHO
RESULTANTES DA LEI GERAL DE PROTEÇÃO DE DADOS 152**

XERXES GUSMÃO

**11 EFICÁCIA ESPACIAL DA LGPD: DOCTRINA DOS EFEITOS E
SUA APLICAÇÃO NO TRATAMENTO TRANSFRONTEIRIÇO DE
DADOS NAS RELAÇÕES DE TRABALHO 168**

RAPHAEL MIZIARA

**12 PRINCÍPIOS NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS:
DO NÚCLEO COMUM AOS DESAFIOS DE CONCRETIZAÇÃO 181**

JULISE LEMONJE

**13 DADOS PESSOAIS: O QUE SÃO? QUEM OS DETÉM? COMO E
POR QUE OS COLETA? 191**

FRANCIANO BELTRAMINI

**14 A CRIANÇA COMO TITULAR E DESTINATÁRIA DA PROTEÇÃO
DE DADOS PESSOAIS FRENTE A CULTURA FRATERNA 205**

GERALDA MAGELLA DE FARIA ROSSETTO E JOSIANE ROSE PETRY VERONESE

**15 AMBIENTE DIGITAL E A PROTEÇÃO DOS DADOS PESSOAIS DA
CRIANÇA E DO ADOLESCENTE 229**

IVANI CONTINI BRAMANTE

16 RESPONSABILIDADE CIVIL NA LGPD 241

LARA ISABEL MARCON SANTOS

17 PROVAS DIGITAIS, LEI GERAL DE PROTEÇÃO DE DADOS E PRINCÍPIO DA PUBLICIDADE PROCESSUAL 249

EROTILDE RIBEIRO DOS SANTOS MINHARRO

18 O DESCARTE DE DISPOSITIVOS TECNOLÓGICOS FRENTE A LGPD 260

VALÉRIA REANI RODRIGUES GARCIA E MANUEL DAVID RODRIGUES MASSENO

19 PROTEÇÃO DE DADOS PESSOAIS NAS RELAÇÕES DE TRABALHO 266

LAURA MEDINA MARTINS MOREIRA E DIOGO ANTONIO PEREIRA MIRANDA

20 LGPD E SUA RELAÇÃO COM A PROTEÇÃO DE DADOS DO EMPREGADO NO TELETRABALHO 277

PALOMA MEDRADO E THOMIRES ELIZABETH PAULIV BADARÓ DE LIMA

21 A PROTEÇÃO AOS DADOS PESSOAIS E SENSÍVEIS DO TRABALHADOR COMO DIREITO FUNDAMENTAL 293

BEATRIZ DE FELIPPE REIS

22 REFLEXÕES ACERCA DA APLICAÇÃO DA LGPD NAS RELAÇÕES DE TELETRABALHO 308

RAQUEL HOCHMANN DE FREITAS

23 CONTORNOS JURÍDICOS NO TRATAMENTO DE DADOS DE COLABORADORES E A LEI GERAL DE PROTEÇÃO DE DADOS

(LGPD)

318

MÁRCIA SANTANA FERNANDES E SÍLVIA WEIGERT MENNA BARRETO

**24 LEI GERAL DE PROTEÇÃO DE DADOS E PRINCÍPIO DA
PROTEÇÃO NA RELAÇÃO LABORAL 327**

RENATA DUVAL MARTINS

**25 A LEI GERAL DE PROTEÇÃO DE DADOS E A (AUSÊNCIA DE)
PROTEÇÃO AOS TRABALHADORES, OU O DITO PELO NÃO DITO 347**

ALMIRO EDUARDO DE ALMEIDA E OSCAR KROST

**26 PROMETEU ACORRENTADO, LGPD E O DIREITO DO
TRABALHO 360**

OSCAR KROST

**27 A LEI GERAL DE PROTEÇÃO DE DADOS E O COMPLIANCE
COMO MEIOS DE SUPERAÇÃO DOS DESAFIOS IMPOSTOS PELO
ATUAL CENÁRIO ECONÔMICO 368**

LINCOLN ZUB DUTRA

28 NEGOCIAÇÃO COLETIVA E LGPD 390

LUCIANE CARDOSO BARZOTTO

**29 O USO DO CONSENTIMENTO PARA TRATAMENTO DE DADOS
DE EMPREGADOS 407**

FERNANDA MASSOTE LEITÃO ALVARENGA

**30 LGPD NAS RELAÇÕES DE TRABALHO: OS RISCOS DE
UTILIZAÇÃO DO CONSENTIMENTO PARA O TRATAMENTO DOS
DADOS DOS TRABALHADORES 419**

FABRÍCIO LIMA SILVA

**31 DO DIREITO À PRIVACIDADE NO AMBIENTE DE TRABALHO:
PERSPECTIVAS A PARTIR DA LEI GERAL DE PROTEÇÃO DE
DADOS** 433

CAROLINA LITVIN SCALETSCY

**32 A RELAÇÃO TRABALHISTA SOB O VIÉS DA PROTEÇÃO DE
DADOS E PRIVACIDADE: DUE DILIGENCE DE CANDIDATOS E
EMPREGADOS, INCIDENTES COM DADOS PESSOAIS E POSSÍVEL
REPARAÇÃO A DANOS** 446

FLÁVIA ALCASSA E ADRIANNE LIMA

**33 LEI GERAL DE PROTEÇÃO DE DADOS: RESPONSABILIDADE
PATRONAL NO TRATAMENTO DE DADOS PESSOAIS E SENSÍVEIS
DO TRABALHADOR** 462

RODRIGO GOLDSCHMIDT E MAX ANTÔNIO SILVA VIEIRA

**34 TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS LIGADOS A
SAÚDE DO TRABALHADOR À LUZ DA LEI GERAL DE PROTEÇÃO
DE DADOS PESSOAIS (LGPD)** 475

MARINA RICHARD DE TOLEDO E RODRIGO GOLDSCHMIDT

**35 O TRABALHO EM TEMPOS DE REVOLUÇÃO TECNOLÓGICA E
DA PANDEMIA DE COVID-19: PROTEÇÃO DE DADOS PESSOAIS E
PRECARIZAÇÃO LABORAL - SEGREGAÇÃO E/OU COOPERAÇÃO?** 486

GERALDA MAGELLA DE FARIA ROSSETTO E ENDY DE GUIMARÃES E MORAES

**36 A IMPORTÂNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS
PARA O MEIO AMBIENTE DO TRABALHADOR** 501

CLÁUDIO JANNOTTI DA ROCHA, FÁBIO SIQUEIRA MACHADO E ALBERTO NEMER NETO

37 LGPD E RELAÇÕES DE TRABALHO: A IMPORTÂNCIA DO TRATAMENTO DE DADOS SENSÍVEIS COMO FORMA DE COMBATE À DISCRIMINAÇÃO E PROTEÇÃO DOS TRABALHADORES LGBTIQ+ 517

HELEN RODRIGUES DE SOUZA E EYDIE CRISTINA DE SOUZA

38 O IMPACTO DA LGPD NO CONTROLE DE PONTO POR RECONHECIMENTO FACIAL 535

MARIANA RUZZI

39 O RECONHECIMENTO DA PEJOTIZAÇÃO E OS REFLEXOS NAS RELAÇÕES DE TRABALHO DIANTE DA LGPD 547

JULIANA BORTONCELLO FERREIRA

40 O USO DE INTELIGÊNCIA ARTIFICIAL NA DESPEDIDA DO TRABALHADOR 559

ANA PAULA ÁVILA, LUCIANA ARANALDE E MÁRCIA SANTANA FERNANDES

41 LEI GERAL DE PROTEÇÃO DE DADOS - ANÁLISE JURISPRUDENCIAL DAS DECISÕES EMANADAS DA JUSTIÇA DO TRABALHO 577

RICARDO CALCINI E FELIPE CAMARGO DE ARAÚJO

SEGUNDA PARTE

A PROTEÇÃO DOS DADOS SOBRE O PRISMA JURISDICIONAL

STF. ACÓRDÃO. PROTEÇÃO DOS DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO 585

MINISTRA ROSA WEBER

ACÓRDÃO. TRT 4. Art. 18 LGPD 587

DESEMBARGADOR WILSON CARVALHO DIAS

**ACÓRDÃO. TRT4. CUMPRIMENTO DE OBRIGAÇÃO LEGAL PELO
CONTROLADOR 588**

DESEMBARGADOR FABIANO HOLZ BESERRA

ACÓRDÃO. TRT4. SINDICATO E LGPD 602

DESEMBARGADORA BRÍGIDA JOAQUINA CHARÃO BARCELOS

**SENTENÇA. NEGATIVA DE ACESSO A DADOS PESSOAIS
TRATADOS (ART. 9º DA LGPD) 605**

JUIZ PAULO ROBERTO DORNELLES JUNIOR

**SENTENÇA. DADOS PESSOAIS E PROCESSO JUDICIAL
ELETRÔNICO 614**

JUIZ MAX CARRION BRUECKNER

SENTENÇA. LGPD E EXIBIÇÃO DE DOCUMENTOS 614

JUIZ MAURICIO DE MOURA PECANHA

**SENTENÇA. PROTEÇÃO DE DADOS DE PESSOA JURÍDICA.
INAPLICABILIDADE 615**

JUÍZA LINA GORCZEWSKI

TERCEIRA PARTE GLOSSÁRIO

AGENTES DE TRATAMENTO (art. 5º, IX e art. 37) 627

FERNANDA JULIANE BRUM CORRÊA

ANONIMIZAÇÃO (art. 5.º, XI) 628

FERNANDA JULIANE BRUM CORRÊA

APLICAÇÃO DA LGPD	629
GILBERTO DESTRO	
APLICAÇÃO DA LGPD NO ÂMBITO LABORAL	629
GILBERTO DESTRO	
ARMAZENAMENTO (art. 5º, X)	630
ALINE DAL BÓ CORREA	
AUTODETERMINAÇÃO INFORMATIVA	631
DANIELA FALCADI COELHO	
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (art 5º, XIX)	632
CAMILA DOZZA ZANDONAI	
BANCO DE DADOS (art 5.º, IV)	635
ALINE DAL BÓ CORREA	
BLOQUEIO (art. 5º, XIII)	635
ALINE DAL BÓ CORREA	
BOA-FÉ (art. 6º)	635
ALINE DAL BÓ CORREA	
BOAS PRÁTICAS (art. 50)	635
ALINE DAL BÓ CORREA	
<i>BONA FIDE OCCUPATIONS</i>	636

RAPHAEL MIZIARA

CONSENTIMENTO (art 8º) 637

FERNANDA JULIANE BRUM CORRÊA

CONTROLADOR (art. 5.º, VI) 639

FERNANDA JULIANE BRUM CORRÊA

CRIANÇA E ADOLESCENTE (art. 14) 639

BÁRBARA FAGUNDES

DADO ANONIMIZADO (art. 5º, III) 641

FERNANDA JULIANE BRUM CORRÊA

DADO BIOMÉTRICO 642

MARCELO LUCCA

DADO PESSOAL (art. 5º, I) 645

MAX CARRION BRUECKNER

DADO PESSOAL SENSÍVEL - I (art. 5º, II) 646

MAX CARRION BRUECKNER

DADO PESSOAL SENSÍVEL - II 646

MARCO AURÉLIO SERAU JUNIOR

DIREITO DOS TITULARES 649

GILBERTO DESTRO

ELIMINAÇÃO (art 5º, XIV)	650
SUELEN HENTGES	
ENCARREGADO DE DADOS - I	651
RODRIGO THOMAZINHO COMAR	
ENCARREGADO - II (art. 5º, VIII)	653
FERNANDA JULIANE BRUM CORRÊA	
FINALIDADE ESPECÍFICA (art. 9º, I)	654
ALINE DAL BÓ CORREA	
FINS EXCLUÍDOS DA LEI (art. 4º)	654
ALINE DAL BÓ CORREA	
FISCALIZAÇÃO (art. 52)	655
ALINE DAL BÓ CORREA	
GOVERNANÇA (art. 50)	655
ALINE DAL BÓ CORREA	
GRANULARIDADE	655
FERNANDA JULIANE BRUM CORRÊA	
HONRA (art 2º da LGPD e art. 5º, X, da CRFB)	656
ALINE DAL BÓ CORREA	
HABEAS DATA	656
DENISE FINCATO	

INFORMAÇÃO, DIREITO À	659
LUCIELI BRENDA	
INTIMIDADE (art. 2º LGPD e CRFB)	660
ALINE DAL BÓ CORREA	
IMAGEM (art. 2º LGPD e CRFB)	660
ALINE DAL BÓ CORREA	
JUDICIÁRIO E TRATAMENTO DE DADOS (art. 25 e art. 26)	661
ALINE DAL BÓ CORREA	
LEGÍTIMO INTERESSE (art. 10)	661
ALINE DAL BÓ CORREA	
LIVRE ACESSO (art. 6º, IV)	661
ALINE DAL BÓ CORREA	
MICROEMPRESAS, STARTUPS E EMPRESAS DE INOVAÇÃO PERANTE A LGPD	661
GERALDA MAGELLA DE FARIA ROSSETTO	
MONITORAMENTO DE EMPREGADOS E LGPD	664
SUELEN HENTGES	
NÃO DISCRIMINAÇÃO (art. 6º, IX)	664
LUCIANE CARDOSO BARZOTTO E VIVIAN MARIA CAXAMBU GRAMINHO	
OPERADOR (art. 5.º, VII)	668
FERNANDA JULIANE BRUM CORRÊA	

ÓRGÃO DE PESQUISA (art. 5º XVIII)	668
ALINE DAL BÓ CORREA	
PRINCÍPIOS	669
GILBERTO DESTRO	
PRIVACY BY DEFAULT	670
PÂMELA ADRIELLE PERTILE DOS PASSOS E SÂMARA KENYA DE OLIVEIRA	
PRIVACIDADE BY DESIGN (art. 46)	670
ROSANA KIM JOBIM	
PSEUDONIMIZAÇÃO (art. 13, § 4º)	671
FERNANDA JULIANE BRUM CORRÊA	
QUALIDADE DOS DADOS (art. 5º, V)	671
ALINE DAL BÓ CORREA	
RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS	672
LUCIANE ERBANO ROMEIRO	
RESPONSABILIDADE (art. 31)	672
BRUNA CASIMIRO SICILIANI	
REVOGAÇÃO (art 15, III)	674
ALINE DAL BÓ CORREA	
SAÚDE	674
BÁRBARA FAGUNDES	

SEGURANÇA	676
MARCELA CASANOVA VIANA ARENA	
SEGURANÇA EM LGPD	676
PAULO GUSTAVO MAGELLA DE FARIA QUINAN E GERALDA MAGELLA DE FARIA ROSSETTO	
TRATAMENTO DE DADOS	680
MARCELA CASANOVA VIANA ARENA	
TÉRMINO DO TRATAMENTO (arts. 15 e 16)	681
BÁRBARA FAGUNDES	
TITULAR (art. 5.º, V e art. 17)	682
FERNANDA JULIANE BRUM CORRÊA	
TRANSFERÊNCIA INTERNACIONAL - I (art. 5º, XV)	682
JAQUELINE MARIA MENTA	
TRANSFERÊNCIA INTERNACIONAL - II (ART. 5º, XV)	685
ELEONORA COELHO DOZZA	
TRANSPARÊNCIA (art. 10 § 2º)	688
ALINE DAL BÓ CORREA	
USO COMPARTILHADO DE DADOS (art. 5.º, XVI)	688
ALINE DAL BÓ CORREA	
VÍCIO DE CONSENTIMENTO	688
FERNANDA JULIANE BRUM CORRÊA	

PRIMEIRA PARTE

ARTIGOS JURÍDICOS

1. PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL AUTÔNOMO NA CONSTITUIÇÃO BRASILEIRA DE 1988¹

DATA PROTECTION AS AUTONOMOUS FUNDAMENTAL RIGHT IN THE BRAZILIAN CONSTITUTION OF 1988

INGO WOLFGANG SARLET²

Resumo

Embora no seu texto original a Constituição Brasileira de 1988 não tenha contemplado expressamente um direito fundamental à proteção de dados pessoais, tal direito foi reconhecido como implicitamente positivado pelo Supremo Tribunal Federal, em maio de 2020. Em 20 de outubro de 2021, o Senado Federal aprovou a versão final do projeto de emenda constitucional nº 17/2019, incorporando um direito fundamental à proteção de dados pessoais ao catálogo constitucional de direitos. No presente texto, o que se pretende é discutir o conteúdo desse direito fundamental na condição de direito autônomo, para além da proteção da privacidade e da autodeterminação informacional.

Palavras-Chave: Proteção de Dados Pessoais – Direito Fundamental Autônomo – Constituição Brasileira de 1988

Abstract

Although the Brazilian Constitution of 1988, in its original version, didn't contemplate a explicit fundamental right to personal data protection, the Federal Supreme Court recognized that right as a implicit one in May 2020. On October 20, 2021, the Federal Senate approved the final version of the constitutional amendment proposal nº 17/2019, including a fundamental right to personal

1 O presente texto corresponde à versão atualizada e, em diversos pontos relevantes, ajustada e reescrita, de trabalho publicado na obra coletiva contendo os textos relativos às conferências ministradas por ocasião da VII Jornada Interamericana de Direitos Fundamentais e Democracia, 2020 (na forma de webinar), que, por sua vez, corresponde à versão substancialmente reduzida, reestruturada e ajustada de artigo publicado na Revista Direitos Fundamentais & Justiça, Belo Horizonte, ano 14, n. 42, p. 175-214, jan./jun. 2020.

2 Professor Titular de Direito Constitucional e Coordenador do Programa de Pós-Graduação em Direito (Mestrado e Doutorado) e Professor do Programa de Pós-Graduação em Ciências Criminais, ambos da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Desembargador aposentado do Tribunal de Justiça do Rio Grande do Sul. Advogado e parecerista.

data protection in the constitutional bill of rights. This paper aims to discuss the contents of that fundamental right as an autonomous right, reaching beyond the protection of privacy and informational self-determination.

Keywords: Personal Data Protection – Autonomous Fundamental Right – Brazilian Constitution of 1988.

1. Introdução

A proteção dos dados pessoais alcançou uma dimensão sem precedentes no âmbito da assim chamada sociedade tecnológica, notadamente a partir da introdução do uso da tecnologia da informática e da ampla digitalização que já assumiu um caráter onipresente e afeta todas as esferas da vida social, econômica, política, cultural contemporânea no mundo.

No que diz respeito à esfera do Direito, que tem sido convocado a regular também essa matéria, a despeito de a instituição e subsequente ampliação em termos quantitativos e qualitativos da proteção jurídica de dados pessoais ter-se iniciado no limiar da década de 1970, reconhecimento de um direito humano e fundamental à proteção dos dados pessoais, contudo, teve de esperar ainda um tempo considerável para ser incorporado de modo abrangente à gramática jurídico-constitucional, à exceção dos paradigmáticos exemplos da Constituição da República Portuguesa de 1976³ e da Constituição Espanhola de 1978⁴.

Nesse sentido, note-se que mesmo já no limiar da terceira década do século 21, ainda existem Estados constitucionais onde um direito fundamental à proteção de dados não é reconhecido, pelo menos na condição de direito expressamente positivado na Constituição, muito embora tal direito seja, em vários casos, tido como implicitamente positivado, sem prejuízo de uma mais ou menos ampla regulação legislativa e administrativa, ademais de significativo desenvolvimento na esfera jurisprudencial.

No caso do Brasil, a Constituição Federal de 1988 (CF) não contemplou no seu texto um direito fundamental autônomo à proteção de dados pessoais, que veio a ser reconhecido como direito implicitamente positivo pelo STF somente em maio de 2020, por ocasião do julgamento do mérito da ADI 6387-DF, relatada pela ministra Rosa Weber. Como consequência dessa importante e paradigmática decisão da Corte Suprema brasileira, mas também por influência da aprovação e entrada em vigor, em duas etapas, da primeira Lei Geral de Proteção de Dados (LGPD) – Lei n. 13.709/2018, foi acelerado o processo de tramitação, no Congresso Nacio-

3 A proteção dos direitos fundamentais no campo da informática está detalhadamente previsto no artigo 35 da Constituição Portuguesa, aqui transcrito na sua versão inicial: “(utilização da informática) 1. Todos os cidadãos têm o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a rectificação dos dados e a sua actualização. 2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos. 3. É proibida a atribuição de um número nacional único aos cidadãos”. Note-se que tal dispositivo foi alterado três vezes por leis de revisão constitucional de 1982, 1989 e 1997, tendo sido substancialmente atualizado e ampliado.

4 Art. 18, nº 4. *La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.* Cuida-se aqui, na versão original de 1978, de uma proteção indireta dos dados pessoais, visto que não há menção expressa aos mesmos.

nal, de uma proposta de emenda à Constituição (PEC nº 17/2019), que, oriunda do Senado Federal, sofreu ajustes na Câmara dos Deputados e acabou sendo, com esta mesma redação, aprovada pelo Senado em 20.10.2021, inserindo um direito fundamental à proteção de dados pessoais no artigo 5º, da CF, ademais de dispor sobre as competências da União na matéria.

De acordo com a redação dada pela PEC 17/2019, o *caput* do art. 5º da CF passa a vigorar acrescido do seguinte inciso LXXIX: “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”. No que diz respeito ao sistema de repartição de competências, o *caput* do art. 21 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXVI: “organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei”, ao passo que o *caput* do art. 22 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXX: “proteção e tratamento de dados pessoais”.

À vista disso, o que aqui se pretende, é tecer algumas considerações acerca dos fundamentos e do conteúdo, na condição de direito fundamental autônomo, do direito à proteção de dados pessoais na ordem constitucional brasileira, de modo a demonstrar o acerto da tese de que o âmbito de proteção de tal direito vai além da proteção à vida privada e mesmo da livre autodeterminação informacional.

2. A fundamentalidade material e formal do direito à proteção de dados pessoais – sentido e alcance

Como já adiantado, um direito humano e fundamental autônomo na esfera do direito constitucional positivo e do direito internacional dos direitos humanos ainda não é de longe onipresente nos textos de boa parte das constituições (em especial as mais antigas) e dos tratados internacionais de direitos humanos.

Ao nível do direito internacional público, tanto no âmbito do sistema universal de proteção da ONU quanto na esfera do direito europeu, um direito à proteção de dados tem sido deduzido em especial do direito à privacidade, embora com este não se confunda. Nesse sentido, a orientação adotada pela Comissão da ONU para Direitos Humanos, interpretando o alcance do artigo 17 do Pacto Internacional de Direitos Civis e Políticos, assim como a jurisprudência da Corte Europeia de Direitos Humanos (CEDH) e do Tribunal de Justiça da União Europeia (TJUE), **forte** no artigo 8º da Convenção Europeia⁵.

Foi somente na Convenção nº 108 para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais (1981)⁶, comumente intitulada de Convenção de Estrasburgo, bem como, quase 20 anos mais tarde, no artigo 8 da Carta de Direitos Fundamentais da União Europeia (doravante CDFUE), do ano 2000⁷ - que o direito à proteção de dados finalmente alçou a condição de

5 Cf., por todos, SCHIEDERMAIR, Stephanie. Einleitung. In: SIMITIS, Spiros; HORNUNG, Gerit; SPIECKER GENANNT DÖHMANN, Indra (Coord.). *Datenschutzrecht*. Baden-Baden: Nomos, 2019. p. 201.

6 CONSELHO DA EUROPA. *Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais*, de 28 de janeiro de 1981. Disponível em: <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>. Acesso em: 15 nov. 2019.

7 PARLAMENTO EUROPEU. *Carta de Direitos Fundamentais da União Europeia*, de 7 de dezembro de 2000. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/>

direito fundamental de natureza autônoma, mas vinculando, como tal, apenas os Estados integrantes da União Europeia, o que se deu apenas com a entrada em vigor do Tratado de Lisboa, em 2009⁸.

No caso do Brasil, como já antecipado, a CF, embora faça referência, no art. 5.º, XII, ao sigilo das comunicações de dados (além do sigilo da correspondência, das comunicações telefônicas e telegráficas), não contemplou, no seu texto originário, expressamente um direito fundamental à proteção e livre disposição dos dados pelo seu respectivo titular, sendo o reconhecimento de tal direito algo ainda relativamente recente na ordem jurídica brasileira.

A proteção dos dados pessoais, por outro lado – para além da referência ao sigilo da comunicação de dados –, também encontrou, desde o início, salvaguarda parcial e indireta mediante a previsão da ação de *habeas data* (art. 5.º, LXXII, da CF), ação constitucional, com *status* de direito-garantia fundamental autônomo, que precisamente busca assegurar ao indivíduo o conhecimento e mesmo a possibilidade de buscar a retificação de dados constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, ao mesmo tempo em que se trata de uma garantia procedimental do exercício da autodeterminação informacional⁹.

Com relação ao sigilo da comunicação de dados, contudo, há que ter cautela, razão pela qual se impõe o registro, com base na lição de Danilo Doneda, de que não se trata, neste caso, do direito à proteção de dados pessoais em si nem de seu fundamento direto. Para melhor compreensão da assertiva, valemo-nos aqui da própria fala do autor:

[Se,] por um lado, a privacidade é encarada como um direito fundamental, as informações pessoais em si parecem, a uma parte da doutrina, serem protegidas somente em relação à sua “comunicação”, conforme art. 5º, XII, que trata da inviolabilidade da comunicação de dados. Tal interpretação traz consigo o risco de sugerir uma grande permissividade em relação à utilização de informações pessoais. Nesse sentido, uma decisão do STF, relatada pelo ministro Sepúlveda Pertence, reconheceu expressamente a inexistência de uma garantia de inviolabilidade sobre dados armazenados em computador com fulcro em garantias constitucionais...O sigilo, no inciso XII do art. 5º, está referido à comunicação, no interesse da defesa da privacidade.... Obviamente o que se regula é comunicação por correspondência e telegrafia, comunicação de dados e telefônica... A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si,

TXT&from=EN. Acesso em: 15 nov. 2019.

8 DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Joaçaba, *Espaço Jurídico Journal of Law*, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 15 nov. 2019.

9 MENDES, Laura Schertel. Habeas Data e autodeterminação informativa: dois lados da mesma moeda. *Revista Direitos Fundamentais e Justiça*, a. 12, n. 39, p. 185-216, jul./dez. 2018.

mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho... A decisão tem sido, desde então, constantemente mencionada como precedente em julgados nos quais o STF identifica que a natureza fundamental da proteção aos dados está restrita ao momento de sua comunicação¹⁰.

À míngua, portanto, de expressa previsão de tal direito, pelo menos na condição de direito fundamental explicitamente autônomo, no texto originário da CF, e a exemplo do que ocorreu em outras ordens constitucionais, o direito à proteção dos dados pessoais acabou sendo associado e reconduzido a alguns princípios e direitos fundamentais de caráter geral e especial, como é o caso do princípio da dignidade da pessoa humana, do direito fundamental (também implicitamente positivado) ao livre desenvolvimento da personalidade, do direito geral de liberdade, bem como dos direitos especiais de personalidade mais relevantes no contexto, quais sejam – aqui nos termos da CF – os direitos à privacidade e à intimidade¹¹, no sentido do que alguns também chamam de uma “intimidade informática”¹².

Mas, possivelmente, o fundamento constitucional direto mais próximo de um direito fundamental à proteção de dados seja mesmo o direito ao livre desenvolvimento da personalidade, radicado diretamente no princípio da dignidade da pessoa humana e no direito geral de liberdade, o qual também assume a condição de uma cláusula geral de proteção de todas as dimensões da personalidade humana¹³, que, de acordo com tradição jurídica já consolidada no direito constitucional estrangeiro e no direito internacional (universal e regional) dos direitos humanos, inclui o (mas não se limita ao!) direito à livre disposição sobre os dados pessoais, o assim designado direito à livre autodeterminação informativa¹⁴.

A doutrina especializada brasileira, a exemplo e por influência do que se deu em outras ordens jurídicas, também já vinha de há muito tempo e com crescente intensidade advogando a necessidade de, mediante uma leitura harmônica e sistemática do texto constitucional de 1988, se reconhecer um direito fundamental autônomo implicitamente positivado à proteção de dados pessoais¹⁵, o que veio a

10 DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 262

11 Cf. por todos DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

12 Cf., por exemplo, entre nós, SAMPAIO, José Adércio Leite. A suprema inviolabilidade: a intimidade informática e o sigilo bancário. In: SARMENTO, Daniel; SARLET, Ingo Wolfgang (Coord.). **Direitos fundamentais no Supremo Tribunal Federal**: balanço e crítica, Rio de Janeiro: Lumen Juris, 2011. p. 531 e ss.

13 Cf. por todos, MOTA PINTO, Paulo. **Direitos de Personalidade e Direitos Fundamentais**: Estudos. Coimbra: Gestleg, 2018, em especial, p. 33 e ss.

14 MOTA PINTO, Paulo. **Direitos de Personalidade e Direitos Fundamentais**: Estudos, op. cit., p. 642 e ss.

15 Cf., em especial, o já referido DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**, op. cit. 2006, mas também, na sequência, entre outros, LIMBERGER, Têmis. **O Direito à Intimidade na Era da Informática**. Porto Alegre: Livraria do Advogado, 2007; RUARO, Regina Linden; RODRI-

ser confirmado, em abril e maio de 2020, pelo STF, em histórico e paradigmático julgado, tal como já referido.

No citado julgamento, da ADI 6387-DF, relatora ministra Rosa Weber, foi discutida a constitucionalidade da Medida Provisória 954, de 17.04.20, da Presidência da República, que atribuiu às empresas de telecomunicações (fixas e móveis) o dever de disponibilizar os nomes completos, endereços e números de telefone dos usuários PN e PJ para o IBGE durante a pandemia do COVID 19 para efeitos de uso direto e exclusivo de produção de estatísticas oficiais mediante entrevistas domiciliares. O STF, acolhendo a tese da inconstitucionalidade da exigência feita pela Medida Provisória impugnada, reconheceu a ocorrência de violação, pela desproporcionalidade da medida, do direito fundamental à proteção de dados pessoais, na condição de direito autônomo implicitamente positivado, seguindo, no que diz respeito à fundamentação, a orientação geral protagonizada pela doutrina jurídica acima referida.

Além disso, é de sublinhar que apenas em 2020 o Supremo Tribunal Federal proferiu três decisões relevantes relativas à proteção de dados pessoais. Para além do caso do IBGE, o tema foi tratado na ADI 6561 (Cadastros de dependentes químicos)¹⁶ e na ADI 6.529 (Caso Sisbin)¹⁷. Nesse último caso, cujo mérito foi decidido em 11.10.2021, a Corte decidiu que os órgãos componentes do Sistema Brasileiro de Inteligência (Sisbin) somente podem fornecer dados e conhecimentos específicos à Agência Brasileira de Inteligência (Abin) quando for comprovado o interesse público da medida, afastando qualquer possibilidade desses dados atenderem a interesses pessoais ou privados.

Como contraponto, é possível citar a decisão proferida no RE 1.304.294/SP, relatoria da ministra Cármen Lúcia, na qual se entendeu que a divulgação de dados pessoais de empregados de empresas terceirizadas prestadoras de serviços públicos ofende o direito à privacidade desses trabalhadores. O que chama a atenção, no julgado, é o fato de que embora a proteção de dados pessoais tenha sido assegurada, o argumento central foi o da violação do direito à privacidade, o que, pelo menos é o que acaba transparecendo do julgado, não guarda sintonia fina com a concepção de um direito fundamental autônomo à proteção de dados pessoais.

À vista disso, é de se acompanhar o entendimento de Carlos Alberto Molinaro e Gabrielle Bezerra S. Sarlet, no sentido de que a proteção de dados pessoais, e o reconhecimento de um direito fundamental correspondente, de certo modo, “confere um novo e atual sentido à proteção da pessoa humana e da dignidade, da autonomia e das esferas de liberdade que lhes são inerentes”¹⁸.

GUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade de informação. *Direito, Estado Sociedade*, n. 36, jan./jun. 2010, MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**. São Paulo: Saraiva, 2013, BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: A Função e os Limites do Consentimento**. Rio de Janeiro: Forense, 2019. p. 90 e ss.; SARLET, Proteção de dados como direito fundamental na Constituição Federal Brasileira de 1988, *Direitos Fundamentais & Justiça* | Belo Horizonte, ano 14, n. 42, p. 175-214, jan./jun. 2020. Por último, v. RODRIGUEZ, Daniel Piñeiro. **O Direito Fundamental à Proteção de Dados: Vigilância, Privacidade e Regulação**. Rio de Janeiro: Lumen Juris, 2021.

16 ADI 6561/TO, Rel. Min. Edson Fachin, j. da medida cautelar em 13.10.2020.

17 ADI 6529/DF, Rel. Min. Cármen Lúcia, j. da medida cautelar em 13.08.2020.

18 MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra Sales. *Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data*. Direitos

Com a aprovação da PEC 17/2019 e a inserção, pelo Congresso Nacional, de um direito fundamental autônomo, inclusive, diversamente da redação inicial da PEC, contemplando-o com um inciso próprio, acrescido ao artigo 5º, da CF, a própria decisão do STF acabou sendo não somente chancelada, mas também saiu fortalecida pela expressiva legitimação democrática de uma emenda constitucional. Outrossim, independentemente aqui de se aprofundar a discussão sobre a conveniência, necessidade e bondade intrínseca de uma consagração textual de um direito fundamental autônomo à proteção de dados na CF, ou mesmo adentrar a querela sobre se tratar, ou não, de um direito “novo”, o fato é que cerramos aqui fileiras com os que saúdam como benfazeja a opção do Congresso Nacional.

Dentre as razões que aqui poderiam ser colacionadas, destacam-se:

a) a despeito das interseções e articulações com outros direitos, fica assegurada – do ponto de vista também formal (textual) - à proteção de dados a condição de direito fundamental autônomo, com âmbito de proteção próprio;

b) ao direito à proteção de dados passa a ser atribuído de modo inquestionável o pleno regime jurídico-constitucional relativo ao seu perfil de direito fundamental em sentido material e formal já consagradas no texto da CF, bem como na doutrina e na jurisprudência constitucional brasileira, ou seja:

1) como parte integrante da constituição formal, os direitos fundamentais possuem *status* normativo superior em relação a todo o restante do ordenamento jurídico nacional;

2) na condição de direito fundamental, assume a condição de limite material à reforma constitucional, devendo, ademais disso, serem observados os assim chamados limites formais, circunstanciais e temporais, nos termos do artigo 60, parágrafo 1 a 4º, da CF¹⁹;

3) também as normas relativas ao direito à proteção de dados são – nos termos do artigo 5º, § 1º, CF – dotadas de aplicabilidade imediata (direta) e vinculam diretamente todos os atores públicos, bem como – sopesadas as devidas ressalvas– os atores privados.

Acrescente-se, outrossim, que, a teor do artigo 5º, §§ 2º e 3º, CF, o marco normativo que concretiza e formata o âmbito de proteção e as funções e dimensões do direito (fundamental) à proteção de dados, é também integrado – embora tal circunstância seja usualmente negligenciada – pelos tratados internacionais de direitos humanos ratificados pelo Brasil –, destacando-se, para o efeito da compreensão adequada e manejo correto em nível doméstico – a Convenção Americana de São José

Fundamentais & Justiça, a. 13, n. 41, p. 183-212, jul./dez. 2019.

19 Destaque-se, contudo, que inexistente unanimidade respeitante à possibilidade de se atribuir a condição de “cláusula pétrea” quando se tratar de direito incluído por emenda constitucional. De todo modo, adere-se aqui ao entendimento favorável quando a inserção por emenda apenas formalizar o que pode ser tido como um direito fundamental implícito, caso precisamente da proteção de dados pessoais.

da Costa Rica e o Pacto Internacional de Direitos Civis e Políticos, incluindo a sua interpretação pelas instâncias judiciárias e não judiciárias respectivas.

Tal fato assume uma dimensão particularmente relevante, à vista do atual posicionamento do STF sobre o tema, dada a atribuição, aos tratados de direitos humanos devidamente ratificados, hierarquia normativa supra legal, de modo que, ao menos assim o deveria ser, o marco normativo nacional infraconstitucional não apenas deve guardar consistência formal e material com a CF, mas também estar de acordo com os parâmetros de tais documentos internacionais, sendo passível do que se tem designado de um controle jurisdicional de convencionalidade. Além disso, convém lembrar que em se cuidando de tratados internacionais de direitos humanos aprovados pelo rito agravado previsto no § 3º do artigo 5º da CF o seu valor normativo na esfera nacional será equivalente ao das emendas constitucionais.

Nesse contexto, embora não exista (ainda) tratado internacional de direitos humanos específico sobre proteção de dados (ou mesmo tratado geral com referência direta e expressa a um direito humano correspondente) ratificado mediante tal procedimento, o fato é que tal circunstância não tem levado a um isolamento político-legislativo-jurídico do Brasil nessa matéria, do que dá conta, em caráter ilustrativo, a substancial recepção, pela LGPD, do Regulamento Geral Europeu, mas também, na esfera doutrinária e jurisprudencial, de parâmetros dogmáticos e interpretativos, como é o caso, já referido, de um direito à autodeterminação informativa, dentre tantos exemplos que poderiam ser colacionados.

Para encerrar essa primeira etapa do texto e dada a sua relevância não apenas para a compreensão do conteúdo e alcance do direito fundamental à proteção de dados na CF, mas também para efeitos de seu diálogo com a legislação, jurisprudência e mesmo doutrina sobre o tema, importa sublinhar que diversos diplomas legais em vigor já dispõem sobre aspectos relevantes da proteção de dados, destacando-se aqui a Lei de Acesso à Informação (Lei 12.527/2011) e o assim chamado Marco Civil da Internet (Lei 12.965/2014) e o respectivo Decreto que o regulamentou (Decreto 8.771/2016), mas especialmente a Lei Geral de Proteção de Dados (Lei 13.709, de 2018).

Assim, uma compreensão/interpretação/aplicação constitucionalmente adequada do direito fundamental à proteção de dados deverá sempre ser pautada por uma perspectiva sistemática, que, a despeito do caráter autônomo (sempre parcial) desse direito, não pode prescindir do diálogo e da interação (por vezes marcada por concorrências, tensões e colisões) com outros princípios e direitos fundamentais, que, dentre outros pontos a considerar, auxiliam a determinar o seu âmbito de proteção, inclusive mediante o estabelecimento de limites diretos e indiretos.

3. A autonomia do direito fundamental à proteção de dados pessoais - para além da privacidade e da autodeterminação informativa

Como já adiantado, o conteúdo (no sentido do âmbito de proteção normativo) de um direito fundamental à proteção de dados pessoais, embora fortemente articulado com o princípio da dignidade da pessoa humana e de outros direitos

fundamentais, em especial o direito ao livre desenvolvimento da personalidade e alguns direitos especiais de personalidade, como é o caso, entre outros, do direito à privacidade e do assim chamado direito à autodeterminação informativa, não se confunde com o do objeto da proteção de tais direitos.

É por tal razão, aliás, que a própria opção terminológica pela proteção de dados pessoais assume uma importância que vai muito além da mera novidade representada pela terminologia em si, porquanto, radica numa viragem concepcional, visto que parte do pressuposto de que dados, para efeitos de sua proteção jurídico-constitucional, devem ser compreendidos em sentido amplo, no sentido da inexistência de dados pessoais irrelevantes em face do processamento eletrônico na sociedade de informação, notadamente pelo fato de que, sendo os dados projeções da personalidade, o seu tratamento, seja qual for, potencialmente pode violar direitos fundamentais²⁰.

De todo modo, a compreensão do âmbito de proteção de um direito fundamental à proteção de dados pessoais envolve sempre um contraste com o de outros direitos, destacando-se, nesse contexto, o direito à privacidade e o direito à autodeterminação informativa, os quais, por seu turno, embora também autônomos entre si, também apresentam zonas de contato importantes.

Pela sua relevância para o desenvolvimento do direito à proteção de dados pessoais, calha retomar, em rápidas pinceladas, o caso da Alemanha, porquanto é lá que se costuma situar o reconhecimento, pela primeira vez, do assim chamado direito à autodeterminação informativa, não no texto constitucional, mas por conta de paradigmática decisão do Tribunal Constitucional Federal, de 15.12.1983, sobre a constitucionalidade de aspectos da lei do censo aprovado pelo Parlamento Federal, cuja realização foi suspensa liminarmente pela Corte em 13.04.1983, muito embora a existência de decisões anteriores envolvendo, ao fim e ao cabo, a proteção de dados pessoais²¹.

Na sua multicitada decisão, o Tribunal Constitucional Federal alemão, contudo, não reconheceu diretamente um direito fundamental à proteção de dados pessoais, mas sim, deduziu, numa leitura conjugada do princípio da dignidade da pessoa humana e do direito ao livre desenvolvimento da personalidade, um direito fundamental implícito à autodeterminação informativa, que consiste, em suma e de acordo com o Tribunal, na prerrogativa de cada indivíduo decidir em princípio e substancialmente sobre a divulgação e utilização de seus dados pessoais²².

O próprio Tribunal Constitucional, contudo, na mesma decisão, alertou para o fato de que o direito à autodeterminação informativa não assegura a cada cidadão um controle absoluto sobre os seus dados, visto que, dada a inserção e responsabilidade comunitária e social do ser humano, este deve tolerar eventuais limitações

20 Cf., por todos, MENDES, Laura Schertel; DONEDA, Danilo. Comentário à Nova Lei de Proteção de Dados (Lei 13.709/2018): O Novo Paradigma da Proteção de Dados. *Revista de Direito do Consumidor*, v. 120, nov./dez. 2018. p. 22. Para maior desenvolvimento, v., em especial, BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: A Função e os Limites do Consentimento**, op. cit., p. 59 e ss.

21 Aqui costuma ser referida, dentre outras, decisão de 16.07.1969 (“Mikrozensus-Entscheidung”), na qual o Tribunal Constitucional assentou que a Lei Fundamental proíbe que o ser humano tenha sua inteira personalidade registrada e catalogada compulsoriamente (v. *BVerfGE* 27, p. 6).

22 Cf., *BVerfGE* 65, p. 42 e ss.

do direito quando em prol do interesse geral²³.

De acordo com Hans-Peter Bull, primeiro encarregado da agência federal de proteção de dados alemã, o cerne moral e político das preocupações do Tribunal Constitucional foi (e é) o da garantia da liberdade dos cidadãos em face da repressão por parte do Estado, de modo que a argumentação deduzida na decisão foi orientada de acordo com o objetivo da proteção da liberdade de ação do ser humano, sendo a transparência da coleta de informações um meio para alcançar tal finalidade²⁴.

Na condição de direito de defesa (direito à não intervenção arbitrária) o direito à autodeterminação informativa consiste em um direito individual de decisão, cujo objeto (da decisão) são dados e informações relacionados a determinada pessoa-indivíduo²⁵.

A relação do direito à autodeterminação informativa com o princípio da dignidade da pessoa humana, portanto, é, em certo sentido, dúplice, pois se manifesta tanto pela sua vinculação com a noção de autonomia quanto com a do livre desenvolvimento da personalidade e de direitos especiais de personalidade conexos, de tal sorte que a proteção dos dados pessoais envolve também a salvaguarda da possibilidade concreta de tal desenvolvimento, para o qual a garantia de uma esfera privada e íntima são indispensáveis.

Não há sobreposição, contudo, entre autodeterminação informativa e proteção de dados, nem privacidade e outros direitos de personalidade. Isso já se dá – mas não exclusivamente – pelo fato de o direito à autodeterminação informativa apresentar uma dupla dimensão individual e coletiva, no sentido de que garantida constitucionalmente não é apenas (embora possa ser, como direito subjetivo individual, o mais importante) a possibilidade de cada um decidir sobre o acesso, uso e difusão dos seus dados pessoais, mas também – e aqui a dimensão metaindividual (coletiva) – se trata de destacar que a autodeterminação informativa constitui precondição para uma ordem comunicacional livre e democrática, distanciando-se, nessa medida, de uma concepção de privacidade individualista e mesmo isolacionista à feição de um direito a estar só (*right to be alone*)²⁶.

Dito de outro modo, “a proteção de dados é, enquanto proteção de direitos fundamentais, espinha dorsal de uma democracia liberal”²⁷.

No concernente às suas interfaces com o direito à privacidade, também inexistente, como já adiantado, superposição completa dos respectivos âmbitos de proteção. Proteção de dados pessoais e, da mesma forma, autodeterminação informati-

23 Cf. *BVerfGE* 65, p. 44.

24 Sobre a dedução interpretativa do direito pelo Tribunal Constitucional, v., por todos, a síntese de BULL, Hans-Peter. **Informationelle Selbstbestimmung** – Vision oder Illusion?. Tübingen: Mohr Siebeck, 2009. p. 29 e ss.

25 Cf. ALBERS, Marion. Umgang mit personenbezogenen Informationen und Daten. In: HOFMANN-RIEM, Wolfgang; SCHMIDT-ASSMANN, Eberhard; VOSSKUHLE, Andrea (Coord.). *Grundlagen des Verwaltungsrechts*. 2. ed. München: C.H. Beck, 2012. v. 2. p. 146-47.

26 Cf. HORNUNG, Gerrit; SCHNABEL, Christoph. Data protection in Germany I: The populational census decision and the right to informational self-determination. *Computer Law & Security Report*, v. 25, i. 1, 2009. p. 85-86.

27 Cf. SPIECKER GENANNT DÖHMANN, Indra. Kontexte der Demokratie: Parteien, Medien und Sozialstrukturen (1. Referat). *VVDStRL*. Berlin: De Gruyter, 2018. v. 77. p. 55-56.

va vão além da privacidade e de sua proteção, ao menos no sentido tradicional do termo, caracterizado por uma lógica de “recolhimento” e “exposição”²⁸.

Nessa perspectiva, é crucial que se tenha presente que embora a proteção de dados tenha sido deduzida (associada), em diversos casos, do direito à privacidade (v.g., nos EUA, o conceito de *informational privacy*) ou, pelo menos, também do direito à privacidade, como no caso da Convenção Europeia de Direitos Humanos (nos termos da exegese do artigo 8º levada a efeito pela CEDH), o fato é que o objeto (âmbito de proteção) do direito à proteção de dados pessoais é mais amplo, porquanto, com base num conceito ampliado de informação, abarca todos os dados que dizem respeito a uma determinada pessoa natural, sendo irrelevante à qual esfera da vida pessoal se referem (íntima, privada, familiar, social), descabida qualquer tentativa de delimitação temática²⁹.

O que se pode afirmar, sem temor de incorrer em erro, é que seja na literatura jurídica, seja na legislação e jurisprudência, o direito à proteção de dados vai além da tutela da privacidade, cuidando-se, de tal sorte, de um direito fundamental autônomo, diretamente vinculado à proteção da personalidade. Aliás, não é à toa que Bruno Ricardo Bioni alertou para o fato de que o entendimento, hoje amplamente superado, de que o direito fundamental à proteção de dados consiste em mera evolução do direito à privacidade, é uma “construção dogmática falha”³⁰.

4. Considerações finais

Como se pode verificar, a despeito da sua bem-vinda inserção no texto constitucional, a autonomia do direito fundamental à proteção de dados pessoais não decorre necessariamente dessa circunstância, o que se deve ao fato de que, independentemente de sua previsão textual, se trata de um direito implicitamente positivado, de acordo com o que de há muito sustenta a doutrina nacional e estrangeira e foi também reconhecido pelo STF.

Além disso, é possível reafirmar, também aqui, que mediante a sua incorporação ao catálogo constitucional de direitos, o direito fundamental à proteção de dados pessoais assegura maior sustentação ao marco regulatório infraconstitucional, bem como fortalece a sua aplicação pelos órgãos do poder judiciário, dentre outras vantagens já apontadas.

Particularmente relevante é o fato de que a condição de direito fundamental autônomo vem acompanhada de um conjunto de prerrogativas traduzidas por um regime jurídico reforçado e uma dogmática sofisticada, mas que deve ser, em especial no caso brasileiro, desenvolvida e traduzida numa praxis que dê ao direito à proteção de dados pessoais a sua máxima eficácia e efetividade, notadamente na esfera da articulação da proteção de dados com outros direitos e garantias fundamentais e bens jurídicos e interesses de estatura constitucional, sempre salvaguardada sua autonomia e seu respectivo núcleo essencial.

28 RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. **O direito à proteção de dados pessoais na sociedade de informação**, op. cit., p. 189.

29 Cf., por todos, KARG, Moritz. Artikel 4, Nr. 1. In: SIMITIS, Spiros; HORNING, SPIECKER GENANT DÖHMANN, Indra. *Datenschutzgesetz*. Baden-Baden: Nomos, 2019. p. 287-290.

30 Cf. BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: A Função e os Limites do Consentimento**, op. cit., p. 95.

REFERÊNCIAS

ALEXY, Robert. **Theorie der Grundrechte**. 2. ed. Frankfurt a.M. Suhrkamp, 1994.

ANDRADE, Fábio Siebeneichler de. Notas sobre a aplicabilidade dos direitos da personalidade à pessoa jurídica como evolução da dogmática civil. *RJLB*, a. 4, n. 5, p. 806-837, 2018.

ANDRADE, José Carlos Vieira de. **Os Direitos Fundamentais na Constituição Portuguesa de 1976**. Coimbra: Almedina, 1987.

BILBAO UBILLOS, Juan Maria. **Los derechos fundamentales en la frontera entre lo público y lo privado**. La noción de “state action” en la jurisprudencia norteamericana. Madrid: McGraw-Hill, 1997.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: A Função e os Limites do Consentimento**. Rio de Janeiro: Forense, 2019.

BULL, Hans-Peter. **Informationelle Selbstbestimmung – Vision oder Illusion?**. Tübingen: Mohr Siebeck, 2009.

CANARIS, Claus-Wilhelm. Considerações a respeito da posição de proibições de discriminação no Sistema de Direito Privado. *Revista Direitos Fundamentais e Justiça*, a. 7, n. 22, jan./mar. 2013.

CANARIS, Claus-Wilhelm. **Grundrechte und Privatrecht**. Berlin-New York: Walter de Gruyter, 1999.

CONSELHO DA EUROPA. *Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais*, de 28 de janeiro de 1981. Disponível em: <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>. Acesso em: 15 nov. 2019.

DIMOULIS, Dimitri; MARTINS, Leonardo. **Teoria Geral dos Direitos Fundamentais**. São Paulo: RT, 2007.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Joaçaba, *Espaço Jurídico Journal of Law*, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 15 nov. 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**. Rio de Janeiro: Renovar, 2006.

DREIER, Horst. Art. 2 I – allgemeines Persönlichkeitsrecht. In: DREIER, Horst (Coord.). **Grundgesetz Kommentar**. 3. Auf. Tübingen: Mohr Siebeck, 2013.

DREIER, Horst. **Subjektiv-rechtliche und objektiv-rechtliche Grundrechtsgehalte**. *JURA*, 1994.

DUQUE, Marcelo Schenk. *Direito Privado e Constituição*. Drittwirkung dos Direitos Fundamentais. São Paulo: Revista dos Tribunais, 2013.

FACHIN, Luiz Edson; RUZYK, Carlos Eduardo Pianovski. Direitos fundamentais, dignidade da pessoa humana e o novo código civil: uma análise crítica. In: SARLET, Ingo Wolfgang (Coord.). **Constituição, direitos fundamentais e**

direito privado. Porto Alegre: Livraria do Advogado, 2003.

GOMES CANOTILHO, José Joaquim; MOREIRA, Vital. **Constituição da República Portuguesa anotada**, 4. ed. Coimbra: Coimbra Editora, 2007.

GOMES CANOTILHO, José Joaquim. Omissões normativas e deveres de proteção. *In*: DIAS, Jorge de Figueiredo (Coord.). **Estudos em homenagem a Cunha Rodrigues**. Coimbra: Coimbra Editora, 2001. v. II.

GRIMM, Dieter. A função protetiva do Estado. *In*: SOUZA NETO, C. P.; SARMENTO, D. **A Constitucionalização do Direito**. Rio de Janeiro: Lumen Juris, 2007.

HARTMANN, Ivar. Liberdade de expressão e capacidade comunicativa: um novo critério para resolver conflitos entre direitos fundamentais informacionais. *Direitos Fundamentais & Justiça*, a. 12, n. 39, p. 145-183, jul./dez. 2018.

HESSE, Konrad. *Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland*. 20. ed. Heidelberg: C. F. Müller, 1995.

HILGENDORF, Eric; FELDLE, Jochen (Ed.). **Digitalization and the Law**. Baden-Baden: Nomos, 2018.

HOFFMANN, Christian; LUCH, Anika; SCHULZ, Sönke E.; BORCHERS, Kim Corinna. **Die digitale Dimension der Grundrechte**. Das Grundgesetz im digitalen Zeitalter. Baden-Baden: Nomos, 2015.

HOFMANN-RIEM, Wolfgang. Reclaim Autonomy: Die Macht digitaler Konzerne. *In*: AUGSTEIN, Jakob (Coord.). **Reclaim Autonomy**. Selbstermächtigung in der digitalen Weltordnung. Frankfurt am Main: Suhrkamp, 2017.

HORNUNG, Gerrit; SCHNABEL, Christoph. Data protection in Germany I: The populational census decision and the right to informational self-determination. *Computer Law & Security Report*, v. 25, i. 1, 2009.

IPSEN, Jörn. **Staatsrecht II – Grundrechte**. 17. Auf. Vahlen, 2014.

JARASS, Hans; PIEROTH, Bodo. **Grundgesetz für die Bundesrepublik Deutschland**: Kommentar. München: C. H. Beck. 13. Auf. 2014.

KARG, Moritz. Artikel 4, Nr. 1. *In*: SIMITIS, Spiros; HORNUNG, SPIECKER GENANNT DÖHMANN, Indra. **Datenschutzgesetz**. Baden-Baden: Nomos, 2019.

KLOEPFER, Michael. **Verfassungsrecht II**. München: C. H. Beck. 13. Auf. 2010.

KÜHLING, Jürgen. Datenschutz und die Rolle des Rechts. *In*: STIFTUNG FÜR DATENSCHUTZ (Ed). **Die Zukunft der informationellen Selbstbestimmung**. Berlin: Erich Schmidt Verlag, 2016.

LEONARDI, Marcel. **Fundamentos de Direito Digital**. São Paulo: Revista dos Tribunais, 2019.

LIMBERGER, Têmis. **O Direito à Intimidade na Era da Informática**. Porto Alegre: Livraria do Advogado, 2007.

MANSSEN, Gerrit. **Staatsrecht I Grundrechtsdogmatik**. München: Verlag Franz Vahlen, 1995.

MARINONI, Luiz Guilherme. **Técnica processual e tutela dos direitos**. 4. ed. São Paulo: Revista dos Tribunais, 2013.

MENDES, Laura Schertel. Habeas Data e autodeterminação informativa: dois lados da mesma moeda. *Revista Direitos Fundamentais & Justiça*, a. 12, n. 39, p. 185-216, jul./dez. 2018.

MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**. São Paulo: Saraiva, 2013.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à Nova Lei de Proteção de Dados (Lei 13.709/2018): O Novo Paradigma da Proteção de Dados. *Revista de Direito do Consumidor*, v. 120, nov./dez. 2018.

MIRANDA, Jorge; MEDEIROS, Rui. **Constituição Portuguesa Anotada**. 1. ed. Coimbra: Coimbra Editora, 2006.

MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra Sales. *Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data*. *Direitos Fundamentais & Justiça*, a. 13, n. 41, p. 183-212, jul./dez. 2019.

MOTA PINTO, Paulo. **Direitos de Personalidade e Direitos Fundamentais: Estudos**, Coimbra: Gestlegal, 2018.

MURSWIEK, Dietrich; RIXEN, Stephan. Persönliche Freiheitsrechte. In: SACHS, Michael. **Grundgesetz Kommentar**. 8. ed. München: C.H.Beck, 2018.

PARLAMENTO EUROPEU. *Carta de Direitos Fundamentais da União Europeia*, de 7 de dezembro de 2000. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN>. Acesso em: 15 nov. 2019.

PIEROTH, Bodo; SCHLINK, Bernhard. **Grundrechte**. Staatsrecht II. 11. ed. Heidelberg: C. F. Müller, 1995.

REINHARDT, Jörn. Conflitos de direitos fundamentais entre atores privados: “efeitos horizontais indiretos” e pressupostos de proteção de direitos fundamentais. *Direitos Fundamentais & Justiça*, ano 13, n. 41, p. 59-91, jul./dez. 2019.

RODRIGUES JÚNIOR, Otávio Luís. **Direito Civil Contemporâneo: Estatuto Epistemológico, Constituição e Direitos Fundamentais**. 2. ed. São Paulo: GEN, 2019.

RODRIGUEZ, Daniel Piñeiro. **O Direito Fundamental à Proteção de Dados**. Vigilância, Privacidade e Regulação. Rio de Janeiro: Lumen Juris, 2021.

ROSSNAGEL, Alexander; WEDDE, Peter; HAMMER, Volker; PORDESCH, Ulrich. **Digitalisierung der Grundrechte?** Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik. Opladen: Westdeutscher Verlag, 1990.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade de informação. *Direito, Estado Sociedade*, n. 36, jan/jun. 2010.

RUFFERT, Matthias. Privatrechtswirkung der Grundrechte. Von Lüth zum Stadionverbot – und darüber hinaus? n. 1, Jus 2020.

SAMPAIO, José Adércio Leite. A suprema inviolabilidade: a intimidade informática e o sigilo bancário. In: SARMENTO, Daniel; SARLET, Ingo Wolfgang (Coord.). **Direitos fundamentais no Supremo Tribunal Federal: balanço e crí-**

tica, Rio de Janeiro: Lumen Juris, 2011.

SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. Porto Alegre: Livraria do Advogado, 2018.

SARLET, Ingo Wolfgang. Direitos Fundamentais e Direito Privado, algumas considerações em torno da vinculação dos particulares aos direitos fundamentais. *In*: SARLET, Ingo Wolfgang (Coord.). **A Constituição Concretizada**: Construindo Pontes para o Público e o Privado. Porto Alegre: Livraria do Advogado, 2000.

SARLET, Ingo Wolfgang. Proteção de dados como direito fundamental na Constituição Federal Brasileira de 1988, *Direitos Fundamentais & Justiça* | Belo Horizonte, ano 14, n. 42, p. 175-214, jan./jun. 2020.

SARLET, Ingo Wolfgang; FERREIRA NETO, Arthur M. **O Direito ao “Esquecimento” na Sociedade de Informação**. Porto Alegre: Livraria do Advogado, 2018.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional**. 3. ed. São Paulo: Revista dos Tribunais, 2014.

SARMENTO, Daniel. **Direitos Fundamentais e Relações Privadas**. Rio de Janeiro: Lumen Juris, 2003.

SCHIEDERMAIR, Stephanie. Einleitung. *In*: SIMITIS, Spiros; HORNUNG, Gerrit; SPIECKER GENANNT DÖHMANN, Indra (Coord.). **Datenschutzrecht**. Baden-Baden: Nomos, 2019.

SCHLIESKY, Utz; HOFFMANN, Christian; LUCH, Anika D.; SCHULZ, Sönke E.; BORCHERS, Kim Corinna. **Schutzpflichten und Drittwirkung im Internet**. Das Grundgesetz im digitalen Zeitalter. Baden-Baden: Nomos, 2014.

SILVA, Virgílio Afonso da. **A Constitucionalização do Direito**. Os direitos fundamentais nas relações entre particulares. São Paulo: Malheiros, 2005.

SPIECKER GENANNT DÖHMANN, Indra. Kontexte der Demokratie: Parteien, Medien und Sozialstrukturen (1. Referat). *VVDStRL*. Berlin: De Gruyter, 2018.

_____. O direito à proteção de dados na internet em casos de colisão, *in*: *Revista Direitos Fundamentais & Justiça*, a. 12, n. 38, p. 17-33, jan./jun. 2018.

STARCK, Christian. Art. 2 Abs. 1 – Schutz des Art. 2 Abs. 1 vor Eingriffen durch die öffentliche Gewalt. *In*: VON MANGOLDT; KLEIN; STARCK. *Grundgesetz Kommentar*, v. 1, 7. Auf. München: C.H.Beck, 2018.

STEINMETZ, Wilson. **A vinculação dos particulares a direitos fundamentais**. São Paulo: Malheiros, 2004.

STERN, Klaus. Idee und Elemente eines Systems der Grundrechte. *In*: KIRCHHOF, J. Isensee-P. (Coord.). **Handbuch des Staatsrechts der Bundesrepublik Deutschland**. Heidelberg: C. F. Müller, 1992. v. 5.

WOLFF, Heinrich Amadeus. Schutz personenbezogener Daten. *In*: PECHSTEIN, Matthias; NOWAK, Carsten; HÄDE, Ulrich (Coord.). *Frankfurter Kommentar EUV – GRC – AEUV*. Tübingen: Mohr Siebeck, 2017. v. 1.

2. A LEI GERAL DE PROTEÇÃO DE DADOS E SEUS IMPACTOS NAS RELAÇÕES DE TRABALHO

IURI PINHEIRO³¹ E VÓLIA BOMFIM³²

1. Introdução

A Quarta Revolução Industrial (SCHWAB, 2016)³³ está sendo vivenciada através de novas tecnologias, que se baseiam em análise massiva de dados (“big data”) a partir da inteligência artificial e da robótica, dentre outros fatores, em um mundo no qual os objetos são conectados uns aos outros (internet das coisas).

Os dados, cada vez mais, são processados e valorados economicamente, sendo considerados o principal insumo da sociedade contemporânea e equiparados ao petróleo de outros tempos. Por isso mesmo, afirma-se que a economia é dirigida por dados (“data driven economy”).

Diante de tamanha magnitude, a disciplina e regulação do uso de dados passou a ser uma pauta central em vários países e, sobretudo, um compromisso da agenda internacional, de modo a assegurar o seu uso íntegro e evitar concorrência desleal.

O Conselho da Europa disciplinou o tratamento de dados pessoais desde 1973, através da Resolução nº 22 de 1973 e da Resolução nº 29 de 1974, ambas versando sobre princípios para proteção de informações pessoais em bancos de dados automatizados, no setor público e privado.

Contudo, o tratamento mais abrangente da matéria no âmbito da União Europeia foi realizado em 1995 através da Diretiva nº 46, que foi sucedida pelo Regulamento Geral da Proteção de Dados, GDPR (sigla em inglês), o qual entrou em vigor em 25 de maio de 2018.

No Brasil, viveu-se um longo período de anomia legislativa específica, mas que não significa dizer que vivíamos um estado de absoluta desproteção, afinal, a privacidade e a intimidade são valores inscritos no catálogo de direitos fundamentais (art. 5º, X, da CF/88). O inciso XII do artigo 5º da Constituição expressamente protege o sigilo dos dados e da correspondência. Além disso, existem outras manifestações infraconstitucionais, a exemplo do Código de Defesa do Consumidor (arts. 43 a 45); Lei nº 9.507, de 12.11.1997 (Habeas Data); Lei nº 12.414, de 9.06.2011 (Cadastro Positivo); Lei nº 12.527, de 18.11.2011 (Lei do Acesso à

31 Juiz do Trabalho, Coordenador da Pós-Graduação de Compliance Trabalhista, LGPD e Prática Trabalhista, Professor de diversas instituições, dentre elas PUC-Minas. Professor-Convitado de Escolas Judiciais dos TRTs e do TST (ENAMAT). Escritor de obras jurídicas, especialmente do *Manual do Compliance Trabalhista e Manual da Terceirização*. Formação em Compliance Laboral pela Wolters Kluwer (Espanha).

32 Advogada Trabalhista e Consultora Jurídica. Desembargadora Aposentada do TRT da 1ª Região. Coordenadora Científica da Pós-Graduação de Compliance Trabalhista, LGPD e Prática. Professora de diversas instituições e de Escolas Judiciais. Mestre e Doutora em Direito. Participou da Comissão de Reforma Trabalhista da Câmara dos Deputados. Escritora de obras jurídicas, especialmente do *Manual de Direito do Trabalho* em sua 17ª edição.

33 SCHWAB, Klaus. *A quarta revolução industrial*. São Paulo: Edipro, 2016.

Informação); e Lei nº 12.965, de 23.04.2014 (Marco Civil da Internet).

Entretanto, o Brasil carecia de uma efetiva disciplina sobre o tratamento de dados pessoais, o que vinha, de modo recorrente, despertando desconfiança da comunidade internacional acerca da confiabilidade de compartilhamento de dados no âmbito brasileiro.

Após muitos debates e entraves de processo legislativo, em 15 de agosto de 2018 foi publicada a Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) com prazo de *vacatio legis* que foi alterado diversas vezes, postergando sistematicamente a entrada em vigor.

Apesar da nova lei, outros dispositivos legais e infraconstitucionais podem ser aplicados para complementá-la em seus vazios, como expressamente previsto no artigo 64.

Renovadas as desconfianças sobre a confiabilidade brasileira no tratamento de dados, a LGPD, finalmente, teve sua vigência iniciada em 18/09/2020, exceto no que se refere às sanções administrativas, previstas para entrar em vigor em 01/08/2021.

Entretantes, ainda que as sanções administrativas estejam em período de vacância, seus princípios e deveres já são dotados de juridicidade e podem ensejar responsabilidade civil em caso de descumprimento³⁴, sendo premente a necessidade de compreensão deste relevante diploma legal.

2. A relevância da proteção de dados no contexto das relações de trabalho

O art. 1º da LGPD aponta como finalidade da lei a proteção dos “direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”, sem fazer qualquer distinção quanto ao tipo de relação jurídica em que se dê o tratamento de dados pessoais.

Essa disciplina ampla é coerente com a própria denominação do diploma, intitulado de Lei “Geral” de Proteção de Dados, que deve, assim, espriar os seus efeitos pelas mais variadas espécies de relações, ostentando autêntica transversalidade.

Diversamente do GDPR³⁵, a lei brasileira não contempla expressa disposição sobre o direito do trabalho³⁶, mas sua incidência a ele é irrefutável, pois a relação de trabalho sequer teria como se iniciar e desenvolver sem a coleta, recepção, armazenamento e retenção³⁷ de dados pessoais dos empregados ou candidatos a empregos.

Importante destacar que o elevado fluxo de dados nas relações de trabalho assume grandes proporções e atrai especial atenção sobre a questão, uma vez que o empregador, desde a fase pré-contratual (processos seletivos e admissão), passan-

34 A propósito, o próprio Supremo Tribunal Federal, no julgamento da ADI 6387, invocou a principiologia da LGPD (que tem assento constitucional – privacidade e intimidade) para suspender o compartilhamento de dados de usuários por prestadoras de serviços de telecomunicações ao IBGE, o que era autorizado pela Medida Provisória nº 954/20.

35 O art. 88 do GDPR traz regras expressas sobre o tratamento de dados no contexto laboral.

36 Uma das poucas disposições relacionadas ao âmbito trabalhista é a previsão constante do art. 5º, II, que indica ser dado pessoal sensível a filiação a sindicato.

37 Os verbos utilizados nesta passagem são apenas alguns daqueles compreendidos dentro do conceito de “tratamento” de dados que foi enunciado pelo art. 5º, X, da LGPD.

do pela fase contratual e chegando até a fase pós-contratual, tem acesso e se torna responsável pelo armazenamento e guarda de dados pessoais dos trabalhadores.

Entre os dados pessoais que merecem cuidado, pode-se citar, em singela ilustração, a própria documentação pessoal de identificação dos trabalhadores, o monitoramento de correspondências eletrônicas, as mensagens trocadas em aplicativos de comunicação, a captura de imagens dos trabalhadores no local de trabalho, o registro de chamadas no âmbito da prestação de um serviço de telemarketing, as chamadas em sistemas de teleconferência, o registro biométrico da jornada de trabalho.

Mesmo que a legislação brasileira não tenha regulamentado a aplicação da proteção de dados no âmbito das relações de trabalho, é essencial investigar as causas legitimadoras do tratamento de dados nas relações de trabalho, bem como a forma de operacionalizá-las, considerando-se as necessidades decorrentes da dinâmica dos negócios.

Assim, é extremamente importante que os profissionais da área trabalhista, sob o viés de um sistema de gestão de riscos, tenham especial atenção sobre as obrigações impostas pela legislação e se preparem para adequar as rotinas trabalhistas às exigências de proteção de dados.

3. Fundamentos da Lei Geral de Proteção de Dados

A LGPD enuncia, no início do seu texto, os fundamentos que devem nortear a disciplina de dados pessoais:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

- I - o respeito à privacidade;
- II - a autodeterminação informativa;
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV - a inviolabilidade da intimidade, da honra e da imagem;
- V - o desenvolvimento econômico e tecnológico e a inovação;
- VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Além de corresponderem a fundamentos inspiradores da criação da própria norma (função normogênica ou informadora), esses sete fundamentos devem ser compreendidos como balizamentos essenciais para a correta definição do sentido e alcance da disciplina de proteção de dados.

Todos os fundamentos são de extremo relevo, mas um deles, até então, não era muito difundido e por isso passamos a explorá-lo de forma destacada.

Cuida-se do direito à autodeterminação informativa, que também pode ser denominado de direito à privacidade decisional e informacional.

Explica-se.

Durante muito tempo, acreditou-se que os dados das pessoas naturais faziam parte do patrimônio da empresa que os coletava. A valoração econômica da atividade empresarial, muitas vezes, correspondia ao quantitativo de dados que tratava. Após vazamentos e utilização indevida e muitas vezes abusiva, vem a lei para regular, e não impedir, o tratamento dos dados das pessoas físicas, dando ao seu titular, e só a este, o direito de informação, decisão e disponibilidade.

Este direito foi reconhecido inicialmente pelo Tribunal Constitucional Alemão, em 1982, no julgamento do caso da Lei do Censo Alemã, a qual foi declarada inconstitucional porque, para realização do censo demográfico, haveria a coleta excessiva de dados, como bem lembra a autora portuguesa Teresa Coelho³⁸.

JJ Gomes Canotilho³⁹ ensina que o direito geral à autodeterminação informativa se traduz, fundamentalmente, na faculdade de o particular determinar e controlar a utilização dos seus dados pessoais.

Trata-se de um direito fundamental, visto que diretamente ligado à privacidade e intimidade (art. 5º, X, da CF/88).

A propósito, tramita no Congresso Nacional a PEC nº 17/2019, que altera a Constituição da República para incluir a proteção de dados pessoais de forma expressa entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais

Como exemplo prático no cotidiano das relações de trabalho, pode-se citar o caso da entrega de atestados médicos, nos quais tenha constado a indicação de uma doença (CID⁴⁰).

É inequívoco que o empregado possui o direito de que a informação sobre seu estado de saúde não seja compartilhada entre os demais trabalhadores até mesmo pelo elevado potencial discriminatório, mas, por outro lado, a empresa tem o dever de guarda da documentação de seus empregados, inclusive para fins de reflexos previdenciários.

É fundamental, assim, que a empresa esteja preparada para criar rotinas seguras. Os atestados médicos devem, preferencialmente, ser armazenados em setor específico de segurança e medicina ocupacional, mas esse procedimento deve ser feito com proteção adequada para não incorrer em violação à privacidade.

Para a guarda segura, pode-se citar como possibilidade o armazenamento digital com a utilização de criptografia, anonimização ou pseudonimização, recursos esses cogitados pela própria LGPD e que demandarão o trabalho conjunto com a tecnologia da informação.

Todos os empregados devem ser informados e alguns devem ser treinados para o armazenamento, descarte e demais formas de tratamento de dados pessoais e sensíveis, inclusive os que aparentemente não lidam com dados, como a faxineira,

38 MOREIRA, Teresa Coelho. **A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação**: Contributo para um estudo dos limites do poder de controlo electrónico do empregador. Coimbra: Almedina, 2010.

39 CANOTILHO, JJ Gomes. **Direito Constitucional e Teoria da Constituição**. Coimbra: Almedina, 2003.

40 CID – Código de Identificação da Doença

o contínuo ou o garçom, pois podem ter acesso fortuito a um documento esquecido no ambiente de trabalho. Compete ao empregador (controlador) a adoção das medidas de precaução e proteção aos dados de todos os trabalhadores.

4. Princípios da LGPD

Além de fundamentos, a LGPD enuncia 10 princípios que devem orientar as operações de tratamento de dados em seu art. 6º, o qual se transcreve na sua integralidade:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demons-

tração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medida

Os princípios são premissas estruturantes que informam, conformam e orientam a aplicação das outras normas, sendo por isso mesmo considerados os alicerces ou vigas-mestras do edifício jurídico.

Por isso, é muito importante ter em mente todos esses princípios acima enumerados, que são de clareza explicativa e que devem sempre ser ponderados quando do tratamento dos dados pessoais.

Os três primeiros princípios acima indicados formam um tripé do núcleo duro de legitimação do tratamento de dados, eis que sempre será preciso ponderar criteriosamente se a operação realizada está se restringindo à finalidade específica que justifica o seu uso; se é adequado ao fim pretendido e se está sendo realizado sem excessos, limitando apenas ao necessário.

Embora denominado pela LGPD de Princípio da Necessidade, essa última premissa também vem sendo denominada de Princípio da Minimização.

5. Conceituações centrais da LGPD e suas implicações nas relações de trabalho

O art. 5º da LGPD equivale a uma espécie de dicionário da LGPD, apresentando diversos conceitos essenciais à compreensão da lei.

Por limitação de espaço, esse texto cuidará dos aspectos centrais, reservando para outra oportunidade o aprofundamento de outras questões.

5.1 Dados Pessoais e Dados Pessoais Sensíveis

Antes de analisar as hipóteses e formas de tratamento, é essencial compreender o que são dados pessoais e dados pessoais sensíveis.

A teor do art. 5º, I e II, da LGPD, dado pessoal é a “informação relacionada a pessoa natural identificada ou identificável”, enquanto dado pessoal sensível é o “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”.

Podem ser citados como dados pessoais o nome, estado civil, escolaridade, endereço, filiação, idade, correspondência eletrônica, o CPF, o número do registro civil, dentre outros.

Os dados sensíveis são dados pessoais associados a determinados contextos que sejam capazes, em tese, de gerar uma discriminação injustificada.

A LGPD apresenta um rol de situações que qualificam dados pessoais como sensíveis, mas não declina se o rol é exemplificativo ou taxativo.

Considerando a ausência de limitação do texto e que, naturalmente, existem diversos outros contextos passíveis de gerar tratamento discriminatório, não se mostra razoável entender tal rol como taxativo, sendo possível até mesmo que a Autoridade Nacional de Proteção de Dados aborde outras hipóteses caracterizadoras, com fundamento no seu papel complementar conferido pelo art. 55-J da LGPD.

5.2 Tratamento de Dados Pessoais

Outra compreensão fundamental é entender que tipo de operação seria alcançada pela LGPD, cumprindo observar que a legislação utiliza o verbo “tratar” e que ela define o que seria tratamento de dados pessoais no inciso X do art. 5º como sendo “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”.

Perceba-se que o conceito de tratamento de dados pessoais é extremamente elástico e envolve 20 núcleos verbais, conferindo, portanto, ampla proteção aos dados pessoais.

5.3 Sujeitos do Tratamento de Dados Pessoais

No que se refere aos sujeitos envolvidos no tratamento de dados, a legislação traz quatro figuras que merecem destaque:

- a) titular de dados pessoais;
- b) controlador;
- c) operador e
- d) encarregado (denominado no direito comparado como Data Protection Officer – DPO).

5.3.1 Titular dos Dados Pessoais

O inciso V do art. 5º intitula o titular como sendo a “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”.

Em que pese à pessoa jurídica sejam aplicáveis, no que couber, os direitos da personalidade (art. 52 do Código Civil e artigo 223-B da CLT), perceba-se que a LGPD consignou como destinatário de proteção de dados pessoais e sensíveis apenas a pessoa natural.

Merece reflexão mais cuidadosa a incidência da LGPD em favor de microempreendedor individual (MEI), do empregador doméstico⁴¹ e do empregador pessoa física, como os profissionais liberais. Isto porque todos esses se constituem em pessoas naturais, normalmente com hipossuficiência econômica⁴² em relação às empresas.

É importante lembrar que MEI é uma ficção jurídica criada pela Lei Complementar 128, através da qual uma pessoa natural exerce individualmente uma atividade empresarial, mas, ainda assim, se assegura a obtenção de CNPJ, desde que atendidas certas limitações legais.

A possibilidade de ter CNPJ poderia induzir a uma compreensão de que o MEI não seria destinatário da LGPD, mas o simples fato de possuir CNPJ não equivale

41 Entendo que o artigo 4º, I da Lei 13.709/18 não se aplica aos empregadores domésticos, pois não utilizam os dados do empregado doméstico para fins “exclusivamente” particulares, uma vez que, por força de lei, o patrão compartilha dados de seus empregados com o e-social e demais órgãos competentes. Além disso, empregador doméstico é o que consome a mão de obra doméstica para fins “não lucrativos” – artigo 1º da LC 150/15. A expressão “não lucrativo” tem conceito diverso de fins “não econômicos”.

42 Este raciocínio também foi o adotado pelo artigo 899, § 9º da CLT, pois tratou diferentemente o empregador doméstico, microempreendedores individuais, entre outros, para fins de depósito recur-

a dizer que se trata de pessoa jurídica.

Com efeito, o art. 44 do Código Civil aponta quais são as pessoas jurídicas de direito privado e apenas contempla as empresas individuais de responsabilidade limitada (EIRELI), figura que com aquela não se confunde.

Não sendo o MEI uma pessoa jurídica, mas sim uma pessoa física empreendedora a quem a lei faculta a obtenção de CNPJ para fins fiscais, é lícito concluir ser alcançado pela proteção da LGPD, tanto para proteção de seus dados como para respeitar os dados de seus empregados.

O mesmo raciocínio pode ser aplicado ao empregador doméstico e aos demais empregadores que sejam pessoas naturais, pois são ao mesmo tempo titulares de seus dados pessoais, logo, protegidos pela LGPD, mas por outro lado devem obediência à LGPD no que se refere aos dados de seus empregados, com certas restrições.

No âmbito específico da relação de trabalho, o titular de dados pessoais será, quase sempre, o empregado, mas também pode ser aplicado aos terceirizados, autônomos e demais prestadores de serviços.

5.3.2 Controlador e Operador

O controlador e o operador estão definidos, respectivamente, nos incisos VI e VII do art. 5º como sendo a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” e a “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”.

Aplicando tais conceitos ao âmbito da relação de trabalho, o empregador inequivocamente desempenhará a função de controlador.

A figura do operador poderá ou não existir a depender de ter havido, ou não, a contratação de uma pessoa natural ou jurídica pelo empregador para em seu nome realizar o tratamento de dados pessoais. Portanto, pode o empregador cumular o papel de controlador e operador.

Situação que vem suscitando debates é se o empregado que realiza o tratamento de dados pessoais em uma determinada empresa ostentaria a condição de operador.

O Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT) editou a Resolução nº 9, de 2 de setembro de 2020, instituindo uma política de privacidade no âmbito daquele tribunal e, em seu art. 5º, classificou o Presidente do Tribunal como Controlador e os servidores como Operadores.

Caso adotada essa mesma perspectiva para o âmbito privado, os empregados que tratam os dados por ordem do controlador (patrão) ostentariam a condição de operadores.

Importante destacar que a questão não é meramente teórica porque aquele que seja classificado como operador responde solidariamente⁴³ pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese

43 Aliás, a legislação trabalhista também prevê, conforme o artigo 223-E da CLT, que o empregador responda junto com o causador do dano moral (outro empregado) na proporção da ação ou omissão que ocasionou o dano extrapatrimonial.

em que o operador equipara-se ao controlador, a teor do art. 42, § 1º, I, da LGPD.

Em que pese a complexidade da questão, não se pode ignorar que, ao executar tarefas e ordens, o empregado está “presentando” o empregador. Em outras palavras, é como se o próprio empregador estivesse atuando, diversamente da hipótese em que o empregador contrata uma outra pessoa (física ou jurídica) para realização do tratamento de dados.

A partir dessa perspectiva, é possível defender que o empregador é um mero executor de ordens subordinado, não assumindo a condição de controlador ou operador, salvo quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, quando a própria LGPD o considera como controlador por equiparação⁴⁴.

Por outro lado, é possível também advogar que não há qualquer vedação legal para que o encargo de operação de dados seja assumido por empregado, hipótese em que, ao aceitar o encargo, estará, conseqüentemente, obrigado a respeitar as instruções do controlador.

O cargo é eminentemente técnico, não sendo obrigatória a concessão de função de confiança gratificada para o exercício da função de operador.

5.3.3 Encarregado

Por sua vez, na conformidade do art. 5º, VIII, da LGPD, o encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador (empregador), os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Importante destacar que, na redação inicial, o encarregado deveria ser uma pessoa natural, mas a Lei n.º 13.853/19 suprimiu essa exigência, abrindo espaço para que o encarregado seja pessoa jurídica através de terceirização de serviços (isso também é permitido na GDPR – art. 37º, VI).

Essa alternativa pode se tornar atrativa pela possibilidade de delegar a tarefa a alguém especializado, mas, por outro lado, exige muita responsabilidade.

Isso porque o art. 4º-A da Lei 6.019 exige que toda prestadora de serviços tenha capacidade econômica compatível com a execução do contrato, exigindo uma “due diligence” muito criteriosa.

Além disso, a terceirização elevará a exposição de dados e o risco de vazamento, reforçando a necessidade de investigar com muito cuidado para quem se está terceirizando.

Em se tratando de empresas do mesmo grupo econômico, entendemos ser possível a indicação de um só encarregado, seja ele empregado ou não de apenas uma delas, para representar todas, por força da incidência do direito comparado (art. 37º, II, da GDPR c/c art. 8º da CLT). Mesmo tendo a Lei 13.467/17 eliminado, quase por completo, a teoria do empregador único, ainda assim será possível a nomeação de apenas um encarregado para todas as empresas do grupo, independentemente de ser este grupo vertical (por subordinação) ou horizontal (por

⁴⁴ Há quem defenda que a caracterização de controlador por equiparação apenas ocorreria no caso de o empregado não seguir as instruções lícitas do controlador em virtude de o dispositivo em questão fazer alusão ao termo “hipótese” no singular. Contudo, parece-nos que o termo “hipótese” se refere a qualquer das duas situações, até por que elas foram tratadas como opções alternativas, além de não existir motivo razoável que justifique um tratamento diverso.

coordenação).

Outra polêmica será sobre a necessidade de indicação de encarregado no âmbito doméstico, para os profissionais liberais com poucos empregados e para o MEI (que só pode ter um empregado), já que o art. 41 não traz exceção. Entendemos que é dispensável a contratação de um encarregado nestas hipóteses, podendo o controlador cumular o cargo de encarregado. Além disso, o § 3º do artigo 41 prevê que a ANPD pode estabelecer dispensa de indicação, o que nos parece razoável para esses casos.

O art. 41, § 2º, da LGPD prevê as atividades do encarregado nos seguintes termos:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

A partir dessas atribuições, muitas controvérsias surgirão. A primeira delas é se as referidas atribuições não demandariam a necessidade de uma autonomia incompatível com a figura da relação de emprego, visto que o encarregado terá que se reportar à autoridade nacional de proteção de dados, dela receber comunicações e adotar providências.

Em que pese tal reflexão, entendemos que não há qualquer óbice ao desempenho de tal função por empregados próprios especializados no tema, até porque existem diversos trabalhadores técnicos e especialistas, muitos regidos por normas específicas, que imputam deveres legais que vão além das obrigações do contrato de trabalho (médicos, arquitetos, engenheiros etc).

Nesse tocante, pontua-se também que a existência de uma legislação específica a ser observada pelo encarregado, além da possibilidade de normas complementares que podem ser editadas pela ANPD, poderá futuramente permitir a constituição de sindicatos próprios, caracterizando o encarregado como categoria diferenciada.

Se o empregador atribuir tal função a um empregado que concorde com tal encargo, é recomendável a elaboração de aditivo contratual.

Relevante pontuar o cuidado de zelar para que eventual cumulação de funções não resulte em conflito de interesses, o que assume contorno muito particular em relação àqueles que exerçam a função de advogados da empresa, ou operador de tecnologia da informação.

Isso porque o artigo 2º, parágrafo único, inciso VIII, alínea “b”, do Código de Ética da Ordem dos Advogados do Brasil estabelece que são deveres do advogado abster-se de patrocinar interesses ligados a outras atividades estranhas à advocacia, em que também atue.

E, no dia 28 de setembro de 2018, em sessão plenária, o Conselho Geral da Ordem dos Advogados – Conselho Regional de Lisboa – deliberou aprovar o parecer emitido no âmbito do processo n.º 14/PP/2018-G, em que foi relator o Dr. Zacarias Carvalho, segundo o qual “(n)os termos do disposto no artigo 83º, nºs 1, 2 e 6, do Estatuto da Ordem dos Advogados, os advogados estão impedidos de exercer a advocacia e, assim, impedidos de exercer o mandato forense ou a consulta jurídica, para entidades para quem exerçam, ou tenham exercido as funções de Encarregado de Proteção de Dados”⁴⁵.

Assim, caso o advogado tenha contrato ou esteja constituído para defender ou patrocinar interesses do controlador, não deverá, sob pena de flertar com infração ético-disciplinar, exercer as atribuições de encarregado de proteção de dados do mesmo cliente.

Outra polémica centra-se na necessidade, ou não, de o encarregado ser detentor de conhecimento jurídico-regulatório.

O § 4º do art. 41 da LGPD previa expressamente que o encarregado deveria ser detentor de tal conhecimento jurídico-regulatório e ser apto a prestar serviços especializados em proteção de dados, mas a disposição restou vetada pela Presidência da República, sob a seguinte justificativa:

A propositura legislativa, ao dispor que o encarregado seja detentor de conhecimento jurídico regulatório, contraria o interesse público, na medida em que se constitui em uma exigência com rigor excessivo que se reflete na interferência desnecessária por parte do Estado na discricionariedade para a seleção dos quadros do setor produtivo, bem como ofende direito fundamental, previsto no art. 5º, XIII da Constituição da República, por restringir o livre exercício profissional a ponto de atingir seu núcleo essencial.

Em que pese o veto, é extremamente recomendável que o encarregado seja dotado de conhecimento jurídico-regulatório, até porque a natureza de suas atribuições reclama destacado conhecimento da LGPD.

6. Hipóteses Autorizativas do Tratamento de Dados Pessoais e de Dados Pessoais Sensíveis e a contextualização com a relação de trabalho

6.1 Premissas gerais

O art. 7º da LGPD estipula as bases legais para o tratamento de dados pessoais, enquanto o art. 11 enumera as hipóteses autorizativas do tratamento de dados pessoais sensíveis:

45 Disponível em: <<https://crlisboa.org/docs/ParecerDPOvf1.pdf>> Acesso em: 29 set.2020.

<p>Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:</p> <p>I – mediante o fornecimento de consentimento pelo titular;</p> <p>II – para o cumprimento de obrigação legal ou regulatória pelo controlador;</p> <p>III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;</p> <p>IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;</p> <p>V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;</p> <p>VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);</p> <p>VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro;</p> <p>VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;</p> <p>VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)</p> <p>IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou</p> <p>X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.</p>	<p>Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:</p> <p>I – quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;</p> <p>II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:</p> <p>a) cumprimento de obrigação legal ou regulatória pelo controlador;</p> <p>b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;</p> <p>c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;</p> <p>d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);</p> <p>e) proteção da vida ou da incolumidade física do titular ou de terceiro;</p> <p>f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou</p> <p>f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019)</p> <p>g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.</p>
--	---

O confronto entre os dois dispositivos permite concluir que uma grande diferença entre as bases de tratamento dos dados pessoais e dados pessoais sensíveis é que o interesse legítimo do controlador ou de terceiro (inciso IX do art. 7º) é causa autorizadora apenas para os primeiros.

Por outro lado, ao mencionar o exercício regular de direitos, a LGPD prevê que estes justificariam o tratamento de dados pessoais não-sensíveis (art. 7º) apenas diante de processos judiciais, administrativos e arbitrais, enquanto que para o tratamento de dados pessoais sensíveis o exercício regular de direitos não está restrito a processos.

Essa maior abertura para tratamento de dados com fundamento no exercício regular de direito permitirá, muitas vezes, o tratamento de dados sensíveis em organizações de tendência.

Questão de extrema importância é o procedimento do tratamento de dados pessoais.

Cabe ao controlador identificar cuidadosamente as bases legais que autorizam o tratamento e, havendo mais de uma hipótese, ancorar-se naquela que seja mais segura e específica.

Isso porque, conforme apontado nos Princípios da LGPD, o tratamento de dados deve ser adequado, limitado ao estritamente necessário e restrito à finalidade legitimadora específica.

Além disso, não se pode ignorar que o titular dos dados teve assegurado pela LGPD, em seu art. 9º, o direito à informação, tendo legitimidade de saber qual a causa legitimadora e a finalidade do tratamento dos seus dados pessoais.

No âmbito das relações de trabalho, as hipóteses que legitimarão o tratamento de dados pessoais de modo mais recorrente serão:

- a) cumprimento de obrigação legal ou regulatória;
- b) execução de contrato ou de procedimentos preliminares relacionados ao contrato;
- c) exercício regular de direitos em processo judicial, administrativo ou arbitral.

Os procedimentos preliminares a um potencial contrato legitimam o acesso a informações sobre o candidato, mas recomenda-se muita cautela nos dados que serão exigidos a partir do anúncio de um emprego, atendo-se ao estritamente necessário ao exercício da função.

Assim, como regra, deve-se evitar a formulação de exigências relacionadas ao gênero, estado civil, existência de filhos, pretensão de contrair matrimônio, religião⁴⁶, doenças prévias, patrimônio genético, antecedentes criminais e investigação de vida financeira⁴⁷.

Por incrível que pareça, ainda há formulários que pedem a indicação de contatos de referências, situação absolutamente desnecessária e que não é tolerada pela LGPD.

Em relação à fase contratual, haverá um vasto leque de dados que será necessário para sua execução e para atender a comandos legais, a exemplo de dados

46 Esse dado pode vir a ser justificável em algumas situações, tais como diante de organizações de tendências em relação a funções inseridas na zona de tendência da organização.

47 Esses dois últimos temas serão objeto de análise em tópico específico adiante.

tratados em função da jornada, valor do salário, descontos, faltas, motivos das faltas, doenças, acidentes, situações conjugais e familiares que podem ter reflexos em providências da empresa, como o pagamento de pensão, inclusão de dependente no plano de saúde, entre outros.

Existem alguns dados que constam ordinariamente dos modelos de livros e ficha de registros de empregados, mas que podem ser questionados também sob a ótica de minimização, a exemplo da filiação, cuja necessidade é bem questionável, exceto se os pais forem dependentes do imposto de renda.

No que concerne à qualificação dos filhos, estes dados geralmente serão necessários para fins do salário-família, havendo, portanto, obrigação legal legitimadora para tanto.

No período pós-contratual, existem diversos dados que são necessários para fins da formalização da rescisão contratual, inclusive exame médico demissional.

6.2 A checagem de antecedentes (“Background Checks” e “Pre-employment vetting”)

Os termos “Background Check” e “Pre-employment vetting”⁴⁸ podem ser compreendidos como um processo de verificação dos antecedentes de empregados e/ou candidatos a uma vaga de emprego por meio de funcionários especificamente designados para determinada atribuição, com ou sem o auxílio de terceiros, a fim de verificar se ambos estão em conformidade com a cultura empresarial, agregando valor à atividade empresarial desenvolvida e diminuindo o risco inerente à própria atividade.

O processo inclui a confirmação do histórico de emprego, autenticação de credenciais educacionais, como diplomas, licenças e certificações profissionais, verificação de perfis de mídia social, revisão de relatórios de crédito e pesquisa de antecedentes criminais ou prisão, e geralmente começa depois que o candidato passa pelo processo seletivo de contratação.

Apesar de as políticas de verificação sofrerem variações, o essencial é estabelecer diretrizes claras a fim de se observar as melhores práticas. O processo de triagem para uma empresa deve ser padrão entre os candidatos, o que significa que todo candidato considerado para uma vaga deve passar pela mesma verificação de antecedentes. Assim, mesmo quando os empregadores contratam empresas externas para realizar a respectiva triagem, eles devem ser obrigados a seguir o mesmo protocolo.

A objetividade também é crucial, pois a discriminação racial, de gênero e outros tipos de vieses devem ser eliminados o máximo possível.

6.2.1 Quais são os principais motivos relacionados ao “Background Checks” e “Pre-employment vetting”?

O processo de triagem de dados dos respectivos empregados e candidatos está diretamente relacionado com as questões da segurança (“safety”), conformidade legal (“legal compliance”), responsabilidade (“liability issues”) e ajuste da empresa (“company fit”).

Por isso, o empregador deve criar um ambiente seguro para os seus clientes, empregados e para a própria sociedade, construindo a sua reputação e confiança

48 Cf. <https://searchhrsoftware.techtarget.com/definition/employee-vetting>.

com os respectivos grupos mencionados, pois a confiança é essencial para o desenvolvimento de um empreendimento bem sucedido. Sem embargo, caso o empregador não proceda com cautela e vigilância nas suas escolhas, provavelmente será responsabilizado pelos riscos e consequências advindas do desenvolvimento da sua respectiva atividade.

As verificações de antecedentes de emprego são realizadas rotineiramente quando estivermos diante de imposição legal (“legal compliance”). Do mesmo modo, a responsabilidade também costuma ser um motivo comum pelo qual o empregador realiza uma verificação de antecedentes visto que determinado empregado pode ser fonte de conflitos na empresa, não se adaptando ao ambiente de trabalho seja por dificuldade de trabalhar em equipe e/ou em razão de não respeitar os seus superiores hierárquicos.

6.2.2 Quando é admitido na ordem jurídica brasileira que o empregador exija certidão de antecedentes criminais ou proceda à consulta de restrições de crédito?

A jurisprudência do C. TST⁴⁹ se orienta no sentido de que a consulta a restrições de crédito seria medida conspiratória à Constituição Federal por força da sua proibição de discriminação no âmbito da relação de trabalho (Art. 7º, XXXI), seguindo os parâmetros estabelecidos pela Convenção 111 da OIT.

Pondera-se, ainda, que órgãos de proteção ao crédito, em que pese destinados a uma proteção pública, existem para proteger o crédito e não para inviabilizar o emprego, de modo que sua utilização para fins da relação de emprego desatenderia a finalidade para qual o dado pessoal foi lançado.

Além disso, a recolocação no mercado de trabalho é justamente uma maneira de permitir ao devedor saldar as suas dívidas do trabalhador, de modo que se a ele for negado o trabalho por restrições de crédito, haveria um aprisionamento no estado de débito.

Deve ser ressaltado ainda o teor do artigo 1º, da Lei nº 9.029/95, que prevê a proibição de práticas discriminatórias nas relações de trabalho e artigo 373-A da CLT.

Além da feição discriminatória, com a publicação da lei 12.347/10, foi revogado o art. 508 da CLT, que considerava como justa causa, para efeito de rescisão de contrato de trabalho do empregado bancário, a falta contumaz de pagamento de dívidas legalmente exigíveis, o que revelaria ter sido também uma opção política do país não legitimar esse tipo de invasão, segundo os autores Iuri Pinheiro e Fabrício Lima⁵⁰.

Por outro lado, as buscas de referência e bons antecedentes dos candidatos são uma espécie de discriminação positiva e são importantes para verificar o denominado ajuste da empresa (“company fit”) ou integração do empregado à cultura organizacional conforme foi abordado no tópico anterior.

Por fim, a exigência de certidão de antecedentes criminais já foi objeto de decisão vinculante do Tribunal Superior do Trabalho (TST), em acórdão publicado em

49 Por todos: RR - 209-39.2011.5.05.0027, Relator Ministro: Alexandre de Souza Agra Belmonte, Data de Julgamento: 30/11/2016, 3ª Turma, Data de Publicação: DEJT 02/12/2016.

50 LIMA, Fabrício; PINHEIRO, Iuri. **Manual do compliance trabalhista: teoria e prática**. Salvador: Ed. JusPodivm, 2020.

22/09/2017, no julgamento do Recurso Repetitivo (RR) 243000-58.2013.5.13.0023, com a fixação da tese jurídica prevalecente que a exigência de certidões de antecedentes criminais somente se justifica em casos excepcionais, em virtude da existência de lei, natureza do ofício ou elevado grau de fidúcia.

A própria tese fixada no Tema 01 da Tabela de Recursos Repetitivos elenca atividades em relação às quais é legítima a exigência de certidão de antecedentes criminais:

II) a exigência de Certidão de Antecedentes Criminais de candidato a emprego é legítima e não caracteriza lesão moral quando amparada em expressa previsão legal ou justificar-se em razão da natureza do ofício ou do grau especial de fidúcia exigido, a exemplo de empregados domésticos, cuidadores de menores, idosos ou deficientes (em creches, asilos ou instituições afins), motoristas rodoviários de carga, empregados que laboram no setor da agroindústria no manejo de ferramentas de trabalho perfurocortantes, bancários e afins, trabalhadores que atuam com substâncias tóxicas, entorpecentes e armas, trabalhadores que atuam com informações sigilosas. Vencidos parcialmente os Exmos. Ministros Augusto César de Carvalho, relator, Aloysio Corrêa da Veiga, Walmir Oliveira da Costa e Cláudio Mascarenhas Brandão, que não exemplificavam;

Como ilustração de trabalhadores que lidam com informações sigilosas pode-se citar o caso de operador de telemarketing, que atua diariamente com intenso fluxo de dados, sendo, assim, justificável a exigência à luz da jurisprudência da SBDI-1 do C. TST⁵¹.

6.3 Utilização de dados biométricos de seus empregados

O dado biométrico foi expressamente catalogado pelo inciso II do art. 5º da LGPD como dado pessoal sensível, sendo necessário refletir se sua utilização no âmbito das relações de trabalho seria compatível com a LGPD.

Em primeiro lugar, é preciso salientar que biometria não se restringe apenas à impressão digital, podendo ser extraída a partir da íris, face, voz ou até mesmo deambulação.

Uma forma frequente de utilização de dado biométrico na relação de emprego é para fins de registro de ponto.

O art. 74 da CLT estipula a necessidade de registro de ponto, admitindo que tal se dê por meio manual, mecânico ou eletrônico. A Portaria 1510/2009, do então Ministério do Trabalho, autorizou o registro de ponto biométrico de empregados.

O Princípio que pode suscitar dúvidas sobre a legitimidade de utilização desse tipo de dado é da Necessidade ou Minimização, já que existem outros meios su-

51 E-ED-RR - 182000-05.2013.5.13.0008, Relatora Ministra: Maria Cristina Irigoyen Peduzzi, Data de Julgamento: 24/05/2018, Subseção I Especializada em Dissídios Individuais, Data de Publicação: DEJT 01/06/2018.

postamente menos invasivos e que permitem o controle de ponto (folha manual ou cartão magnético).

Conquanto seja possível, de fato, assinalar a jornada por outros meios diversos da biometria, não há meio tão eficaz quanto este para assegurar a integridade dos horários lançados nos respectivos registros e a autoria.

E a fidedignidade desses registros é essencial e extremamente saudável para ambas as partes, evitando alegações de desvirtuamento da jornada pela existência, por exemplo, de controle paralelo e permitindo a justa e real apuração do saldo de horas.

O tratamento do dado biométrico para fins de jornada estaria, assim, assegurado pelo cumprimento de obrigação legal pelo controlador (art. 11, II, a, da LGPD).

Além disso, o registro biométrico também pode ser utilizado para outras formas de controle de acesso e segurança na empresa, o que também se legitimaria mesmo sem o consentimento do titular pela alínea “g” do mesmo dispositivo para “garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais”.

Mesmos nessas hipóteses excepcionais, é importante que não existam abusos, sendo que os dados deverão ser utilizados com a finalidade estrita para os quais foram colhidos, com a criação de mecanismos para o tratamento e proteção, sob pena de violação aos ditames da Lei Geral de Proteção de Dados.

6.4 O risco do tratamento de dados pessoais na relação de trabalho tendo como base o consentimento

Embora seja possível se cogitar do consentimento como causa legitimadora do tratamento de dados pessoais (art. 7º, I) ou até mesmo de dados pessoais sensíveis (art. 11, II), a sua incidência no âmbito das relações de trabalho é cercada de preocupações.

Isso porque o art. 5º, XII, proclama que o consentimento deve ser entendido como a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”.

A expressão “livre” pressupõe verdadeira opção do titular dos dados, pressuposto que despertará dúvida sobre sua ocorrência no âmbito de uma relação como a trabalhista, marcada pelo desequilíbrio de poder e, em regra, pela dependência econômica.

Não serão raras as alegações de que o empregado não teve legítima escolha, a ele tendo sido imputado o consentimento como fator condicionante de manutenção do vínculo de emprego.

A propósito, o considerando 43 do GDPR prevê expressamente que “a fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto (“imbalance of power”) entre o titular dos dados e o responsável pelo seu tratamento”.

Exatamente em função disso, o GT 29, órgão consultivo europeu independen-

te, considera problemática a questão de os empregadores procederem ao tratamento de dados pessoais dos empregados com base no consentimento, uma vez que é questionável que esse consentimento seja dado espontaneamente.

A discussão se torna mais suave quando tratarmos dos dados do hiperssuficiente, pois, a estes foi destinado o parágrafo único do artigo 444 da CLT, que permite a transação e renúncia de alguns direitos, desde que não violem a Constituição e os artigos 611-A e 611-B da CLT.

Por isso, como medida de “compliance”, para qualquer tipo empregado, visando à gestão e mitigação de riscos, é recomendável evitar a utilização do consentimento como base legal de tratamento de dados no âmbito das relações de trabalho.

Contudo, caso o empregador pretenda obter o consentimento, é necessário observar o art. 8º, caput e § 1º, da LGPD, que estipula que o consentimento deve ser fornecido “por escrito ou por outro meio que demonstre a manifestação de vontade do titular” e que, caso seja fornecido por escrito, deve “constar de cláusula destacada das demais cláusulas contratuais”. Logo, sempre deverá ser expresso o consentimento.

Podemos citar, como exemplo, a necessidade de o empregado consentir expressamente para critérios de avaliação de sua produtividade pela empresa, com rankings e tabelas comparativas com outros empregados.

Algumas empresas têm inserido cláusula específica e destacada nos contratos formais de trabalho, mas, considerando a natureza de contrato de adesão do contrato de trabalho e que é delas o ônus de comprovar a validade do consentimento (art. 8º, § 2º), seria ainda mais prudente a celebração de um documento em separado.

Outro aspecto extremamente relevante é a granularidade do consentimento, que se aplica na hipótese de coleta de diversos documentos com finalidades distintas.

Considerando a proibição de consentimento generalista (art. 8º, § 4º), quando estivermos diante da pretensão de tratamento de diversos dados, deve ser assegurado ao titular dos dados a indicação pontual e específica de quais dados ele deseja consentir e para qual finalidade específica, em detrimento da prática de mercado materializada pelo “all or nothing”.

A granularidade, portanto, é a possibilidade de indicação específica e pontual e é um mecanismo revelador da liberdade do consentimento exigida pelo art. 5º, XII, da LGPD.

A empresa deve observar, também, que a obtenção do consentimento não lhe permite compartilhar dados com outros controladores sem a obtenção de consentimento específico para tanto, a teor do art. 7º, § 5º, da LGPD.

Esse destaque é de extrema importância para o âmbito das relações de trabalho porque muitos dados são compartilhados pelo empregador com planos de saúde, previdência privada e empresas terceirizadas.

Merece realce, ainda, a dispensa de consentimento para o tratamento de dados tornados manifestamente públicos pelo titular (art. 7º, § 4º), o que muitas vezes pode ocorrer através de publicação em redes sociais públicas.

Contudo, é imperioso destacar que a mesma legislação estipula no § 3º do art. 7º que o tratamento de dados pessoais públicos deve atender a finalidade, boa-fé e interesse público e que o § 6º do mesmo dispositivo vaticina que “eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular”.

Ao buscar a obtenção do consentimento, também é importante que a empresa esteja atenta ao fato de que, nos termos do § 5º do art. 8º da LGPD, o empregado pode revogá-lo a qualquer momento, mediante “manifestação e por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação”, o que, mais uma vez, demonstra a fragilidade de justificar o tratamento dos dados apenas sob essa perspectiva.

7. Término do Tratamento de Dados

O término do tratamento de dados tem uma importância digna de destaque porque é preciso compreender até que momento seria possível continuar o tratamento dos dados pessoais para fazer a sua devida gestão.

O tema é disciplinado pelo art. 15 da LGPD nos seguintes termos:

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - fim do período de tratamento;

III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

O art. 16 da LGPD estipula a necessidade de eliminação dos dados pessoais após as causas do art. 15, mas autoriza a sua conservação em quatro hipóteses:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

O inciso I legitima que os dados permaneçam armazenados durante o prazo prescricional das pretensões associadas porque, em eventual judicialização de um

conflito, haverá a necessidade de produção probatória, a qual muitas vezes é retratada de modo documental, sendo assim legítimo que os dados permaneçam em poder do controlador até o fim do prazo prescricional.

Embora uma primeira leitura possa conduzir a uma impressão simplista de sugerir a guarda pelo prazo prescricional trabalhista de dois anos após fim do contrato ou dos cinco últimos anos do ajuizamento de uma ação (art. 7º, XXIX, da CF/88), é recomendável não cair nesse “conto da sereia”.

Isso porque a prescrição trabalhista é permeada de controvérsias, a exemplo de prescrição total ou parcial, e existem hipóteses em que o prazo prescricional está suspenso ou impedido de correr. A título de exemplo, ilustramos três delas:

- a) existência de absolutamente incapazes (hipótese muito comum em caso de falecimento de trabalhador) ou do menor de 18 anos (art. 440 da CLT);
- b) doenças ocupacionais, que podem se manifestar apenas depois de determinado lapso temporal e que têm o início de contagem do prazo prescricional apenas com a sua ciência inequívoca (Súmula 230 do STF e Súmula 278 do STJ);
- c) vínculo de emprego (imprescritível – artigo 11 da CLT).

Por isso, o ideal é não se limitar ao prazo literal de prescrição, sendo possível a guarda mais prolongada ou até mesmo indeterminada em relação a documentos essenciais para se defender de pretensões imprescritíveis.

É pertinente, se viável economicamente, a técnica da anonimização de dados pessoais prevista no inciso IV do art. 16.

8. Negociação Coletiva para o tratamento de dados pessoais

Em um primeiro momento pode soar inusitado cogitar de negociação coletiva para tratamento de dados pessoais, mas uma reflexão mais profunda permite perceber a extrema relevância de enfrentamento do tema.

Em que pese o silêncio da LGPD acerca do assunto, o GDPR, em seu art. 88, prevê expressamente a sua possibilidade de pactuação:

Os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção dos bens do empregador ou do cliente e para efeitos do exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho.

Considerando o art. 8º da CLT, que autoriza a utilização do direito comparado como fonte supletiva, é lícito cogitar da importação de referida autorização, mas com a reflexão de sua compatibilidade e dos limites de tal aplicabilidade no âmbito interno.

É oportuno rememorar que a Lei 13.467/2017 consagrou a denominada prevalência do negociado sobre o legislado, o que pode levar ao debate sobre a validade de negociação coletiva que flexibilize os critérios e requisitos para o tratamento de dados.

Entendemos, contudo, não ser possível flexibilizar as proteções constitucionais, como o direito à privacidade e à intimidade, revestindo-se de natureza de direito fundamental, de modo que a transação seria maculada pela inconstitucionalidade.

Entretanto, não se pode ignorar a existência de um relevante campo de atuação sindical, relacionada a formas e procedimentos de tratamento de dados pessoais para viabilizar os diversos benefícios normativos que são instituídos por normas coletivas ou até mesmo procedimentos para tornar viável a concessão de obrigação legal de forma coletiva. A norma coletiva poderia, com relativa facilidade, prever a adoção de um só encarregado para as empresas do grupo, sepultando a discussão doutrinária a respeito do tema, ou, dispor sobre direitos do operador, por exemplo.

A rigor, diversas normas coletivas estipulam direitos que, para serem exercidos, demandam tratamento de dados pessoais ou até sensíveis, como a concessão de plano de saúde. Caberá à norma indicar os dados que serão necessários, quem os repassará, quando e por quanto tempo ficarão armazenados.

9. Responsabilidade Civil

Os artigos 42 a 45 da Lei 13.709/18 tratam da responsabilidade civil patrimonial e extrapatrimonial dos agentes de tratamento de dados (controlador e operador).

Há forte tendência doutrinária⁵² em se adotar apenas a responsabilidade subjetiva, com culpa presumida e, via de consequência, em afastar o entendimento de responsabilidade civil objetiva⁵³ do empregador, por aplicação do artigo 42 e incisos II e III do artigo 43 da LGPD, que expressamente isenta de responsabilidade aquele que não violou a lei. A exceção se faz às relações de consumo, pois excluídas pelo artigo 45 da Lei 13.709/18.

A tese tem amparo, também, no fato de a reparação de dano decorrente de responsabilidade objetiva estar regulada genericamente no Código Civil, lei de mesma hierarquia que a LGPD. Logo, a lei posterior pode revogar a anterior de mesma hierarquia, ou a especial revogar a geral, como é o caso.

Entretanto, mesmo antes do Código Civil (parágrafo único do art. 927) a jurisprudência já vinha alargando o conceito de “culpa”, cujo requisito é necessário

52 Disponível em : <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais-culpa-ou-risco>. Acesso em: 30 set. 2020.

53 Aparentemente o artigo 223-A da CLT também afastou a responsabilidade objetiva decorrente de dano extrapatrimonial. A expressão “apenas” contida no *caput* do art. 223-A da CLT deixa clara a intenção do legislador da não aplicação de outras normas de mesma hierarquia acerca do dano extrapatrimonial trabalhista.

para o dever de indenizar. A culpa presumida nasce da premissa do dever de que todos temos de não prejudicar ninguém e praticar atos com segurança. Ainda que não se confunda com a culpa presumida, a atividade de risco é mero desdobramento dessa tese, pois a pessoa que explora economicamente a atividade de risco deve ser responsabilizada pelos prejuízos materiais e morais daí decorrentes.

Por isso e considerando que a LGPD (lei especial) não trouxe a culpa como elemento necessário para configuração de responsabilidade, defendemos que, em tese, é possível a aplicação da responsabilidade objetiva.

10. Conclusão

A Lei Geral de Proteção de Dados dispõe sobre os critérios, limites e penalidades para o tratamento de dados da pessoa natural. Não há proibição ao tratamento de dados, ao contrário, a Lei 13.709/18 deu ao titular dos dados o empoderamento destes e o direito de autodeterminação informativa, regulamentou o legítimo exercício e previu punições administrativas para os casos de ilicitude.

REFERÊNCIAS

CANOTILHO, JJ Gomes. *Direito Constitucional e Teoria da Constituição*. Coimbra: Almedina, 2003.

LIMA, Fabrício; PINHEIRO, Iuri. *Manual do compliance trabalhista: teoria e prática*. Salvador: Ed. JusPodivm, 2020.

MOREIRA, Teresa Coelho. *A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: Contributo para um estudo dos limites do poder de controlo electrónico do empregador*. Coimbra: Almedina, 2010.

SCHWAB, Klaus. *A quarta revolução industrial*. São Paulo: Edipro, 2016.

3. RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS DOS TRABALHADORES: DILEMAS EM TORNO DA ANÁLISE DE RISCO

DATA PROTECTION IMPACT ASSESSMENT OF EMPLOYEES' PERSONAL DATA: DILEMMAS AROUND RISK ANALYSIS

CLAUDIA LIMA MARQUES⁵⁴ E CÍNTIA ROSA PEREIRA DE LIMA⁵⁵

Resumo

A proteção de dados pessoais parte do pressuposto da vulnerabilidade dos titulares de dados, pois estão sujeitos ao controle das atividades de tratamento de dados realizadas pelos controladores e operadores. Neste sentido, fica evidente a forte aproximação deste tema com o Direito do Trabalho, que também se estrutura a partir da vulnerabilidade dos empregados face aos empregadores. Um dos pontos de intenso debate sobre a LGPD é o relatório de impacto à proteção de dados (RIPD), pois ainda não está claro seu caráter obrigatório para todas as situações ou não, além da falta de uniformidade quanto à metodologia para análise de risco. Este artigo enfrenta o tema, evidenciando a elaboração deste documento pelo empregador diante do tratamento de dados pessoais de seus funcionários.

Palavras-Chave: Lei Geral de Proteção de Dados. Princípio da Segurança. Princípio da Prevenção. Doutrina do Diálogo das Fontes.

Abstract

The protection of personal data is based on the assumption of data subjects' vulnerability, as they are subject to the control of data processing activities carried out by controllers and operators. In this sense, one can notice the approximation of this issue with Labor Law, which is also structured on the vulnerability of employees towards employers. One of the points of intense debate about the LGPD is the data protection impact assessment (DPIA), as it is not yet clear whether it is mandatory for all situations or not, in addition to the lack of uniformity regarding the methodology for risk analysis. This article addresses these issues, highlighting the preparation of this document by the employer in view of the processing of personal data of its employees.

Keywords: Data Protection General Law. Security Principle. Prevention Principle. Laws Dialogue Doctrine.

54 Professora Titular e Diretora da Faculdade de Direito da Universidade Federal do Rio Grande do Sul. Doutora iuris utriusque (Heidelberg), L.L.M. (Tübingen). Ex-Presidente do Instituto Brasileiro de Política e Direito do Consumidor – Brasilcon. Presidente do Comitê de Proteção Internacional dos Consumidores da International Law Association ILA (Londres) e Diretora do Centro de Estudos Europeus e Alemães – CDEA (UFRGS-PUCRS-DAAD). cmarques.ufrgs@gmail.com

55 Professora Associada de Direito Civil da Faculdade de Direito da USP Ribeirão Preto – FDRP. Doutora em Direito Civil pela USP. Livre-docente em Direito Civil pela USP. Pós-doutorado em Direito Civil pela *Università degli Studi di Camerino* (Itália) e *Fordham Law School* (Nova York). Presidente do Instituto Avançado de Proteção de Dados – IAPD. cintiar@usp.br

1. Introdução

No atual contexto da sociedade informacional, é cediço que o poder econômico se mede pela capacidade de coletar e armazenar informações que identificam ou possam identificar pessoas, que são utilizadas de maneira muito criativa com evidente geração de lucros. Assim, as *big players* da economia informacional são as corporações que detêm um volume imensurável de dados pessoais, como *Google*, *Facebook*, *WhatsApp*, *YouTUBE*, *Amazon*, dentre outras cuja movimentação está fundada nos dados pessoais como verdadeiras *commodities*.⁵⁶

Neste contexto, fica evidente a importância de uma Lei Geral de Proteção de Dados Pessoais para equacionar e equilibrar os interesses em jogo: de um lado, a busca de lucro pelos agentes de tratamento de dados pessoais; de outro, a proteção à autodeterminação informativa.

Inicialmente, a proteção de dados pessoais era vista como um desdobramento do direito à privacidade. No entanto, Stefano Rodotà⁵⁷ caracteriza a evolução cultural e jurídica do termo “privacidade”, sistematizando tal evolução em quatro aspectos que destacam a privacidade, e hoje a proteção de dados, como um “elemento constitutivo da cidadania”, quais sejam:

- 1) do direito de ser deixado só ao direito de manter o controle sobre suas próprias informações;
- 2) da privacidade ao direito à autodeterminação informativa;
- 3) da privacidade a não discriminação;
- 4) do segredo ao controle.

Em síntese, Stefano Rodotà⁵⁸ afirma que a privacidade, na sociedade informacional, não pode ser mais apenas entendida como o “direito de ser deixado só”; em verdade, a tutela dos dados pessoais garante ao titular conhecer, controlar, identificar e interromper o fluxo de informações que lhe digam respeito.

Em outro texto, Stefano Rodotà⁵⁹ destaca uma diferença importante: o direito à privacidade possui tutela estática e negativa, enquanto a tutela dos dados pessoais, estruturada a partir de regras sobre o tratamento de dados, poderes de intervenção, dentre outras, possui uma tutela dinâmica, ou seja, surge com a coleta dos dados e permanece com eles durante a circulação e armazenamento.

56 PARISER, Eli. **The filter bubble**: how the new personalized web is changing what we read and how we think. Nova York: Penguin Book, 2011. pp. 45 – 46: “What all of this means is that your behavior is now a commodity, a tiny piece of a market that provides a platform for the personalization of the whole Internet. We’re used to thinking of the Web as a series of one-to-one relationships: You manage your relationship with Yahoo separately from your relationship with your favorite blog. But behind the scenes, the Web is becoming increasingly integrated. Businesses are realizing that it’s profitable to share data. Thanks to Acxiom and the data market, sites can put the most relevant products up front and whisper to each other behind your back.” (grifo nosso)

57w Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali. **Rivista Critica del Diritto Privato**, anno XV, n. 1, março 1997, pp. 583 – 609. pp. 588 – 591.

58 Privacy..., *op. cit.*, p. 521.

59 Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla *privacy*. **Europa e Diritto Privato**, fasc. 01, pp. 01 – 11, Milão: Giuffrè, 2004. p. 03. No mesmo sentido: FINOCCHIARO, Giusella. **Privacy e protezione dei dati personali**: disciplina e strumenti operativi. Bologna: Zanichelli, 2012. pp. 04 – 05.

Sobre tal distinção, Giusella Finocchiaro⁶⁰ destaca que determinado dado pessoal, ainda que não seja privado, é objeto de tutela pela legislação sobre proteção de dados pessoais. Portanto, conclui que a definição de dado pessoal não faz referência direta nem indireta à privacidade. Em suma, o objeto do direito à privacidade é diverso do objeto do direito à proteção dos dados pessoais. O primeiro é assegurar o resguardo de parcela de sua vida privada; o segundo, por sua vez, é proteger os titulares de dados viabilizando o acesso e controle de suas informações (ainda que de conhecimento público) e impedindo que sejam objeto de tratamento em desacordo com as regras e códigos de condutas. Portanto, é imperiosa a análise do direito à proteção de dados pessoais como um direito autônomo.⁶¹

Além de ser um direito autônomo, a proteção de dados pessoais é um direito fundamental,⁶² merecendo toda atenção do legislador infraconstitucional e dos aplicadores do Direito. A fim de manter sempre atual a LGPD, sua base é essencialmente principiológica, trazendo em seu bojo, além da boa-fé⁶³, dez princípios balizadores das atividades de tratamento de dados pessoais. São eles: da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção, da não discriminação e da responsabilização e prestação de contas (art. 6º da LGPD).

Sob a ótica principiológica, é necessária a análise da implementação de mecanismos focados na identificação e mitigação dos riscos decorrentes da manipulação de dados pessoais, especialmente numa sociedade de extrema vigilância líquida exercida por meio tecnológico contra todos, buscando-se, desta forma, evitar severos danos aos titulares de dados.⁶⁴ Destaca-se, assim, a tríade de princípios trazidos na LGPD: da segurança, da prevenção e da prestação de contas.

Insculpido no art. 6º, inciso VI da LGPD, o princípio da segurança é entendido como a “utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão”. Sem dúvida, a violação de dados pessoais põe em xeque os direitos dos titulares de dados, desta maneira, os agentes de tratamento de dados possuem o ônus de estabelecer medidas eficazes para compelir os acessos não autorizados às informações pessoais dos titulares dos dados e, consequentemente, a ocorrência de eventuais danos⁶⁵.

60 *op. cit.*, p. 36 – 37: “Da qui l’ulteriore riprova che il diritto alla riservatezza e il diritto alla protezione dei dati personali non coincidono, con riferimento ai beni oggetto dei diritti. Nel primo caso, l’oggetto della tutela è costituito dalle vicende riservate, intese come vicende intime o familiari; nel secondo caso, l’oggetto della tutela è invece costituito dai dati e dalle informazioni, anche se privi di contenuto riservato”.

61 Cf. LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a Efetividade da Lei Geral de proteção de Dados**. São Paulo: Editora Almedina, 2020. p. 90.

62 A Proposta de Emenda à Constituição (PEC) nº 17/2019 pretende inserir o inciso XII-A ao art. 5º, e o inciso XXX ao art. 22 da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria.

63 Cf. MARQUES, Claudia Lima. **Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais**. 9. ed. rev. e atual. São Paulo: Revista dos Tribunais, 2019. p. 905.

64 ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**. Nova York: Public Affairs, 2019.

65 LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a Efetividade da Lei**

O princípio da prevenção está intimamente relacionado a este e vem descrito na LGPD (inciso VIII do art. 6º) como a “*adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais*”.

Enquanto o princípio da responsabilização e prestação de contas (inciso X, art. 6º da LGPD), também chamado de *accountability*, é a: “demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas”. A LGPD prevê, portanto, que os agentes de tratamento de dados devem observar e cumprir todas as exigências legais, mas que também devem comprovar a eficácia dessas medidas. Em outras palavras, deve ser adotado um modelo de governança capaz de assegurar o cumprimento de tais obrigações e, ao mesmo tempo, a organização e manutenção de documentos que comprovem que tais obrigações estão sendo satisfeitas.

Miriam Wimmer⁶⁶ realça que os princípios previstos na LGPD não são criações inéditas do legislador brasileiro, pois eles são inspirados em princípios já consolidados em documentos internacionais e leis de proteção de dados de outros países.

Pode-se acrescentar que estes princípios, como visto, não são criações da LGPD, pois estão insculpidos em outras leis como leis trabalhistas e o Código de Defesa do Consumidor, dentre outras, fortalecendo ainda mais a doutrina do “Diálogo das Fontes”.⁶⁷

Neste sentido, deve-se realizar o mesmo diálogo entre a LGPD e o Direito do Trabalho no que diz respeito à caracterização do Relatório de Impacto à Proteção de Dados Pessoais, hipóteses em que tal análise seja obrigatória e a metodologia empregada.

2. Do Relatório de Impacto à Proteção de Dados Pessoais e sua aplicação nas relações trabalhistas

Muito se tem falado sobre o denominado “Relatório de Impacto à Proteção de Dados”, conhecido pela sigla RIPD. Mas em que consiste este documento, quais são as hipóteses nas quais tal documento é obrigatório, qual metodologia deve ser empregada e sua importância como uma ferramenta de mitigação de riscos e prevenção nas relações trabalhistas?

Na verdade, a Lei Geral de Proteção de Dados (Lei n. 13.709/2018) fala muito pouco sobre esse documento. Este documento é mencionado dentre os conceitos elencados no art. 5º da LGPD inc. XVII, no art. 10, § 3º (quando a base legal para o tratamento de dados for o legítimo interesse) e no art. 38 (com ênfase aos dados pessoais sensíveis).

Geral de proteção de Dados. São Paulo: Editora Almedina, 2020. p. 204-206.

66 Capítulo 4 – A LGPD e o balé dos princípios: tensões e convergências na aplicação dos princípios de proteção de dados pessoais ao setor público. *In*: FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antonio. **A Lei Geral de Proteção de Dados Pessoais: Aspectos Práticos e Teóricos Relevantes no Setor Público e Privado.** São Paulo: Revista dos Tribunais, 2021. pp.163 – 186. p. 166.

67 MARQUES, Claudia Lima. Superação das antinomias pelo diálogo das fontes: o modelo brasileiro de coexistência entre o Código de Defesa do Consumidor e o Código Civil de 2002. **Revista de Direito do Consumidor**, vol. 51, pp. 34-67, jul. – set., 2004; MARQUES, Claudia Lima (orgs.) **Diálogo das fontes. Do conflito à coordenação das normas do direito brasileiro.** São Paulo: Revista dos Tribunais, 2012.

Portanto, caberá à ANPD regulamentar esse tema nos termos do art. 55-J, inc. XIII da LGPD: “editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei”.

Algumas leis específicas podem exigir tal documento, por exemplo, a Medida Provisória n. 954/2020, que autorizava o compartilhamento de informações dos consumidores pelas empresas de telefonia móvel e fixa com o IBGE, cuja eficácia ficou suspensa após o julgamento das Ações Diretas de Inconstitucionalidade (ADI n. 6387, n. 6388, n. 6389, n. 6390 e n. 6393) pelo Supremo Tribunal Federal.⁶⁸

O art. 3º, § 2º da MP 954/2020 exigia o Relatório de Impacto à Proteção de Dados Pessoais nos termos da LGPD, mesmo antes da entrada em vigor da lei, *in verbis*: “A Fundação IBGE informará, em seu sítio eletrônico, as situações em que os dados referidos no *caput* do art. 2º foram utilizados e divulgará relatório de impacto à proteção de dados pessoais, nos termos do disposto na Lei nº 13.709, de 14 de agosto de 2018.”⁶⁹ Esta seria uma hipótese na qual tal documento deve ser obrigatório, pois se trata de tratamento de dados em massa; no entanto, com razão, tal Medida Provisória teve sua eficácia suspensa pelo julgamento das ADIs acima mencionadas.

2.1 Conceito e conteúdo do Relatório de Impacto à Proteção de Dados Pessoais

O inc. XVII do art. 5º da LGPD traz um conceito do que vem a ser o Relatório de Impacto à Proteção de Dados Pessoais, a saber: “documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco”.

Pode-se afirmar, portanto, que neste documento deve-se conter, minimamente: a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados (conforme o disposto no parágrafo único do art. 38 da LGPD).

O objetivo desse documento é realizar uma avaliação dos riscos às liberdades civis e aos direitos fundamentais envolvidos no tratamento de dados pessoais como consta da definição do inc. XVII do art. 5º da LGPD. No entanto, a proteção de dados pessoais é um direito fundamental, restando a pergunta se tal documento será sempre obrigatório para as atividades de tratamento de dados.

Neste documento, há a descrição do tratamento de dados, bem como a avaliação de sua necessidade e proporcionalidade aos riscos envolvidos com tal atividade. O ideal é realizar essa avaliação antes do tratamento de dados pessoais. Esse documento é um processo contínuo, pois deve ser revisitado constantemente a fim de se verificar se as medidas de segurança apontadas para mitigar os riscos continuam eficazes tendo em vista a evolução tecnológica.

68 Disponível em: https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&pesquisa_inteiro_teor=false&sinonimo=true&plural=true&radicais=false&buscaExata=true&page=1&pageSize=10&queryString=ADI%206387&sort=_score&sortBy=desc

69 Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm

2.2 Hipóteses nas quais o Relatório de Impacto à Proteção de Dados Pessoais é obrigatório

O art. 35 do GDPR traz regras específicas para o denominado “*Data Protection Impact Assessment (DPIA)*”, a saber:

1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação.

O WP 29 elaborou um parecer n. 248⁷⁰ sobre o tema, oferecendo diretrizes sobre este documento, além de uma relação das hipóteses nas quais este documento é obrigatório.

São nove as circunstâncias nas quais o DPIA será obrigatório:

- 1) Avaliação de crédito (*Credit Scoring*)
- 2) Criação de perfis a partir de decisões automatizadas
- 3) Monitoramento sistemático (ex. câmeras de segurança)
- 4) Tratamento de dados pessoais sensíveis
- 5) Tratamento de dados pessoais em massa
- 6) Combinação de duas ou mais operações de tratamento de dados
- 7) Tratamento de dados pessoais de vulneráveis
- 8) Tratamento de dados com aplicação de tecnologias novas
- 9) Tratamento de dados que impeça o exercício de um ou mais direitos assegurados aos titulares de dados

Na Europa, discute-se se basta constatar uma destas circunstâncias para a obrigatoriedade do DPIA, ou se basta constatar mais de uma delas. O ideal seria determinar a obrigatoriedade se coexistirem duas ou mais destas circunstâncias.

No Brasil, ainda não se tem uma definição de circunstâncias nas quais esse relatório de impacto seja obrigatório; caberá à ANPD tal definição em resolução específica sobre RIPD consoante inc. XIII do art. 55-J da LGPD.

Consoante o que dispõe a LGPD, em se tratando de tratamento de dados com base no legítimo interesse (§ 3º do art. 10 da LGPD) ou se tratando de tratamento de dados pessoais sensíveis (art. 38 LGPD), este documento é obrigatório. Nas outras situações, o Relatório de Impacto à Proteção de Dados será facultativo. Muitas implementações da LGPD estão elaborando o RIPD sempre, fundamentando no princípio da responsabilidade e prestação de contas (*accountability*). No entanto, entendemos que este documento deve ser elaborado com parcimônia, pois se deve

70 Disponível em: <https://ec.europa.eu/newsroom/article29/items/611236>

adotar a metodologia adequada, bem como as medidas de salvaguardas eficientes, caso contrário, o agente de tratamento de dados poderá produzir prova contra si mesmo, documentando algo que não existe ou impraticável.

2.3 Metodologia de análise de riscos

Quanto à metodologia, existem várias metodologias para fazer essa avaliação. A ISO 29.134 tem diretrizes para aplicar tal metodologia. Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento. Como exemplo, os parâmetros escalares podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança.

A *Commission Nationale de l'Informatique et des Libertés (CNIL)* fornece gratuitamente uma ferramenta para efetuar de forma guiada um DPIA, mas com base no GDPR⁷¹. No Brasil, em novembro de 2020, o Ministério da Economia liderou um estudo sobre o tema, resultando no Guia de Avaliação de Riscos de Segurança e Privacidade⁷², neste documento, são oferecidos alguns modelos de matriz de risco:

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

Tabela 8. Matriz de Probabilidade X Impacto (CCGD, 2020).

Probabilidade (P)	15	75	150	225
	10	50	100	150
	5	25	50	75
		5	10	15
		Impacto (I)		

Tabela 9. Legenda de cores (CCGD, 2020).

Legenda (Cor)	Classificação do nível de risco
Verde	Baixo
Amarelo	Moderado
Vermelho	Alto

71 Disponível em: <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment>

72 Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-avaliacao-de-riscos-de-seguranca-e-privacidade.pdf>

tanto, o ideal seria padronizar tal metodologia para resguardar maior segurança tanto aos agentes de tratamento de dados quanto aos titulares de dados pessoais.

3. Aspectos específicos do Relatório de Impacto à Proteção de Dados Pessoais nas relações trabalhistas

Os empregadores detêm uma série de informações sobre os trabalhadores, inclusive dados pessoais sensíveis, tais como aqueles relacionados à saúde, por exemplo, ao tratar dados relacionados a atestados de afastamento por motivo de saúde, dentre outros.

Além disso, levando-se em consideração o tamanho do empregador associando-se ao número dos empregados, o tratamento de dados pode ser considerado como tratamento de massa.

Outro ponto a ser destacado é o tratamento de dados pessoais com base no interesse legítimo, uma cláusula geral que alarga o rol previsto no art. 7º da LGPD, ou seja, as hipóteses legais nas quais está autorizado o tratamento de dados pessoais. Tema que também será regulado pela ANPD.

Destá forma, entendemos que nestas três situações acima descritas o Relatório de Impacto à Proteção de Dados passa a ser obrigatório. No entanto, deve ser elaborado de maneira técnica a fim de se evidenciar uma análise adequada sobre o nível de risco envolvido no tratamento de dados pessoais nestas circunstâncias. Não se trata de “achismo”, e sim, uma metodologia que requer domínio da arte, caso contrário, ao invés de mitigar os riscos envolvendo o tratamento de dados, pode acentuar estes riscos. Vejamos: se a análise é feita de maneira superficial a ponto de se concluir que o risco é baixo, o agente de tratamento de dados não tomará as medidas de segurança técnicas e organizacionais adequadas, favorecendo as condições para os incidentes de segurança com dados pessoais; por outro lado, se for atribuído um risco elevado de maneira leviana, há uma assunção de culpa por parte do agente de tratamento de dados que cria um risco elevado, acentuando-se as consequências da responsabilidade civil.

4. Considerações finais

A aproximação axiológica entre LGPD e o Direito do Trabalho é evidente, justificando o diálogo das fontes de maneira a manter a coesão de todo o sistema. Portanto, os princípios do Direito do Trabalho, notadamente o princípio da proteção, e os princípios elencados no art. 6º da LGPD, revelam a necessidade de aplicação coerente das normas trabalhistas e da LGPD.

Alguns exemplos explicitam esta aproximação, como o princípio da *accountability* e a possibilidade da inversão do ônus da prova prevista expressamente no § 2º do art. 42 da LGPD.

Tendo em vista o tratamento de dados pessoais relacionados aos trabalhadores, tais como os relacionados à saúde, à convicção político partidária, orientação sexual etc., ou seja, dados pessoais sensíveis (art. 5º, inc. II da LGPD), impõe um olhar cuidadoso do empregador ao monitorar os possíveis riscos para que sejam

implementadas medidas de segurança técnicas e organizacionais de modo a reduzir possíveis danos decorrentes do tratamento de dados.

Os agentes de tratamento de dados não podem realizar as atividades de tratamento de dados quando sabem ou deveriam saber do seu alto grau de periculosidade à proteção dos titulares de dados pessoais, a menos que tais riscos sejam identificados, mapeados e mitigados por medidas de segurança técnicas e organizacionais. Esta regra pode ensejar o princípio da precaução, cujo instrumento deve ser o Relatório de Impacto à Proteção de Dados Pessoais, considerado pela lei como “documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco” (inc. XVII do art. 5º da LGPD).

Diante disto, este tema deverá ser cuidadosamente regulado pela Autoridade Nacional de Proteção de Dados, atentando-se para as hipóteses nas quais tal procedimento será obrigatório para trazer clareza e segurança jurídica tanto aos agentes de tratamento de dados quanto para os titulares de dados pessoais.

REFERÊNCIAS

FINOCCHIARO, Giusella. **Privacy e protezione dei dati personali**: disciplina e strumenti operativi. Bologna: Zanichelli, 2012.

LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a Efetividade da Lei Geral de proteção de Dados**. São Paulo: Editora Almedina, 2020.

MARQUES, Claudia Lima (orgs.) **Diálogo das fontes. Do conflito à coordenação das normas do direito brasileiro**. São Paulo: Revista dos Tribunais, 2012.

_____. **Contratos no Código de Defesa do Consumidor**: o novo regime das relações contratuais. 9. ed. rev. e atual. São Paulo: Revista dos Tribunais, 2019.

_____. Superação das antinomias pelo diálogo das fontes: o modelo brasileiro de coexistência entre o Código de Defesa do Consumidor e o Código Civil de 2002. **Revista de Direito do Consumidor**, vol. 51, pp. 34-67, jul. – set., 2004.

PARISER, Eli. **The filter bubble**: how the new personalized web is changing what we read and how we think. Nova York: Penguin Book, 2011.

RODOTÀ, Stefano. Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali. **Rivista Critica del Diritto Privato**, anno XV, n. 1, março 1997, pp. 583 – 609.

_____. Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla *privacy*. **Europa e Diritto Privato**, fasc. 01, pp. 01 – 11, Milão: Giuffrè, 2004.

WIMMER, Miriam. Capítulo 4 – A LGPD e o balé dos princípios: tensões e convergências na aplicação dos princípios de proteção de dados pessoais ao setor público. *In*: FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Anto-

nio. **A Lei Geral de Proteção de Dados Pessoais: Aspectos Práticos e Teóricos Relevantes no Setor Público e Privado.** São Paulo: Revista dos Tribunais, 2021. pp.163 – 186.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism.** Nova York: Public Affairs, 2019.

4. RUMO AO DIREITO FUNDAMENTAL DE PROTEÇÃO DE DADOS PESSOAIS: ALGUMAS APROXIMAÇÕES NA SEARA TRABALHISTA⁷³

EDUARDO K. ZAFFARI⁷⁴ E TÊMIS LIMBERGER⁷⁵

1. Introdução

A Lei Geral de Proteção de Dados Brasileira- LGPD (Lei nº 13.709, de 14/08/2018) foi aprovada após a revelação de que dados de 87 milhões de usuários⁷⁶ foram repassados à firma britânica *Cambridge Analytica*, que trabalhou na campanha de Donald Trump, eleito presidente dos EUA, em 2016. Deste modo, teve-se a confirmação da prática de violação de dados pessoais. Assim, o presidente executivo do *Facebook*, Mark Zuckerberg, prestou declarações no Congresso Norte Americano e no Parlamento Europeu⁷⁷.

Há muito tempo já se sabia que os dados dos usuários da Internet eram utilizados para se fazer um perfil de consumo, e se suspeitava que pudessem ter uso para manipulação política⁷⁸. Assim, além da oferta comercial direcionada que ocorre devido à formação do perfil do usuário consumidor, tem-se, também: a coleta da informação para utilização nas campanhas eleitorais, monitoramento das declarações dos candidatos com relação ao impacto que causam no eleitorado, favorável ou não; e robôs localizados, por vezes, longinquamente, que automaticamente conferem um universo de seguidores ao candidato, impactando positivamente o sítio eletrônico do elegível, que, ainda que falsamente, passa a ter muitos seguidores.

No contexto atual da Internet, verifica-se a exposição constante e exacerbada das pessoas nas redes sociais. É a denominada sociedade do espetáculo⁷⁹. As informações e os fatos da vida são noticiados e ilustrados com fotos no *Facebook*. Pode-se fazer uma paródia do velho brocardo latino: “quem não está no *face*, não está no mundo”.

Há certeza de que hoje existe o denominado “homem de cristal”, na Internet, no sentido de que há uma ampla visibilidade a respeito das informações e dados que a pessoa disponibiliza e interesses que possui, a partir da consulta e visita aos sítios eletrônicos que faz na Internet, dados que ficam armazenados e contribuem para a formação de um perfil, que na maioria das vezes é repassado a outras empresas, sem o consentimento do usuário.

⁷³ Este artigo foi finalizado em 25 outubro de 2021.

⁷⁴ Mestre em Direito pela Universidade do Vale do Rio dos Sinos – UNISINOS. Especialista em Direito do Trabalho pelo Cetra. Especialista em Direito Tributário pelo Instituto Brasileiro de Estudos Tributários - IBET. Professor de Direito da Universidade Luterana do Brasil – ULBRA. Advogado.

⁷⁵ Doutora em Direito Público pela Universidade Pompeu Fabra - UPF de Barcelona. Pós-doutora em Direito pela Universidade de Sevilha. Professora do Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos – UNISINOS. Advogada, Procuradora de Justiça do MP/RS (aposentada).

⁷⁶ Com a estimativa de que 43 mil brasileiros tenham sido incluídos.

⁷⁷ ZUCKERBERG contra a parede. Revista ISTOÉ, São Paulo, p. 66, 18 abr. 2018.

⁷⁸ CASTELLS, Manuel. *Ruptura: a crise da democracia liberal*. Rio de Janeiro: Zahar, 2018.

⁷⁹ DEBORD, Guy. *A sociedade do espetáculo*. Rio de Janeiro: Contraponto, 1997.

Recentemente, foi aprovada a PEC nº 17/2019⁸⁰, que erigiu a proteção de dados a um novo direito fundamental no ordenamento jurídico brasileiro, criando o art.5º, XII- A, da CF, em consonância com o que a proteção constitucional do artigo 8º da Carta de Direitos da União Europeia. E, ainda, estabelecendo a competência privativa da União para legislar sobre a matéria, art. 22, XXX, da CF.

Assim, o objeto deste estudo é averiguar: qual a proteção jurídica que pode ser oferecida ao usuário, em geral, e ao trabalhador, especificamente, no ordenamento jurídico brasileiro e europeu (Regulamento Geral de Proteção de Dados Europeu-RGPD – EU 2016/679) e da LGPD? Neste contexto, o artigo vai se ocupar de verificar aspectos desse novo fenômeno de exposição constante das pessoas nas redes sociais, buscando instrumentos jurídicos e ferramentas que possam ser utilizados para verificar quais informações estão sendo armazenadas a respeito do usuário e do trabalhador, garantindo que, sem o consentimento do cidadão, estas informações não possam ser utilizadas para um fim diverso ao que forem coletadas.

2. Do contexto normativo de proteção de dados na Europa e no Brasil: na perspectiva laboral

2.1 O Regulamento Geral de Proteção de Dados – RGPD

O novo Regulamento Geral de Proteção de Dados – RGPD/UE 2016/679 entrou em vigor a partir de 25/5/2018, após dois anos de promulgação, em 4/5/2016. O objetivo do RGPD é duplo: regular um direito (à proteção de dados) e garantir a liberdade (a livre circulação dos dados), à semelhança do que já ocorria com a Diretiva Comunitária nº 46/95.

Assim, a proteção do direito fundamental prevalece sobre o interesse econômico dos responsáveis e encarregados do processamento de dados, como foi reconhecido pelo Tribunal de Justiça, na sentença proferida em 13/05/2014⁸¹, segundo o Google Espanhol e Agência Espanhola de Proteção de Dados.

O RGPD e o direito fundamental à proteção de dados (art. 8º da Carta Europeia de Direitos Humanos) têm como âmbito material de aplicação: aqueles que têm um arquivo automatizado contendo dados pessoais.

No tocante ao aspecto territorial, o RGPD é aplicável no âmbito da União Europeia e de outros países, ainda que não comunitários, desde que, a partir de relação jurídica ou comercial, afetem os dados de cidadãos ou empresa estabelecida na UE. Assim, o princípio da segurança jurídica tem sua incidência para além do território europeu, considerando que os dados circulam livremente, independentemente das fronteiras de um país.

Outro aspecto importante é do consentimento do interessado (art. 4.11 do RGPD), como sendo toda manifestação de vontade livre, específica, informada e inequívoca pela qual o interessado aceita, seja mediante uma declaração ou uma clara ação afirmativa, o tratamento de dados pessoais que lhe são relacionados.

Assim, a novidade é que se especificam duas formas de expressar o consentimento: mediante declaração ou mediante uma clara ação afirmativa. Deste modo,

80 Disponível em: <https://www1.folha.uol.com.br/mercado/2021/10/senado-aprova-pec-que-inclui-protacao-de-dados-como-direito-fundamental.shtml>? Acesso em: 20 out. 2021.

81 Acórdão do Tribunal de Justiça Europeu (Grande Secção), em 13/05/2014.

não cabe mais o denominado consentimento tácito (o silêncio, as alternativas já marcadas ou a inação).

Logo, fica claro que o silêncio ou a inação não podem considerar-se como uma declaração de consentimento, pois este tem que ser um ato afirmativo claro e para finalidades específicas.

O Princípio da Finalidade já se fazia presente desde o Convênio 108/1981 e foi incorporado pela DC nº 46/1995, mantendo-se no atual RGPD, no sentido de que os dados coletados para uma finalidade específica não podem ser utilizados para outra.

Comentando o então projeto do atual RGPD, Sanchez Bravo⁸² já propugnava que toda a informação dirigida ao público, em virtude do Princípio da Transparência, deve ser de fácil acessibilidade e compreensão, utilizando-se de uma linguagem simples e clara.

O Regulamento foi pensado para a publicidade na Internet e outras situações tecnológicas complexas. Por isso, faz-se necessário que o interessado possa saber e compreender se seus dados estão sendo recolhidos por quem e para que (finalidade). Especial atenção deve-se conferir aos menores, que são os efetivamente cuidados em sua vida privada.

O RGPD traz novidades, algumas aplicáveis especificamente ao que aqui se debate: princípio de *accountability* ou responsabilidade pró-ativa-transparência, em caso de que haja dano ou prejuízo material ou imaterial: o valor pode chegar a € 20.000.000 de euros, ou, tratando-se de empresas, até 4% da receita global, o que for mais elevado⁸³.

O RGPD pretende fazer mais simples a proteção dos dados, reduzindo os encargos administrativos às empresas, ao mesmo tempo em que implementa a *accountability*⁸⁴. Assim, o RGPD supõe uma simplificação normativa e a supressão ou flexibilização de algumas exigências das leis nacionais que os mercados consideravam burocráticas. Por outro lado, o RGPD introduz novas garantias para a proteção das pessoas físicas no tocante ao tratamento de seus dados pessoais, que provêm em grande medida da cultura jurídica anglo-saxã e do âmbito da autorregulação.

É estabelecido um novo princípio, o da “responsabilidade proativa” – artigo 5.2, e no artigo 24 trata da responsabilidade do encarregado do tratamento de dados, para que seja capaz de demonstrar que o tratamento está em conformidade com o RGPD.

82 SÁNCHEZ BRAVO, Álvaro A. **Hacia un nuevo marco europeo de protección de datos personales: empoderamiento de los ciudadanos en la sociedad tecnológica**. In: FERNANDEZ, Yarina Amoroso (Org.). **Sociocibernética e Infoética**: contribución a una nueva cultura y praxis jurídica. Habana - Cuba: Editorial UNIJURIS, 2015, v. 1, p. 124. “Toda información dirigida al público, en virtud del principio de transparencia, debe ser fácilmente accesible y fácil de entender, utilizándose un lenguaje sencillo y claro. Especialmente pensado para la publicidad en línea, y otros entornos tecnológicos complejos, se hace necesario para que el interesado pueda saber y comprender si sus datos están siendo recogidos, por quién, para hacer qué. Especialmente, deberá prestarse atención a los menores, para que ese lenguaje sencillo y claro, sea comprensible con facilidad.” Tradução livre da autora.

83 No caso da violação de dados ocorrida no Facebook, caso considerado que o RGPD já seria aplicável, a multa chegaria a R\$ 6 bilhões.

84 REIGADA, Antonio Trancoso. In: PIÑAR MANÁS, José Luis, **Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad**. Madrid: Reus, 2016, p. 463.

Deste modo, o Regulamento transforma as obrigações do responsável que estavam na Diretiva em um princípio de responsabilidade, introduzindo a *accountability*. Como consequência da proatividade, diferentemente da passividade do tempo da Diretiva, ao responsável é devido declarar e notificar os tratamentos de dados, colocar legendas informativas, responder perante os cidadãos sobre os direitos de acesso, retificação, cancelamento e oposição, e implementar medidas de segurança descritas na norma. O RGPD determina que o responsável seja reflexivo e que avalie os riscos prováveis (alto, médio ou baixo), adotando as medidas a cada caso concreto, tentando prevenir riscos que podem acontecer, avaliando as possibilidades de risco e analisando as medidas preventivas que podem ser adotadas, quando necessárias. Para isso, o perfil do responsável pelo tratamento dos dados é no sentido de que tenha iniciativa e diligência para avaliar os possíveis riscos que advenham e diligentemente adote medidas preventivas, atualizando-as quando necessário. O Regulamento se afasta da antiga figura do Responsável definida na Diretiva 95/46 e na antiga LOPD (Lei Orgânica de Proteção de Dados Pessoais – Lei nº 15/1999, que sucedeu a Lei nº 5/1992), desenhando um modelo mais moderno do responsável, mais atual, inspirado no modelo anglo-saxônico de responsável *accountability* e de *compliance*, que não se limita a cumprir a determinação legal, mas se adiante a prevenir possíveis descumprimentos.

Um dos direitos novos trazidos no RGPD e que não encontra sucedâneo no direito brasileiro é o direito à desconexão digital do trabalhador (artigo 88)⁸⁵, reconhecendo a necessidade de descanso nos períodos que extrapolam a jornada de trabalho. Com a covid-19 e o trabalho remoto, tal direito ganhou extrema relevância.

Deste modo, o RGPD se atualiza para ir além da codificação estruturada a partir de preceitos para o descumprimento e pretende se atualizar na perspectiva de prospecção da legislação, estimulando as boas práticas e não apenas reprimindo.

2.2 Da legislação no Brasil

O Brasil tem a proteção constitucional à privacidade prevista no artigo 5º, X, CF e o Marco Civil (Lei nº 12.965/2014), que em seu artigo 3º, III, prevê a proteção dos dados pessoais, na forma da lei. Agora, tem-se a LGPD, que completa o sistema. O Marco Civil prevê o consentimento na coleta dos dados (artigo 7º, IX) e o agir de maneira transparente (artigo 9º, II), tal qual acontece na normativa.

O Provedor somente é responsabilizado se não cumprir a ordem judicial de retirada dos dados (artigo 19), burocratizando a celeridade da via administrativa que acontecia, até então.

A Autoridade de Proteção de Dados Pessoais foi criada como integrante da Presidência da República, porém é reconhecida esta caracterização transitória, podendo ser submetida ao regime autárquico especial, conforme artigo 55-A, §1º, da Lei nº 13.853/2019.

Na seara trabalhista, é importante ressaltar que os dados do trabalhador se constituem em dados sensíveis, pois consta a vinculação com os dados sindicais e, por vezes, de saúde, artigo 5º, II, da LGPD. A legislação trabalhista coíbe práticas discriminatórias, vedando-se na fase pré-contratual a exigência de testes, exames

85 RALLO LOMBARTE, Artemi. **Del derecho a la protección de datos a la garantía de nuevos derechos digitales. Tratado de Protección de Datos**. Tirant lo blanch: Valencia, 2019, p. 43.

ou qualquer prática relativa à esterilização, gravidez ou reabilitação profissional. A adoção de recrutamento fundamentado na distinção de sexo, origem, raça, cor, estado civil, situação familiar, deficiência, idade, dentre outros, é expressamente proibida pela Lei 9.029/1995⁸⁶. Por outro lado, certas profissões admitem, expressamente, a exigência de dados sobre antecedentes criminais, como as Leis 7.102/1983⁸⁷ e 10.826/2003⁸⁸, ou exames toxicológicos, nos termos do artigo 168, 6º, da Consolidação das Leis do Trabalho⁸⁹, ressaltando a sensibilidade no trato dos dados do candidato ao emprego.

Com razão, afirma Godinho⁹⁰ que, na fase pré-contratual, será possível eventual obrigação indenizatória quando presentes prejuízos decorrentes da contratação de empregado nesta fase.

Tanto nas fases contratual como na pós-contratual, dados relativos à saúde do trabalhador, como exames, doenças e acidentes de trabalho, especialmente previstos no Programa de Controle Médico de Saúde Ocupacional constantes na NR 7⁹¹, deverão ser resguardados pelo empregador.

Isso significa que há de se proteger de uma maneira mais contundente, pois vai além do dado pessoal. Os dados sensíveis têm uma especial proteção, pois se vazarem poderão causar situações de discriminação, comprometendo o princípio constitucional da Igualdade, previsto no artigo 5º, “caput”, da CF.

E, ainda, a empresa deve formular projeto de adequação à LGPD, pois isso fará com que esteja em conformidade com a proteção de dados do trabalhador, na seara jurídica, dos recursos humanos e do setor de tecnologia de informação. A implementação da lei requer o esforço multidisciplinar. Os investimentos em prevenção da empresa visa comprovar as suas boas práticas e são considerados, em juízo e administrativamente, caso haja algum revés.

Percebe-se, desde logo, que a LGPD é tímida se comparada ao RGPD, mas representa um passo importante em direção à formação da cultura da proteção dos dados pessoais.

86 BRASIL. Lei nº 9.029, de 13 de abril de 1995. Proíbe a exigência de atestados de gravidez e esterilização, e outras práticas discriminatórias, para efeitos admissionais ou de permanência da relação jurídica de trabalho, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/19029.htm. Acesso em: 22 out. 2021.

87 BRASIL. Lei nº 7.102, de 20 de junho de 1983. Dispõe sobre segurança para estabelecimentos financeiros, estabelece normas para constituição e funcionamento das empresas particulares que exploram serviços de vigilância e de transporte de valores, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7102.htm. Acesso em: 22 out. 2021.

88 BRASIL. Lei nº 10.826, de 22 de dezembro de 2003. Dispõe sobre registro, posse e comercialização de armas de fogo e munição, sobre o Sistema Nacional de Armas – Sinarm, define crimes e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7102.htm. Acesso em: 22 out. 2021.

89 BRASIL. Decreto-Lei nº 5.452, de 1º de maio de 1943. Aprova a Consolidação das Leis do Trabalho. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 22 out. 2021.

90 GODINHO DELGADO, Maurício. **Curso de Direito do Trabalho**. São Paulo: LTr, 2017.p. 9.1145-1146.

91 NR 7, com redação dada pela Portaria MTb 1031, de 06/12/2018. Disponível em: <https://www.gov.br/trabalho-e-previdencia/pt-br/composicao/orgaos-especificos/secretaria-de-trabalho/inspecao/seguranca-e-saude-no-trabalho/normas-regulamentadoras/nr-07.pdf>. Acesso em: 22 out. 2021.

3. Da evolução do direito de estar só à tutela da proteção de dados pessoais

No Brasil, os direitos à intimidade e à privacidade estão referidos no artigo 5º, X, da Constituição Federal - CF⁹², reconhecendo a distinção proveniente da doutrina e jurisprudência alemãs, da teoria das esferas ou dos círculos concêntricos⁹³. As esferas da vida privada comportam o grau de interferência que o indivíduo suporta com relação a terceiros. Para tal, leva-se em consideração o grau de reserva do menor para o maior. Assim, no círculo exterior está a privacidade; no intermediário, a intimidade; e, no interior desta, o sigilo. Deste modo, a proteção legal torna-se mais intensa à medida em que se adentra no interior da última esfera.

O preceito constitucional consagra a regra do fornecimento da informação pública, ressaltando o sigilo imprescindível à segurança da sociedade e do Estado – art. 5º, XXXIII, da CF⁹⁴. Na regulamentação ao dispositivo da Constituição, a Lei de Acesso à Informação Pública, em seu art. 3º, I, estabelece que para assegurar o direito de acesso à informação pública será observada a publicidade como preceito geral e do sigilo como exceção. Tem-se, ainda, o Marco Civil da Internet e a Lei de Proteção de Dados Brasileira.

A legislação de proteção de dados teve três fases de desenvolvimento: 1ª) 1970 – primeiras legislações *Land Hass*; 2ª) criação das Agências de Proteção de Dados – Lei Francesa, que foi a primeira experiência; 3ª) a livre circulação de dados e unificação do direito comunitário⁹⁵.

Frente ao fenômeno informático, desenvolveu-se a noção de autodeterminação informativa⁹⁶, que equivale à liberdade informática com um valor indiscutível na sociedade da informação⁹⁷. Sua função consiste em garantir aos cidadãos direitos de informação, acesso e controle dos dados que lhes concernem. Essa faculdade não é

92 BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 out. 2021.

93 COSTA JR., Paulo José da. **O direito a estar só: tutela penal da intimidade**. São Paulo: RT, 1970, p. 31, citando HENKEL, Der Strafschutz des Privatlebens.

94 BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 out. 2021.

95 LIMBERGER, Têmis. **O Direito à Intimidade na Era da Informática: A necessidade de proteção dos dados pessoais**. 1. ed. Porto Alegre: Livraria do Advogado, 2007.

96 PÉREZ LUÑO, Antonio Enrique. **Manual de informática y derecho**. Barcelona: Editorial Ariel S.A., 1996, p. 44.

97 Sustentando a mesma posição da tese afirmativa de um direito, a partir do artigo 18.4 da CE: DA- VARA RODRIGUEZ, Miguel Ángel. **Manual de Derecho Informático**. Madrid: Aranzadi, 1993, p. 65. MURILLO, Pablo Lucas. **El derecho a la autodeterminación informativa**. Madrid: Tecnos, 1990, p. 157-8 (Temas Clave de la Constitución Española) e Informática y protección de datos personales. Cuadernos e Debates, Madrid nº 43, 1993, p. 47-87. HIGUERAS, Manuel Heredero. La nueva ley alemana de protección de datos. Boletín de Información del Ministerio de la Justicia, ano XLVI, nº 1630, 1992, p. 1765. RUIZ MIGUEL, Carlos. **La configuración constitucional del derecho a la intimidad**. Madrid: Tecnos, 1995, p. 94/7. BENDA, Ernesto. Dignidad Humana y derechos de la personalidad. In: **Manual de Derecho Constitucional**. Madrid: Marcial Pons, 1996, p. 132. Em sentido contrário, não reconhecendo o nascimento de um novo direito fundamental: DENNINGER, E. El derecho a la autodeterminación informativa. In: **Problemas actuales de la documentación y la informática jurídica**. PÉREZ LUÑO, Antonio E. (Org.). Madrid: Tecnos, 1987, p. 271.

intrassubjetiva, mas sim uma autodeterminação do sujeito no seio de suas relações com os demais cidadãos e o poder público. O livre desenvolvimento da personalidade estaria dividido em duas liberdades. De um lado, a liberdade para decidir realizar ou não determinados atos e a faculdade para comportar-se ou atuar de acordo com essa decisão. De outro, a autodeterminação informativa referente à liberdade do indivíduo para determinar se deseja tornar públicas informações a seu respeito, bem como a quem cedê-las e em que ocasião. É paradigmática a sentença do Tribunal Constitucional Federal Alemão com relação à Lei do Censo⁹⁸, em 1983.

Com a expansão das novas tecnologias em rede, em 2008, o Tribunal Constitucional Federal Alemão atualizou a autodeterminação informativa, a partir do novo direito fundamental à garantia de confidencialidade e integridade dos sistemas técnico-informacionais⁹⁹, acentuando a aludida migração das relações sociais e condução da vida do indivíduo para o ambiente técnico-informacional. A decisão ficou restrita à atuação do poder público, mas é amplamente reconhecido o impacto que pode causar no setor privado, igualmente.

A discussão teórica, a respeito de ser a autodeterminação informativa um novo direito ou faceta do direito à intimidade evoluiu para a positivação do reconhecimento da proteção dos dados pessoais, de forma autônoma. Isto significa a proteção de todos os dados de caráter pessoal que digam respeito ao cidadão. Esses dados devem ser objeto de um tratamento legal, com finalidade específica e com consentimento da pessoa interessada.

A proteção dos dados pessoais é um direito autônomo com relação à intimidade ou privacidade, nos países europeus, veja-se o Tratado de Lisboa, artigo 16-B¹⁰⁰, que ratificou a Carta de Nice¹⁰¹, contemplando o direito fundamental à proteção dos dados pessoais (artigo 8º), em caráter autônomo à intimidade (artigo 7º). O diploma explicitador dos direitos fundamentais da União Europeia demonstra estar sintonizado com as questões oriundas do ciberespaço.

No Brasil, o STF, por meio da ADI nº 6387¹⁰² consagrou o direito à proteção

98 Sentença de 15/12/1983, do Tribunal Constitucional Alemão, Boletín de Jurisprudencial Constitucional, nº 33, janeiro 1984, p. 137. A questão discutida neste julgamento, que se tornou paradigmático, era com relação à Lei do Censo, que fazia demasiadas perguntas, o que poderia atentar diretamente contra os direitos fundamentais de liberdade de opinião, inviolabilidade de domicílio e liberdade de expressão. O objetivo do Tribunal era aprofundar as bases constitucionais da proteção de dados relativas à pessoa. A norma básica em referência era o direito geral de respeito à personalidade garantido pelo art. 2.1 (Direito Geral de Personalidade), combinado com o art.1.1 (a dignidade da pessoa humana) da Lei Fundamental de Bonn.

99 MENKE, Fabiano. *A proteção de dados e novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão*. In: MENDES, G.F.; SARLET, I.W.; COELHO, A.Z. P. (Org.). **Direito, Inovação e Tecnologia**. 01 ed. São Paulo: Saraiva, 2014, v., p. 205-230.

100 UNIÃO EUROPEIA. Jornal Oficial da União Europeia. Tratado de Lisboa. C 306, 50º ano, 17 de dezembro de 2007. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:306:FULL:PT:PDF>. Acesso em: 06 set. 2018.

101 UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia, de 07 de dezembro de 2000. Carta de Nice. Disponível em: http://www.europarl.europa.eu/charter/default_pt.htm. Acesso em: 10 set. 2018.

102 BRASIL. Supremo Tribunal Federal (STF). Ação Direta de Inconstitucionalidade 6387. Disponível em <https://redir.stf.jus.br/paginadorpub/paginador.jsp?> Acesso em: 22 de outubro de 2021.

dos dados pessoais. Antes da aprovação da PEC 17/2019, Sarlet¹⁰³ já sustentava o direito fundamental à proteção de dados pessoais. A importância no reconhecimento de um novo direito fundamental correspondente confere um novo e atual sentido à proteção da pessoa humana e da dignidade, da autonomia e das esferas que são inerentes. Como consequências, tem um *status* normativo superior, a inclusão como cláusula pétrea, artigo 60, § 1º a 4º, da CF e as consequências da eficácia, art.5, §1º e §§2ª e 3º da CF.

A inexistência de autoridades administrativas para proteção dos dados, tal qual existem na Europa, leva à sobrecarga dos tribunais, propiciando uma judicialização excessiva¹⁰⁴.

4. Exposições virtuais e consequências reais

Diante da exposição constante das pessoas nas redes sociais, o risco de vazamento de informações e imagens fica potencializado. Outrora os riscos existiam, mas eram diminuídos, se comparados aos dias de hoje.

Pérez Luño designa *metamorfose da intimidade*¹⁰⁵. Uma metamorfose no direito à intimidade que se expressa duplamente: do original direito a estar só individualmente à perspectiva de estar no âmbito social e coletivo; e desde o direito à personalidade ao deslocamento que aponta para órbita patrimonial¹⁰⁶.

O primeiro significado da intimidade (direito a estar só) se situa na esfera de *foro interno*, de solidão, de ensimesmamento e autoconfinamento pessoal, consequentemente, este conceito corre o risco de ser inexplicável e carecer de qualquer relevância jurídica; ou se, ao contrário, toma-se como ponto de referência suas implicações e projeções intersubjetivas no âmbito do “foro externo”, corre-se o risco de deformar a intimidade, de coisificá-la, de diluí-la em um conjunto de tópicos sociais, e vendê-la em seu antônimo, isto é, na sua alteração; ou seja, em que deixe de ser ela mesma para ser traída, levada e tiranizada pelo outro¹⁰⁷.

Existe algum ponto de mediação nesta polaridade do dilema, aparentemente insolúvel?

Antonio Enrique Pérez Luño estima que sim. A concepção de intimidade como isolamento e ensimesmamento não é necessariamente incompatível com suas pro-

103 SARLET, Ingo. *Fundamentos constitucionais: o direito fundamental à proteção de dados*. In: MENDES, Iur [et al.] (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

104 PERLINGEIRO, Ricardo. *A codificação do direito à informação na América Latina*. Revista de Direito Administrativo & Constitucional A&C. Ano 14, n. 56 – abr./jun. Belo Horizonte: Fórum, 2014, p.224.

105 PÉREZ LUÑO, Antonio Enrique. **Los derechos humanos en la sociedad tecnológica**. Madrid: Universitas, 2012, p. 115.

106 A respeito da evolução do direito à intimidade, veja-se artigo produzido no Anuário nº 10 da Unisinos. LIMBERGER, Têmis. *Acesso à informação pública em rede: a construção da decisão adequada constitucionalmente*. In: STRECK, Lenio Luiz; ROCHA, Leonel Severo; ENGELMANN, Wilson Engelmann. (Org.). **Constituição, sistemas sociais e hermenêutica**. Anuário do Programa de Pós-Graduação em Direito da Unisinos. 1ed. Porto Alegre e São Leopoldo: Livraria do Advogado e Unisinos, 2013, p. 259/276.

107 ORTEGA Y GASSET, J. *El hombre y la gente*, en Obras Completas, Alianza Editorial & Revista de Occidente, vol.7, Madrid, 1983, apud PÉREZ LUÑO, Antonio Enrique. **Los derechos humanos en la sociedad tecnológica**. Madrid: Universitas, 2012, p. 116.

jeções sociais, caso se coloque como um primeiro momento de seu processo formativo. Esse *intus* ou fase solitária e interna da intimidade se encontraria conformada por ideias, que reclamariam sua posterior exteriorização em ações. O isolamento confinado em si mesmo somente seria capaz de fabricar mundos exteriores fantasmagóricos, condenados a degenerar em puro solipsismo. A dimensão interna e ensimesmada da intimidade para realizar-se plenamente precisa extroverter-se; a convivência é indispensável na nossa vida, necessita apoiar-se em outras vidas¹⁰⁸.

Há a necessidade de superação de minha subjetividade imediata pelo confronto com uma subjetividade exterior (observe-se aqui a proposição hegeliana do movimento dialético de afirmação, negação e negação da negação). O reconhecimento de minha liberdade e de meu querer inclui, necessariamente, a subjetividade exterior, pois tem como pressuposto o reconhecimento delas (minha liberdade e querer) por instâncias mediadoras, como a família, as corporações e Estado¹⁰⁹.

Assim, para que se possa exercer a vontade livre e autônoma, é necessário que se admita e reconheça uma mútua restrição de direitos e deveres, o que deverá ser realizado através das instâncias mediadoras (sermos *membros de*). Noutras palavras, conforme leciona Weber, “[...] o Estado, dentro da eticidade, é condição de possibilidade da realização da vontade livre, isto é, autônoma”¹¹⁰. É exatamente através dessa mediação em que se encontra a concretização do conceito de liberdade, que é a segunda natureza proposta por Hegel, que é a eticidade (ou mediação social da vontade).

Essa abertura da convivência se exercita por formas de comunicação e de linguagem que se integram e socializam no mais íntimo de nosso ser, assim o ser mais íntimo de cada homem já está informado, modelado por uma determinada sociedade. Isto porque a própria noção de intimidade ou de privacidade é uma categoria cultural, social e histórica¹¹¹.

Assim, o núcleo significativo da intimidade se deslocou, inclusive se pode afirmar que foi ao seu oposto, desde o âmbito solitário do ensimesmamento à esfera dos usos sociais em que se manifesta e se exterioriza em termos de alteração. A decantação da cultura europeia da intimidade e privacidade, que pretende traduzir a noção anglo-saxã de privacidade, assim como a categoria dos denominados dados pessoais e perfis de personalidade, que se projetam sobre um conjunto mais amplo e global das relações intersubjetivas, refletem esta tendência paradoxal em direção a uma *socialização da intimidade*¹¹².

108 GARCÍA MORENTE, Ensayo sobre la vida privada (1935); se cita por la nueva Ed. De la Facultad de Filosofía de la Universidad Complutense, Madrid, 1992, p. 36, “apud” PÉREZ LUÑO, Antonio Enrique. **Los derechos humanos en la sociedad tecnológica**. Madrid: Universitas, 2012, p.116.

109 WEBER. Thadeu. Ética e Filosofia do **Direito**: autonomia e dignidade da pessoa humana. Petrópolis, RJ: Vozes, 2013. p. 88.

110 WEBER. Thadeu. Ética e Filosofia do direito: autonomia e dignidade da pessoa humana. Petrópolis, RJ: Vozes, 2013. p. 96.

111 ORTEGA Y GASSET, J. *El hombre y la gente*, en Obras Completas, Alianza Editorial & Revista de Occidente, vol.7, Madrid, 1983, apud PÉREZ LUÑO, Antonio Enrique. **Los derechos humanos en la sociedad tecnológica**. Madrid: Universitas, 2012, p. 116.

112 CABEZUELO ARENAS, A.L. *Derecho a la intimidad*, con Prólogo de L. H. CLAVERÍA GOSÁLBEZ, Tirant to Blanch, Valencia, 1998; CLAVERÍA GOSÁLBEZ, L. H. Reflexiones sobre los derechos

Outro aspecto que merece referência é o fato de que houve um deslocamento do âmbito do direito de personalidade ao âmbito patrimonial, considerando que muitas pessoas recebem quantias patrimoniais expressivas para exporem sua intimidade, negociando esta exposição, principalmente em programas televisivos¹¹³.

A intimidade, que foi concebida inicialmente como integrante dos direitos de personalidade e um dos mais destacados exemplos, atualmente, com os novos perfis coletivos e sociais, que conformam o exercício do direito à intimidade, encontra-se condicionada aos acontecimentos sociais. Com isso, a intimidade corre o risco de ser submetida aos modismos e, inclusive, às exigências de mercado.

Por isso, na sociedade da informação e de consumo, a intimidade se converteu, em muitas ocasiões, em uma mercadoria cujo valor se calcula em termos da lei da oferta e da procura. Nestas ocasiões, a intimidade de cada um vale o que os demais, em especial os meios de comunicação, estão dispostos a pagar para publicizá-la¹¹⁴.

Deste modo, o direito à intimidade somente se mantém como direito da personalidade dotado dos atributos de inviolabilidade, irrenunciabilidade e inalienabilidade para os menores, enquanto que para os maiores pode ser objeto de transações consentidas, de renúncias e cessões, em troca das correspondentes prestações econômicas. Constata-se, então, que para os adultos perdeu sua dimensão de direito da personalidade para integrar-se no sistema de direitos patrimoniais¹¹⁵.

Assim, a metamorfose do direito à privacidade, segundo Pérez Luño, trouxe mudanças importantes. Deslocou-se do âmbito interno - direito a estar só a uma perspectiva social e coletiva e da condição de integrante de direito da personalidade passou a direito patrimonial, porque integra a ótica negocial para muitas pessoas, na condição desfrutada pela maioria, subsistindo apenas para os menores.

A *reinvenção da privacidade* é como Stefano Rodotà¹¹⁶ denomina o fenômeno atual, enquanto a construção da identidade efetua-se em condições de dependência crescente do exterior. Nesta perspectiva, assume um novo significado a liberdade de expressão como elemento essencial da pessoa e de sua situação na sociedade. Isto modifica a relação entre esfera pública e privada e a própria noção de privacidade. Reforça-se a noção de cidadania com outros poderes que caracterizam a cidadania do novo milênio, a partir da constitucionalização da pessoa humana.

Quando se consideram as questões suscitadas pela inovação tecnológica, ocor-

de la personalidad a la luz de la LO1/82 de 5 de mayo de 1982, em Anuario de Derecho Civil, octubre-diciembre, 1983, pp. 1243/1268; M. GALÁN JUAREZ, *Intimidad, Nuevas dimensiones de un nuevo derecho*, Editorial Universitaria Ramón Areces & Servicio de Publicaciones de la Universidad Rey Juan Carlos I, Madrid, 2005, p. 79 ss.; PÉREZ LUÑO, A. E. *Intimidad y protección de datos personales: del habeas corpus al habeas data*, en Estudios sobre el derecho a la intimidad, ed. a cargo de L. GARCÍA SAN MIGUEL, 1982, cit., Tecnos, Madrid, 1992, p. 36 ss.; id., *Libertad informática y leyes de protección de datos personales*, en colab. Con M.G. LOSANGO y M.F. GUERRERO MATEUS, Centro de Estudios Constitucionales, Madrid, 1989.

113 Programa televisivo exibido por emissora nacional denominado Big Brother Brasil.

114 PÉREZ LUÑO, Antonio Enrique. **Los derechos humanos en la sociedad tecnológica**. Madrid: Universitas, 2012, p. 120.

115 PÉREZ LUÑO, Antonio Enrique. **Los derechos humanos en la sociedad tecnológica**. Madrid: Universitas, 2012, p. 121.

116 RODOTÀ, Stefano. **El derecho a tener derechos**. Madrid: Trotta, 2014, p. 293.

re o denominado *tsunami digital*¹¹⁷. Como consequência desta transformação, o critério de segurança pública se converte em exclusivo critério de referência.

Isto significa que as pessoas estão cada vez mais transparentes e os organismos públicos mais afastados do controle jurídico e político, ocasionando uma nova distribuição de poderes políticos e sociais.

O denominado *tsunami digital* pode ser considerado desde outros pontos de vista, começando pela identidade. Nesta perspectiva, o direito de acesso aos dados representa um aliado forte, em termos de proteção jurídica, que permite manter o controle sobre as próprias informações, seja qual for o sujeito que as gestiona, o local em que se encontrem e as modalidades de sua utilização. Direito essencial à construção da identidade, já que confere poder para cancelamento nos seguintes casos: dados falsos, ilegitimamente recolhidos, conservados muito além do tempo previsto, os inexatos ou para completação.

O “conhece-te a ti mesmo” já não é uma operação voltada ao interior, mas devido a esta nova perspectiva vai-se ao exterior e à suposta necessidade de conhecer quem somos na dimensão eletrônica, onde se desenvolvem questões importantes nas nossas vidas. Considerando hoje a dinâmica que caracteriza a recolhida dos dados e os sujeitos que a utilizam, cada vez é menos verossímil uma identidade como *sou o que digo que sou*, pois que haveria que substituí-la por *tu és o que Google diz que és*¹¹⁸.

A construção da identidade fica entregue por completo aos algoritmos. A construção da identidade é interior e exterior. O sistema deve então: a) fazer explícito o fluxo de dados para permitir o controle da pessoa interessada; b) respeitar o princípio da minimização dos dados, tratando somente aqueles necessários em um contexto determinado; c) impor limites às conexões entre bancos de dados.

A nova abstração produz um esvaziamento do humano, de modo que é problemático afirmar que nos encontramos frente a uma nova antropologia.

Manuel Castells¹¹⁹ - um dos maiores sociólogos da atualidade no estudo das redes sociais e Internet - adverte para o perigo da exposição exacerbada nas redes, aos programas de vigilância governamentais. Chega a afirmar de forma contundente que a privacidade na rede mundial de computadores acabou, no denominado mundo virtual.

Apesar do gasto de bilhões de dólares em segurança eletrônica, tornou-se evidente que, numa rede, a segurança só é tão boa quando a segurança do elo mais fraco está protegida. Penetrando-se na rede, em qualquer ponto, pode-se percorrer seus nós com relativa facilidade.

Isto envolve a (in)capacidade que tem um Estado de agir sobre um comportamento, que tem lugar em outra jurisdição – isso será limitado pelas velhas formas de poder baseadas na territorialidade.

Castells adverte a respeito do *Panóptico Eletrônico*¹²⁰. Há uma ameaça funda-

117 THE FUTURE Group: Freedom, Security, Privacy: European Home Affairs in an Open World; jun. 2008. In: RODOTÀ, Stefano. **El derecho a tener derechos**. Madrid: Trotta, 2014, p.298.

118 RODOTÀ, Stefano. **El derecho a tener derechos**. Madrid: Trotta, 2014, p. 300.

119 CASTELLS, Manuel. **A Galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade**. Rio de Janeiro: Zahar, 2003, p. 145 e 152.

120 CASTELLS, Manuel. **A Galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade**. Rio de Janeiro: Zahar, 2003, p.148.

mental à liberdade sob o novo ambiente de policiamento global: a estruturação do comportamento cotidiano pelas normas dominantes da sociedade. A liberdade de expressão era a essência do direito à comunicação irrestrita na época em que a maior parte das atividades diárias não era relacionada à esfera pública. Mas em nosso tempo, uma proporção significativa da vida cotidiana, inclusive o trabalho, o lazer, a interação pessoal, tem lugar na Internet. A maior parte da atividade econômica, social e política é de fato um híbrido de interação *on-line* e física. Em muitos casos, estão imbricadas.

Assim, viver num panóptico eletrônico equivale a ter metade de nossas vidas permanentemente expostas a monitoramento.

A segunda perda é a liberdade, isto é, o direito de se fazer o que se quer. Por que isso? Por que a ameaça à privacidade traduz-se na redução potencial de liberdade?

Destarte, é impossível conceber direitos e garantias tendo como referência espaços do passado, especialmente nas dinâmicas sociais, no que diz respeito ao direito à privacidade.

5. Considerações finais

O Brasil experimenta um incremento legislativo a partir da aprovação do direito fundamental à proteção dos dados pessoais. Tal visa imprimir maior vigor à LGPD.

Na seara trabalhista é muito importante que sejam respeitados os direitos do trabalhador, pois os dados laborais, identitários, sindicais e, por vezes, dados de saúde, também são considerados sensíveis. Caso vazem, poderão causar situações de discriminação. Por isso, é importante que as empresas promovam a sua adequação à LGPD. A prevenção é extremamente positiva, pois assinala o compromisso com as boas práticas, o que é levado em conta tanto no âmbito administrativo e/ou judiciário, caso exista algum revés.

O RGPD na Europa é fruto de uma legislação evoluída nas últimas cinco décadas. Contemplando mecanismos de transparência, no consentimento informado para coleta de dados, agência de proteção de dados, responsabilidade do encarregado da proteção de dados, agindo preventivamente e proativamente, diante da possibilidade de violação de dados e, na seara laboral, o direito à desconexão digital do trabalhador.

Da tríade de autores estudados, tem-se sucintamente que: Pérez Luño propugna a Metamorfose da Privacidade, Rodotà, a Reinvenção da Privacidade, e Manuel Castells atualiza o simbolismo do Panóptico, e diz que se vive sob a vigilância de um Panóptico eletrônico, afirmando que a privacidade deixará de existir nas relações virtuais.

A formação de uma cultura de proteção de dados pessoais é extremamente importante e representa ganhos ao cidadão/trabalhador, à empresa e ao Estado, diante da potencial utilização das novas tecnologias na pandemia da covid-19, que assolou o mundo.

REFERÊNCIAS

BENDA, Ernesto. *Dignidad Humana y derechos de la personalidad*. In: Manual de Derecho Constitucional. Madrid: Marcial Pons, 1996.

BRASIL Disponível em <http://www.folha.uol.com.br/mercado/2021/10/>

senado-aprova-pec-que inclui-protecao-de-dados-como-direito-fundamental.shtml? Acesso em: 20 de outubro de 2021

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 22 out. 2021.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 10 set. 2018.

BRASIL. **Decreto-Lei 5.452, de 1º de maio de 1943**. Aprova a Consolidação das Leis do Trabalho. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm>. Acesso em: 22 out. 2021.

BRASIL. **Lei nº 10.826, de 22 de dezembro de 2003**. Dispõe sobre registro, posse e comercialização de armas de fogo e munição, sobre o Sistema Nacional de Armas – Sinarm, define crimes e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l7102.htm>. Acesso em: 22 out. 2021.

BRASIL. **Lei nº 7.102, de 20 de junho de 1983**. Dispõe sobre segurança para estabelecimentos financeiros, estabelece normas para constituição e funcionamento das empresas particulares que exploram serviços de vigilância e de transporte de valores, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l7102.htm>. Acesso em: 22 out. 2021.

BRASIL. **Lei nº 9.029, de 13 de abril de 1995**. Proíbe a exigência de atestados de gravidez e esterilização, e outras práticas discriminatórias, para efeitos admissionais ou de permanência da relação jurídica de trabalho, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9029.htm>. Acesso em: 22 out. 2021.

BRASIL. Ministério do Trabalho. **NR 7: redação dada pela Portaria MTb 1031 de 06/12/2018**. Disponível em: <<https://www.gov.br/trabalho-e-previdencia/pt-br/composicao/orgaos-especificos/secretaria-de-trabalho/inspecao/seguranca-e-saude-no-trabalho/normas-regulamentadoras/nr-07.pdf>>. Acesso em: 22 out. 2021

BRASIL. Supremo Tribunal Federal (STF). **Ação Direta de Inconstitucionalidade 6387**. Disponível em <https://redir.stf.jus.br/paginadorpub/paginador.jsp>? Acesso em: 22 de outubro de 2021.

CABEZUELO ARENAS, A.L. *Derecho a la intimidad*, con Prólogo de L. H. CLAVERÍA GOSÁLBEZ, Tirant to Blanch, Valencia, 1998.

CASTELLS, Manuel. *A Galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade*. Rio de Janeiro: Zahar, 2003.

CASTELLS, Manuel. *Ruptura: a crise da democracia liberal*. Rio de Janeiro: Zahar, 2018.

CLAVERÍA GOSÁLBEZ, L. H. Reflexiones sobre los derechos de la personalidad a la luz de la LO1/82 de 5 de mayo de 1982, em *Anuario de Derecho Civil*, outubro-dezembro, 1983, pp. 1243/1268.

COSTA JR., Paulo José da. *O direito a estar só: tutela penal da intimidade*. São Paulo: RT, 1970, p. 31, citando HENKEL, Der Strafschutz des Privatlebens.

DAVARA RODRIGUEZ, Miguel Ángel. *Manual de Derecho Informático*. Madrid: Aranzadi, 1993.

DEBORD, Guy. *A sociedade do espetáculo*. Rio de Janeiro: Contraponto, 1997.

DENNINGER, E. *El derecho a la autodeterminación informativa*. In: Problemas actuales de la documentación y la informática jurídica, PÉREZ LUÑO, Antonio E. (Org.). Madrid: Tecnos, 1987.

GARCÍA MORENTE, *Ensayo sobre la vida privada* (1935); se cita por la nueva Ed. De la Facultad de Filosofía de la Universidad Complutense, Madrid, 1992, p. 36, *apud* PÉREZ LUÑO, Antonio Enrique. *Los derechos humanos en la sociedad tecnológica*. Madrid: Universitas, 2012.

GODINHO DELGADO, Maurício. *Curso de Direito do Trabalho*. São Paulo: LTr, 2017. p. 9.1145-1146.

HIGUERAS, Manuel Heredero. *La nueva ley alemana de protección de datos*. Boletín de Información del Ministerio de la Justicia, ano XLVI, nº 1630, 1992.

LIMBERGER, Têmis. *Acesso à informação pública em rede: a construção da decisão adequada constitucionalmente*. In: STRECK, Lenio Luiz; ROCHA, Leonel Severo; ENGELMAN, Wilson (Org.). *Constituição, sistemas sociais e hermenêutica*. Anuário do Programa de Pós-Graduação em Direito da Unisinos. Porto Alegre e São Leopoldo: Livraria do Advogado e Unisinos, 2013, p. 259-276.

LIMBERGER, Têmis. *O Direito à Intimidade na Era da Informática: A necessidade de proteção dos dados pessoais*. 1. ed. Porto Alegre: Livraria do Advogado, 2007.

M. GALÁN JUAREZ, *Intimidad, Nuevas dimensiones de un nuevo derecho*, Editorial Universitaria Ramón Areces & Servicio de Publicaciones de la Universidad Rey Juan Carlos I, Madrid, 2005.

MENKE, Fabiano. *A proteção de dados e novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão*. In: MENDES, G.F.; SARLET, I.W.; COELHO, A. Z. P. (Org.). *Direito, Inovação e Tecnologia*. 1 ed. São Paulo: Saraiva, 2014, v., p. 205-230.

MURILLO, Pablo Lucas. *El derecho a la autodeterminación informativa*. Madrid: Tecnos, 1990 (Temas Clave de la Constitución Española) e Informática y protección de datos personales. Cuadernos e Debates, Madrid nº 43, 1993, p. 47-87.

ORTEGA Y GASSET, J. *El hombre y la gente*, en *Obras Completas*, Alianza Editorial & Revista de Occidente, vol.7, Madrid, 1983, *apud* PÉREZ LUÑO, Antonio Enrique. *Los derechos humanos en la sociedad tecnológica*. Madrid: Universitas, 2012.

PÉREZ LUÑO, Antonio Enrique. *Intimidad y protección de datos personales: del habeas corpus al habeas data*, en *Estudios sobre el derecho a la intimidad*, ed. A cargo de L. GARCÍA SAN MIGUEL, 1982, cit., Tecnos, Madrid, 1992, p. 36 ss.; id., *Libertad informática y leyes de protección de datos personales*, en colab. con M.G. LOSANGO y M.F. GUERRERO MATEUS, Centro de Estudios Constitucionales, Madrid, 1989.

PÉREZ LUÑO, Antonio Enrique. *Los derechos humanos en la sociedad tecno-*

lógica. Madrid: Universitas, 2012.

PÉREZ LUÑO, Antonio Enrique. *Manual de informática y derecho*. Barcelona: Editorial Ariel S.A., 1996.

PERLINGEIRO, Ricardo. A codificação do direito à informação na América Latina. *Revista de Direito Administrativo & Constitucional A&C*. Ano 14, n. 56 – abr./jun. Belo Horizonte: Fórum, 2014.

RALLO LOMBARTE, Artemi. Del derecho a la protección de datos a la garantía de nuevos derechos digitales, Tratado de Protección de Datos. RALLO LOMBARTE, Artemi (Director), Tirant lo blanch: Valencia, 2019.

REIGADA, Antonio Trancoso “in” Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad, director PIÑAR MANÁS, José Luis, Madrid: Reus, 2016.

RODOTÀ, Stefano. *El derecho a tener derechos*. Madrid: Trotta, 2014.

RUIZ MIGUEL, Carlos. *La configuración constitucional del derecho a la intimidad*. Madrid: Tecnos, 1995.

SÁNCHEZ BRAVO, Álvaro A. *Hacia un nuevo marco europeo de protección de datos personales: empoderamiento de los ciudadanos en la sociedad tecnológica*. In: FERNANDEZ, Yarina Amoroso (Org.). *Sociocibernética e Infoética: contribución a una nueva cultura y praxis jurídica*. 1ed.Habana - Cuba: Editorial UNIJURIS, 2015, v. 1.

SARLET, Ingo. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: MENDES, Iuri [et al.] (org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

UNIÃO EUROPEIA. *Carta dos Direitos Fundamentais da União Europeia*, de 07 de dezembro de 2000. Carta de Nice. Disponível em: <http://www.europarl.europa.eu/charter/default_pt.htm>. Acesso em: 10 set. 2018.

UNIÃO EUROPEIA. *Jornal Oficial da União Europeia*. Tratado de Lisboa. C 306, 50º ano, 17 de dezembro de 2007. Disponível em: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:306:FULL:PT:PDF>>. Acesso em: 06 set. 2018.

WEBER, Thadeu. *Ética e Filosofia do Direito: autonomia e dignidade da pessoa humana*. Petrópolis, RJ: Vozes, 2013.

ZUCKERBERG contra a parede. *Revista ISTOÉ*, São Paulo, p. 66, 18 abr. 2018.

5. DESCOMPLICANDO OS AGENTES DE TRATAMENTO, COM BASE NA LEI GERAL DE PROTEÇÃO DE DADOS

SELMA CARLOTO¹²¹

1. Introdução

Os agentes de tratamento são o controlador e o operador e estes poderão responder solidariamente por desconformidades, já que a Lei Geral de Proteção de Dados reconhece a responsabilidade solidária entre os agentes de tratamento, resguardadas as situações nas quais existe excludente de responsabilidade de ambos, ou do operador.

A Lei Geral de proteção de Dados preconiza no artigo 5º, inciso IX, que o controlador e o operador são agentes de tratamento.

O controlador é o agente de tratamento responsável, ao qual competem as decisões referentes ao tratamento de dados pessoais. Este é quem determina os objetivos e meios do processamento, assim como os seus meios e objetivos.

Na legislação da União Europeia, o controlador se denomina contratante, ou responsável pelo tratamento, e passou a ser tarefa imprescindível, na jornada de implementação e conformidade, definir quem é o controlador e quem é o operador. Em regra, o controlador é uma entidade que decide sobre os elementos-chave de um processamento.

Já o operador trata dados, de acordo com as instruções do controlador. Podemos dizer que consiste em uma verdadeira “terceirização de atividades de tratamento” para outras entidades, sejam pessoas jurídicas ou naturais. Não existe impedimento para uma pessoa natural ser contratada como operadora em atividades específicas de tratamento de dados, sendo considerada operadora de dados, mas os empregados, os servidores públicos, os sócios, assim como outras pessoas naturais que integram e estão vinculados a uma pessoa jurídica, expressando sua vontade, não poderão ser considerados agentes de tratamento, operadores ou controladores neste cenário. Na verdade, a entidade responderá pelos atos destes prepostos, que agem e tratam dados e seu nome.

O Parecer 1/2010 do Grupo de Trabalho do artigo 29, na União Europeia, ainda elaborado durante a vigência da Diretiva 95/46/CE sobre os conceitos de responsá-

121 Autora das obras: *Compliance Trabalhista*, *Lei Geral de Proteção de Dados enfoque nas relações de Trabalho*, *Manual Prático de Adequação à Lei Geral de Proteção de Dados* e coordenadora/autora da obra *LGPD Comentada, enfoque nas relações de trabalho*. Pesquisadora da USP, Departamento de Direito Civil, de Lei Geral de Proteção de Dados. Exin Data Protection Officer (certificação de DPO). Professora convidada da Fundação Getúlio Vargas da FGV- Direito Rio e dos MBAs de Gestão de Pessoas, Gestão Empresarial e Gestão Comercial da área de Direito. Membro do Instituto Nacional de Proteção de Dados. Mestre pela Universidade de São Paulo (USP). Doutoranda em engenharia da informação na Universidade Federal do ABC em Inteligência Artificial. Doutorado em Direito do Trabalho na Universidade Federal de Buenos Aires (UBA). Especialista pela FADISP. Autora dos livros publicados na Argentina, Editorial Quorum, *Manual de Derecho Laboral e Interesses Metaindividuais e ações coletivas*. E-mail: selmacarloto@hotmail.com inst.selmacarloto@hotmail.com

vel pelo tratamento, ou controlador e operador ou subcontratante, WP 169, já nos brindava com o conceito de responsável pelo tratamento dos dados e trazia a sua relação com o conceito de subcontratante, que corresponde ao operador, no Brasil.

O controlador era inicialmente denominado, na Convenção nº 108 do Conselho da Europa, de “responsável pelo ficheiro”, e o termo foi substituído por “responsável pelo tratamento” de dados pessoais. A Diretiva introduziu também o conceito de “subcontratante”, que não era mencionado na Convenção nº 108.

Os conceitos iniciais foram formulados durante as negociações relativas ao projeto de proposta da Diretiva 95/46/CE, no início da década de 90 e o conceito inicial de responsável pelo tratamento foi basicamente retirado da Convenção de número 108 do Conselho da Europa, adotada em 1981.

BRASIL	EQUIVALENTE NA UNIÃO EUROPEIA
CONTROLADOR	RESPONSÁVEL
OPERADOR	SUBCONTRATANTE

2. Identificando os agentes de tratamento

A Lei Geral de Proteção de Dados do Brasil se inspirou inicialmente na Diretiva 94/46/CE, foi promulgada e entrou em vigor durante o Regulamento Geral de Proteção de Dados da União Europeia. É importante destacar que o Regulamento Geral de Proteção de Dados revogou a Diretiva, mas incorporou suas bases legais de legitimidade de tratamento, princípios, assim como vários institutos e conceitos, como dos agentes de tratamento, responsável e subcontratante.

No Brasil, os agentes de tratamento, nos termos da Lei Geral de Proteção de Dados, são: o controlador e o operador.

CONTROLADOR: é agente de tratamento e poderá ser uma pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. É o agente de tratamento responsável, principal.

OPERADOR: é agente de tratamento e poderá ser uma pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

O principal elemento distintivo entre estes atores é o poder de decisão, admitindo-se que o controlador forneça instruções para que um terceiro (“operador”) realize o tratamento em seu nome. Um controlador pode compartilhar dados, por exemplo, para um contador, empresa de folha de pagamento, transportadora, courier, entre outros, os quais apenas poderão tratar dados de acordo com as instruções claras do controlador, não podendo ser utilizados para finalidade distinta, ou além daquela determinada pelo controlador.

O operador, subcontratante, na União Europeia, poderá apenas decidir sobre certos assuntos, como, por exemplo, qual software usar, a segregação de acesso e outras medidas técnicas e administrativas de segurança da informação, o que não altera seu papel como operador.

Talvez ficasse mais claro se no Brasil tivéssemos repetido as nomenclaturas

eleitas e utilizadas pela legislação da União Europeia, não dando uma falsa ideia de que o empregado, um servidor, ou departamento poderiam ser agentes de tratamento e assim polo passivo em uma ação judicial dos entes legitimados para ações civis públicas, ou mesmo em uma ação individual, ou uma sanção da Autoridade Nacional de Proteção de Dados.

Esta diferenciação é fulcral não apenas para os profissionais especializados na área, mas também para o cidadão comum e, sobretudo, em uma implementação por uma empresa ou entidade, principalmente pelo papel assumido pelo controlador como responsável pelas atividades de tratamento, que detém poder de decisão.

Tínhamos já anteriormente importantes documentos que nos ajudavam na interpretação da Lei Geral de Proteção de Dados e nas diferenças entre os agentes de tratamento e mesmo o DPO, ou encarregado (o qual não é agente de tratamento), como a *guideline* da União Europeia de número 07/2020 do CEPD (Comitê Europeu de Proteção de Dados) e o anterior parecer do Grupo de Trabalho do Artigo 29 de número 1/2010.

A Autoridade Nacional de Proteção de Dados, no Brasil, preocupada com a identificação dos agentes de tratamento e as dúvidas recorrentes sobre esta temática, constatada não apenas em empresas privadas, mas principalmente em órgãos públicos, publicou o Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, em 2021, o qual pode ser encontrado no site do governo federal.

De acordo com este guia, os agentes de tratamento (controlador e o operador) poderão ser pessoas naturais ou jurídicas, de direito público ou privado, **devendo estes ser definidos a partir de seu caráter institucional. Importante destacar que os empregados, como subordinados, os servidores públicos, ou as equipes de trabalho de uma organização, não serão considerados controladores (autônomos ou conjuntos), nem operadores já que atuam sob o poder diretivo do agente de tratamento.**¹²²

Desta forma, um contador que trabalha internamente, como empregado, assim como um departamento de contabilidade, com empregados da entidade controladora, são vinculados à pessoa jurídica, não sendo agentes de tratamento. Já se a empresa controladora contratar um contador pessoa natural externo, ou um escritório externo de contabilidade, por exemplo, estes passarão a ser operadores.

Destaquemos ainda que o guia da Autoridade Nacional de Proteção de Dados preconiza que: **sempre que falamos de pessoa jurídica, a organização é que será o agente de tratamento para os fins da Lei Geral de Proteção de Dados**, sendo que esta estabelecerá as regras para o tratamento de dados pessoais, as quais serão executadas por seus representantes ou prepostos.

A pessoa jurídica, sempre que esta existir, será o agente de tratamento, controlador ou operador. Será controlador se tomar decisões e der instruções sobre as atividades de tratamento. Será operador se seguir estas instruções e apenas tratar os dados de acordo com as orientações lícitas daquele.

122 ANPD. GUIA ORIENTATIVO PARA DEFINIÇÕES DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS E DO ENCARREGADO. Disponível em: Guia Orientativo para Definições dos Agentes de Tratamento <https://www.gov.br/pt-br/assuntos/noticias>. Acesso em: 25 jun 2021.

Gerentes, sócios e empregados do controlador são vinculados a este e quem responde é o controlador. Empregados e outras pessoas naturais vinculadas ao operador também atuarão em nome deste. Isto é, se um empregado ou gestor der causa a um vazamento, assim como um servidor, o responsável será o agente de tratamento, restando a este apenas as sanções disciplinares que poderá impor àqueles, desde uma advertência até uma justa causa, dependendo da proporcionalidade, gravidade e reincidência e a possibilidade de ação regressiva por dolo ou culpa, se houver prévio ajuste contratual, nos termos do artigo 462 da CLT, parágrafo 1º. Do mesmo modo responderá um servidor, nos termos da Constituição Federal de 1988, artigo 37, parágrafo 6º.

Sendo responsável, é muito importante o agente de tratamento colocar no contrato de trabalho de seus empregados o dever de sigilo no tratamento de dados, além de ter uma política de segurança da informação com instruções, da qual o empregado irá assinar termo de responsabilidade de que seguirá as orientações e termos de confidencialidade. Também deverão ser oferecidos treinamentos de segurança da informação.

A política de segurança da informação deverá incluir cláusulas como a política da mesa limpa e da tela limpa, proibição de permanência em outros setores, proibição de compartilhamento de senhas, entre outras instruções.

Outro ponto importante é que o agente de tratamento será definido para cada operação de tratamento de dados pessoais e por conclusão a mesma empresa ou organização poderá ser controladora e operadora, mas apenas se em tratamentos distintos e de acordo com sua atuação, em diferentes operações de tratamento. Por exemplo, um contador geralmente é operador quando faz atividade de departamento pessoal, assim como em relação aos próprios empregados, mas será controlador em eventual auditoria.

3. Pessoa natural como agente de tratamento

Quando a Lei Geral de Proteção de Dados conceitua controlador e operador e traz que podem ser pessoas naturais, não está se referindo a empregados, equipes, departamentos, gestores, sócios **ou servidores**. Se estes fossem agentes de tratamento, os empregados e servidores passariam a estar no polo passivo de ações individuais e coletivas, nos termos do artigo 42 da LGPD, e poderiam sofrer sanções da Autoridade Nacional, a qual, na sua função educativa, entre outras, como a de conscientizar, regulamentar, **fiscalizar o cumprimento da LGPD e aplicar sanções**, em seu primeiro guia do Brasil, já demonstrou a preocupação com a possibilidade deste cenário com interpretações equivocadas, no Brasil, ao eleger este tema como o primeiro para a elaboração de um guia orientativo, entre tantos temas a tratar e regulamentar.

Uma pessoa natural poderá ser controladora como, por exemplo, um advogado, ou um médico tratando os prontuários de seus pacientes, já que estes tomam decisões nas atividades de tratamento. Da mesma forma, um vendedor que tem sua tenda de pipoca, ou cachorro quente, ou uma pequena loja, mas nunca os empregados vinculados a estes.

Estas entidades serão controladoras sempre que atuem de acordo com os próprios interesses e tiverem poder de decisão sobre as finalidades e os elementos

essenciais de tratamento; e serão operadoras quando atuarem de acordo com os interesses do controlador, sendo-lhes facultada apenas a definição de elementos não essenciais à finalidade do tratamento.

O guia da Autoridade Nacional de Proteção de Dados, da mesma forma que a *guideline* 07/2020, da União Europeia, reza que os funcionários atuarão em subordinação às decisões do controlador, não se confundindo, portanto, com os operadores de dados pessoais:

Daí decorre que não são controladoras as pessoas naturais que atuam como profissionais subordinados a uma pessoa jurídica ou como membros de seus órgãos. É o caso de empregados, administradores, sócios, servidores e outras pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta. Nesse sentido, a definição legal de controlador não deve ser entendida como uma norma de distribuição interna de competências e responsabilidades. De forma diversa, trata-se de comando legal que atribui obrigações específicas à pessoa jurídica, de modo que esta assume a responsabilidade pelos atos praticados por seus agentes e prepostos em face dos titulares e da ANPD.¹²³

O operador deverá ser uma entidade distinta do controlador.

Trazemos alguns exemplos didáticos da Autoridade Nacional de Proteção de Dados.

Um ótimo exemplo seria considerarmos uma relação existente entre uma empresa “A” e sua contabilidade, ou uma empresa de gestão de folha de pagamento, ou mesmo uma nuvem, sendo que a empregadora tomará as decisões sobre o tratamento destes dados. Neste exemplo, a empresa empregadora seria a controladora, a qual toma as decisões referentes aos tratamentos dos dados pessoais, enquanto a segunda (contabilidade, empresa de gestão de folha de pagamento ou uma nuvem) seria a operadora, já que realiza os tratamentos em nome do controlador.

A empresa de contabilidade, operadora, receberá os dados coletados pela controladora. Estes dados serão compartilhados e realizar-se-á o tratamento, de acordo com as suas orientações e determinações; além da finalidade indicada pela controladora e caso venha a realizar qualquer tratamento de dados fora do que foi orientado pelo controlador, a contabilidade será responsabilizada.

4. Exemplos práticos do Guia Orientativo da Autoridade Nacional de Proteção de Dados para Definições dos Agentes de Tratamento da Autoridade Nacional de Proteção de Dados

“Exemplo 1 - Médica profissional liberal:

123 ANPD. GUIA ORIENTATIVO PARA DEFINIÇÕES DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS E DO ENCARREGADO. Disponível em: Guia Orientativo para Definições dos Agentes de Tratamento <https://www.gov.br/pt-br/assuntos/noticias>. Acesso em: 25 jun 2021.

Uma médica, profissional liberal, armazena os prontuários e os demais dados pessoais de seus pacientes no computador de seu consultório. **A médica, pessoa natural, é a controladora dos dados pessoais.**¹²⁴ (*destaques nossos*)

“Exemplo 2 - Médica empregada de um hospital:

Uma médica é empregada de um hospital, constituído sob a forma de associação civil sem fins lucrativos. Nessa condição, atua como principal representante do hospital junto a um serviço de armazenamento de dados de pacientes em nuvem, inclusive assinando os contratos correspondentes. **O hospital, isto é, a associação civil, pessoa jurídica de direito privado, é o controlador na hipótese.** A médica, por atuar sob o poder diretivo da organização, não se caracteriza como agente de tratamento.¹²⁵ (*destaques nossos*)

“Exemplo 3 - Servidores públicos:

Uma autarquia, entidade da administração pública indireta, com personalidade jurídica própria, deseja utilizar um novo software para aprimorar o gerenciamento dos funcionários da instituição. Para isso, a Secretaria de Gestão Corporativa da entidade delega à Diretoria de Gestão de Pessoas (DGP) a tarefa de **determinar os meios pelos quais este software será implementado.** Após algumas reuniões, a DGP decide pela contratação da empresa terceirizada SIERRA para desenvolver o software em parceria com a equipe interna da Diretoria de Tecnologia da Informação (DTI). Embora a delegação de decisão quanto aos meios para a DGP possa sugerir que essa diretoria atue como operadora de dados, esta não é a análise correta: como a DGP é uma unidade administrativa da autarquia, a delegação interna não altera o papel do agente de tratamento, uma vez que, como exposto, o operador será sempre pessoa distinta do controlador. O mesmo raciocínio se aplica para a DTI. **Desse modo, a autarquia será a controladora de dados e a empresa SIERRA será a operadora de dados. A Secretaria e as Diretorias, assim como os seus respectivos servidores, são apenas unidades organizacionais do ente controlador de dados, razão pela qual não se caracterizam como agentes de tratamento.**¹²⁶ (*destaques nossos*)

“Exemplo 4 - Órgão público contratante de um serviço de inteligência artificial:

Um órgão público, vinculado à União, contrata uma solução de inteligência artificial fornecida por uma sociedade empresária com a finalidade específica de realizar o tratamento automatizado de decisões com base em um banco de dados gerido pelo órgão. **Seguindo as instruções fornecidas** pelo gestor público responsável e estabelecidas em contrato, a sociedade empresária realiza as operações necessárias para viabilizar o tratamento dos dados em questão. **A União, pessoa jurídica de direito público, é a controladora na hipótese.** Não obstante, o ór-

124 ANPD. GUIA ORIENTATIVO PARA DEFINIÇÕES DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS E DO ENCARREGADO. Disponível em: Guia Orientativo para Definições dos Agentes de Tratamento <https://www.gov.br/pt-br/assuntos/noticias>. Acesso em: 25 jun 2021.

125 ANPD. GUIA ORIENTATIVO PARA DEFINIÇÕES DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS E DO ENCARREGADO. Disponível em: Guia Orientativo para Definições dos Agentes de Tratamento <https://www.gov.br/pt-br/assuntos/noticias>. Acesso em: 25 jun 2021.

126 ANPD. GUIA ORIENTATIVO PARA DEFINIÇÕES DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS E DO ENCARREGADO. Disponível em: Guia Orientativo para Definições dos Agentes de Tratamento <https://www.gov.br/pt-br/assuntos/noticias>. Acesso em: 25 jun 2021.

ção público responsável detém obrigações legais específicas em face dos titulares e da ANPD, conforme previsto na LGPD. A sociedade empresária é a operadora, uma vez que realiza o tratamento dos dados conforme as instruções fornecidas pelo controlador. Por fim, o gestor público responsável, por atuar como servidor público subordinado à União, não se caracteriza como agente de tratamento.”¹²⁷ (*destaques nossos*)

5. Controladoria conjunta

Sempre que estivermos diante de mais de um responsável pelo tratamento de dados pessoais, ambos com poder de decisão, tomando decisões conjuntas, teremos uma controladoria conjunta. Estes agentes responderão solidariamente nos termos do artigo 42, parágrafo 1º, inciso II, que reza que os controladores **diretamente** envolvidos no tratamento do qual decorrerem danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no artigo 43 da LGPD. Diferentemente do que ocorre quando são compartilhados dados para pagamento de empregados em um banco, um órgão do governo, ou um plano de saúde, que tomam decisões independentes, sendo os responsáveis por seus tratamentos, como controladores independentes.

A controladoria conjunta estará presente sempre que presentes os critérios trazidos pela *guideline* 07/2020¹²⁸ do CEPD da União Europeia e que o Guia orientativo da ANPD para definições de agentes de tratamento for observado:

- 1) Deverá existir o poder de decisão no tratamento de dados pessoais conjunto, ou de mais de um agente de tratamento.
- 2) Deverá existir interesse mútuo de pelo menos dois controladores e que tenham finalidades próprias no mesmo tratamento.
- 3) Estes controladores conjuntos deverão tomar decisões conjuntas, comuns ou convergentes, tanto sobre os elementos essenciais como sobre as finalidades do tratamento.

Importante destacarmos que todos os critérios deverão ser seguidos concomitantemente para termos controladores ou responsáveis conjuntos.

Seguem alguns exemplos de controladores conjuntos do Guia Orientativo para Definições dos Agentes de Tratamento:

“Exemplo 1 – Campanha de marketing de empresas I: **decisões comuns.**

As empresas ARGENTINA e BRASIL lançaram um produto de marca conjunta COSMÉTICO e desejam organizar um evento para promover este produto. Para esse fim, **decidem compartilhar dados de seus respectivos clientes e banco de dados de clientes potenciais e decidir sobre a lista de convidados para o**

127 ANPD. GUIA ORIENTATIVO PARA DEFINIÇÕES DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS E DO ENCARREGADO. Disponível em: Guia Orientativo para Definições dos Agentes de Tratamento <https://www.gov.br/pt-br/assuntos/noticias>. Acesso em: 25 jun 2021.

128 EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, set. 2020. Disponível em: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf. Acesso em: 25 jun. 2021.

evento com base nesses dados. Elas também concordam sobre as modalidades de envio dos convites para o evento, como coletar feedback durante os eventos e sobre as ações de marketing de acompanhamento. Por fim, contratam a agência de marketing DINAMARCA para executar a campanha. A agência traz sugestões de como os clientes poderiam ser mais bem alcançados e define os canais, ferramentas e produtos da campanha. **As empresas ARGENTINA e BRASIL podem ser consideradas controladores conjuntos** para o tratamento de dados pessoais relacionados com a organização do evento e promoção do produto da marca COSMÉTICO, por terem definido, em conjunto, a finalidade e os elementos essenciais dos dados tratados nesse contexto. **Já a agência de marketing DINAMARCA atuará como operadora de dados** para as empresas ARGENTINA e BRASIL. Ainda que opine sobre os meios de tratamento, ela não é a responsável pela tomada de decisão final, limitando-se a definir elementos não essenciais como os canais, ferramentas e produtos da campanha. **Caso a agência de marketing DINAMARCA contrate serviços de terceiros de armazenamento de dados em nuvem, por exemplo, essa empresa prestadora de serviços será caracterizada como suboperadora.**¹²⁹ (*destaques nossos*)

“Exemplo 2 - Campanha de marketing de empresas II: **decisões autônomas**

Considere-se agora que a campanha descrita no exemplo anterior foi tão bem-sucedida que, em um segundo momento, a empresa ARGENTINA contrata a agência de marketing DINAMARCA para divulgar seus produtos ESPELHO e FACA. Pouco tempo depois, a empresa BRASIL toma a mesma decisão para divulgação dos produtos GARRAFA e HALTERE. Ambas as empresas passam a usar a lista de clientes que haviam compartilhado anteriormente. **Nesta situação, que envolve a divulgação de produtos produzidos exclusivamente pela empresa ARGENTINA ou pela empresa BRASIL, estas atuarão como controladores singulares**, cada uma atuando em suas próprias campanhas. A agência de marketing DINAMARCA continuará como operadora de dados para cada empresa.”¹³⁰ (*destaques nossos*)

A Lei Geral de Proteção de Dados atribui maior responsabilidade ao controlador, ainda que havendo responsabilidade solidária entre os agentes de tratamento. Dentro de suas atribuições, este deverá elaborar Relatório de Impacto à Proteção de Dados Pessoais, comunicar incidentes à ANPD, elaborar o ROPA (registro das atividades de tratamento de dados pessoais) e sua responsabilidade se dá nos termos dos artigos 42 a 45 da LGPD.

Os controladores, assim como os operadores, serão obrigados a reparar qualquer dano que provocarem, seja patrimonial, moral, individual ou coletivo, em razão do exercício de atividade de tratamento de dados pessoais, em violação à LGPD.

129 ANPD. GUIA ORIENTATIVO PARA DEFINIÇÕES DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS E DO ENCARREGADO. Disponível em: Guia Orientativo para Definições dos Agentes de Tratamento <https://www.gov.br/pt-br/assuntos/noticias>. Acesso em: 25 jun 2021.

130 ANPD. GUIA ORIENTATIVO PARA DEFINIÇÕES DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS E DO ENCARREGADO. Disponível em: Guia Orientativo para Definições dos Agentes de Tratamento <https://www.gov.br/pt-br/assuntos/noticias>. Acesso em: 25 jun 2021.

O operador deverá agir conforme as obrigações previstas na LGPD e seguir as orientações lícitas do controlador, caso contrário, responderá, solidariamente, pelos danos causados em razão do tratamento de dados pessoais realizado.

Qualquer desconformidade à Lei Geral de Proteção de Dados, ou a não observância de um ou a mais de um dos seus dispositivos poderá gerar sanções da Autoridade Nacional de Proteção de Dados, ou de outras entidades, como o Procon, nas relações de consumo, além de ações individuais e coletivas, no Judiciário, com pedido de dano moral individual ou coletivo e eventual dano material.

No rigor da lei, o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular pode esperar.

6. Conclusão

Diante de uma nova cultura e um novo cenário que nasceu, em virtude da crescente necessidade de proteção aos direitos **fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural**, trazida principalmente por novas tecnologias muitas vezes imperceptíveis e por um mundo novo dominado por tecnologia e algoritmos, em que os controladores passam a ser responsáveis pelo compromisso, isoladamente ou em conjunto, com diferentes graus de autonomia e responsabilidade, assim como os operadores, ambos agentes de tratamento, assumindo a responsabilidade pelas suas atividades de tratamento, não seria justo transferir esta responsabilidade aos seus trabalhadores, equipes, departamentos, diretores, gerentes e outros empregados, assim como aos servidores.

Os empregados, administradores, sócios, servidores e outras pessoas naturais são apenas vinculados à pessoa jurídica, ou uma entidade e seus atos expressam a atuação desta, podendo responder apenas posteriormente, em ação regressiva, nos termos da Consolidação das Leis do Trabalho, se empregados, por dolo, ou culpa, quando ajustado contratualmente e até serem dispensados por justa causa, ou nos termos de outras legislações para os demais, ao descumprirem as políticas internas de segurança da informação e instruções da empresa. Mesmo os sócios não responderão inicialmente, em eventual demanda judicial, mas sim a entidade, sem que haja inicialmente um incidente de desconsideração de personalidade jurídica, ou por sanções da ANPD.

Com exemplos específicos trazidos e retirados da experiência diária das autoridades de proteção de dados em guias e pareceres, neste pequeno artigo fizemos esforços para orientar e contribuí de forma clara, eficaz e didática, a respeito de uma das dúvidas com que mais nos deparamos nas entidades que iniciam esta nova jornada de conformidade, que não terá mais volta, devido ao avanço tecnológico que vivemos e tende a aumentar.

6. O CONSENTIMENTO DO TRABALHADOR E O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS PESSOAIS

TERESA COELHO MOREIRA¹³¹

1. O progresso da humanidade está, muitas vezes, associado ao fascínio perante a ciência e a tecnologia por originarem inovações que fazem avançar a humanidade: da roda ao microprocessador, do ábaco ao computador, da imprensa escrita à Internet e à *web*, *inter alia*¹³². E, atualmente, a Inteligência Artificial¹³³ veio para ficar e incide sobre inúmeros aspectos da vida das pessoas em geral e dos trabalhadores em especial desde o momento de formação do contrato de trabalho¹³⁴, passando pela execução do mesmo¹³⁵ e terminando na sua cessação¹³⁶. A própria União Europeia, num Documento de 8 de abril deste ano sobre *Linhas Éticas para uma Inteligência Artificial de Confiança*, estabeleceu que deveria defender-se sempre o respeito pela autonomia humana, pela transparência, pela privacidade e pela proteção de dados pessoais, assegurando a defesa da igualdade e a proibição da discriminação, defendendo sempre a pessoa humana nas suas várias vertentes. A

131 Doutora em Direito. Professora Auxiliar com Agregação da Escola de Direito da Universidade do Minho. Membro integrado do JusGov – Centro de Investigação em Justiça e Governação e Coordenadora do Grupo de Investigação em Direitos Humanos do mesmo. Coordenadora científica do *Livro Verde sobre o Futuro do Trabalho*. 2021.tmoreira@direito.uminho.pt

132 Ver o esquema com diferentes fases de evolução apresentado em JEAN-MICHEL RODES, GENEVIEVE PIEJUT e EMMANUELLE PLAS, *Memory of the Information Society*, UNESCO, Paris, 2003, p. 11.

133 Há que referir que não existe um conceito unívoco de Inteligência Artificial, principalmente porque tem de relacionar-se com outro conceito que também é difícil de definir e que é o de inteligência humana, e que a mesma coloca várias questões que ultrapassam, largamente, o âmbito deste nosso artigo. Mas, apenas para referir algumas, desde logo a questão da proteção e propriedade dos dados que constituem a base de trabalho para a Inteligência Artificial; ou questões relativas à responsabilidade, por exemplo, no caso dos carros autónomos; ou o direito à privacidade porque todos vamos deixando uma série de pistas digitais que permitem a comparação à entrada de determinados locais de uma cópia digitalizada e a imagem da pessoa em causa e, em especial no caso das relações de trabalho, o trabalhador encontra-se, por esta via, amplamente radiografado e informações colocadas online podem perdurar no ciberespaço por muito tempo, correndo o risco de ficarem completamente desatualizadas e com a inerente descontextualização dos dados.

134 Através de novas formas de contratação online, *inter alia*, com o recurso a um novo tipo de entrevistas, ou de recurso a plataformas digitais de emprego.

135 Através de, *inter alia*, um novo tipo de formação ao longo da vida, de um novo controlo, o controlo eletrónico/digital, um novo tempo de trabalho, ou de um novo tipo de Direito Coletivo.

136 Cf., para maiores desenvolvimentos, *inter alia*, OIT, *Trabalhar para um Futuro Melhor*, Genebra, 2019, e TERESA COELHO MOREIRA, *Direito do Trabalho na Era Digital*, Almedina, Coimbra, 2021 e “Algumas questões sobre o Regulamento Geral de Proteção de dados e as relações de trabalho”, in *O Regulamento Geral de Proteção de Dados e as Relações de Trabalho*, Estudos APODIT, volume VI (coordenação MARIA DO ROSÁRIO PALMA RAMALHO e TERESA COELHO MOREIRA), AAFDL, 2020 e WEF, *The Future of Jobs Report*, 2018.

própria OIT defendeu o mesmo quando propugna que deve fazer-se uma “uma abordagem da inteligência artificial baseada no “ser humano no comando”, que garanta que decisões finais que afetem o trabalho sejam tomadas por seres humanos”, e que “a gestão de algoritmos, a vigilância e o controlo através de sensores e de outras formas de monitorização precisam de ser regulados para proteger a dignidade dos trabalhadores. O trabalho não é uma mercadoria; nem é um robô”¹³⁷.

2. Por outro lado, o dom da ubiquidade é apanágio divino. Porém, atualmente, a Internet granjeou esse atributo, colocando cada vez mais incisivamente questões delicadas à privacidade. E a informática entronizou-se como um verdadeiro símbolo da nossa cultura, a tal ponto de se denominar a sociedade moderna como *sociedade informática ou sociedade de informação* e como a era da *Big Data*¹³⁸, que coloca novos desafios à privacidade das pessoas em geral, e dos trabalhadores em especial, parecendo dar-se prevalência ao valor económico relacionado com os dados pessoais e não ao seu valor jurídico¹³⁹. O computador transformou a economia, a sociedade, a cultura e, inclusive, o ser humano. Esta nova realidade não poderia passar à margem do Direito do trabalho, de maneira tal que hoje é corrente a expressão de *nudez tecnológica* do trabalhador, na medida em que existe uma automatização de dados sobre o mesmo que, muitas vezes, incide sobre aspectos que fazem parte da sua privacidade e que, por isso, estão protegidos e tutelados juridicamente. Estes dados tornaram-se uma nova forma de economia e com um alto valor económico e social.

3. Atendendo aos perigos inerentes a esta situação, a Comissão Europeia elaborou a 25 de janeiro de 2012 um “pacote de medidas” destinadas a alterar a regulamentação da proteção de dados pessoais numa espécie de *Revolução Copernicana*, apresentando uma Proposta de Regulamento sobre Proteção de Dados Pessoais. E, após um longo périplo legislativo, foi aprovado o Regulamento Geral de Proteção de Dados Pessoais 2016/679, de 27 de abril, que previa um período transitório de dois anos para a sua total aplicação, que aconteceu a 25 de maio de 2018, devendo as organizações utilizar aquele período de tempo para se adaptarem às novas regras.

4. Neste Regulamento existe o art. 88.º com a epígrafe *Tratamento no contexto laboral*, e que é bastante importante porque permite que “Os Estados-Membros possam estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção dos bens do empregador ou do cliente e para efeitos do exercício e gozo,

137 Última op. cit., p. 13, e p. 45.

138 OMER TENE e JULES POLONETSKY, “Privacy in the Age of Big Data: A Time for Big Decisions”, in *Stand. L. Rev. Online*, vol. 64, n.º 63, 2012, p. 63, assim como JOSHUA GRUENSPECHT, “Reasonable Grand Jury Subpoenas: Asking for Information in the Age of Big Data”, in *Harvard Journal of Law Technology*, vol. 24, n.º 2, 2011, pp. 544-545.

139 Neste sentido veja-se ROLF H. WEBER, “Big Data: Sprengkörper des Datenschutzrechts?”, in *Jusletter IT Die Zeitschrift für IT und Recht*, 11 de dezembro de 2013.

individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho, sendo que estas normas incluem medidas adequadas e específicas para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados, com especial relevo para a transparência do tratamento de dados, a transferência de dados pessoais num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta e os sistemas de controlo no local de trabalho, devendo os Estados-Membros notificarem a Comissão das disposições de direito interno que adotarem nos termos do n.º 1, até 25 de maio de 2018 e, sem demora, de qualquer alteração subsequente das mesmas”.

Este artigo resulta da consciencialização das inúmeras possibilidades de controlo através das novas tecnologias, assim como das diferenças em termos de proteção laboral relativamente ao tratamento de dados pessoais dos trabalhadores nos diferentes Estados-Membros.

Tendo em atenção a redação deste artigo e a ampla proteção conferida no Código do Trabalho relativamente a esta matéria, consideramos muito positivo que o legislador português o tenha acionado na Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, no art. 28.º - com a epígrafe *Relações laborais* - em que, no n.º 1, prevê que “o empregador pode tratar os dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no Código do Trabalho e respetiva legislação complementar ou noutros regimes setoriais, com as especificidades estabelecidas no presente artigo.”

5. A relação de trabalho exige, por vezes, o tratamento de inúmeros dados pessoais dos trabalhadores, na aceção do art. 4.º, n.º 1, do Regulamento Geral de Proteção de Dados Pessoais, assim como o tratamento dos mesmos¹⁴⁰, na medida em que é necessária a obtenção de informação e esta é arquivada, acedida e analisada. Vários são os dados que poderão ser alvo deste tratamento, desde dados pessoais como os CV, certificados de formação, candidaturas, notas de entrevistas, assim como dados pessoais sensíveis¹⁴¹, como sejam os dados biométricos, os dados de saúde, dados genéticos, ou, ainda, imagens de videovigilância ou dados de geolocalização. É ainda possível o tratamento de dados pessoais relacionados com a formação sobre quando o trabalhador iniciou a sua jornada de trabalho e quando terminou através de *logins* informáticos - que poderão utilizar o recurso a dados biométricos -, ou de sistemas de controlo de assiduidade, que também poderão utilizar estes mesmos dados.

6. Em primeiro lugar, tem-se desde logo a questão que surgiram e continuam a surgir constantemente novas tecnologias extremamente invasoras da privacidade das pessoas em geral e dos trabalhadores em especial e o Regulamento Geral teve isso em atenção. Surgem a todo o momento tecnologias de seguimento dos trabalhadores e das suas comunicações eletrónicas que podem violar a privacidade dos trabalhadores. Este monitoramento pode infringir os direitos de privacidade dos

140 Art. 4.º, n.º 2, do RGPD.

141 Cf. art. 9.º, n.º 1, do RGPD.

trabalhadores, independentemente de o mesmo ocorrer de forma sistemática ou ocasional. O risco não se limita à análise do conteúdo das comunicações. Assim, a análise de metadados sobre uma pessoa pode permitir um monitoramento detalhado, igualmente invasivo da privacidade, da vida e até dos padrões de comportamento de um trabalhador.

Na verdade, hoje em dia vivemos na sociedade de *Big Data*, onde imperam os megadados que se referem a conjuntos enormes de dados detidos por empresas, governos, entre outras entidades, que são depois amplamente analisados através de algoritmos e que resultam da confluência de várias tecnologias desde o *cloud-computing*, da Internet das Coisas, da Inteligência Artificial e das comunicações de banda muito larga¹⁴². Sendo assim, atendendo a esta enorme possibilidade de controlo, à diluição crescente entre o mundo *offline* e o *online* e a possibilidade de conexão com vários instrumentos de trabalho, o empregador tem de respeitar vários direitos dos titulares dos dados pessoais que são, no caso das relações de trabalho, os trabalhadores.

7. Uma das ideias presentes no Regulamento Geral de Proteção de Dados com enorme importância para a relação de trabalho é a definição de consentimento do titular de dados pessoais para tratamento de dados.

Na verdade, este Regulamento Geral retirou o acento tónico do consentimento como fundamento jurídico válido para o tratamento de dados pessoais quando, nos termos do considerando 43, “exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento”, como é o caso, claramente, da relação de trabalho. Este considerando é muito importante porque significa que, para que um tratamento de dados pessoais realizado pelo empregador seja válido, terá de assentar noutros princípios que não o mero consentimento do trabalhador. E esta ideia é reforçada quer pela redação do próprio art. 4.º, ao definir que o consentimento do titular dos dados é “uma manifestação de vontade, livre¹⁴³, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento”, quer pelo próprio art. 7.º, sobretudo os números 1 e 4, que estabelecem, respetivamente, que “quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais”, e que “ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive

142 Para maior informação, veja-se *Opinion 03/2013 on purpose limitation*, de 3 de abril de 2013, do Grupo de Proteção de Dados do art. 29.º.

143 Sublinhado nosso, sendo que este é o que falta numa relação de trabalho. As relações de trabalho são um exemplo paradigmático da existência de relações privadas desiguais não só no plano factual mas também no plano jurídico. Na verdade, no plano factual, os sujeitos contraentes – trabalhador e empregador – não dispõem da mesma liberdade no que concerne à celebração do contrato nem à estipulação de cláusulas contratuais, o que origina o aparecimento de um desequilíbrio contratual que se acentua em alturas de desemprego generalizado. No plano jurídico, a conclusão do contrato de trabalho coloca o trabalhador numa situação de subordinação face ao empregador. Assim, figurando-se o domínio económico e social de uma parte, não se pode invocar, sem mais, o princípio da liberdade contratual, para se poder escolher arbitrariamente a contraparte, ou seja, o trabalhador.

a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato”¹⁴⁴.

Parece-nos, sem dúvida, que a noção de consentimento, entendido como uma manifestação de vontade livre, específica e informada, é um conceito de difícil concretização e de difícil preenchimento no contexto de uma relação de trabalho e, por isso, saúda-se, vivamente, a redação e a clarificação realizada no Regulamento.

Na verdade, não pode deixar de atender-se a que o Direito do trabalho surgiu como um ramo do Direito que pretendia proteger os trabalhadores perante os arbítrios do empregador, sendo que a história laboral do Direito é, em boa medida, a dos limites aos poderes dos empregadores com o fim de proteger socialmente os trabalhadores. A sua autonomização alicerça-se na tentativa de superar as insuficiências da aplicação do Direito civil às relações contratuais laborais, onde a igualdade das partes era meramente formal. E se, inicialmente, a resposta passou pela consagração de determinados direitos coletivos, *maxime*, a liberdade sindical, ligada à ideia da despersonalização que acompanhou o trabalho na Revolução Industrial, rapidamente se começou a entender que os direitos dos trabalhadores poderiam ser ameaçados através de outras formas e meios, nomeadamente através da violação dos direitos de que era titular enquanto pessoa.

A relação laboral assenta, como é comumente aceite, na ideia de que as partes envolvidas não se encontram em pé de igualdade, apresentando-se o empregador como a parte contratual mais forte, dotada de um poder de conformação da prestação a que o trabalhador está submetido. Este, quando celebra um contrato de trabalho, aliena uma parte da sua autonomia e da sua liberdade, ficando colocado numa situação de dependência perante o empregador, que não se configura somente na ótica jurídica, mas também, quase sempre, na perspetiva económica, o que conduz à ideia defendida de que “com independência do que possam dizer os economistas, o trabalho não é uma mercadoria mas sim uma emanação da natureza humana, íntima e indissociavelmente unida a esta. O trabalhador não vende uma suposta energia laboral, separável da sua pessoa, antes, compromete na prestação laboral a sua própria pessoa”¹⁴⁵.

Considera-se que, no âmbito laboral, o requisito do consentimento fica relegado para um segundo plano, já que o trabalhador interessado se encontra numa

144 É interessante notar que o Grupo de Proteção de Dados Pessoais do art. 29.º, no seu Parecer 15/2011 sobre a definição de consentimento, de 13 de julho de 2011, já tinha defendido que, para que o consentimento fosse válido como legitimador do tratamento de dados pessoais, teria de ser livre, considerando que “o consentimento apenas será válido se a pessoa em causa puder exercer uma verdadeira escolha e não existir nenhum risco de fraude, intimidação, coação ou consequências negativas importantes se o consentimento for recusado. Se as consequências do consentimento comprometerem a liberdade de escolha da pessoa, o consentimento não será livre. A própria diretiva prevê, no artigo 8.º, n.º 2, alínea a), que, em certos casos, a serem determinados pelos Estados-Membros, a proibição de tratamento de categorias especiais de dados pessoais não pode ser ultrapassada pelo consentimento da pessoa em causa. Um exemplo disto é o caso em que a pessoa em causa está sob a influência do responsável pelo tratamento dos dados, como no caso de um vínculo laboral. Neste exemplo, embora não necessariamente, a pessoa em causa pode encontrar-se numa situação de dependência em relação ao responsável pelo tratamento dos dados - devido à natureza da relação ou a circunstâncias especiais - e pode temer retaliações se não consentir no tratamento dos seus dados”.

145 MELGAR, Antonio Montoya. *La buena fe en el Derecho del Trabajo*. Madrid: Tecnos, 2001, p. 9.

posição de desigualdade em relação ao responsável pelo tratamento, isto é, o empregador, desigualdade na sua necessidade de obtenção de um posto de trabalho, no caso dos candidatos a emprego, ou de manutenção do mesmo, no caso de trabalhadores. Não parece que neste tipo de relação se possa falar de um consentimento prestado livremente, principalmente quando o consentimento é requisito para a obtenção de um serviço essencial ou, no caso que aqui nos interessa, para a manutenção de um posto de trabalho, não podendo falar-se aqui de uma verdadeira liberdade de escolha¹⁴⁶.

Quando uma das partes está submetida ao poder contratual de outrem, não usufruindo de suficiente margem de defesa dos seus próprios interesses e de autoafirmação, o seu consentimento em relação ao contrato e aos vários termos deste não confere qualquer garantia substancial de integrar uma manifestação verdadeira de autodeterminação.

Na verdade, no Direito do trabalho não pode dar-se por adquirida, bem ao contrário, a ideia de que tudo funciona como no Direito Civil relativamente à figura do consentimento do lesado. É que na génese da separação das águas entre o Direito do trabalho e o Direito Civil está exatamente a ideia de que a igualdade formal não contribuía para um real equilíbrio negocial entre trabalhador e empregador. Este é o domínio onde é particularmente verdadeira a afirmação de Lacordaire de que “a liberdade oprime e a lei liberta”. A lei libertadora é o Direito do trabalho. Aqui o trabalhador encontra-se numa situação de inferioridade contratual perante o empregador e, por isso, o seu consentimento quase sempre é irrelevante. Assim, no que concerne ao consentimento do trabalhador, é necessário não só que seja um consentimento esclarecido mas, principalmente, que seja prestado livremente, isto é, sem qualquer tipo de pressão. Parece-nos que este é o requisito essencial para a aplicação desta figura e que, tendo em atenção o facto de o trabalhador ser o contraente mais débil da relação jurídico-laboral, raramente acontece¹⁴⁷.

146 O mesmo foi defendido pelo Grupo de Trabalho do art. 29.º, Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679, adotadas em 28/11/2017, última redação revista e adotada em 10/04/2018, p. 7, quando estabelecem que “Atendendo à dependência que resulta da relação empregador/trabalhador, é improvável que o titular dos dados possa recusar ao seu empregador o consentimento para o tratamento dos dados sem que haja medo ou risco real de consequências negativas decorrentes da recusa. É improvável que um trabalhador responda livremente ao pedido de consentimento do empregador para, por exemplo, ativar sistemas de controlo como a observação do local de trabalho através de câmaras ou preencher formulários de avaliação, sem sentir qualquer tipo de pressão para dar esse consentimento. Por conseguinte, o GT29 considera problemática a questão de os empregadores procederem ao tratamento de dados pessoais dos seus trabalhadores atuais ou futuros com base no consentimento, uma vez que é improvável que esse consentimento seja dado de livre vontade. Relativamente à maior parte deste tratamento de dados no local de trabalho, o fundamento legal não pode nem deve ser o consentimento dos trabalhadores [artigo 6.º, n.º 1, alínea a)], devido à natureza da relação entre empregador e trabalhador”.

147 Para Paulo Mota Pinto, “é necessário ter em atenção a verificação da “integridade do consentimento”, dado que em determinadas situações de necessidade “as pessoas podem ser levadas a limitar a reserva sobre a sua vida privada por temerem as consequências de uma eventual recusa”, dando como exemplo a relação entre o trabalhador e o empregador para o exercício de certas formas de controlo ou para a realização de determinados testes. Torna-se assim necessário existir uma “prevenção da liberdade e do esclarecimento do titular”. PINTO, Paulo Mota. *A limitação voluntária do direito à reserva sobre a intimidade da vida privada*. In: Estudos em Homenagem a Cunha Rodrigues. Coimbra:

Contudo, não pode deixar de ter-se em atenção que na relação laboral torna-se necessária a recolha de numerosas informações dos trabalhadores para a correta execução do contrato de trabalho, sendo, assim, este tratamento uma consequência quase *natural* deste tipo de relações. Atendendo a tudo isto, defende-se uma inevitável evolução no sentido de colocar o pressuposto legitimador do tratamento de dados pessoais não no consentimento individual do trabalhador mas na ampliação do número de pressupostos alternativos a este consentimento. Entende-se que deve assumir importância a técnica de tipo objetivo, isto é, que assente a legitimidade do tratamento no respeito pelo princípio da finalidade e no prosseguimento de fins específicos e não de outros, colocando o acento tónico neste princípio e na ideia do tratamento ser pertinente e necessário, respeitando sempre o princípio da proporcionalidade.

Esta construção parece-nos trazer uma maior dose de garantia do ponto de vista laboral, já que, ainda que o consentimento do trabalhador tenha sido prestado¹⁴⁸, se o tratamento não respeitar estes princípios, isto é, se não for pertinente, nem necessário, ou não tiver uma finalidade lícita, será sempre ilícito. O carácter irrenunciável dos direitos de personalidade a isso obsta¹⁴⁹.

8. Assim, tendo em atenção a irrelevância do consentimento, o tratamento de dados pessoais dos trabalhadores na relação de trabalho só poderá ser feito atendendo a certos princípios fundamentais que são os que já existem atualmente nos artigos 14.º a 22.º do CT, mas que agora foram de certa forma clarificados e reforçados pelo Regulamento Geral de Proteção de Dados Pessoais.

Desta forma, o único fundamento que pode legitimar o tratamento de dados pessoais na relação de trabalho é a prossecução de interesses legítimos da entidade empregadora aferíveis em função do caso concreto, e nos termos do art. 6.º, n.º 1, alínea b), do RGPD, quando o tratamento for necessário para a execução do contrato de trabalho.

Assim, o empregador, antes da adoção de qualquer medida de controlo eletrónico que implica um tratamento de dados pessoais do trabalhador que, ainda mais, podem ser sensíveis, tem de respeitar o princípio da finalidade. Este princípio está previsto no art. 5.º, n.º 1, alínea b), do Regulamento e significa que os dados de carácter pessoal apenas podem ser recolhidos quando existam motivos determinados, explícitos e legítimos, e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades, indicando que os dados pessoais dos trabalhadores só podem ser tratados se respeitarem estes pressupostos, sendo essencial a definição precisa destas finalidades.

Este princípio constitui o princípio verdadeiramente cardinal da proteção de dados, sendo os demais princípios função deste, na medida em que os dados devem ser adequados, pertinentes e não excessivos em relação à finalidade pretendida; devem ser exatos, completos e atualizados em função da finalidade; e só devem ser conservados pelo tempo que a finalidade exige.

Assim, a finalidade pretendida pelo empregador tem de ser legítima, isto é, deve estar em conformidade com o ordenamento jurídico e ser especialmente res-

Coimbra Editora, 2001, vol. 2, p. 539-540.

148 Sem a verdadeira liberdade que é essencial.

149 Para maiores desenvolvimentos, vd. TERESA COELHO MOREIRA, Direito do Trabalho, *op. cit.*

peitadora dos valores fundamentais.

O empregador terá, ainda, de respeitar sempre o princípio da proporcionalidade, previsto no art. 5.º, n.º 1, alínea c) do Regulamento Geral. Este princípio é considerado um princípio fundamental, sendo atualmente entendido como um princípio de controlo e um mecanismo de equilíbrio entre os diferentes direitos em causa, e tende a realizar a procura do equilíbrio entre as obrigações do trabalhador, que emanam do seu contrato de trabalho, e o âmbito de liberdade constitucional da sua privacidade, garantindo que a modulação deste direito fundamental vai ser realizada na medida estritamente imprescindível ao seu correto respeito, isto é, com as restrições na quantidade, na qualidade e no procedimento.

O empregador terá, por último, previamente à adoção de qualquer medida de controlo, de respeitar o princípio da transparência que consiste no conhecimento da vigilância e do controlo exercido pelo empregador, sendo essencial para o correto tratamento de dados pessoais das pessoas, em geral, e dos trabalhadores, em especial, devendo estes saber o como, quando, onde e de que forma o controlo é feito. Este direito, aliás, está reforçado no Regulamento Geral de Proteção de Dados.

Tendo em atenção a obrigatoriedade do princípio da transparência e da informação quer aos trabalhadores, quer aos seus representantes, depreende-se não ser admissível o controlo oculto ou secreto sobre os trabalhadores através destes meios por violar o princípio da boa-fé empresarial, que tem consagração expressa no CT nos arts. 102.º e 126.º.

7. PROTECCIÓN DE DATOS DE SALUD EN EL ÁMBITO LABORAL: UNA PERSPECTIVA ESPAÑOLA

*PROTECTION OF HEALTH DATA IN THE WORKPLACE:
A SPANISH PERSPECTIVE*

FRANCISCA RAMÓN FERNÁNDEZ¹

Resumen

En el presente trabajo se realiza un análisis de la regulación aplicable a la protección de datos de salud en el ámbito laboral teniendo en cuenta la legislación del Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Se atenderá a distintas perspectivas como son los datos de salud del trabajador en relación con distintas aplicaciones informáticas, así como los datos genéticos en relación con la privacidad y la intimidad. La metodología que vamos a utilizar se centra en el análisis de la legislación referida, así como distinta normativa relacionada con la salud. Los objetivos serán: determinar la protección que la legislación otorgar al trabajador en relación con sus datos de salud en el ámbito laboral. Las principales conclusiones del estudio indican que es preciso la regulación de la inteligencia artificial, así como la figura del donante de datos, con la finalidad de dotar de seguridad jurídica a los datos especialmente sensibles como es el caso de los datos de salud.

Palabras-clave: Protección de Datos. Relaciones laborales. Salud. Privacidad.

Abstract

In this work, an analysis of the regulation applicable to the protection of health data in the labor field is carried out in relation to the legislation of Regulation (EU) 2016/679, of April 27, 2016, regarding the protection of health physical persons in what concerns the processing of personal data and the free circulation of these data and the Organic Law 3/2018, of 5 December, of Protection of Personal Data and guarantee of digital rights. Different perspectives will be taken into account, such as the data of health of the worker in relation to different computer applications, as well as the genetic data in relation to privacy and intimacy. The methodology that we are going to use is centered on the analysis of the referred legislation, as well as a distinct normative related to health. The objectives will be: to determine the protection that the legislation grants to the worker in relation to his health data in the work environment. The main conclusions of the studio indicate that the regulation of artificial intelligence is needed, as well as the figure of the data giver,

¹ Licenciada y Doctora en Derecho por la Universitat de València, España. Actualmente es Profesora titular de Derecho civil adscrita a la Escuela Técnica Superior de Ingeniería del Diseño (ETSID) de la Universitat Politècnica de València. Ficha pública: <http://www.upv.es/ficha-personal/frarafer> ORCID: <https://orcid.org/0000-0002-0936-8229>. frarafer@urb.upv.es.

with the purpose of providing legal security to particularly sensitive data, such as in the case of health data.

Keywords: Data Protection. Work relationships. Health. Privacy.

1. Introducción

La protección de datos referente a la salud en el ámbito laboral plantea distintas cuestiones en relación con la utilización y destino de los datos. Partiendo de la Declaración Universal de los Derechos Humanos en que se indica que todos los seres humanos nacen libres e iguales en dignidad y derechos, y que todo individuo tiene derecho a la vida, a la libertad y a la seguridad de su persona.

Nos proponemos en el presente estudio realizar un análisis de la principal legislación aplicable a la protección de datos de salud en el ámbito laboral, por lo que analizaremos las siguientes normas, en lo que resulte aplicable:

a) Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos²;

a) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales³;

b) Ley 1/2019, de 20 de febrero, de Secretos Empresariales⁴;

c) Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público⁵;

Indicar que existe la Propuesta de Reglamento sobre gobernanza europea de datos (Ley de gobernanza de datos) contempla la cesión de datos con fines altruistas, así como la puesta a disposición de los mismos de forma voluntaria.

2. Datos del trabajo en el ámbito laboral: una perspectiva general

La mencionada Ley Orgánica 3/2018 establece una regulación específica en el ámbito de protección de datos en el ámbito de la salud.

El artículo 87 regula el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral, indicando lo siguiente:

1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador;

2. El empleador podrá acceder a los contenidos derivados del uso de medios

2 DOUE núm. 119, de 4 de mayo de 2016. Disponible en: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807>. Acceso el: 17 oct. 2021.

3 BOE núm. 294, de 06 de diciembre de 2018. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673>. Acceso el 17 oct. 2021. Véase también:

Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (BOE núm. 126, de 27 de mayo de 2021). Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2021-8806>. Acceso el: 17 oct. 2021.

4 BOE núm. 45, de 21 de febrero de 2019. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2019-2364>. Acceso el: 17 oct. 2021.

5 DOUE L 172/56, de 26 de junio de 2019. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=uriserv:OJ.L_.2019.172.01.0056.01.SPA. Acceso el: 17 oct. 2021.

digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos;

3. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores;

4. El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados;

5. Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.

Otros preceptos que resultan de interés son el artículo 89, que regula el derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo; el artículo 90, que se dedica al derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sónicos en el lugar de trabajo; el artículo 90, enfocado al derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral; el artículo 91, que contempla los derechos digitales en la negociación colectiva.

Junto a ello hay que indicar el artículo 20 bis del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, ⁶referente a los derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión.

3. Tratamiento de los datos de salud. Los datos genéticos

La Declaración Internacional sobre Datos Genéticos Humanos, de 16 de octubre de 2003, de la UNESCO, define los datos genéticos humanos como “información sobre las características hereditarias de las personas, obtenida por análisis de ácidos nucleicos u otros análisis científicos”.

Según la Ley 14/2007, de 2 de julio, de investigación biomédica⁷ el dato de carácter personal es una información sobre las características hereditarias de una persona. Se indica que es obtenida por análisis de ácidos nucleicos u otros análisis científicos.

Dentro de las categorías especiales de datos se encuentran los datos referentes a la salud, tal y como indica el artículo 9 de la Ley Orgánica 3/2018. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

La Disposición adicional decimoséptima de la Ley Orgánica 3/2018, respeto

⁶ BOE núm. 255, de 24 de octubre de 2015. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2015-11430>. Acceso el: 17 oct. 2021.

⁷ BOE núm. 159, de 4 de julio de 2007. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-2007-12945>. Acceso el: 19 oct. 2021.

del tratamiento de los datos de salud, establece una serie de criterios de dicho tratamiento en consonancia con lo que indica el Reglamento (UE) 2016/679:

1. Se encuentran amparados en las letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679 los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados en las siguientes leyes y sus disposiciones de desarrollo:

a) La Ley 14/1986, de 25 de abril, General de Sanidad.

b) La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

c) La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

d) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

e) La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.

f) La Ley 14/2007, de 3 de julio, de Investigación biomédica.

g) La Ley 33/2011, de 4 de octubre, General de Salud Pública.

h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

i) El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio.

j) El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre.

2. El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios:

a) El interesado o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.

b) Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública.

c) Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.

En tales casos, los responsables deberán publicar la información establecida por el artículo 13 del Reglamento (UE) 2016/679 del Parlamento

Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.

Para los tratamientos previstos en esta letra, se requerirá informe previo favorable del comité de ética de la investigación.

d) Se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica.

El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá:

1º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.

2º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando:

i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.

ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.

e) Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, a los efectos del artículo 89.2 del Reglamento (UE) 2016/679, podrán excepcionarse los derechos de los afectados previstos en los artículos 15, 16, 18 y 21 del Reglamento (EU) 2016/679 cuando:

1º Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados.

2º El ejercicio de tales derechos se refiera a los resultados de la investigación.

3º La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley.

f) Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación

en salud pública y, en particular, biomédica, se procederá a:

1° Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.

2° Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.

3° Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.

4° Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679.

g) El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial.

En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679.

h) En el plazo máximo de un año desde la entrada en vigor de esta ley, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados.

En cuanto a los principios rectores específicos aplicables a los datos genéticos podemos destacar el derecho a la intimidad, y el respeto a la autonomía de la voluntad, y la confidencialidad de los datos genéticos⁸. Junto a ello se establece la prohibición de comerciar con los datos genéticos de carácter personal. Destaca en la regulación la necesidad de consentimiento por escrito y expreso para el tratamiento de los datos genéticos de carácter personal. Se establece también el deber de confidencialidad y el derecho a la protección de los datos genéticos, indicando que deben ser conservados durante cinco años⁹.

8 Véase más ampliamente sobre la confidencialidad: RAMÓN FERNÁNDEZ, Francisca. La mediación electrónica, la confidencialidad y la protección de datos de carácter personal. InDret. Revista para el análisis del Derecho, n. 3, p. 1-28, 2014. Disponible en: <https://indret.com/la-mediacion-electronica-la-confidencialidad-y-la-proteccion-de-datos-de-caracter-personal/>. Acceso el: 17 oct. 2021.

9 Se puede consultar: RAMÓN FERNÁNDEZ, Francisca. Transparencia y protección de datos especialmente protegidos en genética y la salud desde el punto de vista civil y del buen gobierno.

La normativa que hemos indicado, tanto el Reglamento (UE) 2016/679 como la Ley Orgánica 3/2018, por lo que se refiere a la protección de datos de salud, y especialmente los datos genéticos, establece la prohibición del tratamiento de los datos genéticos, y los datos relativos a la salud; determina las excepciones por interés público esencial, medicina preventiva o laboral, y por salud pública. Indica las razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y seguridad sanitarios y de productos, incluidos medicamentos. Y también se indica si se utiliza con fines de archivo en interés público, de investigación científica, histórica o estadística.

Se admite la reutilización de los datos personales con fines de investigación en salud y biomedicina, en los casos de obtención del consentimiento para una finalidad concreta, y su posterior utilización para finalidades o áreas de investigación relacionadas con el área del estudio inicial. Hay que atender a lo indicado en el Reglamento (UE) 2016/679 respecto a la información: identidad, fines de tratamiento, destinatarios...

Se considera como lícito la utilización de datos personales que hayan sido seudonimizados con fines de investigación en salud y biomedicina. Hay que tener en cuenta la separación técnica y funcional del equipo y las personas que anonimicen los datos, atender a los supuestos de reidentificación, y las garantías y excepciones en el caso de tratamiento con fines de archivo en interés público.

En el tratamiento con fines de investigación en salud pública y biomedicina, hay que atender a los siguientes aspectos:

- a) Evaluar el impacto para conocer los riesgos;
- d) La investigación científica deberá ser sometida a las normas de calidad;
- e) La adopción de medidas destinadas a garantizar que los investigadores no accedan a datos de identificación de los interesados;
- f) Representante legal.

Por su parte, el artículo 88 contempla el tratamiento en el ámbito laboral.¹⁰ De esta forma, dispone el precepto lo siguiente:

Diario La Ley, p. 1-15, 2018; La sanidad móvil: la protección de datos referentes a la salud y la genética. En: RAMÓN FERNÁNDEZ, Francisca (coord.). Marco Jurídico de la Ciencia de Datos (pp. 197-250). Valencia: Tirant lo Blanch, 2020; El acceso a los datos y contenidos gestionados por prestadores de servicios de la sociedad de la información de personas fallecidas: análisis de los límites. Revista métodos de información, v. 11, n. 20, p. 31-58, 2020. DOI: <https://doi.org/10.5557/IIMEI11-N20-059087>. Disponible en: <http://www.metodosdeinformacion.es/mei/index.php/mei/article/view/IIMEI11-N20-059087/1006>. Acceso el: 17 oct. 2021; Inteligencia artificial en la relación médico-paciente: Algunas cuestiones y propuestas de mejora. Revista Chilena de Derecho y Tecnología, v. 10, n. 1, p. 329-351, 2021. DOI: 10.5354/0719-2584.2021.60931. Disponible en: <https://rchdt.uchile.cl/index.php/RCHDT/article/view/60931>. Acceso el: 17 oct. 2021.

¹⁰ Véase: RAMÓN FERNÁNDEZ, Francisca. Instalación de cámaras ocultas de videovigilancia en el trabajo en la jurisprudencia del TEDH. En: RUDA GONZÁLEZ, A. y JEREZ DELGADO, C. (dir.), KUBIKA, M. L. (coord.). Estudios sobre Jurisprudencia Europea. Materiales del V Encuentro anual del Centro español del European Law Institute (pp. 59-73). Madrid: Sepin, 2021. Disponible en: https://www.sepin.es/tienda-online/articulo/articulo.aspx?id_articulo=6616. Acceso el: 17 oct. 2021.

1. Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

2. Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.

En relación con los convenios colectivos y los convenios de empresa se pueden establecer normas específicas referente al tratamiento de datos personales de los trabajadores dentro de su ámbito del trabajo, por ejemplo, en relación con las condiciones de los datos personales y su tratamiento previo el consentimiento del trabajador, los fines de la contratación, la ejecución del contrato laboral, gestión, organización y planificación del trabajo, la igualdad y seguridad, así como la salud y el disfrute de derechos y prestaciones laborales a efectos de la rescisión de la relación laboral.

4. El consentimiento informado y los datos

Respecto al consentimiento informado, tenemos que tener en cuenta la normativa siguiente: Ley 10/2014, de 29 de diciembre, de la Generalitat, de salud de la Comunitat Valenciana¹¹, modificada por Ley 8/2018, de 20 de abril, de modificación de la Ley 10/2014, de 29 de diciembre, de salud de la Comunitat Valenciana¹². Se indica en el artículo 43, la prestación del consentimiento puede ser verbal o escrito (en el caso de intervenciones, procedimientos diagnósticos y terapéuticos invasores y, en general, ante la aplicación de procedimientos que supongan riesgos o inconvenientes de notoria y previsible repercusión negativa sobre la salud del paciente).

Relación del consentimiento informado con el derecho fundamental de la integridad física y moral. En el ámbito nacional, destaca la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica¹³. Indica que el consen-

11 BOE núm. 35, de 10 de febrero de 2015. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2015-1239>. Acceso el: 20 oct. 2021.

12 BOE núm. 117, de 14 de mayo de 2018. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-2018-6402>. Acceso el: 20 oct. 2021.

13 BOE núm. 274, de 15 de noviembre de 2002. Disponible en: <https://www.boe.es/buscar/act>.

timento informado es la conformidad libre, voluntaria y consciente de un paciente, manifestada en el pleno uso de sus facultades después de recibir la información adecuada, para que tenga lugar una actuación que afecta a su salud.

5. Los datos empresariales: el secreto empresarial

Actualmente se aplica la Ley 1/2019, de 20 de febrero, de Secretos Empresariales.

Las organizaciones valoran sus secretos empresariales tanto como los derechos¹⁴ de propiedad industrial e intelectual, y utilizan la confidencialidad como una herramienta de gestión de la competitividad empresarial, de transferencia de conocimiento público-privada y de la innovación en investigación, con el objetivo de proteger información que abarca no solo conocimientos técnicos o científicos, sino también datos empresariales relativos a clientes y proveedores, planes comerciales y estudios o estrategias de mercado.

Todo tratamiento de datos de carácter personal que deba efectuarse en virtud de los apartados precedentes se llevará a cabo de conformidad con la normativa de la Unión Europea y española en materia de protección de datos de carácter personal¹⁵.

6. Los donantes de datos: aplicación en el ámbito laboral

Son distintas las aplicaciones¹⁶ relacionadas con la salud que comparten datos. Sin embargo, estos datos están anonimizados, y un profesional de la medicina no podría acceder a los mismos e identificar al paciente, por lo que no podría intervenir a tiempo ante una incidencia médica.

Pero si nosotros somos donantes de datos, permitimos dar a conocer esta información, y puede ser de gran utilidad para la predicción médica (avisarnos el médico de un riesgo inminente).

Los datos médicos gozan del máximo nivel de protección, pero también disponer de ellos puede ser indispensable para avanzar en la investigación. ¿Se podrían “expropiar” los datos médicos en aras de un fin superior al individual? Podría plantearse si se podría recurrir a la figura de la expropiación aplicable a la propiedad privada, en el caso de datos médicos que puedan ser necesarios para un bien de la colectividad. Ello también se relaciona con el ODS 3 relativo a Salud y Bienestar, ya que tanto la inteligencia artificial, como los datos médicos pueden contribuir a alcanzarlo.

php?id=BOE-A-2002-22188. Acceso el: 20 oct. 2021.

14 BOE núm. 45, de 21 de febrero de 2019. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2019-2364>. Acceso el: 20 oct. 2021. Cfr. RAMÓN FERNÁNDEZ, Francisca. Secretos empresariales en documentos y ficheros electrónicos y la protección de datos personales y garantía de los derechos digitales. Tabula, n. 22, p. 73-92, 2019.

15 RAMÓN FERNÁNDEZ, Francisca. La normativa de protección de datos y derechos digitales en el ámbito de los recursos humanos: un reto para la sociedad y la legislación. En: ¿Se puede crear capital social? Innovación y tecnología: retos para los recursos humanos de las organizaciones, (pp. 197-250). Valencia: Tirant lo Blanch, 2019.

16 RAMÓN FERNÁNDEZ, Francisca. La protección de datos en las aplicaciones móviles de diagnóstico de enfermedades genéticas. Un estudio jurídico. Revista métodos de información, v. 8, n. 14, p. 5-25, 2017. DOI: <https://doi.org/10.5557/mei.v8i14.829>. Disponible en: <http://www.metodosdeinformacion.es/mei/index.php/mei/article/view/IIMEI8-N14-005025/940>. Acceso el: 17 oct. 2021.

Sería necesario establecer una regulación específica sobre la figura del donante de datos.

7. La discriminación del trabajo por datos de salud

La Ley 4/2018, de 11 de junio, por la que se modifica el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por Real Decreto Legislativo 1/2007, de 16 de noviembre¹⁷, se orienta a evitar la discriminación en el ámbito de la salud en relación con los datos personales. La presente ley encuentra su origen en la iniciativa aprobada por el Pleno del Parlamento de Navarra, en su sesión de 19 de enero de 2017, en el ejercicio de las previsiones contenidas en el artículo 87.2 de la Constitución. La finalidad de esta modificación normativa se encuentra en la necesidad de erradicar del ordenamiento jurídico aquellos aspectos que limiten la igualdad de oportunidades y promuevan la discriminación por cualquier motivo, en este caso, por ser portadoras del VIH/SIDA, u otras condiciones de salud, en lo que respecta al ámbito de contenidos discriminatorios en determinados negocios jurídicos, prestaciones o servicios¹⁸.

8. Los datos y el trabajo a distancia

La Ley 10/2021, de 9 de julio, de trabajo a distancia¹⁹, establece en su artículo 17 la regulación del derecho a la intimidad y a la protección de datos:

1. La utilización de los medios telemáticos y el control de la prestación laboral mediante dispositivos automáticos garantizará adecuadamente el derecho a la intimidad y a la protección de datos, en los términos previstos en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, de acuerdo con los principios de idoneidad, necesidad y proporcionalidad de los medios utilizados.

2. La empresa no podrá exigir la instalación de programas o aplicaciones en dispositivos de propiedad de la persona trabajadora, ni la utilización de estos dispositivos en el desarrollo del trabajo a distancia.

3. Las empresas deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos legal y constitucionalmente. En su elaboración deberá participar la representación legal de las personas trabajadoras.

Los convenios o acuerdos colectivos podrán especificar los términos dentro de los cuales las personas trabajadoras pueden hacer uso por motivos personales de los equipos informáticos puestos a su disposición por

17 BOE núm. 142, de 12 de junio de 2018. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-2018-7832>. Acceso el: 20 oct. 2021.

18 Así, RAMÓN FERNÁNDEZ, Francisca. Discriminación por condiciones de salud. Protección de datos y consumidores: una reflexión tras la reforma de la Ley General para la defensa de los consumidores y usuarios. *Revista de Derecho Privado*, n. 1, p. 47-61, 2019.

19 BOE núm. 164, de 10 de julio de 2021. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2021-11472>. Acceso el: 20 oct. 2021.

parte de la empresa para el desarrollo del trabajo a distancia, teniendo en cuenta los usos sociales de dichos medios y las particularidades del trabajo a distancia.

9. Datos del trabajador y situación de pandemia por la COVID-19

El control empresarial de la temperatura corporal de los trabajadores ante la vicisitud de la covid-19 plantea distintas cuestiones en relación a las garantías de los derechos fundamentales, y la determinación de los límites respecto a la realización de dicho test de temperatura. Se discute si se vulnera o no la privacidad del trabajador, ya que estamos ante un dato sensible. La finalidad era la necesidad de prevención de los contagios, pero ello puede entrar en conflicto con la protección de los datos de salud del trabajador²⁰.

La limitación del derecho fundamental a la protección de datos para el tratamiento de los datos personales (datos de salud y datos de localización con fines epidemiológicos) encontraría su fundamento en la protección de intereses vitales del interesado y de terceros (artículo 6.2 c) RGPD), en un deber de colaboración basado en la seguridad pública y en la competencia de la autoridad según el artículo 3 de la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública para adoptar medidas oportunas para el control de los enfermos.

10. Conclusiones

Impera realizar una utilización responsable de los datos por parte de las entidades. Estamos hablando de sujetos, de personas, y debe privilegiarse los derechos de las mismas.

Es preciso articular de forma clara la figura del donante de datos, para que los datos que se compartan sean seguros y se mantenga la privacidad, las vías legales oportunas y teniendo en cuenta la decisión del individuo de donar dichos datos, ya que prima el principio de autonomía de la voluntad.

Los datos son el elixir de la medicina del futuro, una medicina que se caracterizará por la predicción ayudada por la inteligencia artificial. Si la medicina del siglo 20 fue preventiva, la del siglo 21 es predictiva, anticipándose a las enfermedades que podamos padecer, y precisamente para poder disponer de aplicaciones de diagnóstico y tratamiento que se basan en los datos facilitados y que le permitirá diseñar tratamientos “diana” para combatirlos, precisamente basándose en la información de otras personas que la hayan padecido anteriormente, a través de sus datos.

Por tanto, si donar órganos salva vidas, donar datos también salva vidas. Parametrizar los comportamientos y las probabilidades resultará de vital importancia.

Agradecimientos

Trabajo realizado en el marco del Proyecto I+D+i «Retos investigación» del

20 RAMÓN FERNÁNDEZ, Francisca. El derecho a la vida y a la protección de la salud en las medidas adoptadas en España como consecuencia de la covid-19. Una reflexión sobre su oportunidad. Estudios Constitucionales, v. 18, n. 2, p. 51-86, 2020. DOI: 10.4067/S0718-52002020000200051. Disponible en: <https://scielo.conicyt.cl/pdf/estconst/v18n2/0718-5200-estconst-18-02-51.pdf>. Acceso el: 17 oct. 2021.

Programa estatal de I+D+i orientado a los Retos de la Sociedad del Ministerio de Ciencia, Innovación y Universidades RTI2018-097354-B-100 (2019-2022) y Proyecto de I+D+i Retos MICINN (PID2019-108710RB-I00, 2020-2022), y Grupo de Investigación de Excelencia Generalitat Valenciana “Algorithmical Law” (Proyecto Prometeu 2021/009, 2021-2024).

REFERENCIAS

RAMÓN FERNÁNDEZ, Francisca. Discriminación por condiciones de salud. Protección de datos y consumidores: una reflexión tras la reforma de la Ley General para la defensa de los consumidores y usuarios. *Revista de Derecho Privado*, n. 1, p. 47-61, 2019.

RAMÓN FERNÁNDEZ, Francisca. El acceso a los datos y contenidos gestionados por prestadores de servicios de la sociedad de la información de personas fallecidas: análisis de los límites. *Revista métodos de información*, v. 11, n. 20, p. 31-58, 2020. DOI: <https://doi.org/10.5557/IIMEI11-N20-059087>. Disponible en: <http://www.metodosdeinformacion.es/mei/index.php/mei/article/view/IIMEI11-N20-059087/1006>. Acceso el: 17 oct. 2021.

RAMÓN FERNÁNDEZ, Francisca. El derecho a la vida y a la protección de la salud en las medidas adoptadas en España como consecuencia de la covid-19. Una reflexión sobre su oportunidad. *Estudios Constitucionales*, v. 18, n. 2, p. 51-86, 2020. DOI: 10.4067/S0718-52002020000200051. Disponible en: <https://scielo.conicyt.cl/pdf/estconst/v18n2/0718-5200-estconst-18-02-51.pdf>. Acceso el: 17 oct. 2021.

RAMÓN FERNÁNDEZ, Francisca. Instalación de cámaras ocultas de video-vigilancia en el trabajo en la jurisprudencia del TEDH. En: RUDA GONZÁLEZ, A. y JEREZ DELGADO, C. (dir.), KUBIKA, M. L. (coord.). *Estudios sobre Jurisprudencia Europea. Materiales del V Encuentro anual del Centro español del European Law Institute* (pp. 59-73). Madrid: Sepin, 2021. Disponible en: https://www.sepin.es/tienda-online/articulo/articulo.aspx?id_articulo=6616. Acceso el: 17 oct. 2021.

RAMÓN FERNÁNDEZ, Francisca. Inteligencia artificial en la relación médico-paciente: Algunas cuestiones y propuestas de mejora. *Revista Chilena de Derecho y Tecnología*, v. 10, n. 1, p. 329-351, 2021. DOI: 10.5354/0719-2584.2021.60931. Disponible en: <https://rchdt.uchile.cl/index.php/RCHDT/article/view/60931>. Acceso el: 17 oct. 2021.

RAMÓN FERNÁNDEZ, Francisca. La mediación electrónica, la confidencialidad y la protección de datos de carácter personal. *InDret. Revista para el análisis del Derecho*, n. 3, p. 1-28, 2014. Disponible en: <https://indret.com/la-mediacion-electronica-la-confidencialidad-y-la-proteccion-de-datos-de-caracter-personal/>. Acceso el: 17 oct. 2021.

RAMÓN FERNÁNDEZ, Francisca. La normativa de protección de datos y derechos digitales en el ámbito de los recursos humanos: un reto para la sociedad y la legislación. En: *¿Se puede crear capital social? Innovación y tecnología: retos para los recursos humanos de las organizaciones*. Valencia: Tirant lo Blanch, 2019, p. 197-250.

RAMÓN FERNÁNDEZ, Francisca. La protección de datos en las aplicaciones móviles de diagnóstico de enfermedades genéticas. Un estudio jurídico. Revista métodos de información, v. 8, n. 14, p. 5-25, 2017. DOI: <https://doi.org/10.5557/mei.v8i14.829>. Disponible en: <http://www.metodosdeinformacion.es/mei/index.php/mei/article/view/IIMEI8-N14-005025/940>. Acceso el: 17 oct. 2021.

RAMÓN FERNÁNDEZ, Francisca. La sanidad móvil: la protección de datos referentes a la salud y la genética. En: RAMÓN FERNÁNDEZ, Francisca (coord.). Marco Jurídico de la Ciencia de Datos (pp. 197-250). Valencia: Tirant lo Blanch, 2020.

RAMÓN FERNÁNDEZ, Francisca. Secretos empresariales en documentos y ficheros electrónicos y la protección de datos personales y garantía de los derechos digitales. Tabula, n. 22, p. 73-92, 2019.

RAMÓN FERNÁNDEZ, Francisca. Transparencia y protección de datos especialmente protegidos en genética y la salud desde el punto de vista civil y del buen gobierno. Diario La Ley, p. 1-15, 2018.

8. PROTEÇÃO DE DADOS E O SISTEMA JUDICIAL PORTUGUÊS – UMA SÍNTESE

DATA PROTECTION AND THE PORTUGUESE JUDICIAL SYSTEM – A SYNTHESIS

JOSÉ JOAQUIM FERNANDES OLIVEIRA MARTINS¹*

“A justiça está entre a piedade e a crueldade: o justo propende para a parte de piedoso, o justiceiro para a de cruel”

PADRE ANTÓNIO VIEIRA, *Comento ou Homilia sobre o Evangelho da segunda-feira da primeira semana de Quaresma*

Resumo

Partindo do regime atualmente vigente em Portugal para a proteção de dados pessoais, reflete-se sobre a sua aplicação e compatibilização no âmbito do sistema judicial português.

Palavras-chave: Proteção de dados pessoais; Regulamento Geral sobre a Proteção de Dados; Sistema judicial.

Abstract

Based on the regime currently in force in Portugal for the protection of personal data, consideration is given to its application and compatibility in the Portuguese judicial system.

Keywords: Protection of personal data; General Data Protection Regulation; Judicial system.

1. Introdução

1.1 As sociedades hodiernas têm, mais recentemente, “acordado” para as questões relativas à proteção de dados pessoais, embora, como o refere ISABEL MARIA CURTO TEIXEIRA, “A preocupação com a proteção dos dados pessoais não é um fenómeno recente nem um epifenómeno passageiro”.

De resto, Portugal foi algo precursor nesta matéria, uma vez que, com o seu Art. 35.º, a Constituição da República Portuguesa “apresentou-se como pioneira na proteção constitucional dos cidadãos perante o tratamento de dados pessoais informatizados, procedendo ao reconhecimento e garantia daquilo que a doutrina portuguesa, por inspiração germânica, veio a designar de «direito à autodeterminação informacional ou informativa»”.

Como referem GOMES CANOTILHO/VITAL MOREIRA, *Constituição da República Portuguesa Anotada*, 3.ª Edição, Coimbra, 1993, p. 215-216, este artigo garante “um conjunto de direitos fundamentais em matéria de *defesa contra o tratamento informático de dados pessoais*”:

“(a) direito de acesso das pessoas aos registos informáticos para conhecimento dos seus dados pessoais deles constantes (n.º 1), bem como a retificação e complementação dos mesmos; (b) direito ao sigilo em relação aos responsáveis de fichei-

¹ Licenciado e Mestre em Direito pela Faculdade de Direito da Universidade de Coimbra. Juiz de Direito no Juízo do Trabalho da Figueira da Foz, Portugal.

ros automatizados e a terceiros dos dados pessoais informatizados e direito à sua não interconexão (n.º 2); (c) direito ao não tratamento informático de certos tipos de dados pessoais”, que integram o “*direito à autodeterminação informacional*”.

Efetivamente, sucedem-se as intervenções do legislador nesta matéria, na União Europeia, em Portugal e no Brasil, como se passará a expor.

Assim, tal ocorreu na União Europeia, por via, desde logo, do Artigo 8.º da Convenção Europeia dos Direitos do Homem (“Direito ao respeito pela vida privada e familiar 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros”), do Artigo 8.º da Carta dos Direitos Fundamentais da União Europeia (“Proteção de dados pessoais 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente”), e, mais detalhada e recentemente, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados Regulamento Geral sobre a Proteção de Dados Europeu (doravante Regulamento).

Em Portugal, essa intervenção, mais recentemente, ocorreu com a Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica portuguesa, do Regulamento (UE) 2016/679 já referido, e, no Brasil, com a Lei Geral de Proteção de Dados Pessoais Brasileira, que tem muitos pontos de contacto com esse Regulamento.

Toda esta atividade legislativa resulta, desde logo, do facto de estarmos em plena Revolução Digital, também designada de Quarta Revolução Industrial, assentando no avançado desenvolvimento tecnológico e informático e que deu origem à atual sociedade global de comunicação e informação globalizada, em que são muito importantes os *Big Data*/Megadados.

Assim,

Uma nova era está a surgir, estimulada por um conjunto de tecnologias disruptivas dos quais são bons exemplos a robótica, a inteligência artificial, a realidade aumentada, o *big-data*, a nanotecnologia, a biologia, a genética e a internet das coisas. Esta revolução industrial não se caracteriza por ter uma tecnologia hegemónica, mas pela convergência e sinergia entre elas.

De facto, os dados pessoais vão ser, em larga medida, um dos principais ativos económicos a ter em conta futuramente, falando-se, por exemplo e na esteira de MANUEL CASTELLS, do surgimento do capitalismo informacional global, sendo a sua titularidade, o acesso aos mesmos e a sua utilização questões muito importantes a resolver pelo ordenamento jurídico, que se tem desdobrado em intervenções legislativas, procurando, primordialmente, salvaguardar os direitos dos titulares desses dados.

Em suma,

o convulsivo contexto de digitalização da vida social a que vimos assistindo nas últimas décadas, incrementou a dispersão da informação pessoal dificultando, na prática, as possibilidades de conhecimento e controlo do seu titular. O imperativo da proteção de dados pessoais tem sido, justamente, assegurar esse conhecimento e controlo.

E ainda,

Em larga medida, a legislação sobre proteção de dados pessoais parte de um pressuposto geral: a posição de vulnerabilidade e de desvantagem estrutural das pessoas singulares numa sociedade marcada pela circulação de fluxos informacionais, de várias origens, com vários destinos e finalidades.

2 . Proteção de dados em Portugal

Como já se referiu, a proteção de dados pessoais em Portugal assenta, atualmente, na aplicação do Regulamento Geral sobre a Proteção de Dados e da Lei n.º 58/2019, de 8 de agosto, não cabendo (minimamente) no âmbito deste artigo fazer uma análise detalhada e minuciosa desses dois instrumentos normativos, bastante complexos, de resto, mas apenas breves e esparsas referências ao regime que resulta dos mesmos, em particular ao primeiro (uma vez que o segundo apenas “assegura a execução, na ordem jurídica interna” desse Regulamento).

O Regulamento Geral sobre a Proteção de Dados “estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados” (Art. 1.º, n.º 1), sendo que “defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais” (n.º 2), aplicando-se ao “tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinado” (Art. 2.º, n.º 1).

Este Regulamento prevê, no seu Art. 5.º, uma série de princípios relativos ao tratamento de dados pessoais – licitude, lealdade e transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação, integridade e confidencialidade e responsabilidade, que são depois desenvolvidos e con-

cretizados nos artigos seguintes, prevendo também categorias especiais de dados pessoais, com um regime muito diverso.

Existe também, neste Regulamento, uma norma específica relativa ao tratamento de dados pessoais relacionados com condenações penais e infrações: “O tratamento de dados pessoais relacionados com condenações penais e infrações ou com medidas de segurança conexas com base no artigo 6.º, n.º 1, só é efetuado sob o controlo de uma autoridade pública ou se o tratamento for autorizado por disposições do direito da União ou de um Estado-Membro que prevejam garantias adequadas para os direitos e liberdades dos titulares dos dados. Os registos completos das condenações penais só são conservados sob o controlo das autoridades públicas” (Art. 10.º).

Por seu lado, é evidente que o direito à proteção dos dados pessoais não é um direito absoluto, antes podendo conflitar com outros direitos ou interesses tutelados pelo direito comunitário e nacional, pelo que o legislador comunitário acabou por recorrer ao princípio da concordância prática, tentando “harmonizar da melhor maneira os preceitos divergentes” e preservar, o mais possível, os valores em conflito, sacrificando-os proporcionalmente de acordo com vários fatores (conteúdo e função destes, as várias soluções do caso concreto), sem pôr em causa o seu conteúdo essencial, exigindo-se, claro, “que o sacrifício de cada um dos valores constitucionais seja necessário e adequado à salvaguarda dos outros”.

Deste modo e procurando realizar essa concordância prática, o Art. 23.º, n.º 1 deste Regulamento dispõe que “O direito da União ou dos Estados-Membros a que estejam sujeitos o responsável pelo tratamento ou o seu subcontratante pode limitar por medida legislativa o alcance das obrigações e dos direitos previstos nos artigos 12.º a 22.º e no artigo 34.º, bem como no artigo 5.º, na medida em que tais disposições correspondam aos direitos e obrigações previstos nos artigos 12.º a 22.º, desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para assegurar, designadamente: a) A segurança do Estado; b) A defesa; c) A segurança pública; d) A prevenção, investigação, deteção ou repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública; e) Outros objetivos importantes do interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, incluindo nos domínios monetário, orçamental ou fiscal, da saúde pública e da segurança social; f) A defesa da independência judiciária e dos processos judiciais; g) A prevenção, investigação, deteção e repressão de violações da deontologia de profissões regulamentadas; h) Uma missão de controlo, de inspeção ou de regulamentação associada, ainda que ocasionalmente, ao exercício da autoridade pública, nos casos referidos nas alíneas a) a e) e g); i) A defesa do titular dos dados ou dos direitos e liberdades de outrem; j) A execução de ações cíveis”.

Outra expressão desta tentativa de compatibilizar vários direitos consta também do Art. 85.º do Regulamento, que diz respeito à liberdade de expressão e de informação, uma vez que essas liberdades, essenciais em qualquer estado de direi-

to democrático, podem ser colocadas em causa por uma tutela excessiva ou desproporcionada dos dados pessoais, prescrevendo que “1. Os Estados-Membros conciliam por lei o direito à proteção de dados pessoais nos termos do presente regulamento com o direito à liberdade de expressão e de informação, incluindo o tratamento para fins jornalísticos e para fins de expressão académica, artística ou literária. 2. Para o tratamento efetuado para fins jornalísticos ou para fins de expressão académica, artística ou literária, os Estados-Membros estabelecem isenções ou derrogações do capítulo II (princípios), do capítulo III (direitos do titular dos dados), do capítulo IV (responsável pelo tratamento e subcontratante), do capítulo V (transferência de dados pessoais para países terceiros e organizações internacionais), do capítulo VI (autoridades de controlo independentes), do capítulo VII (cooperação e coerência) e do capítulo IX (situações específicas de tratamento de dados) se tais isenções ou derrogações forem necessárias para conciliar o direito à proteção de dados pessoais com a liberdade de expressão e de informação”, como sucede igualmente, agora para permitir a transparência e a fiscalização da atividade das instituições públicas, no Art. 86.º, com a seguinte redação: “Os dados pessoais que constem de documentos oficiais na posse de uma autoridade pública ou de um organismo público ou privado para a prossecução de atribuições de interesse público podem ser divulgados pela autoridade ou organismo nos termos do direito da União ou do Estado-Membro que for aplicável à autoridade ou organismo público, a fim de conciliar o acesso do público a documentos oficiais com o direito à proteção dos dados pessoais nos termos do presente regulamento”.

Finalmente, cabe referir que a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016 “estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública” (Art. 1.º, n.º 1), prevendo, nesse âmbito muito específico, um regime algo diverso do Regulamento já aludido (sendo que a Lei n.º 59/2019, de 8 de agosto, “Aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais”, transpondo para o direito português esta Diretiva).

3. Sistema judicial português

3.1 O Art. 202.º, n.º 1 da Constituição da República Portuguesa dispõe que “Os tribunais são os órgãos de soberania com competência para administrar a justiça em nome do povo”, sendo que “As audiências dos tribunais são públicas, salvo quando o próprio tribunal decidir o contrário, em despacho fundamentado, para salvaguarda da dignidade das pessoas e da moral pública ou para garantir o seu normal funcionamento” (Art. 206.º).

Extrai-se desta última norma a importância que o legislador constitucional deu à publicidade e à consequente transparência do funcionamento dos tribunais, ligada também à sua legitimidade e legitimação perante o “povo”, sendo a exceção, só admitida em situações muito específicas, a não publicidade das audiências judiciais.

E, como é natural, o funcionamento do sistema judicial português assenta tam-

bém na recolha, utilização e consideração de dados que constam dos processos judiciais, incluindo dados pessoais, uma vez que

os organismos públicos e as polícias também não podem prescindir de todas as funcionalidades que as novas tecnologias oferecem, mormente no que tange à prestação de serviços públicos essenciais e à prevenção da criminalidade. Sublinhe-se que as empresas e o próprio Estado necessitam, de forma ímpar, nos nossos dias, de cada vez mais informação para prosseguirem as suas missões.

Esses dados pessoais são, aliás, de natureza muito sensível, bastando pensar, por exemplo, nos dados que constam nos processos criminais ou laborais e nos danos que poderiam causar aos seus titulares se fossem objeto de divulgação pública ou cedidos ilicitamente a terceiros.

Em Portugal, onde os processos judiciais são agora todos eles eletrónicos, é evidente que, face à possibilidade de intrusões ilegítimas nas redes de dados judiciais, há uma grande necessidade de proteção dos dados pessoais constantes dos mesmos, que deve depois ser compatibilizada com o funcionamento do próprio sistema judicial, como se verá na secção seguinte.

4. Proteção de dados e finalidades, pressupostos e funcionamento do sistema judicial

4.1 Como acabou de se referir, é necessário efetuar uma (sempre difícil) concordância prática entre as finalidades e os pressupostos essenciais de qualquer sistema judicial, que dizem respeito, por exemplo, aos direitos fundamentais garantidos aos sujeitos processuais (como, desde logo, o direito ao contraditório), e a tutela dos dados pessoais que estão recolhidos nos respetivos processos judiciais.

Seria, assim, necessário que em Portugal se previsse a forma de execução no sistema judicial do regime constante no Regulamento, o que ainda não sucedeu e causa bastantes dificuldades quanto ao modo concreto como esse Regulamento se aplica nesta matéria, dado que

Quanto à Lei de Execução do RGPD para o sistema judicial, no Decreto que resultou da Proposta de Lei nº 126/XIII, o legislador conferia aos magistrados judiciais e do MP a responsabilidade pelo tratamento de dados no âmbito de processos da sua competência, e excluía, expressamente, a CNPD da supervisão do tratamento efetuado no exercício das funções e competências processuais dos tribunais e do Ministério Público. Ora, o diploma, objeto de veto presidencial, ressuscitava a Comissão para a Coordenação da Gestão dos Dados Referentes ao Sistema Judicial, que passaria a designar-se Comissão de Coordenação da Gestão da Informação do Sistema

Judiciário. Esta Comissão teria uma nova composição e competências acrescidas. Na fundamentação preambular do legislador, o objetivo seria “prevenir a intervenção de uma autoridade administrativa no exercício de funções judiciais, assegurando-se o respeito pela independência dos tribunais e pela autonomia do Ministério Público”.

Ora,

o Decreto em apreço foi devolvido ao Parlamento, nos termos constitucionais, tendo o Presidente da República considerado que o modelo escolhido pelo legislador – de autoridade de controlo e de autoridade de coordenação – não garantia o cumprimento, na ordem jurídica interna, do RGPD, quanto às áreas específicas de funções dos Tribunais, no exercício da independência da função jurisdicional, e do Ministério Público, no desempenho, com autonomia, das suas funções e competências processuais.

Desta forma e lamentavelmente, é ainda a Lei n.º 34/2009 de 14 de julho, que “Estabelece o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial”, o que

coloca problemas especialmente complexos e controversos, sobretudo no respeitante à determinação do(s) responsável(eis) pelo tratamento do dados, com a(s) correspondente(s) responsabilidade(s) proativa(s) (*accountability*, Art.º 5.º n.º 2, 24.º, 25.º e 32.º do RGPD) e a inerente imputabilidade das responsabilidades civil (Art.º 82.º do RGPD e Art.º 33.º da Lei n.º 58/2019, de 8 de agosto, a segura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679) e contraordenacional (Art.º 83.º do RGPD, Art.ºs 37.º a 45.º da Lei n.º 58/2019 e, ainda, a Lei n.º 67/2007, de 31 de dezembro, aprova o regime da responsabilidade civil extracontratual do estado e demais entidades públicas).

De todo o modo, ocorreram, mais recentemente, algumas alterações legislativas relativas à proteção de dados pessoais no sistema judicial, uma vez que

O DL n.º 97/2019, de 26/07 introduziu alterações relevantes nas normas do Código de Processo Civil relacionadas com o tratamento informático dos processos e com a sua publicidade, que convocam novos desafios de conjugação do mesmo com o RGPD, exigindo quer às Secretarias Judiciais, quer aos Magistrados Judiciais deveres

acrescidos de verificação da concordância entre a publicidade dos processos e o RGPD.

Efetivamente, o Art. 132.º, n.º 4 do Código de Processo Civil Português tem atualmente a seguinte redação: “A tramitação eletrónica dos processos deve garantir a respetiva integralidade, autenticidade e inviolabilidade, bem como o respeito pelo segredo de justiça e pelos regimes de proteção e tratamento de dados pessoais e, em especial, o relativo ao tratamento de dados referentes ao sistema judicial”, acabando por transpor, diretamente, para o domínio da legislação adjetiva civil parte dos princípios constantes do Regulamento.

Assim,

(b) A tramitação eletrónica do processo corre na plataforma Citius (art. 3.º, n.º 1, RTE [Portaria n.º 280/2013, de 26 de agosto, na sua redação atual]), a qual deve assegurar as garantias e cumprir os requisitos estabelecidos no n.º 4. Entre essas garantias consta a proteção de dados pessoais nos termos do estabelecido no RGPD (tb L 34/2009, de 14/7)

Por sua vez, o Art. 164.º, n.º 3 do Código de Processo Civil tem agora a seguinte redação: “O acesso a informação do processo também pode ser limitado, em respeito pelo regime legal de proteção e tratamento de dados pessoais, quando, estando em causa dados pessoais constantes do processo, os mesmos não sejam pertinentes para a justa composição do litígio”, de onde se retira:

(a) Dos dados pessoais que constam do processo só devem ser fornecidos (mesmo às partes) aqueles que sejam pertinentes para a “justa composição do litígio” (n.º 3). (b) Os art. 27.º ss. L 34/2009, de 14/7, estabelecem regras sobre o acesso de dados pessoais constantes do processo. O regime abrange o regime da consulta por “utilizadores” (art. 29.º L 34/2009) e dentro destes, com diferentes restrições, por magistrados e f.j. (art. 30.º L 34/2009), pelas partes e respetivos m.j. (art. 31.º L 34/2009) e pelos magistrados do MP (art. 32.º L 34/2009). (c) O art. 34.º L 34/2009 ressalva o direito de acesso ao processo, mas este direito, além de só poder exercido nas condições definidas no art. 163.º, n.o 2, também só pode ser exercido com as limitações imposta pela própria L 34/2009. 6 (a) Qualquer questão relacionada com o acesso aos dados pessoais que constam dos autos é apreciada pelo juiz do processo (art. 23.º, al. b), L 34/2009). (b) A decisão do juiz constitui um ato administrativo judicial. A decisão é sempre recorrível em um grau, independentemente do valor da causa.

Analisando estes normativos, cumpre referir que

se podem levantar questões delicadas em processos que em princípio serão públicos, com vista até a salvaguardar

os Magistrados titulares de cada processo, na medida em que assim o entendam relevante, salienta-se que há inúmeros casos de processos, por defeito públicos à luz dos citados preceitos, e que por isso passaram a poder ser consultados por via eletrónica, sem que sequer seja aventado interesse legítimo, nomeadamente nos termos do art. 27.º, n.º 4 da Portaria n.º 280/2013 de 26 de Agosto. Ora tais processos podem conter dados que por via do RGPD não devem ser acessíveis ao público nesses termos.

De todo o modo, continua a mesma autora,

Deste enquadramento decorre que não está em causa a legitimidade do acesso e tratamento de tais dados por parte do Tribunal, para a apreciação e decisão da causa, pois tal acesso não é sequer abrangido ou regulado pelo RGPD e o art. 9º reitera essa licitude. Cuida-se aqui apenas do acesso, da publicidade a terceiros que nada têm a ver com a causa e que não têm sequer que justificar a necessidade ou finalidade desse acesso. Nessas situações, consagra-se assim nas recentes alterações ao Código de Processo Civil supra referidas a possibilidade, e com ela a responsabilidade, de restringir a publicidade desses processos com fundamento no RGPD. A concreta forma de restrição dessa publicidade não está definida na lei nem em qualquer procedimento ou ferramenta informática, atualmente, cabendo assim a cada concreto Magistrado titular definir os moldes em que o desejar fazer ou considerar adequado no processo.

Como se alcança, todas estas normas procuram dar uma solução equilibrada para os potenciais conflitos que possam existir entre a proteção dos dados pessoais constantes de processos judiciais e a forma de funcionamento constitucionalmente consagrada e prevista do sistema judicial, procurando compatibilizar, adequar e preservar o essencial desses dois valores constitucionalmente consagrados, sendo, todavia, importante, que seja regulamentada, a breve trecho, a forma de execução do Regulamento no sistema judicial português, em termos consonantes com o regime resultante do Regulamento e com a própria arquitetura constitucional desse sistema.

4.2 Outro problema (grave) que se suscita em Portugal é o da titularidade e controlo das redes de dados, sistemas e programas informáticos em que é efetuada a tramitação eletrónica dos processos judiciais, dado que é o Ministério da Justiça, por intermédio do Instituto de Gestão Financeira e Equipamentos da Justiça, I.P., que os tem na sua tutela e controlo.

Ora, atendendo à independência dos tribunais constitucionalmente prevista,

que é, a meu ver, colocada em causa quando as principais ferramentas informáticas pelas quais se administra a justiça (que é agora em larga medida uma justiça digital e até telemática) estão sob controlo do poder executivo, entende-se que deveria competir aos Conselhos Superiores (da Magistratura, dos Tribunais Administrativos e Fiscais e do Ministério Público) a gestão e a tutela dessas redes e sistemas informáticos e a definição/criação/manutenção, com a audição dos magistrados e de outros operadores judiciais, dos programas informáticos nos quais são tramitados os processos judiciais.

Assim, considera-se que deverão ser esses Conselhos Superiores a serem os responsáveis pela proteção dos dados pessoais constantes destes processos, cumprindo com as obrigações previstas no Regulamento, sob pena de, no fundo, existirem duas entidades com responsabilidades concorrentes ou de os magistrados judiciais serem responsabilizados por algo em que nunca tiveram qualquer intervenção efetiva.

Esta assunção das respetivas responsabilidades pelos Conselhos Superiores é, assim, importante para que o sistema judicial possa acautelar os riscos inerentes à existência de dados pessoais muito sensíveis em processos eletrónicos e que podem ser objeto de ciberataques, sendo fundamental que se mantenham circunscritos a esses processos e à sua utilização no próprio sistema judicial ou para outras finalidades legítimas e previstas legalmente.

De facto,

para garantir a proteção dos dados pessoais, é necessário saber quais os perigos que existem no ciberespaço, na maior parte das vezes, desconhecidos de cada um de nós, e reconhecer as fragilidades técnicas e humanas existentes, sendo certo que só através do equilíbrio entre estes dois vetores será possível assegurar a proteção de dados pessoais de uma forma segura e condizente com a realidade atual.

Assim, é também necessário que o próprio sistema judicial (e não antes a tutela política do sistema de justiça) assuma como sua a necessidade de tutela destes dados pessoais e de cumprimento das obrigações previstas no Regulamento, sem o que lhe poderá ser imputado tudo o que de mal ocorra a este respeito (a “justiça”, como um todo inorgânico, acaba por ser, muitas vezes, culpada de tudo o que corre de mal no sistema judicial), o que não se basta, de todo o modo, com meras alterações legislativas, dado que

Com o aumento dos Ciberataques, a proteção dos dados pessoais está, mais do que nunca, dependente da Cibersegurança, pelo que tentar proteger aqueles sem o recurso a esta última torna-se um desígnio ilusório e que dependerá, não apenas de alterações legislativas, mas sobretudo da melhoria das medidas de segurança que venham a ser implementadas e da forma como são executadas.

4.3 Como se sabe, em muitos países existem bases de dados de decisões judiciais, em especial dos tribunais superiores, livremente acessíveis e disponíveis *online*, sendo que

A análise informatizada de dados do Poder Judiciário pode auxiliar tanto magistrados quanto advogados e servidores públicos. No lado dos tribunais é possível viabilizar mais racionalidade, celeridade e efetividade à prestação jurisdicional. Já para os advogados, muitas aplicações podem se mostrar atrativas, principalmente no que se refere a justiça preditiva: pode-se, por exemplo, determinar a posição dominante de um tribunal sobre casos específicos, verificar quais acórdãos e obras doutrinárias costumam ser referenciados, e até mesmo calcular a probabilidade de sucesso em uma ação judicial.

Porém, é também claro que essas bases de dados, em especial se reproduzirem integralmente as decisões judiciais, podem conter dados pessoais ou elementos que permitem facilmente a identificação das partes e dos dados relativos às mesmas. É, pois, importante que, como sucede em Portugal, esses dados pessoais sejam retirados das decisões, permitindo que as mesmas cumpram esse papel relevante já aludido supra, sem que coloquem a descoberto dados pessoais dos diversos sujeitos ou intervenientes processuais.

De resto, há países europeus que vão ainda mais longe, como sucedeu em França com a “Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice”, cujo Art. 33° prescreve agora que as decisões judiciais são colocadas à disposição do público de forma gratuita e na forma eletrónica, mas os nomes e apelidos das pessoas físicas aí mencionadas são ocultadas previamente, podendo também ser ocultados (para proteger, por exemplo, a sua segurança) os dados dos próprios magistrados e oficiais de justiça, sendo que, em todos os casos, esses dados relativos aos magistrados não podem ser reutilizados para avaliar, analisar, comparar ou prever as suas práticas profissionais.

Se se compreende alguma preocupação do legislador com a utilização destes dados por sistemas de inteligência artificial, em particular para prever decisões futuras, a verdade é que dificilmente se poderia aceitar, entre nós, que existissem decisões judiciais divulgadas publicamente, sem que se soubesse quem as subscreveu, sendo curioso ver como decorrerá a aplicação prática desta lei em França e as suas consequências futuras.

Conclusão

Escreveu-se no Acórdão do Tribunal Constitucional Português n.º 403/2015 que

A introdução de novas tecnologias digitais nas redes de comunicações públicas trouxe consigo uma grande capacidade e possibilidade de tratamento de dados pessoais, e determinou a necessidade de acautelar novos requisitos específicos de proteção de dados pessoais e da privacidade dos utilizadores. De facto, os novos meios de comunicação, disponíveis a um custo cada vez menor e

acessíveis a um número cada vez maior de pessoas vieram multiplicar os riscos para a privacidade dos seus utilizadores.

Se a revolução digital deu origem a um “mundo novo” digital, globalizado e em que o contacto interpessoal e o acesso à informação nunca foi tão fácil e rápido, é também verdade que acarreta muitos riscos e perigos, em particular no que diz respeito à proteção dos dados pessoais de todos nós.

A nossa “pegada digital” é cada vez maior e pode, se não houver essa tutela dos danos pessoais, colocar em causa a nossa reserva da vida privada, o que também poderá suceder, de forma muito grave, se não forem protegidos e utilizados devidamente os dados pessoais (ou até pessoalíssimos) que constam dos processos judiciais em que temos alguma intervenção.

Cumpre, pois, efetuar uma adequada ponderação entre essa evidente necessidade de tutela e as funções, finalidades e direitos inerentes aos processos judiciais, que estão numa evidente tensão dialética, sendo importante que o legislador português adequa a forma de funcionamento do sistema judicial ao Regulamento Geral sobre a Proteção de Dados, que veio, no fundo, revolucionar a forma concreta como eram protegidos esses dados no espaço europeu.

Em resumo, procurou dar-se um pequeno (e muito modesto) contributo, mais de síntese do que propriamente inovador e vindo de quem está dentro desse sistema e aí trabalha quotidianamente, para abordar algumas das questões relativas à proteção de dados pessoais em Portugal e à sua operacionalização no âmbito do sistema judicial português, constituindo mais um simples ponto de partida do que um verdadeiro ponto de chegada.

NOTAS

1 Proteção de dados e processo civil – Recentes alterações legislativas e novas problemáticas, p. 1, consultado, tal como os restantes textos com essa referência, online em 24/10/2021 (refira-se que, devido ao período de tempo decorrido entre a elaboração do texto e a sua revisão final, verificou-se que parte dos textos consultados já não estão disponíveis ou terão sido deslocados para outros sítios, tendo também existido dificuldades na formatação do texto para a sua edição final por efeito da inserção das respetivas hiperligações, pelo que se optou por as retirar e fazer unicamente a menção que a fonte foi consultada online).

2 Francisca Cardoso Resende Gomes, O conteúdo do direito fundamental à proteção de dados à luz do novo Regulamento Geral de Proteção de Dados: em especial, a problemática do controlo das decisões automatizadas in Anuário da Proteção de Dados 2020, p. 106, consultado online.

3 E já antes na Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, revogado pelo Regulamento, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, cumprindo destacar igualmente a Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro de 1981, que “foi o primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados. Visa «garantir [...] a todas as pessoas singulares [...] o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal». O Protocolo que altera a Convenção visa alargar o seu âmbito de aplicação, aumentar o nível de proteção de dados e melhorar a sua eficácia” – consultado online.

4 Cfr., sobre as suas semelhanças e diferenças, Manuel David Masseno, GDPR [RGPD] E LGPD: similaridades e diferenças, consultado online.

5 E também, subsequentemente, doutrinal e jurisprudencial, tratando-se de uma área do direito que tinha anteriormente uma relevância muito mais reduzida e que agora assumiu quase que uma nova centralidade, desde logo por ter uma evidente repercussão na atividade diária das empresas e de outras instituições, incluindo as estatais.

6 Ou ainda Indústria 4.0 – cfr. Luciana da Silva Ribeiro/Paulo Resende da Silva, Impacto da Indústria 4.0 nas organizações, na perspectiva do Brasil e Portugal in Revista da UI_IPSantarém. Edição Temática: Ciências Exatas e Engenharias 8(4), p. 153, consultado online, escrevendo que “Nas palavras de Klaus Schwab (2016) «estamos no início de uma revolução que está mudando fundamentalmente, a forma como vivemos, trabalhamos e nos relacionamos um com o outro»”.

7 Adotando esta última designação em português e dando uma explicação para o surgimento deste conceito, v. Manuel David Masseno, Como a União Europeia procura proteger os cidadãos consumidores em tempos de Big Data, p. 3, consultado online: “Simplificando, a Big Data resulta da confluência de três avanços tecnológicos, de origem diferente, mas que se reforçaram entre si. Designadamente, decorre da Computação em Nuvem, a qual passou a possibilitar o armazenamento de volumes crescentes de dados, com disponibilidade permanente e uma fiabilidade assegurada pela redundância, tudo isto com custos cada vez menores. A que se juntaram as comunicações de banda muito larga, em fibra ótica e ponto a ponto, com velocidades de acesso tais que deixaram de ser necessário manter centros de dados próprios, também com custos decrescentes. A ambas, acresceram algoritmos de análise assentes em Inteligência Artificial, mais do que em força bruta computacional, ainda que distribuída, pelo menos na pendência da computação quântica, os quais vieram acrescentar a viabilidade de gerir pacotes cada vez maiores de dados, em tempo real. Finalmente, a proliferação de sensores interligados, a que se tem dado o nome de Internet das Coisas, ou de Tudo, conduziu ao multiplicar da informação disponível, a qual respeita sempre e em definitiva aos cidadãos-consumidores”.

8 Paulo Novais/Pedro Miguel Freitas, Inteligência Artificial e Regulação de algoritmos, p. 6, consultado online.

9 Jéssica Andrade Modesto, Breves considerações acerca da monetização de dados pessoais na economia informacional à luz da Lei Geral de Proteção de Dados Pessoais, p. 38, consultado online, “a economia cada vez mais é marcada por modelos de negócios que utilizam os dados pessoais para as mais diversas finalidades. Na era do big data, a ordem é coletar o máximo de dados que se conseguir antes mesmo de saber se tais informações serão úteis. Isso porque esses dados podem ser tratados de forma a auxiliar a tomada de decisão, bem como serem submetidos a procedimentos que podem agregar bastante valor às organizações empresárias”. Aliás, existem já hoje os chamados “data brokers”, que “têm como núcleo de negócio a alienação ou a cedência de dados pessoais de utilizadores ou consumidores, criando assim uma verdadeira comercialização de dados pessoais” – Tamára Chales, Os Desafios dos Consumidores na Era de Big Data in Anuário da Proteção de Dados 2021, p. 161, consultado online.

10 Marc Pirogan, Digital Society Blog – Making sense of our connected world, consultado online, “Castells observes the formation of a new kind of capitalism that he calls “global informational capitalism”, or in short “informationalism”. This new system is characterized by the processing of knowledge and information through technologies. Networks constitute a pivotal element of this new socio-economic arrangement and represent the organizational logic of society. Networks are defined as “a set of interconnected nodes” that follow very adaptable, open-ended and decentralized structures (Castells, 1996, p. 470)”.

11 Dado que existem evidente “riscos para o âmbito de proteção do direito à reserva sobre a intimidade da vida privada. Estes riscos foram potenciados pela globalização digital e intrínseca inexistência de fronteiras, e justificaram a autonomização do direito à proteção de dados pessoais, cujo bem jurídico tutelado é a privacidade na sua dimensão de direito à autodeterminação informacional, atenta a utilização da informação pessoal que, em última instância, sempre deverá servir a pessoa humana e não, apenas, os interesses das organizações (públicas ou privadas)” – Patrícia Cardoso Dias, Proteção de dados pessoais no contexto da pandemia provocada pelo novo coronavírus SARS-COV-2: aspetos ético-jurídicos relevantes da proteção de dados de saúde no âmbito da emergência de saúde pública, p. 4, consultado online.

12 Graça Canto Moniz, Direitos do titular dos dados pessoais: o direito à portabilidade in Anuário da Proteção de Dados 2018, p. 12, consultado online.

13 Graça Canto Moniz, ob. e loc. cit.

14 Que contém a seguinte definição de dados pessoais: “Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular” (Art. 4.º, 1)).

15 V., sobre as obrigações decorrentes deste Regulamento, por todos e detalhadamente, Teresa Vale Lopes, Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados in Anuário da Proteção de Dados 2018, p. 45-69, consultado online.

16 Sendo certo que já existe jurisprudência em Portugal sobre a relação entre este Regulamento e o direito de acesso aos documentos administrativos – Acórdão do Tribunal Central Administrativo Norte de 21/5/2021, consultado online, e sobre a sua compatibilização com a junção de prova documental em processo laboral (no caso, recibos de vencimento de trabalhadores) – Acórdão da Relação de Coimbra de 26/6/2020, consultado online, sendo de esperar que futuramente surjam muitas mais decisões que se refiram expressamente a este Regulamento.

17 “É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa” – Art. 9.º, n.º 1, sendo que este princípio tem, nos números seguintes, várias exceções e derrogações, em que avulta, por exemplo e numa das temáticas – o consentimento explícito – mais abordadas doutrinariamente, “Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas” (n.º 2, al. a).

18 E muito restritiva face à natureza dos dados em causa, obrigando a que fiquem sob sujeitos ao controlo estatal ou com garantias acrescidas.

19 Vieira de Andrade, Os Direitos Fundamentais na Constituição Portuguesa de 1976, reimpressão, Coimbra, Almedina, 1987, p. 220.

20 Vieira de Andrade, ob. e loc. cit..

21 Prevendo a possibilidade de restrições legalmente previstas aos direitos e obrigações previstos no Regulamento, face aos interesses em causa que justificam essas derrogações e sempre com um limite inultrapassável – “desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática”.

22 Sem analisar mais pormenorizadamente esta Diretiva (que, no fundo, acaba por ter algumas regras idênticas ou similares às do Regulamento, embora adaptando-as ou restringindo os direitos dos titulares dos dados pessoais em função da específica finalidade a que se destina o seu tratamento), temos que na mesma, para além de só se impor a existência de “prazos adequados para o apagamento dos dados pessoais ou para a avaliação periódica da necessidade de os conservar” (Art. 5.º), se preveem diferentes categorias de titulares de dados (e igualmente entre categorias especiais de dados pessoais, em termos similares aos que constam do Regulamento – Art. 10.º), como, desde logo, vítimas, suspeitos e condenados (Art. 6.º), devendo haver uma distinção clara entre essas categorias, dispondo também que os “dados pessoais baseados em factos sejam, na medida do possível, distinguidos dos dados pessoais baseados em apreciações pessoais” (Art. 7.º). Cfr., sobre as diferenças entre o Regulamento e esta Diretiva, Raquel Alexandra Brízida Castro, Proteção de dados e a Diretiva EU 2016/680: O tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais in Cibercriminalidade e Prova Digital, p. 14-15, consultado online.

23 Sendo certo que a secção da Constituição da República Portuguesa relativa aos tribunais é algo lacónica e espalha-se por muito poucos artigos.

24 Que poderá, assim, saber de que forma funcionam os tribunais portugueses e apreciar, criticamente, as decisões dos mesmos e os fundamentos inerentes às mesmas, assistindo, desde logo, aos julgamentos que estiverem na base desses concretos atos jurisdicionais.

25 Inês Oliveira Andrade de Jesus, O direito à proteção de dados pessoais e o regime jurídico das transferências internacionais de dados: a proteção viaja com as informações que nos dizem respeito?

in Anuário da Proteção de Dados 2018, p. 72, consultado online.

26 Verbi gratia, dados relativos à vida pessoal de arguidos e vítimas, como os que dizem respeito crimes cometidos/sofridos e às suas concretas circunstâncias fácticas, bem como dados respeitantes à sua condição pessoal, situação económica e familiar (como sucede com os dados recolhidos nos relatórios sociais relativos a arguidos com vista a aferir da espécie e da medida da pena a aplicar aos mesmos a final).

27 Dados relativos a remunerações e ao seu pagamento e à forma como é prestado o trabalho (horas de entrada e saída), etc.

28 Raquel Alexandra Brízida Castro, ob. cit., p. 13.

29 Raquel Alexandra Brízida Castro, ob. cit., p. 14.

30 Assim, Manuel David Masseno, no excelente e seminal artigo A segurança no tratamento de dados no sistema judicial, em Portugal e no Brasil (cit. A Segurança...), consultado online, que acompanhamos nesta parte de perto, referindo que “continua vigente a Lei n.º 34/2009, na medida em que não contrarie o disposto no RGPD” – p. 148

31 Manuel David Masseno, A Segurança..., loc. cit..

32 Isabel Maria Curto Teixeira, ob. cit., p. 4.

33 Que tem muita importância, dado que o Código de Processo Civil é aplicável subsidiariamente quanto a várias outras legislações adjetivas, como sucede no direito processual laboral ou administrativo.

34 Miguel Teixeira de Sousa, CPC ONLINE: art. 130.º a 149.º, p. 4, consultado online.

35 Miguel Teixeira de Sousa, CPC ONLINE: art. 150.º a 185.º, p. 21, consultado online.

36 Isabel Maria Curto Teixeira, ob. cit., p. 6.

37 Isabel Maria Curto Teixeira, ob. cit., p. 7.

38 Existindo em vários ordenamentos jurídicos europeus normas similares relativas aos sistemas judiciais e com base também neste Regulamento, sendo que o próprio Tribunal de Justiça da União Europeia tem igualmente já várias normas internas relativas aos dados pessoais constantes dos processos que aí correm termos.

39 Neste sentido, “Há, sim, que se procurar estabelecer o diálogo entre estas diferentes fontes normativas, a fim de extrair uma interpretação sistémica que prestigie a proteção de dados pessoais nos casos em que efetivamente exista a necessidade de manter os atos processuais em segredo, nas hipóteses previstas no Código de Processo Civil, não servido a LGPD, de rigor, como meio para alargamento das hipóteses legais já existentes, sob pena de retrocedermos as conquistas obtidas quanto à efetivação do princípio da publicidade e transparência na atuação jurisdicional, em afronta à Constituição Federal” – Dânton Zanetti, Proteção de dados pessoais e publicidade processual: Um contrassenso?, consultado online.

40 Art. 203º da Constituição da República Portuguesa – “Os tribunais são independentes e apenas estão sujeitos à lei”.

41 Em sentido aproximado, escreve Manuel David Masseno, A Segurança..., p. 149, que se está perante as “consequências de uma decisão de base no que se refere ao funcionamento do Sistema Judicial português, a do controle dos meios materiais afetos ao Órgão de Soberania tribunais por parte do Governo, através do Ministério da Justiça”, sendo que “Por isso mesmo e em atenção ao critério presente no RGPD para identificar o «Responsável pelo tratamento», i.e., além das “finalidades”, determina “os meios” e aplica as “medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento”, em especial no atinente aos riscos de segurança (Art.ºs 4.º 7), 24.º n.º 1, 25.º e 32.º n.º 1), este apenas pode ser o Ministério da Justiça, com a inerente assunção de responsabilidades, com a intervenção específica da respetiva Encarregada da Proteção de Dados (Designada pelo Despacho n.º 5643/2018, de 6 de julho). O que ocorrerá em termos dissociados das demais funções dos responsáveis pelo tratamento, sejam estes os Tribunais, o CSM ou o CSTAF”.

42 Diogo Lopes Alves, O papel fundamental da Cibersegurança na Proteção de Dados Pessoais in Anuário da Proteção de Dados 2021, consultado online, p. 122.

43 Diogo Lopes Alves, ob. cit., p. 124.

44 Aline Macohin/João Victor Vieira Carneiro, Web crawling e web scraping em sites de tribunais: Publicidade processual e proteção de dados pessoais nas experiências europeia e brasileira in

Proteção de dados pessoais em perspectiva, p. 535, consultado online.

45 Aline Macohin/João Victor Vieira Carneiro, ob. cit., p. p. 551, escrevem que “Na prática, vários países europeus já anonimizam há algum tempo as decisões,²⁴ tendo em vista que a exposição dos dados pessoais das partes do processo não cumprem os principais propósitos da publicidade das decisões: a transparência do processo decisório e a divulgação de avanços jurisprudenciais (OPIJNEN, 2019, p. 85). A opção pelo termo anonimização, todavia, é questionável, pois ainda há a possibilidade de reidentificar as partes por meio de «quase-identificadores» (quasi-identifiers), por exemplo; dito isto, na maior parte dos casos ocorre somente a pseudonimização dos dados”.

46 Acórdão do Tribunal Constitucional n.º 403/2015, consultado online.

47 Embora seja importante assegurar que a informação disponibilizada online é verídica e fidedigna, no que tem sido uma das grandes dificuldades do mundo cibernético e tem tido repercussões políticas e sociais.

9. O DIREITO AO ESQUECIMENTO, A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) E AS RELAÇÕES DE TRABALHO: BREVES REFLEXÕES

GUILHERME GUIMARÃES FELICIANO^{1*}
E CLAUDIRENE ANDRADE RIBEIRO^{2**}

Resumo

O presente estudo analisa a existência de um direito ao esquecimento no direito brasileiro, de cariz telemático, mesmo após a decisão proferida pelo STF no RE 1.010.606 e a aprovação da Tese de Repercussão Geral n. 786 (aparentemente em sentido contrário). Para tanto, valendo-se do método dedutivo, o artigo explora os conceitos básicos e gerais relacionados ao tema, sobretudo no âmbito da doutrina brasileira e europeia. Conclui-se que, não obstante a tese perfilhada pelo STF pareça sinalizar a inexistência de um direito ao esquecimento no ordenamento brasileiro, tal entendimento há de ser adotado apenas em relação ao direito ao esquecimento de perfil privatístico, quando oposto unicamente à liberdade de imprensa. Essa configuração é reconhecida na segunda parte da decisão, que aponta a possibilidade de excessos concretos, hipóteses em que terá lugar a tutela de alguma das dimensões do que se entende como direito ao esquecimento. Ademais, o artigo 15 da Lei Geral de Proteção de Dados (LGPD), em vigor desde 2020, constitui espécie setorial do direito ao esquecimento, na medida em que garante o término do tratamento de dados e a sua consequente eliminação, tão logo cumprida a finalidade da coleta (se não antes), o que tem particular importância no âmbito das relações de trabalho. Desse modo, a discussão nacional em torno do direito ao esquecimento não está encerrada, antecipando-se que o Supremo Tribunal Federal voltará a ser provocado para decidir novas questões relacionadas ao tema.

Palavras-chaves: 1. Direito ao esquecimento. 2. Lei Geral de Proteção de Dados. 3. Direito à memória. 4. Direito à verdade histórica.

1. Introdução

A assim dita era da sociedade da informação tornou realidade o que antes era real apenas em livros e filmes de ficção científica, como Mil Novecentos e Oitenta e Quatro (ORWELL, 2019), LARANJA Mecânica (1962), BLADE *Runner* (1982) e MATRIX (1999). Nessa nova era, a velocidade nas comunicações interpessoais, sociais, jornalísticas e até mesmo científicas torna-se um lugar-comum universal, notadamente porque o uso consistente e disseminado da *internet* permite que as informações sejam transmitidas em tempo real de/para qualquer lado do mundo

1 Professor Associado II do Departamento de Direito do Trabalho e da Seguridade Social da Faculdade de Direito da Universidade de São Paulo. Juiz Titular da 1ª Vara do Trabalho de Taubaté – SP. Livre-Docente em Direito do Trabalho e Doutor em Direito Penal pela FDUSP. Doutor em Ciências Jurídicas pela Faculdade de Direito de Lisboa.

2 Doutoranda em Direito do Trabalho e Seguridade Social-USP/SP. Mestre em direito agroambiental e em Educação pela UFMT. Especialista em Direito do Trabalho pela PUC/SP. Graduada em Direito e em Geografia, também pela UFMT. Docente na área jurídica. Atualmente é juíza do trabalho titular da 2ª VT de Tangará da Serra - MT. *E-mail:* claudireneribeiro@yahoo.com.br.

em que os interlocutores estejam conectados por intermédio da rede mundial de computadores. E, curiosamente – ou quiçá sintomaticamente –, tais informações parecem ganhar especial “credibilidade” quando chegam por essa via, como se conteúdos informacionais trafegados pela rede fossem necessariamente mais fidedignos do que aqueles encaminhados nos espaços tridimensionais. Algo que, aliás, devolve-nos à fala do sociopata Alex DeLarge em *Laranja Mecânica*:

“It’s funny how the *colors* of the *real world* only seem really real when you viddy them on the screen.”

(Em tradução livre: “É engraçado como as cores do mundo real parecem muito mais reais quando vistas nas telas.”)

Nesse novo contexto, a temática do *direito ao esquecimento* – apesar de sua origem anterior – adquire especial relevância social e jurídica, uma vez que se espraiam os conflitos advindos desse suposto direito, predominantemente de cujo individual, ao colidir com outros direitos de perfil difuso, como o direito à memória e o direito à verdade histórica. Dir-se-ia então que, notadamente em sede trabalhista (mercê do art. 8º, *caput*, *in fine*, da CLT)³, o caráter difuso, coletivo ou “público” sobreleva, em todo caso, o caráter individual?

Chamado a se manifestar sobre o tema, o Supremo Tribunal Federal recentemente fixou, por maioria, a Tese de Repercussão Geral n. 786, no sentido de que a ordem jurídico-constitucional brasileira não admitiria o reconhecimento de um direito ao esquecimento “*tout court*”. A decisão, todavia, não pacificou a matéria. Antes, fez com que se acirrassem ainda mais os debates acerca do tema, uma vez que o verbete aprovado, em sua parte final, parece sinalizar a possibilidade de análise desse direito à luz do caso concreto.

Eis aí o nosso objeto, com o especial foco das relações de trabalho. Pretendemos enfrentá-lo a partir de pesquisa doutrinária e jurisprudencial, sob o método dedutivo, discutindo, a uma, a existência de um direito subjetivo ao esquecimento no direito brasileiro, sobretudo a partir da referida decisão do Excelso Pretório (RE n. 1.010.606), como ainda, no particular contexto da sociedade de informação, a partir dos teores dos artigos 15 e 16 da Lei Geral de Proteção de Dados (Lei n. 13.709, de 14 de agosto de 2018), que asseguram o direito ao apagamento de dados (“término de tratamento” e “eliminação”) como um consectário dos direitos de personalidade da pessoa, com inegável matriz constitucional.

2. Direito ao esquecimento

Na presente seção, apontaremos esquematicamente os aspectos gerais e conceituais do chamado direito ao esquecimento, que geralmente é invocado em contraposição ao direito à memória e à verdade histórica.

Para tanto, levantaremos os fundamentos jurídicos mais recorrentes que lhe

³ “As autoridades administrativas e a Justiça do Trabalho, na falta de disposições legais ou contratuais, decidirão, conforme o caso, pela jurisprudência, por analogia, por equidade e outros princípios e normas gerais de direito, principalmente do direito do trabalho, e, ainda, de acordo com os usos e costumes, o direito comparado, **mas sempre de maneira que nenhum interesse de classe ou particular prevaleça sobre o interesse público**” (g.n.).

dariam sustentação, assim como o histórico dos principais casos em que a matéria foi discutida em sede extraordinária, destacando-se o recente julgado do RE n. 1.010.606, que resultou na fixação da Tese de Repercussão Geral n. 786.

2.1. Direito ao esquecimento *versus* direito à memória: aspectos gerais e conceituais

O direito ao esquecimento deita raízes em expressões recorrentes na doutrina e na jurisprudência de base anglossaxônica, como “*right to privacy*” (direito à privacidade) ou “*right to be alone*” (direito de ser deixado em paz ou de ficar sozinho), que chegam a ser seculares. Na sua configuração conceitual mais atual, todavia, o direito remonta a 1973, quando do julgamento do primeiro caso Lebach pelo *Bunderverfassungsgericht* (tribunal constitucional alemão), ao qual nos reportaremos com vagar na subseção 1.3 (WOHJAN. WISNIEWSKI, 2015). Tal direito é reconhecido, ademais, na maior parte dos ordenamentos jurídicos europeus. Segundo Rosen (2012, p. 88),

“[i]n Europe, the intellectual roots of the right to be forgotten can be found in French law, which recognizes le droit à l’oubli — or the “right of oblivion”.”

A rigor, a expressão “esquecimento” parece não ser a mais adequada para designar o que o direito representa, pois pode levar à ideia de *esquecimento do passado* ou de *apagamento da história* (COELHO, 2020, p. 3; SCHREIBER, 2021; SOUZA, 2020); e não é disso que realmente se trata. De todo modo, como pontificam Oliveira, Schreiber e Souza (2020), a inadequação do termo não pode servir para afastar a tutela de direitos da personalidade que por seu intermédio se visa a resguardar.

Na verdade, a correta compreensão do alcance das expressões “direito ao esquecimento” e “direito à memória e à verdade histórica” é primordial para os ulteriores desdobramentos que virão na sequência, inclusive quanto ao seu acolhimento – ou não – pelo ordenamento jurídico nacional, a despeito do que já se decidiu no âmbito do Excelso Pretório. E há que se iniciar, para tanto, com o respectivo *conceito*.

O direito subjetivo ao esquecimento, entendido *stricto sensu* corresponde ao direito individual de não ser lembrado por situações pretéritas constrangedoras ou vexatórias, ainda que verídicas.^{4, 5} Por via oblíqua, esse direito tutela a vida digna, a imagem, a honra

4 Carlos Afonso alerta para os riscos da ampliação da expressão, como lembrado no recente julgamento do STF. Citava-se o caso de um parque de diversões que evocou o direito ao esquecimento para postular a não divulgação de acidente pretérito com um determinado brinquedo que seria relançado; com isso, pretendia evitar que a imprensa divulgasse os fatos pretéritos e prejudicasse a atividade econômica, em uma demanda seguramente incabível. O autor chama igualmente a atenção para caso em que o STJ decidiu pela desindexação de seu nome nas chaves de busca, em relação às notícias sobre determinado concurso para a magistratura excepcionalmente maculado com uma suposta fraude. Assevera ainda que, em alguns casos, “o direito ao esquecimento pode gerar justamente o seu oposto”. Questiona, ademais, as hipóteses em que políticos buscam lançar mão desse direito para impedir a divulgação de fatos relacionados ao seu passado, especialmente em épocas de eleições. Conclui que não há prejuízo, pois os casos serão tratados à luz “*direito de proteção à imagem, à honra etc.*”. E supõe, enfim, que o debate do tema será retomado pelo STF (como, aliás, também supomos; a decisão no RE 1.010.606 decertou não exauriu todos os desdobramentos desse debate).

5 A autora afirma ainda que a atualidade do fato não deve ser analisada apenas no sentido temporal, mas deve considerar outros elementos, como a sua relevância objetiva para a sociedade.

e a própria saúde psíquica e física do respectivo titular, ensejando a transcendência do trauma⁶ e impedindo que o isolamento oriundo da vergonha leve a relações sociais deficientes, que comprovadamente aumenta a incidência de inúmeras comorbidades, tais como os acidentes vasculares cerebrais e as cardiopatias. (MAURMO, 2017).

Nessa alheta, Melo (2016, p. 4-5) desdobra o direito ao esquecimento em dois sentidos ou acepções. A primeira, denomina de “material”, e a segunda, denomina de “procedimental”. Na primeira acepção, o direito ao esquecimento pressupõe os seguintes elementos essenciais: a) a passagem do tempo;⁷ b) a pretensão do seu titular de transpor informações que já estão na esfera pública de volta para a esfera privada; c) a alegada inexistência de interesse público no dado ou informação; e d) a conexão com “*interesses relacionados à privacidade sob duas concepções clássicas: (a) o direito de ser deixado em paz (the right to be let alone) e (b) o direito de controle sobre o fluxo de informações sobre si*” (MELO, 2016, p. 4). Na segunda vertente (procedimental), já adaptada à realidade da sociedade da informação, o direito ao esquecimento se caracterizaria como um modo de “desindexação” subjetiva, ou seja, o direito de ser pessoalmente desvinculado dos dados depreciativos, ao ensejo de buscas realizadas pelos motores da *internet* (MELO, 2016, p. 5).

Conquanto negue a existência a um direito ao esquecimento no ordenamento jurídico nacional, a mesma autora reconhece-o conceitualmente como a “*prerrogativa de impedir a divulgação de fatos verdadeiros e públicos, que deixariam de ser protegidos contra a censura judicial em razão de seu caráter ofensivo, constrangedor ou até mesmo pela vontade caprichosa da pessoa envolvida*” (MELO, 2016, p. 5).

Por sua vez, Schreiber (2017, p. 2) assevera que, no direito brasileiro,⁸ o direito ao esquecimento vem sendo brandido com uma acepção totalmente diversa da original. Originalmente, trata-se de “*um direito a evitar a recordação opressiva de fatos do passado, que efetivamente ameaça a capacidade do ser humano de se reformular perante a sociedade*”.

De outra parte, o direito à memória e à verdade histórica - que se contraporá ao direito ao esquecimento - pode ser entendido em uma perspectiva privatística e em uma perspectiva pública (ou ao menos difusa). Na primeira perspectiva, deve ser reconhecido como o direito individual de cada uma das vítimas de saber e de fazer saber com integridade os fatos que as envolveram, na inteireza de seus con-

6 Bentivegna e Bauab (2020, p. 3) tratam a recordação do trauma como “*a junção de várias pequenas memórias do evento, com as suas interpretações em cada etapa de sua formação, associadas a sentimentos; normalmente, o sentimento ou o pensamento deflagrador.*” Asseveram também que o tema constitui objeto de estudo da neurobiologia, da neurociência e da psiquiatria, que buscam técnicas de terapias tendentes ao reconhecimento da origem e da emoção causada pelo trauma, no sentido de dissociar as lembranças, resignificá-las ou mesmo esquecer-las; e, nessa esteira, o perdão pode constituir uma atitude importante para a higidez psicológica. (BENTIVEGNA, BAUAB, 2020, p. 3-4).

7 Em recente decisão, a partir do voto do Des. Olindo Menezes (Desembargador convocado do TRF da 1ª Região), a 6ª Turma do Superior Tribunal de Justiça asseverou o seguinte: “[...] 2. A tese do “direito ao esquecimento” não deve ser aplicada em relação a feitos extintos que não possuam lapso temporal significativo em relação a data da condenação, qual seja menos de 10 anos.” (BRASIL, 2021c, aspas internas no original).

8 A conclusão do autor é afirmada em face da decisão proferida pelo C. STJ no Recurso Especial (RE) n. 1.334.097, em cujo bojo o direito ao esquecimento foi definido com o “*direito de não ser lembrado contra sua vontade.*”

textos e desfechos lesivos. Na segunda perspectiva, estamos diante de um interesse difuso “*lato sensu*”, compartilhado por toda a sociedade, de saber e esclarecer os fatos e circunstâncias que geraram graves violações a direitos humanos, sobretudo em períodos e regimes de exceção. No caso do Brasil, como se sabe, essa perspectiva justificou todo o esforço institucional dedicado, nos últimos anos, à constituição/atuação das “comissões da verdade” para apuração dos casos de torturas, mortes, desaparecimentos forçados e ocultações de cadáveres durante o período da última ditadura militar (1964 a 1985).⁹ No plano internacional, aliás, o país ficou particularmente marcado pelas violações perpetradas durante a chamada guerrilha do Araguaia e também, no caso Gomes Lund, pela negativa de acesso das vítimas aos dados estatais, o que ensejou sua condenação no âmbito da Corte Interamericana de Direitos Humanos.

Eis, pois, o que se deve entender, para os efeitos deste estudo, por direito ao esquecimento e por direito à memória e à verdade histórica, nas suas variegadas dimensões. Superado o esforço conceitual, importa agora discutir o substrato normativo para o reconhecimento e a tutela de tais direitos – ou, no que ora importa, para o primeiro deles –, já em seara jurídico-dogmática. É o que faremos a seguir, selecionando as principais bases constitucionais e infraconstitucionais do direito ao esquecimento no âmbito nacional; e, em cotejo, examinaremos igualmente as bases jurisprudenciais que o têm sustentado na Europa, inclusive para embasar as conclusões que finalmente se abraçarão. Nessa vereda, ademais, caberá ainda discutir alguns episódios da rica casuística que a matéria ora discutida apresenta, tanto no direito estrangeiro quanto em nossas próprias plagas.

2.2 Bases constitucionais e infraconstitucionais do direito ao esquecimento

Para efeitos hermenêuticos e operativos (interpretação/aplicação), a identificação e invocação das bases constitucionais e infraconstitucionais do direito ao

⁹ Conquanto se encontrem vozes que ainda questionem a existência de uma ditadura militar durante esse interregno – especialmente na atual quadra, ante os pendores que inspiram a retórica da Presidência da República, mas também muito antes mesmo disso (o próprio Ministro Dias Toffoli, durante os dois anos em que exerceu a presidência do Excelso Pretório, insistiu em identificar os eventos de 31.3.1964 – na verdade, 1.º.4.1964 – como “Movimento de 1964”) –, e ainda que se entenda que durante esse período o país tenha observado alguns avanços legislativos (a exemplo da Lei 4.505/1964 – o Estatuto da Terra –, da Lei 5.478/1968 – pensões alimentícias –, da Lei 6.515/1977 – Lei do Divórcio – e das próprias alterações no Capítulo V do Título II da CLT, sobre medicina e segurança do trabalho), aspecto geralmente citado pelos entusiastas do período, **é curial reconhecer e afirmar que o regime interrompeu a normalidade democrática do país, suprimiu seus instrumentos de democracia representativa e, para mais, generalizou (ou, de muitos modos, “institucionalizou”) a prática de gravíssimos atos violadores dos direitos humanos.** Não por outra razão, após longas lutas de familiares de desaparecidos políticos, exilados e torturados, aprovou-se a Lei 12.528, de 18 de novembro de 2011, instituindo a Comissão Nacional da Verdade, no âmbito da Casa Civil da Presidência da República, para, nos termos do artigo 1.º, “[...] examinar e esclarecer as graves violações de direitos humanos praticadas no período fixado no art. 8.º do Ato das Disposições Constitucionais Transitórias, a fim de efetivar o direito à memória e à verdade histórica e promover a reconciliação nacional”. Tratou-se do primeiro real esforço legislativo para, após a Lei da Anistia (Lei 6.683/1979), promover no Brasil a chamada *justiça de transição*. E muito do que desde então se logrou conquistar, inclusive em termos de reconhecimento público, resgate histórico e até mesmo – na expressão da lei – “reconciliação nacional”, tem-se lamentavelmente perdido com as investidas retóricas negacionistas do atual Presidente da República (v., e.g., AGÊNCIA BRASIL, 27/03/2019).

esquecimento é um pressuposto inexorável. Como é cediço, esse direito não está expressamente previsto na legislação nacional, o que se esgrimiu desde sempre como um óbice jurídico-positivo ao seu reconhecimento. Não haveremos, porém, de trilhar as sendas do legalismo positivista. Optaremos por uma visão mais holística do sistema jurídico nacional, que permite reconhecer as premissas teóricas do direito ao esquecimento nos anteparos do sobreprincípio constitucional da *dignidade da pessoa humana*, fundamento do Estado Democrático de Direito (art. 1º, III, da CRFB)¹⁰ e vetor normogenético das normas-princípios da inviolabilidade da vida privada e da intimidade (art. 5º, X, CRFB).

Não basta, porém, admiti-lo como “possibilidade” do sistema jurídico pátrio. Há que ir além, buscando a sua concretude e os seus limites na extensão legítima dos outros direitos, liberdades e interesses fundamentais que o circunvizinham: a liberdade de imprensa, a liberdade de expressão, o direito à memória e à verdade histórica e o direito de acesso à informação. Exsurgem, nesses ensejos de colisão jusfundamental, indelévels “*hard cases*”. E na maioria dos casos, diante dos eminentes valores lindeiros, torna-se curial recorrer ao princípio da proporcionalidade e exercitar os respectivos juízos da ponderação (ou, para os alinhados, aplicar a lei de ponderação alexyana). Com efeito, ainda que existam o direito à informação, o direito à memória e a própria liberdade de imprensa, os artigos 11, 20 e 21 do Código Civil de 2002, asseguram, em contrapartida, os direitos da personalidade, a proibição de divulgação ofensiva à honra, à boa fama e/ou à respeitabilidade e a inviolabilidade da vida privada.

Com efeito, as premissas acima reportadas constam do Enunciado n. 531 da VI Jornada de Direito Civil, organizada pelo Conselho da Justiça Federal (CJF) e pela Escola Nacional de Formação e Aperfeiçoamento de Magistrados (Enfam). Diz o referido enunciado:

“A tutela da dignidade da pessoa humana na sociedade de informação inclui o direito ao esquecimento”.

Para justificar o verbete, referenciou-se o contexto atual da chamada sociedade da informação – que, não por outro motivo, abriu nossa introdução (*supra*) –, na qual a rápida e irrefreável expansão das comunicações alcança a escala geométrica, exponenciando-se com o progressivo acesso das populações às redes sociais e afins; e, sob tais circunstâncias, a circulação das informações e dos dados (inclusive os verdadeiros) não raro provoca danos de diversas origens e/ou a titulares diversos. Caberá supor que nada disso é sindicável judicialmente? Não em nossa opinião.

Nessa direção, a justificação do enunciado descreve a origem histórica do direito ao esquecimento, oriundo do Direito Penal, onde foi engendrado como importante mecanismo auxiliar na recuperação social de ex-detentos. Cigana e Rocha (2017, p. 212) observam, a propósito, que o processo de ressocialização do apenado ultrapassa o período de cumprimento da pena e inclui o período ime-

¹⁰ Dispõe o art. 1º caput e inc. III da CRFB: “A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: [...] III - a dignidade da pessoa humana”.

diatamente posterior, quando é efetivamente reinserido na sociedade; e, pela óbvia necessidade de que o ex-detento seja aceito pela comunidade de seu entorno, questionam se a exposição indefinida do fato delituoso pelas mídias não constituiria uma espécie de prisão perpétua, comprometendo irremediavelmente a sua ressocialização e a sua autoimagem. Tais reflexões conduzem à conclusão expressa na precitada justificativa, no sentido de que o direito ao esquecimento “[n]ão atribui a ninguém o direito de apagar fatos ou reescrever a própria história, mas apenas assegura a possibilidade de discutir o uso que é dado aos fatos pretéritos, mais especificamente o modo e a finalidade com que são lembrados”.

Modo e finalidade, portanto, são as dimensões do direito à memória e à verdade histórica – e, como respectivo direito instrumental, o da liberdade de imprensa – que devem ser sopesadas, pela via da concordância prática (K. Hesse), para assegurar alguma relevância ontológica e axiológica ao direito ao esquecimento.

Nessa direção, já se podia reconhecer, insita à “*ratio*” do Enunciado 531, a exigência de que as informações pessoais do indivíduo sejam utilizadas apenas segundo a finalidade para a qual foram colhidas. Vale dizer, *finalidade legítima e tratamento adequado*, o que passou a ser expressamente referido no art. 6º, I e II, da Lei Geral de Proteção de Dados Pessoais. É o que diremos na sequência.

2.3. Direito ao esquecimento: breve casuística

Em 1973, na Alemanha, chegou pela primeira vez ao *Bundesverfassungsgericht* (BvG) o chamado caso Lebach. Tratava-se do pleito de um delinquente definitivamente condenado a seis anos de reclusão,¹¹ participe do assassinato de quatro soldados (além de lesões graves a um quinto) que à altura dormiam. Prestes a obter livramento condicional, o autor requereu judicialmente a não divulgação de um documentário de televisão editado cerca de dois anos após os eventos (ocorridos em 1970), que divulgava o nome dos envolvidos.

No julgamento, em junho de 1973, a corte constitucional alemã entendeu que, embora a regra fosse a da prevalência do interesse público em torno da informação, a ponderação concretamente favorecia o autor, em virtude do transcurso do tempo desde os fatos (em razão do que o interesse público não era mais atual) e do direito à efetiva ressocialização. Considerou-se que a exibição implicaria a imposição de uma nova sanção social ao autor do delito, especialmente mediante a divulgação televisiva, de imenso alcance; e, por isso, a exibição não foi autorizada.

Mas o debate não terminou em 1973. Mais de vinte anos depois, em 1996, o caso *Lebach* chegou novamente ao BvG, desta feita, em reclamação constitucional formulada pela empresa de televisão que preparava novo documentário acerca do tema.¹² E, nesse caso, a exibição foi autorizada.

Ainda no âmbito do BvG, cabe reportar o caso Lüth, julgado em 1958, no qual Eich Lüth reivindicava o boicote público aos filmes de Veit Heilan, famoso cineasta do 3º *Reich* que tentava se “reabilitar” perante a cena artística alemã. Naquela oportunidade, porém, a corte constitucional asseverou a impossibilidade de censura prévia às livres manifestações de Lüth, que não poderia ser impedido de

11 Os autores principais foram condenados à morte.

12 Dessa feita, a reclamação perante o BvG foi formulada após um dos autores do crime ter obtido, nas instâncias ordinárias, decisão que vedava a divulgação do programa.

vociferar contra Heilan e dar a conhecer a respectiva biografia pretérita.

Algo mais a oeste, na França, a *Cour d'Appel* de Paris examinou o caso François Ost (1983). À altura, a corte reconheceu o direito ao esquecimento, aplicável ao caso e oponível a todos, ressaltando apenas as hipóteses de relevância histórica. “*In verbis*”:

“[...] qualquer pessoa que se tenha envolvido em acontecimentos públicos pode, com o passar do tempo, reivindicar o direito ao esquecimento; a lembrança deste acontecimentos e do papel que ela possa ter desempenhado é ilegítima se não fundada na história ou se for de natureza a ferir sua sensibilidade, visto que o direito ao esquecimento, que se impõe a todos, inclusive a jornalistas, deve igualmente beneficiar a todos, inclusive aos condenados, que pagaram sua dívida com a sociedade e que tentam nela se reinserir.”

Na esfera nacional, enfim, também se colhem relevantes casos que chegaram às barras do Poder Judiciário, decididos de modo mais ou menos alinhado à tese acolhida pela *Cour d'Appel* (mas, em geral, abonando a existência de um direito ao esquecimento). Apontam-se abaixo três deles.

O primeiro, conhecido como “caso da Chacina da Candelária”,¹³ refere-se ao extinto programa “Linha Direta”, da Rede Globo de Televisão, que referiu, na narrativa de um crime de grande estrépito, o nome de serralheiro anteriormente absolvido pelo tribunal do júri, nos termos do art. 748 do Código de Processo Penal. Na ocasião, o Superior Tribunal de Justiça entendeu pelo direito do recorrente de se ver indenizado.¹⁴ Da ementa da decisão proferida pelo STJ (BRASIL, 2013, p. 2-7), constata-se que o acórdão extremou, por um lado, as hipóteses de exibição de programas televisivos; e, por outro, os ensejos de veiculação de notícias pela *internet*. Ao fazê-lo, salientou a maior complexidade desses últimos, por envolver também questões de interesse nacional; mas, se era certo que o caso se convolara em fato histórico – donde o legítimo interesse público na divulgação do evento criminoso e de sua solução pelas instituições do Estado, além do próprio direito difuso à verdade histórica (entendendo-se que a memória histórica constitui patrimônio cultural da sociedade civil) –, também era certo que o direito ao esquecimento, já consagrado no direito estrangeiro, pronunciava-se como um direito ao futuro, de reconstrução do passado do condenado em crimes que tenham pago por sua

13 Trata-se do assassinato de oito jovens em situação de rua nas proximidades da igreja da Candelária, no Rio de Janeiro, em 1993. Um serralheiro que foi acusado de participação no crime e foi inocentado pelo Tribunal de Juri teve seu nome referido na reportagem.

14 O reexame do caso foi iniciado em 3 de agosto de 2021, pela 4ª Turma do STJ, após a fixação da tese do Tema de Repercussão Geral n. 786 pelo C. STF. Em caso de manutenção da posição adotada em 2013, o processo seguirá para o Supremo Tribunal Federal analisar o recurso extraordinário interposto pela emissora de televisão. O Min. Luís Felipe Salomão, relator do caso, manteve o posicionamento anterior e entendeu que o teor decidido coaduna-se com a tese fixada pelo STF, porquanto se teria identificado, naquela ocasião, *excesso no exercício do direito à liberdade de expressão*. Após o voto do ministro relator, o Min. Raul Araújo pediu vistas, interrompendo-se o julgamento (BRASIL, NOTÍCIAS DO STJ, 05/08/2021).

pena e obtido o direito à eliminação dos apontamentos do crime nos registros de identificação e que o direito de imprensa encontraria limites constitucionais, respaldados “na inviolabilidade da vida privada, intimidade, honra, imagem e, de resto, nos valores da pessoa e da família, prevista no art. 220, §1º, art. 221 e no §3º do art. 222 (...)” (BRASIL, 2013, p. 2).

O segundo, alcunhado de “caso Aída Curi”, envolve o estupro e assassinato de Aída Cury em 14/7/1958,¹⁵ com forte repercussão à época. Os fatos foram revisitados e divulgados pelo mesmo programa “Linha Direta”, três décadas depois, com referências aos nomes de família dos personagens envolvidos, trazendo grande desconforto aos parentes vivos. Esse caso justamente esteve na origem do precedente do Excelso Pretório, no RE 1.010.606, que referiremos a seguir.

Vejamo-lo (RE 1.010.606), pois. Nele, fixou-se a tese de repercussão geral que aparentemente repeliu o direito ao esquecimento do universo de possibilidades jurídicas do direito brasileiro.

2.4 O direito ao esquecimento e a decisão proferida pelo STF no RE 1.010.606

Após encontrar ressonância em boa parte da doutrina nacional e na jurisprudência, especialmente a do STJ, o tema em exame foi objeto de recente decisão por parte do Supremo Tribunal Federal, nos autos do RE 1.010.606, e terminou parcialmente rechaçado. Eis a tese aprovada em plenário, para o Tema n. 786, a partir do voto de S. Ex.^a o Min. Dias Toffoli:

“É incompatível com a Constituição a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e lícitamente obtidos e publicados em meios de comunicação social analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais – especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral – e das expressas e específicas previsões legais nos âmbitos penal e cível” (STF, Tese De Repercussão Geral n. 786).

Entendamo-la melhor, já com a necessária criticidade.

Em debate jurídico realizado no canal “Direito Civil brasileiro”, exibido no *Youtube*,

¹⁵ Em 14.7.1958, a jovem Aída Jacob Curi foi levada por dois rapazes ao topo de um edifício na Avenida Atlântica, no Bairro de Copacabana (Rio de Janeiro), e ali se viu submetida a tortura a abusos sexuais, com o auxílio do porteiro. Aída lutou corporalmente com seus agressores por ao menos 30 minutos, até desmaiar, conforme relevou a perícia. Seu falecimento deveu-se à queda do edifício, do qual foi atirada pelos violadores que, com isso, buscavam esconder o crime. Dos três envolvidos, A.S., o porteiro, foi inocentado da acusação de homicídio e condenado por atentado violento ao pudor e tentativa de estupro; R.G. de S. C., com 19 anos à época, membro de uma família tradicional carioca, foi condenado a 8 anos de 9 meses de prisão; e o adolescente C. M. Ferreira, sobrinho do síndico do prédio, foi condenado pelo homicídio e encaminhado ao Sistema de Assistência ao Menor (SAM).

em informação verbal, Anderson Schreiber (2021, 57') ponderou que “[...] o direito ao esquecimento é a favor de uma verdade histórica contextualizada”, sendo certo que “hoje em dia tudo é lembrado de uma maneira descontextualizada.” Asseverou ainda que a “regra” – outrora, a do esquecimento – foi agora substituída pela *lembrança*; e defendeu que, na realidade, quando se fala em direito ao esquecimento, está-se tratando, em boa medida, de um direito de personalidade (como, aliás, a Tese n. 786 também reconhece, de certo modo). Acrescentou que o maior problema dogmático, no julgamento do C. STF, foi a amplitude do conceito de direito de esquecimento; e, bem assim, a imprecisão semântica da segunda parte da tese à altura fixada.¹⁶

A despeito da crítica, porém, “*decisum habemus*” (e, a partir dele, o possível manto da vinculatividade, “*ex vi*” dos arts. 489, §1º, V e VI, 926 e 927 do CPC, ainda que por via implícita)¹⁷. O que dizer, então, dos dados e informações disponíveis no universo digital? Ou, em geral, das obrigações legais reservadas ao controlador e/ou ao operador de dados? Se não existe um direito ao esquecimento, os dados relativos a qualquer cidadão, uma vez validamente coletados, jamais poderão ser eliminados ou anonimizados? Não há qualquer expectativa temporal legítima para o término do respectivo tratamento?

Obviamente, tais conclusões seriam equivocadas, até porque irrazoáveis. Isto demonstra, a uma, o já reportado excesso semântico na definição que o C. STF emprestou ao “direito ao esquecimento”, ao negar-lhe qualquer acolhida na ordem jurídica brasileira. E nos conecta, a duas, com o objeto do tópico subsequente.

3. Direito ao esquecimento, proteção de dados e direito ao trabalho

Como antecipamos, a celeridade e a facilidade de divulgação e de acesso aos dados pessoais do indivíduo constituem a tônica da chamada sociedade da informação. Retratam bem, nas suas possibilidades e nas suas vulnerabilidades, a condição de privacidade e de intimidade do indivíduo no atual momento social, em que as informações captadas por diversos meios – e especialmente pela via digital – permanecem armazenadas em “nuvem”, disponíveis na rede mundial de computadores, e podem ser facilmente acessadas por qualquer usuário da rede por meio de motores de busca (como o Google, o Bing e o Yahoo).¹⁸ Nesse contexto, a

16 Nesse mesmo ensejo, A. Schreiber (2021) observou, com todo acerto, que a decisão do C. STF valeu-se de diferentes compreensões acerca do expressão “direito ao esquecimento” e terminou por adotar aquela que não seria a mais acertada, por não corresponder à atualmente seguida pela doutrina mais abalizada. De nossa parte, aderimos integralmente à crítica.

17 Diz-se *implícita* porque, a rigor, estamos a falar de *acórdãos proferidos em regime da repercussão geral*, que não estão textualmente elencados no art. 927 do CPC/2015.

18 Os três principais *sites* de busca (ou “motores”), segundo Giraldo (2019) e Neil Patel (S/D), são o *Google*, o *Bing* e o *Yahoo!*; é certo, porém, que, além desses, existem inúmeros outros. Entre todos, o *Google* é, de longe, o mais utilizado em todo o mundo. A importância do *Google* como sítio de pesquisa popular originou inclusive o verbete *Googling* nos atuais dicionários norte-americanos (NEIL PATEL, S/D). Com efeito, o termo *Google* pode ser encontrado no DICTIONARY.COM, que apresenta 3 significados dele derivados: “1) *the proprietary name of a leading internet search engine, founded in 1998.* 2) *verb (used with object), Goo-gled, Goo-gling. (often lowercase) to search the internet for information about (a person, topic, etc.): We googled the new applicant to check her background.* 3) *verb (used without object), Goo-gled, Goo-gling. (often lowercase) to use a search engine such as Google to find information, a website address, etc., on the internet.*”

desregulamentação do uso de dados pessoais representa uma afronta aos direitos de personalidade: uma vez fornecido determinado dado pessoal a determinada empresa, por exemplo, seja no âmbito de relações comerciais, seja no plano das relações trabalhistas ou pessoais, um tal dado poderá ser lançado na rede mundial de computadores e permanecer vulnerável por tempo indeterminado.

No Brasil, apenas no ano de 2020 entrou em vigor a Lei n. 13.709, aprovada em 14 de agosto de 2018, denominada “Lei Geral de Proteção de Dados” (ou, no acrônimo, simplesmente “LGPD”).¹⁹ O diploma regulamenta o tratamento de dados pessoais, inclusive por meios digitais (mas não apenas), por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de tutelar os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (art. 1º, *caput*).

A LGPD brasileira distanciou-se, em muitos aspectos, do padrão internacional ditado pelo RGPD europeu (i.e., o Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, dito “Regulamento Geral sobre a Proteção de Dados”, em vigor para toda a União Europeia). Por alguns desses distanciamentos, merece críticas (assim, *e.g.*, quanto ao emprego de inteligência artificial no tratamento de dados). Nada obstante, acrescentou elementos importantes ao debate nacional, inclusive em torno do direito ao esquecimento, conforme se verificará adiante.

3.1 Aspectos gerais da LGPD: vigência

Como visto, a LGPD recebeu sua atual denominação por meio da Lei 13.853, de 8 de julho de 2019, entrando em vigor em 14 de agosto de 2020, exceto quanto aos artigos 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B, que passaram a vigorar já no dia 28 de dezembro de 2018; e quanto aos artigos 52, 53 e 54, que passaram a vigorar a contar de 1º de agosto de 2021.

Esse confuso marco temporal de vigência, fixado após muitas idas e vindas, está hoje consolidado no art. 65 da LGPD.

3.2 LGPD e direito ao apagamento de dados

Consoante o artigo 12 da Lei n. 13.709/2018, os dados adequadamente anonimizados podem ser utilizados livremente, estando excluídos do escopo de aplicação da lei. A *anonimização* implica, em termos ideais, três estados: 1) a impossibilidade de identificar qualquer pessoa; 2) a baixa probabilidade de se estabelecer qualquer ligação entre os registros de uma pessoa específica e um determinado grupo de dados; e 3) a incapacidade de se inferir, a partir da análise das informações, dados de um indivíduo específico.

Importante ainda lembrar que o artigo 15 supra da mencionada lei, estabelece quatro hipóteses em que o tratamento dos dados pessoais se encerrará, quais sejam: I) quando observado que o propósito foi atingido ou os dados não forem mais imprescindíveis ou oportunos para a consecução do fim desejado; II) termo do prazo de tratamento; III) aviso do titular, que pode revogar o consentimento, nos

¹⁹ Denominação conferida por meio da Lei 13.853, de 8/7/2019, que alterou a ementa da Lei 13.709, de 14/8/2018, cuja redação original era: “Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet)”. Na verdade, recompilou-se o texto original, deu-se redação nova a diversos artigos do texto original e ainda se incluíram outros tantos dispositivos, modificando sensivelmente o primeiro modelo de proteção de dados pessoais. Isso tudo, a propósito, antes mesmo da entrada em vigor de boa parte daquele primeiro modelo.

termos do §5º do art. 8º desta Lei, salvo o interesse público; e IV) ordem judicial, nos casos de descumprimento das regras estipuladas na LGPD.

Encerrado o tratamento dos dados, a regra estipulada no artigo 16 da norma em comento é a de esses serão descartados, exceto nas quatro circunstâncias indicadas em seus IV incisos, que são: I) desempenho de dever imposto ao controlador por lei ou regulamento; II) uso para fins científicos, assegurado, dentro da viabilidade, a anonimização dos dados; III) quando repassados para terceiros, garantidos os encargos do tratamento; e IV) utilização unicamente pelo controlador, proibido o conhecimento por terceiros e assegurado a anonimização dos dados.

No âmbito da União Europeia (EU), a artigo 17 do Regulamento n. 2016/679 do Parlamento Europeu e do Conselho, assegurou o direito ao apagamento dos dados, *subintitulado como “direito a ser esquecido”*. É o que se lê no Considerando n. 66, que enfoca textualmente o *“direito a ser esquecido no ambiente por via eletrônica.”*

Quando da discussão do referido julgamento, Rosen (2012, p. 88) considerou que a previsão desse direito um risco à liberdade de expressão e que, exceto se houvesse uma melhor definição quando ou após a sua aprovação pelo parlamento europeu, implicaria interpretações opostas entre o direito americano e o direito europeu, posto que nos Estados Unidos da América, a liberdade de expressão estaria assegurada na primeira emenda, tanto que fundamentava a recusa da Wikipédia em remover de suas páginas a história de dois alemães que foram condenados pelo assassinato de um ator.

3.3 O direito ao apagamento de dados como uma espécie de direito ao esquecimento e a decisão do STF no RE 1.010.606: aspectos gerais e laborais

Não obstante a tese de repercussão geral aprovada por maioria pelo STF²⁰ tenha, à primeira vista apontado para a inexistência de um direito ao esquecimento, conforme sua primeira parte, a segunda parte da tese deixou em aberto a possibilidade de se analisar *caso a caso* os excessos à liberdade de expressão. E, nesse caso, parece claro que se poderá restringir tais excessos a partir daquilo que originalmente Gerard Lyon-Caen denominou como *“droit à l’oubli”* (1967):²¹ ainda que

20 A tese fixada pelo relator não foi subscrita pelo Min. Edson Fachin, por entender que não retratava a discussão estabelecida em plenário. Expressamente, assevera Fachin que o voto do relator, como externado originalmente, não rejeitava “a existência do direito ao esquecimento” e conteria “uma miríade de posições.” (BRASIL, 2021a, p. 316).

21 Como o próprio Min. Dias Toffoli fez consignar, já na abertura do seu robusto voto (item I, “Perspectiva Histórica”), tratava-se do caso de Madame “S”, uma ex-amante do *serial killer* Henri-Désiré Landru – hoje mais conhecido como o *Barba-Azul de Gambais*, por ter assassinado ao menos sete mulheres –, buscando impedir que o diretor de cinema Claude Chabrol, a *Société Rome-Paris Films* e a distribuidora *Lux Compagnie Cinématographique de France* utilizasse seu nome, sem autorização, em documentário ficcional a respeito da vida de Landru (cfr., por todos, FRAJHOF, 2019, *passim*; em especial, subseção 2.2.1). A autora reclamava em juízo o direito de ver reconhecida a “prescrição” dos fatos que já não seriam relevantes (daí a expressão *“prescription du silence”*); mas, como é fácil perceber, não subsumia adequadamente o núcleo da tese esgrimida entre as categorias jurídicas mais encontradiças. Para melhor nomear a pretensão, Lyon-Caen valeu-se da expressão em comento, situando a pretensão no quadro geral dos direitos subjetivos públicos: *“já envelhecida, ela teria conquistado um direito ao silêncio em relação às loucuras de sua juventude, como um condenado que já purgou a sua culpa”* (PINHEIRO, 2016, p. 140). Mme. “S” obteve êxito em primeiro grau, perante o Tribunal de Grande Instance de La Seine, mas foi derrotada em grau de recurso, na *Cour d’Appel* de Paris, basicamente porque havia *ela própria*, anteriormente, publicado as suas memórias; logo, não

não se lhe dê essa denominação, é isto que estará em jogo.

Com efeito, assim decidiu o Excelso Pretório (fazendo a balança da ponderação pender em favor da liberdade de expressão), no que de essencial se pode transcrever do robusto e estudado voto de S. Ex.^a, o Ministro Dias Toffoli:

[...] Conquanto mais intensa em ordenamentos historicamente mais suscetíveis a riscos à liberdade de expressão, a preocupação com a sensibilidade que envolve, na atualidade, a concretização dessa ordem de liberdade tem tomado proporções globais.

Na “Declaração conjunta do vigésimo aniversário: desafios para a liberdade de expressão na próxima década”(2019), a **Relatoria Especial para Liberdade de Expressão da Organização dos Estados Americanos** vocalizou diversas preocupações com a criação de ambiente que possibilite o exercício da liberdade de expressão, “especialmente no caso do ambiente digital, mas não unicamente nesse”. [...]

A preocupação já havia sido externada em 2018 pela **Declaración Conjunta sobre la Independencia Y la Diversidad de los Medios de Comunicación en la Era Digital**, na qual se apontou especificamente a preocupação com a desindexação de conteúdo por razões de privacidade:

[...]

A preocupação constante da declaração e apontada como uma ameaça tecnológica sintetiza o que ao longo deste voto fiz consignar: **a previsão ou aplicação de um direito ao esquecimento afronta a liberdade de expressão**. A existência de um comando jurídico que eleja a passagem do tempo como restrição à divulgação de informação verdadeira, lícitamente obtida e com adequado tratamento dos dados nela inseridos, precisa estar previsto em lei, de modo pontual, clarividente e sem anulação da liberdade de expressão. Não pode, ademais, ser fruto apenas de ponderação judicial.

Parece-me que, admitir um direito ao esquecimento, [sic] seria uma restrição excessiva e peremptória às liberdades de expressão e de manifestação de pensamento dos autores e ao direito que todo cidadão tem de se manter informado a respeito de fatos relevantes da história social. Ademais, tal possibilidade equivaleria a atribuir, de forma absoluta e em abstrato, maior peso

estaria verdadeiramente aspirando ao “silêncio” em torno de sua vida amorosa com Landru, mas, antes, considerando suas melhores alternativas para fazê-la pública.

aos direitos à imagem e à vida privada, em detrimento da liberdade de expressão, compreensão que não se compatibiliza com a ideia de unidade da Constituição.

[...]

Entendo, assim, que o ordenamento jurídico brasileiro está repleto de previsões constitucionais e legais voltadas à proteção da personalidade, aí inserida a proteção aos dados pessoais, com repertório, jurídico suficiente a que esta norma fundamental se efetive em consagração à dignidade humana.

Em todas essas situações legalmente definidas, é cabível a restrição, em alguma medida, à liberdade de expressão, sempre que afetados outros direitos fundamentais, mas não como decorrência de um pretenso e prévio direito de ver dissociados fatos ou dados por alegada descontextualização das informações em que inseridos, por força da passagem do tempo.

Não há dúvidas de que é preciso buscar a proteção dos direitos da personalidade, pela via da responsabilização diante do abuso no exercício da liberdade de expressão e pela ampliação da segurança na coleta e no tratamento dos dados, a fim de se evitar os acessos ilegais, as condutas abusivas e a concentração do poder informacional. Mas não se protege informações e dados pessoais, porém, com obscurantismo. [...] (negritos no original)

A tese, como se vê (aqui e na subseção 1.4), estende-se aos dados publicados em **meios de comunicação social analógicos ou digitais**. Funda-se essencialmente na ideia de que *“a previsão ou aplicação de um direito ao esquecimento afronta a liberdade de expressão”*; no entanto, tal ideia não parece decorrer, *“concessa venia”*, sequer dos excertos extraídos da Declaração Conjunta sobre a Independência e a Diversidade dos Meios de Comunicação na Era Digital, como se termina por sustentar. A Declaração admite, ao revés, hipóteses legais de remoção ou desindexação de conteúdo *online*, desde que previstas *“em termos claros e específicos”*, para casos nos quais o titular do direito demonstre a existência de danos substanciais à sua privacidade, aptos a superar concretamente os interesses ligados à liberdade de expressão, sob as garantias do devido processo legal²² (ou seja: sob o pálio da

22 Leia-se, no original em inglês: *“The removal or de-indexing of online content pursuant to the so-called ‘right to be forgotten’ raises important freedom of expression concerns and States should, if their legal systems provide for this, ensure that these measures are provided for by law in clear, specific terms, are applicable only where the petitioner demonstrates substantive harm to his or her privacy which overrides any freedom of expression interest involved, are subject to appropriate due process guarantees and are otherwise conducted in a manner which, both procedurally and substantively, fully respects the right to freedom of expression”* (g.n.). O documento, de maio de 2018, é definido como *“Declaration by the United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the*

proporcionalidade, que só se pode adequadamente aferir casuisticamente).

Pouco antes, ademais, o próprio i. relator fazia a devida distinção, ante os horizontes mais dilargados do direito ao esquecimento (como o desenhou, quiçá com excesso), quando está em causa a proteção de dados no meio digital:

[...] O que se observa é que, conquanto os efeitos da passagem do tempo sejam apresentados de distintas formas pelos doutrinadores (descontextualização, fragmentação, prejuízo à psique do envolvido, apelo ao perdão ou perda do interesse público), é ponto comum que o elemento temporal definidor do pretense “direito ao esquecimento” não seria computado pelo transcurso de um exato número de dias, meses ou anos, mas sim por **decorso temporal suficiente para descontextualizar a informação relativamente ao momento de sua coleta.**

[...]

É notório, [sic] que as pretensões relativas ao direito ao esquecimento são desmembráveis em subtipos, consoante o objeto do “esquecimento” (**fatos ou dados**) e o meio de comunicação adotado para veiculação da notícia (**plataformas tradicionais ou virtual**). De tais subdivisões, porém, não concebo a índole de pretensões distintas, razão pela qual **considero pertinente a apreciação em conjunto (sem prejuízo do reconhecimento das especificidades de cada linha do tema).**

[...]

Em conclusão, a partir desses elementos essenciais, podemos entender o nominado direito ao esquecimento como a **pretensão apta a impedir a divulgação**, seja em plataformas tradicionais ou virtual, **de fatos ou dados verídicos e licitamente obtidos, mas que, em razão da passagem do tempo, teriam se tornado descontextualizados ou destituídos de interesse público relevante.** [...]” (negritos no original)

Percebe-se, pois, que o voto *considera* a diversa complexidade que separa o tratamento de dados nas mídias convencionais – coleta, armazenamento, transmissão e publicização “analógica” – e o tratamento de dados no universo *digital* (e, notadamente, na rede mundial de computadores). A distinção se deve, entre outras razões, ao fato de que, no meio digital, não raramente os dados são tratados *sem uma autorização plenamente consciente* do interessado (veja-se, p. ex., o caso

Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information”. Disponível em: <https://www.osce.org/representative-on-freedom-of-media/379351> . Acesso em: 10/10/2021.

das redes sociais e, em especial, do Facebook)²³; e, ademais, pela *potencialização* do dano (veja-se, e.g., o fenômeno da “viralização” de vídeos, fotografias e afins). Nada obstante, com as razões acima transcritas, o relator termina por albergar sob a mesma tese as duas situações (e, supomos, aqui está, do ponto de vista técnico-jurídico, o principal vezo de “generalização” em que incorreu a decisão).²⁴

Assim, porque não considerou destacadamente as hipóteses específicas do mundo digital, a decisão não pode afastar, p. ex., a vertente do direito ao esquecimento ínsita aos artigos 15 e 16 da LGPD (que sequer são referidos na decisão). Com efeito, o direito ao apagamento de dados – ou, na expressão legal, o “término do tratamento de dados” – pode e deve ser compreendido como uma manifestação particular do direito ao esquecimento, ainda que a lei não se utilize de tal expressão.

23 O Facebook chegou a admitir o uso indevido de dados de 87 milhões de usuários, sendo 443 mil no Brasil. V. <https://www.bbc.com/portuguese/geral-43646687>, acesso em 10/10/2021.

24 A esse propósito, analisando as similitudes e as insuperáveis discrepâncias entre as pretensões de direito ao esquecimento num e outro contexto, cfr. MONTERO, VAN ENIS, 2016, pp. 253-254 (a partir de célebre julgado da *Cour d'Appel de Liège* de 24.9.2014). Em sua opinião, ‘[d]ans la décision commentée, les juges font reposer en grande partie leur raisonnement sur le droit à l’oubli judiciaire, consacré de longue date à l’égard des médias classiques. Nul ne niera qu’il existe des ressemblances entre le droit à l’oubli traditionnel et le droit à l’oubli en cause dans la présente affaire. À notre estime, cependant, en voulant à tout prix transposer aux archives numériques le régime applicable au droit à l’oubli classique, les juges peinent à saisir les spécificités du contexte nouveau de la dissémination de l’information sur le net. [...] Tout d’abord, on voit mal ce qui pourrait s’opposer à ce que la solution dégagée puisse également s’appliquer à de nouvelles situations dans le contexte numérique et pour quelle raison cette dernière devrait être limitée au droit à l’oubli strictement judiciaire. La motivation de la Cour nous semble s’expliquer davantage par l’existence d’une jurisprudence existante dans un domaine précis que par une logique de principe. Comme il a été noté, «le droit à l’oubli ne vise pas seulement à échapper aux rappels d’infractions pénales et d’épisodes de surendettement passés, mais permet à chaque individu de prendre ses distances avec des erreurs et des épisodes malchanceux plus triviaux [...] À titre d’exemple, dans une affaire qui concernait une actrice de films pour adultes, l’intéressée dégageait, comme l’intimé en l’espèce, retrouvée sur le devant de la scène médiatique en raison de son propre comportement et avait souhaité se «réhabiliter» aux yeux du grand public. [...] 40. Ensuite, l’analyse de l’accessibilité permanente des archives en ligne comme véritable «redivulgateur» des articles concernés nous paraît frustrante. À notre sens, il s’agit plus précisément de prendre la mesure du maintien de la mise à disposition et d’une accessibilité accrue d’un article sur le réseau. Cette question diffère de celle de la «redivulgateur», qui suppose la réelle volonté de l’éditeur de remettre un article «en ligne», pour reprendre les termes de l’arrêt annoté. Imposer pareille exigence dans l’univers numérique suggère – quod non – que la simple accessibilité de l’information passée est le résultat d’un réexamen par l’éditeur de l’intérêt que peut représenter la diffusion de cette dernière. Or, comme nous l’avons déjà relevé, faire peser pareille obligation sur l’éditeur reviendrait à lui imposer une tâche démesurée qui l’inciterait probablement à supprimer tout service d’archives en ligne. Par ailleurs, l’exigence d’une «redivulgateur» exclurait du champ d’application du «droit à l’oubli» un nombre important de situations. Le problème de l’anonymisation des articles de presse sur le net peut en effet également se poser à l’égard de contenus qui n’auraient été diffusés qu’en ligne, et qui seraient archivés immédiatement, ou dont la diffusion en ligne serait intervenue simultanément à leur publication sur un support de diffusion traditionnel” (g.n.). No caso julgado em Liège, o tribunal de apelação confirmou a condenação civil de um editor de portal *online* que se recusou a atender um pedido de anonimização formulado por uma pessoa natural, relativamente a um processo judicial pretérito. E, como observam os autores, a doutrina tem reconhecido que o “direito de ser esquecido” que se exerce contra um editor de conteúdos *online* tem características próprias, distinguindo-se, por um lado, do direito ao esquecimento judicial “tradicional”, e, de outra parte, distinguindo-se do “direito de desreferenciamento” (ou de desindexação) oponível a motores de pesquisa.

Por essa via, ademais, é certo que se podem identificar obrigações legais derivadas, sindicáveis em juízo, que decerto alcançam todos os empregadores no trato de suas relações contratuais com os respectivos empregados. Citem-se, nessa direção, informações patronais relativas a dados sensíveis de seus trabalhadores, como ainda aquelas relacionadas a eventuais faltas disciplinares praticadas.

No âmbito europeu, a propósito, já se reconhece com tranquilidade, para pessoas naturais (não, porém, para pessoas jurídicas), que

[I]e droit à l'oubli en entreprise, ou droit au déferement, [que] résulte d'un arrêt de la Cour de justice de l'Union européenne (CJUE) depuis mai 2014. Depuis cette date, les citoyens de l'Union Européenne disposent d'un droit à l'oubli, c'est-à-dire le droit de demander la suppression, auprès des moteurs de recherche, les résultats des requêtes portant sur leur nom, dès lors que les données concernées sont « inexactes, non pertinentes, excessives ou inadéquates ». [...] Néanmoins, cette réflexion a le mérite d'ouvrir le débat sur la faute professionnelle et la gestion de l'identité des salariés et futurs candidats, dont la réputation numérique est de plus en plus pesante dans leurs relations avec la hiérarchie et leurs pairs de manière générale. (OPENWORK, 10/10/2018).

A mencionada decisão do TJUE referiu-se a um motor de busca específico (*Google*). Por sua vez, o caso do Tribunal de Apelação de *Liège*, reportado *supra* (nota n. 23), dizia com um editor de conteúdos *online*. Em ambos os casos, o direito “geral” ao esquecimento deve ser ressignificado como *direito ao esquecimento digital*, mesmo porque, em tais casos,

[I]e « droit à l'oubli » comme composante du droit à la vie privée répond à une préoccupation légitime, associée à l'avènement d'une mémoire numérique illimitée. (MONTERO, VAN ENIS, 2016, pp. 255)

Com efeito, um trabalhador demitido com justa causa poderá ter seu nome associado indefinidamente à hipótese do art. 482 da CLT, em redes sociais e motores de busca, independentemente da passagem do tempo? De outra parte, supondo tratar-se de caso relativamente rumoroso, qual o “interesse público” em que uma determinada reportagem em portal jurídico na *internet*, que acaso reporte o teor do julgamento originário em segundo grau (e, logo, um conteúdo *correto* ao tempo da publicação), eternize-se sem a atualização do caso, especialmente se houver revisão total ou parcial junto ao Tribunal Superior do Trabalho? Em situações como essa, a preservação da privacidade e da dignidade ganham expressão, segundo entendemos, conforme o tempo flua e torne cada vez mais remoto o momento histórico da falta disciplinar (ou do seu julgamento em juízo). O Tribunal

de Justiça da União Europeia já reconheceu tal direito, aliás, inclusive para a pessoa natural responsável pela *administração* de empresa gerida de modo ruinoso; (CJUE, 9 Mars 2017)²⁵ com maior razão – e até mesmo em razão dos vetores normativos que regem a condição obreira (como, e.g., o princípio da proteção) –, deve-se reconhecê-lo, conforme as circunstâncias do caso concreto, em favor de *trabalhadores* que se vejam associados a faltas disciplinares no âmbito da empresa.

Assim há sempre de ser, ademais, tendo em conta as circunstâncias particulares de cada caso submetido ao Poder Judiciário, desde que o pretendido “esquecimento” imponha-se a partir de juízos de ponderação que considerem prevalecer, à mercê da *adequação* (“*Geeignetheit*”), da *necessidade* (“*Erforderlichkeit*”) e da *proporcionalidade em sentido estrito* (“*Grundsatz des Angemessenheits*”) (ALEXY, 2004, pp.38 e ss), direitos fundamentais ou personalíssimos que, na espécie, não devam ser infletidos a bem de uma “liberdade de expressão”. Assim será, e.g., se o que estiver em causa, sob o pálio de tal “liberdade”, não for mais do que o propósito de porfiar, de emular – na acepção mais negativa da palavra – ou mesmo o de simplesmente satisfazer uma difusa curiosidade malsã. Observe-se que já se admite, em perspectiva universal, que o Estado-juiz estabeleça restrições de diversas ordens – inclusive *prévias*, onde couber – ao sigilo de comunicações, à liberdade corporal-espacial²⁶ e à liberdade de associação, entre outros direitos, li-

25 De acordo com o TJUE, “[l]es inscriptions qui lient le nom d'une personne physique à une phase critique de la vie de l'entreprise (comme la faillite) ne peuvent être pérennes, à défaut d'un intérêt général spécifique à leur conservation et divulgation”. Tratava-se de uma pretensão de M. Manni, único administrador da sociedade *Italiana Costruzioni*, que sofrera grande prejuízo ao ensejo de negociação comercial imobiliária.

26 Veja-se no Brasil, como exemplo dessas restrições prévias à liberdade de ir e vir – a bem da vida e da integridade física, psíquica e moral da mulher –, o art. 22, III, “a” e “b”, da Lei 11.340/2006 (Lei Maria da Penha), pelo qual, “[c]onstatada a prática de violência doméstica e familiar contra a mulher, nos termos desta Lei, o juiz poderá aplicar, de imediato, ao agressor, em conjunto ou separadamente, as seguintes medidas protetivas de urgência, entre outras: [...] III- proibição de determinadas condutas, entre as quais: a) aproximação da ofendida, de seus familiares e das testemunhas, fixando o limite mínimo de distância entre estes e o agressor; e “b) frequência de determinados lugares a fim de preservar a integridade física e psicológica da ofendida”. Considere-se ainda, na mesma linha, o próprio inciso I do mesmo artigo 22, que autoriza a suspensão da posse e/ou a restrição do porte de armas, a despeito das possibilidades abertas pela Lei 10.826/2003 (Estatuto do Desarmamento), pelas quais, atendidos determinados requisitos formais, o agressor poderia adquirir ou portar arma de fogo, inclusive para a própria proteção. E, convenha-se, o contexto de violência doméstica e familiar *justifica plenamente tais restrições*, ainda se *prévias* a qualquer ato efetivo de agressão; não por outra razão, aliás, a Lei 11.340/2003 teve excelente acolhida na doutrina e na jurisprudência. Em outros contextos, sob diferentes circunstancialidades, não se poderia restringir a dita “liberdade de expressão” (ou de informação), a bem de resguardar a pessoa (inclusive a mulher) contra interesses muitas vezes mesquinhos, senão puramente econômicos? Reflita-se, p. ex. – e é realmente apenas um convite à reflexão, pois não derivaremos maiores conclusões neste texto –, sobre a dramática história de Linda Susan Boreman (1949-2002), conhecida como *Linda Lovelace*, e sua brutal sujeição ao marido Chuck Traynor, que, para além de agredi-la e humilhá-la com frequência, supostamente a obrigou/induziu a gravar filmes pornográficos – sendo “*Deep Throat*” (1972) o mais célebre deles – com níveis profundos de perversão (em um deles, teria sido instada a manter relações sexuais com um cão). Boreman alegou jamais ter recebido qualquer salário por sua atuação em “*Garganta Profunda*”, chegando a afirmar que gravou cenas com uma arma apontada contra a sua cabeça; afirmou, mais, que os produtores William Links, Lou Peraino e Phil Peraino pagaram a seu ex-marido – não a ela – apenas 1.250 dólares, embora a película tenha rendido mais de 600 milhões de dólares. Somente nos anos oitenta,

berdades e garantias fundamentais; (FELICIANO, 2016). Em geral, nesses casos, o que se exige é basicamente o requisito extrínseco da *judicialidade* (i.e., a chancela subjetivada na atuação do órgão jurisdicional competente), para além dos clássicos requisitos intrínsecos da proporcionalidade (*supra*). (GONZALES-CUELLAR SERRANO, 1990). E, se é assim para tão eminentes situações jurídico-subjetivas constitucionais, não é sequer razoável supor que, em relação à liberdade de expressão (e/ou ao direito público de informação), iguais restrições não se possam verificar concretamente.

Se tais restrições serão justificadas por um “direito ao esquecimento” – que, a nosso ver, poderia (e deveria) ser reconhecido, em casos concretos, como derivação do direito geral de personalidade²⁷, especialmente no universo digital –, ou se serão explicadas sucedaneamente por qualquer outro fundamento jurídico racionalmente posto (basicamente porque o Excelso Pretório “desautorizou” o conceito), é definitivamente o que menos importa.

Considerações finais

Embora a passagem do tempo não tenha o condão de apagar o passado e fazer novas as experiências nele vivenciadas, certamente consegue fazer com que

após livrar-se de Traynor – denunciado às autoridades policiais em 1973 – e se casar novamente, afastou-se definitivamente do *set* pornográfico e se tornou ativista contra a indústria da pornografia. Nada obstante, o passado jamais lhe deixou em paz: Susan padeceu com sucessivos quadros de depressão até o acidente automobilístico que a vitimou, em 2002. Jamais buscou impedir, em juízo, a circulação do fatídico filme (e de outros de que participou, antes e depois, entre 1971 e 1975); mas, supondo-se verdadeiras as circunstâncias narradas (inclusive quanto aos ensejos de violência física, psíquica e moral, como também a condição de extrema exploração econômica a que foi submetida, ainda que não se possa refutar, pelas regras então em vigor e à vista das evidências disponíveis, a “licitude” das imagens obtidas e publicadas), *pode-se cogitar do quanto poderia ser justo e pedagógico assegurar judicialmente um “direito ao esquecimento” para quem se submeteu a espetáculos ou obras de caráter público assim degradantes*. Cfr., por todos, a autobiografia *Ordeal* (LOVELACE, McGRADY, 1980, *passim*), reportando, inclusive, a suposta condição pretérita de “*porn slave*”. Ainda a esse respeito, apresentando parcialmente o drama narrado em *Ordeal* (*supra*), pode-se ver a película *Lovalece* (2013), de Rob Epstein e Jeffrey Friedman, com Amanda Seyfried como Lovalece; o filme, porém, foi recebido pela crítica especializada com algum ceticismo (inclusive pela forma como o roteiro teria “simplificado” os obscuros escaninhos da indústria pornográfica norte-americana).

27 A dita “doutrina pluralista” dos direitos de personalidade fragmenta a proteção jurídica da pessoa humana a partir do reconhecimento de direitos personalíssimos “tipificados” em fontes formais do direito interno (o que, no limite, termina por *desguarnecer* aspectos da personalidade ainda não alcançados por textos legislativos, como no Brasil se daria, e.g., com o direito à tranquilidade psíquica, o direito a um projeto de vida - quiçá superado, na esfera trabalhista, com a edição da Lei 13.467/2017 e o art. 223-B da CLT -, o próprio direito ao esquecimento ou mesmo, em uma perspectiva futurista, o direito de não ser clonado). Com efeito, “*as disposições legais não esgotam todo o conteúdo da tutela da personalidade humana, surgindo aspectos que não encontram proteção nas normas legais existentes*” (BELTRÃO, 2005, p. 54); isso é tanto mais verdadeiro quando se constata a progressiva configuração de novas dimensões a serem tuteladas, em vista da evolução dinâmica do conceito de pessoa (humana) e de seus predicamentos. Já por isso, é de rigor reconhecer, à maneira do art. 70º do Código Civil português, a preexistência de um “[...] *direito geral da personalidade [que] pugna pelo reconhecimento de que a personalidade deve ser protegida de forma global, considerando a própria natureza da pessoa, que representa um valor unitário. Proclama-se a existência de um direito que protege a pessoa como um todo, apto a tutelar qualquer aspecto da personalidade, coibir qualquer tipo de comportamento lesivo. A proteção não se esgota em direito tipificados*” (GARCIA, 2007, pp. 73 e ss.). É como pensamos.

determinadas chagas – especialmente as morais e psíquicas – sejam cicatrizadas. Assegurar essa recomposição, na perspectiva da tutela de um direito geral de personalidade, pode seguramente se antepor a um “direito à memória” individual ou coletiva, a depender das circunstâncias de cada caso. Esse direito deve ser preservado, ao revés, quando igualmente alicerçado em interesses jurídicos legítimos, como aqueles relacionados à restauração e salvaguarda dos registros históricos de contextos sangrentos, ditatoriais ou violentos a que se sujeitou determinado grupo social, comunidade ou população nacional. De outra parte, quando tais interesses não estão presentes, ou ainda quando sejam meramente residuais, inaptos a exigir do indivíduo o sacrifício vitalício de sua integridade, o assim chamado “direito ao esquecimento” – ou à honra, ou à imagem, ou à privacidade, ou como se queira denominá-lo (à vista da tese de repercussão geral aprovada por ocasião do julgamento do RE 1.010.606) – deverá ser judicialmente assegurado, particularmente diante dos riscos macrolesivos das exposições pela via digital. Nada obsta, ademais, a que essa tutela se assegure inclusive preventivamente, na linha do que dispõe o art. 70º do Código Civil português quanto à tutela geral da personalidade (“*Independente-mente da responsabilidade civil a que haja lugar, a pessoa ameaçada ou ofendida pode requerer as providências adequadas às circunstâncias do caso, com o fim de evitar a consumação da ameaça ou atenuar os efeitos da ofensa já cometida*”).

Nessa senda, o fundamento da dignidade da pessoa humana – e, por ele, o resguardo de predicamentos irrenunciáveis e indisponíveis do direito geral de personalidade, como a integridade moral e psíquica do indivíduo – remete seguramente para a necessidade de compatibilização entre a liberdade de expressão e os ditos direitos personalíssimos (ou, como entendemos, os aspectos do direito geral de personalidade), mesmo à margem da tipificação legal de um “direito ao esquecimento”. Ademais, na perspectiva do direito digital, há um interesse público primário, essencialmente difuso, que se põe como supedâneo universal das pretensões legítimas ao “esquecimento”, na medida em que, a bem da moralidade pública e da pacificação social, interessa a toda sociedade que determinadas informações individuais, coletadas no bojo das relações contratuais a que habitualmente as pessoas se sujeitam (como, *e.g.*, o contrato de trabalho), sejam anonimizadas ou descartadas após o cumprimento de suas finalidades.

Na tensão entre o tempo e a memória, enfim, melhor seria evocar o Bardo:

*Não, Tempo, não zombarás de minhas mudanças!
As pirâmides que novamente construístes
Não me parecem novas, nem estranhas;
Apenas as mesmas com novas vestimentas.*
(William Shakespeare)

O tempo, com efeito, pode ser cruel, sobretudo se as suas marcas negativas se perenizarem, reconstituindo-se incessantemente, qual pena perpétua, em detrimento de quem já não deveria suportar sobre os ombros o mesmo peso moral de outrora. Sob tais circunstâncias, se a expressão ou a informação pública não possuir real interesse público, a pessoa humana – e a sua individualidade – deve-

rá ter a primazia da proteção. Isto inclusive está subentendido na própria Tese de Repercussão Geral n. 786, a despeito da sua pretendida ruptura conceitual.

REFERÊNCIAS

AGÊNCIA BRASIL. **Para Bolsonaro, não houve ditadura no Brasil**. Brasília, 27/03/2019. Disponível em: <https://agenciabrasil.ebc.com.br/politica/noticia/2019-03/para-bolsonaro-nao-houve-ditadura-no-brasil>, acesso em 10/10/2021.

ALEXY, Roberto. **Epílogo a la teoría de los derechos fundamentales**. Trad. Carlos Berbal Pulido. Madrid: Colegio de Registradores de la Propiedad y Mercantiles de España (Centro de Estudios), 2004.

BELTRÃO, Silvio Romero. **Direitos da personalidade**: De acordo com o novo código civil. São Paulo: Atlas, 2005.

BENTIVEVEGNA, Carlos Frederico Barbosa. BAUAB, José Renato Felix. Direito ao esquecimento: Necessidade jurídica e de saúde. **Revista de Direito e Medicina**, vol. 6, Mai-ago. 2020, p. 1/17.

BLADE Runner. Direção: Ridley Scott. Produção: Michael Deeley. Intérpretes: Harrison Ford; Rutger Hauer; Sean Young; Edward James Olmos e outros. Roteiro: Hampton Fancher e David Peoples. Música: Vangelis. Los Angeles: Warner Brothers, c1991. 1 DVD (117 min). widescreen, color. Produzido por Warner Video Home. Baseado na novela “Do androids dream of electric sheep?” de Philip K. Dick.

BRASIL. **Constituição Federal da República Federativa do Brasil: de 5 de outubro de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 16/8/21.

BRASIL. **Lei 4.504, de 30 de novembro de 1964**. Dispõe sobre o Estatuto da Terra e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l4504.htm. Acesso em 22/8/2021.

BRASIL. **Lei n. 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e p para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm . Acesso em 22/8/2021.

BRASIL. **Lei n. 12.528, de 18 de novembro de 2011**. Cria a Comissão Nacional da Verdade no âmbito da Casa Civil da Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12528.htm . Acesso em 22/8/2021.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em 16/8/21.

BRASIL. Poder Judiciário. **Enunciado n. 531**. VI Jornada de Direito. Civil. Brasília, 2013. Disponível em: cjf.jus.br/enunciados/142. Acesso em 18/8/2021.

BRASIL. Superior Tribunal de Justiça. **Agravo regimental no Habeas corpus (AgRg no HC) n. 642772 / SC**. Relator: Data do julgamento: 04/05/2021, disponível em: <https://scon.stj.jus.br/SCON/pesquisar.jsp> . Acesso em 22/8/2021.

BRASIL. Superior Tribunal de Justiça. Notícias. **Quarta Turma volta a discutir**

violação à honra em programa sobre Chacina da Candelária após decisão do STF sobre direito ao esquecimento. Brasília, 05/8/2021, Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05082021-Quarta-Turma-volta-a-discutir-violacao-a-honra-em-programa-sobre-Chacina-da-Candelaria-apos-decisao-do-STF-sobre.aspx> . Acesso em 18 de agosto de 2021.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial Nº 1.334.097 - RJ (2012/0144910-7)**. Relator: Ministro Luis Felipe Salomão. Órgão julgador: Quarta Turma. Data do Julgamento: 28/5/2013, Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=31006510&num_registro=201201449107&data=20130910&tipo=5&formato=PDF . Acesso em 18/8/2021.

BRASIL. **Supremo Tribunal Federal. Recurso Extraordinário RE 1010606/ RJ**. Relator: Ministro Dias Tófolis. Órgão julgador: Pleno. Data do julgamento: 11/2/2021. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&pesquisa_inteiro_teor=false&sinonimo=true&plural=true&radicais=false&buscaExata=true&page=1&pageSize=10&queryString=tese%20de%20repercuss%C3%A3o%20geral%20direito%20ao%20esquecimento&sort=_score&sortBy=desc . Acesso em 21/8/21.

CIGANA. Paula Fabíola. ROCHA. Maria Célia Albino da. Direito ao Esquecimento: os limites do direito à informação e a liberdade de expressão na era tecnológica. In: Direitos e garantias fundamentais. **II. CONPEDI**. SILVA. Delmo Mattos da. FREITAS. Riva Sobrado de. BEÇAK. Rubens. (Coordenadores) Florianópolis: CONPEDI, 2017. Disponível em: <http://site.conpedi.org.br/publicacoes/27ixg-md9/o61z9nus/jcLr8pW0U47C9875.pdf> . Acesso em 15/8/21.

COELHO. Júlia Costa de Oliveira. **Direito ao esquecimento e seus mecanismos de tutela na internet: como alcançar uma proteção real no universo virtual?** Schreiber. Anderson. MORAES. Bruno Terra de. TEFFÉ. Chiara Spadaccini de. (coordenadores). Indaiatuba, SP: Editora Foco, 2020.

FELICIANO, Guilherme Guimarães. **Por um processo realmente efetivo: Tutela processual de direitos humanos fundamentais e inflexões do *due process of law***. São Paulo: LTr, 2016.

FRAJHOF, Isabella Zalcborg. **O Direito ao esquecimento na internet**. São Paulo: Almedina, 2019.

GARCIA, Enéas Costa. **Direito geral da personalidade no sistema jurídico brasileiro**. São Paulo: Juarez de Oliveira, 2007.

GONZALES-CUELLAR SERRANO, Nicolas. **Proporcionalidad y derechos fundamentales en el proceso penal**. Madrid: Colex, 1990.

LARANJA Mecânica. Direção: Stanley Kubrick. Produção: Warner Bros; Hawk Films, 1971, DVD (137 min.). Intérpretes: Malcolm McDowell, Adrienne Corri, Patrick Magee e outros. Música: Wendy Carlos. Reino Unido/EUA.

LIMA. Erik Noleta Kirk Palma. Direito ao Esquecimento. Discussão europeia e sua repercussão no Brasil. **Revista Legislativa**. Ano 50, n. 199, jul./set. 2013, p. 271/283. Disponível em: https://www12.senado.leg.br/ril/edicoes/50/199/ril_v50_n199. Acesso em: 17/8/2021.

LOVELACE, Linda. McGRADY, Mike. **Ordeal: An autobiography**. New York:

Citadel Press, 1980.

MANSUR, Rafael. Decisão do STF não é ‘pá de cal’ no direito ao esquecimento. Opinião. **Consultor jurídico**. 24 de fevereiro de 2021. Disponível em: <https://www.conjur.com.br/2021-fev-24/mansur-stf-nao-jogou-pa-cal-direito-esquecimento>. Acesso em: 2.9.2021.

MATRIX. Direção: As Wachowski. Produção: Joel Silver. Distribuição: Warner Bros. 1999, (136min). Intérpretes: Keanu Reeves; Laurence Fishburne; Carrie-Anne Moss e outros. Música: Don Davis.

MAURMO. Júlia Gomes Pereira. Direito ao Esquecimento. **Enciclopédia Jurídica da PUC-SP**. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freira (coords.). Tomo Direito Administrativo e Constitucional. Vidal Serrano Nunes Jr., Maurício

MELO. O significado do Direito ao Esquecimento. Termo não parece ser uma boa escolha de palavras. **Conjur**. 22 de nov. de 2016, Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/o-significado-direito-ao-esquecimento-22112016>. Acesso em 22 de agosto de 2021.

MONTERO, Etienne. VAN ENIS, Quentin. Les métamorphoses du droit à l’oubli sur le net. In: **Revue générale de droit civil belge**. [s.l.]: Wolters Kluwer, 2016. n. 5.

OLIVEIRA, Carlos. SCHREIBER, Anderson. SOUZA. Direito ao esquecimento e liberdade de expressão – Tema 786: os impactos da decisão do STF. Debate jurídico. **Canal Direito Civil Brasileiro**. TOSCANO, Rodrigo. (Coordenador). Duração: 1:58:51. Disponível em: [youtube.com/watch?v=as-0A9vvwk8](https://www.youtube.com/watch?v=as-0A9vvwk8). Acesso em 18/08/2021.

OPENWORK. **Le droit à l’oubli en entreprise**. Disponível em: <https://www.openwork.co/fr/blog/le-droit-loubli-en-entreprise>, acesso em 10/10/2021.

ORWELL. George. **1984**. Tradução: Heloisa Jahn e Alexandre Hubner. São Paulo: Companhia das Letras, 2019.

PINHEIRO, Denise. **A liberdade de expressão e o passado: Desconstrução da ideia de um direito ao esquecimento**. Tese de Doutorado. Florianópolis: Universidade Federal de Santa Catarina/Centro de Ciências Jurídicas, 2016.

ROSEN. Jeffrey. The right to be forgotten. **Stanford Law Review**, v. 64, Stanford, Feb. 2021, p. 88-92. Disponível em: <https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/>. Acesso em 21/8/2021.

SARLET, Ingo Wolfgang. Direitos Fundamentais. Do caso Lebach ao caso Google vs. Agencia Espanhola de Proteção de Dados. **Consultor Jurídico**. Disponível em: www.conjur.com.br/2015-jun-05/direitos-fundamentais-lebach-google-vs-agencia-espanhola-protecao-dados-mario-gonzalez. Acesso em 19/08/2021.

SARLET, Ingo Wolfgang. Direitos fundamentais. Do caso Lebach ao caso Google vs. Agencia Espanhola de Proteção de Dados. **Consultor Jurídico**. 5 de junho de 2015. Disponível em: <https://www.conjur.com.br/2015-jun-05/direitos-fundamentais-lebach-google-vs-agencia-espanhola-protecao-dados-mario-gonzalez?imprimir=1>. Acesso em 20/8/2021.

SARLET, Ingo Wolfgang. Direitos Fundamentais. STF e direito ao esquecimen-

to: julgamento a ser esquecido ou comemorado? **Consultor Jurídico**. 5 mar 2021. Disponível em: <https://www.conjur.com.br/2021-mar-05/direitos-fundamentais-stf-direito-esquecimento-julgamento-esquecido-ou-comemorado> . Acesso em 21/8/2021.

SCHREIBER. Anderson. Nossa ordem jurídica não admite proprietários de passado. **Consultor Jurídico**. 12 de junho de 2017. Disponível em: <https://www.conjur.com.br/2017-jun-12/anderson-schreiber-nossas-leis-nao-aditem-proprietarios-passado> . acesso em 22/8/2021.

UNIÃO EUROPEIA. **Regulamento (Ue) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal oficial da União Europeia, L119/1, 4.5.2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679> . Acesso em 21/8/21.

WIKIPEDIA. **Caso Aída Curi**. Disponível em: https://pt.wikipedia.org/wiki/Caso_A%C3%ADda_Curi. Acesso em 21/8/21.

WOHJAN. Bruna Marques. WISNIEWSKI. Alice. Direito ao Esquecimento: Algumas Perspectivas. In: **XII Seminário Internacional de Demandas Sociais e Políticas na Sociedade Contemporânea. VIII mostra de trabalhos jurídicos científicos**. Departamento de Direito. Curso de Direito. CEPEJUR, 2015. Disponível em: <https://online.unisc.br/acadnet/anais/index.php/sidspp/article/view/13227/2271> . Acesso em 22/8/2021.

10. ADAPTAÇÕES NECESSÁRIAS DAS RELAÇÕES DE TRABALHO RESULTANTES DA LEI GERAL DE PROTEÇÃO DE DADOS

NECESSARY ADAPTATIONS OF LABOR RELATIONS RESULTING FROM THE GENERAL DATA PROTECTION LAW

XERXES GUSMÃO¹

Resumo

A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709, de 14 de agosto de 2018, conhecida sob a sigla LGPD, despertou enorme interesse no meio jurídico brasileiro, dados seus relevantes impactos em diferentes áreas. Uma destas, inegavelmente, são as relações de trabalho, as quais, apesar de não contarem com capítulo específico na nova lei, são indiscutivelmente atingidas pelos seus efeitos, considerando-se a grande quantidade de dados pessoais dos empregados que as empresas devem tratar para concretizar um contrato de trabalho. Efetivamente, a Lei Geral de Proteção de Dados Pessoais estende seu alcance a todas as fases contratuais, a saber: pré-contratual, pela necessidade de cautela no tratamento dos dados fornecidos pelo candidato ao emprego; no curso do contrato, na qual a empresa tem naturalmente contato com uma série de dados do empregado; na fase pós-contratual, na qual, apesar da ruptura contratual, a empresa deve ter cuidado no tratamento de dados do antigo empregado. Igualmente a Justiça do Trabalho é influenciada pelas diretrizes da LGPD, seja na questão da publicidade dos seus atos, seja na intrincada temática das provas digitais. Convém, assim, examinar detidamente os efeitos da LGPD na seara laboral, iniciando-se pelos fundamentos jurídicos da lei; passando-se, em seguida, ao exame dos seus efeitos nas relações de trabalho; concluindo-se a análise pelo estudo dos seus impactos na Justiça do Trabalho.

Palavras-chave: Lei Geral de Proteção de Dados Pessoais. Relações de Trabalho. Adaptações necessárias.

Abstract

The General Law for the Protection of Personal Data, Law No. 13.709, of August 14, 2018, known under the acronym LGPD, aroused enormous interest in the Brazilian legal community, given its relevant impacts in different areas. One of these, undeniably, are labor relations, which, despite not having a specific chapter in the new law, are indisputably affected by its effects, considering the large amount of personal data of employees that companies must process to materialize an employment contract. Effectively, the General Law for the Protection of Personal Data extends its scope to all contractual phases, namely: pre-contractual, due to the need for care in the treatment of data provided by the job candidate; in

¹ Mestre e Doutor em Direito do Trabalho e Previdenciário, pela Universidade de Paris 1 – Panthéon-Sorbonne. Professor dos programas de pós-graduação da UNISANTA/SP, da FAESA/ES e da ESA/ES. Autor de livros e artigos científicos. Juiz do TRT da 17ª Região (ES). Email: xerxesgusmao@gmail.com.

the course of the contract, in which the company is naturally in contact with a series of employee data; in the post-contractual phase, in which, despite the contractual break, the company must be careful in the treatment of data from the former employee. Likewise, the Labor Court is influenced by the guidelines of the LGPD, whether in the issue of publicity of its acts, or in the intricate theme of digital evidence. It is therefore appropriate to carefully examine the effects of the LGPD in the labor field, starting with the legal foundations of the law; then moving on to an examination of its effects on labor relations; concluding the analysis through the study of its impacts on the Labor Court.

Keywords: General Law on Protection of Personal Data. Labor relations. Necessary adaptations.

1. Introdução

A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709, de 14/08/2018, conhecida sob sua sigla LGPD, impactou uma série de elementos das relações sociais no Brasil, desde o início da sua vigência.

Como não poderia deixar de ser, as relações de trabalho foram igualmente afetadas, dado seu papel essencial na sociedade brasileira e a utilização de quantidade considerável de dados pessoais dos trabalhadores pelas empresas.

Para melhor compreensão destes impactos na seara laboral, convém examinar, inicialmente, os fundamentos jurídicos da LGPD, que expõem claramente suas linhas diretoras e consequentes efeitos na área trabalhista.

Posteriormente, passar-se-á à análise detida dos impactos da LGPD nas relações de trabalho, em suas diferentes fases: pré-contratual, durante as tratativas para seleção dos candidatos ao emprego; no curso do contrato, no qual os efeitos são variados; pós-contratual, na qual o tratamento dos dados pessoais dos antigos empregados igualmente demanda cautela.

Por derradeiro, serão estudados os efeitos da LGPD na Justiça do Trabalho, seja no que concerne à delicada relação entre a publicidade dos atos judiciais e os cuidados necessários no tratamento de dados pessoais, seja no tocante à atual e intrincada questão das provas digitais, à luz dos parâmetros da LGPD.

2. Fundamentos jurídicos da LGPD

A Lei Geral de Proteção de Dados Pessoais, com início de vigência do seu bloco principal de medidas em 18 de setembro de 2020, é uma lei dotada de fundamentos jurídicos expressamente previstos nos seus artigos iniciais.

Convém, assim, iniciar o presente estudo pelo exame dos principais dentre estes fundamentos jurídicos, para, em seguida, passar propriamente aos impactos da LGPD nas relações de trabalho e na Justiça do Trabalho.

2.1 Objeto

O objeto da LGPD é expressamente previsto pelo seu artigo 1º, nos seguintes termos:

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natu-

ral ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Trata-se, por conseguinte, de lei que se destina a um campo vasto de atuação, pois abrange qualquer operação de tratamento de dados pessoais, não somente aquelas realizadas em meios digitais, desde que realizadas no território nacional (conforme previsão do artigo 3º da LGPD).

Há, contudo, exclusão de algumas operações referentes a dados pessoais, que não são passíveis da proteção da LGPD, na forma do seu artigo 4º. Nesse sentido, a LGPD não se aplica a operações de tratamento de dados pessoais realizadas por pessoa natural para fins exclusivamente particulares e não econômicos.

No mesmo diapasão, é excluído dos efeitos da LGPD o tratamento de dados pessoais realizado para fins exclusivamente jornalísticos e artísticos ou acadêmicos, ou, ainda, para segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

Por fim, as operações de tratamento de dados provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, são igualmente excluídas da LGPD, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

2.2 Princípios

A LGPD se reveste de inegável relevância, dada a importância dos dados pessoais na sociedade atual, em que se tornou simples e comum compartilhar, muitas vezes sem a ciência ou a anuência do titular, os seus dados pessoais.

Seu objetivo principal é, portanto, o de salvaguardar estes dados pessoais, visando proteger direitos fundamentais do seu titular, por meio de fundamentos e princípios específicos.

Nesse sentido, o artigo 2º da LGPD prevê como seus fundamentos:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

- I - o respeito à privacidade;
- II - a autodeterminação informativa;
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV - a inviolabilidade da intimidade, da honra e da imagem;
- V - o desenvolvimento econômico e tecnológico e a inovação;
- VI - a livre iniciativa, a livre concorrência e a defesa do consumidor;
- VII - os direitos humanos, o livre desenvolvimento da

personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Do mesmo modo, os princípios da LGPD são expressamente previstos no rol contido no seu artigo 6º.

São, assim, considerados como princípios da LGPD:

I — Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II — Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III — Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV — Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V — Qualidade de dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI — Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII — Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII — Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX — Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X — Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Existe, portanto, um robusto arcabouço principiológico, dotado de eficácia normativa – como qualquer princípio do nosso ordenamento jurídico, eis que superada a antiga visão atribuindo aos princípios função de mera fonte de inspiração interpretativa -, a ser considerado quando do tratamento de dados pessoais no Brasil.

2.3 Formas de tratamento

O tratamento de dados possui suas formas igualmente previstas pela LGPD, no seu artigo 7º, que enumera as respectivas hipóteses.

Desse modo, o fornecimento de consentimento pelo titular é a primeira modalidade prevista, sendo a preferencial.

Deve-se notar que o consentimento concedido para determinada hipótese de

tratamento não se estende a outras hipóteses, mesmo aquelas mediante compartilhamento, para as quais novos consentimentos são necessários.

No caso de dados pessoais cujo acesso é público, seu tratamento deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização, sendo dispensada, todavia, a exigência do consentimento do titular para dados tornados públicos por ele.

Ademais, a eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

Independente de consentimento, outrossim, o tratamento de dados em algumas hipóteses legais, especialmente: para o cumprimento de obrigação legal ou regulatória pelo controlador; quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Uma vez estabelecidos os fundamentos jurídicos gerais da LGPD, convém passar ao exame específico dos efeitos da LGPD nas relações de trabalho.

3. LGPD e relações de trabalho

Ainda que a LGPD não possua capítulo ou seção específicos sobre a matéria trabalhista, seus efeitos nesta são indiscutíveis, dada a relevância do tratamento de dados nas relações de trabalho, nas quais os interesses das partes são distintos, quicá antagonônicos.

Convém, portanto, realizar-se uma análise pormenorizada dos efeitos nas diferentes fases do contrato de trabalho.

3.1 LGPD na fase pré-contratual

Os efeitos da LGPD já se fazem sentir desde a fase pré-contratual do contrato de trabalho, na qual inúmeros dados pessoais dos candidatos são tratados pela empresa.

Ricardo Calcini e Dino Andrade examinam a questão da seguinte forma:

A fase pré-contratual é a etapa do primeiro contato do candidato com o potencial empregador e geralmente é realizada por terceiros (recrutador, departamento pessoal, empresas especializadas etc.). Nessa fase há disponibilização da vaga, análise do currículo, entrevistas e posterior escolha do candidato selecionado.

Naturalmente, os procedimentos preliminares a um contrato de trabalho legitimam o acesso aos dados pessoais do candidato logo a partir do anúncio de um emprego, devendo o empregador se ater ao estritamente necessário para o exercício da função a ser contratada. Em outras palavras, o empregador pode solicitar ao empregado o nome completo, a data de nascimento, estado civil, escolaridade, o número do CPF, filiação, a numeração do

RG, o endereço de domicílio, o contato telefônico, e-mail pessoal ou corporativo, IP do computador etc.

Ainda na fase preliminar, é proibida a coleta de dados sensíveis que possam gerar qualquer critério discriminatório entre os candidatos. De modo que é de suma importância que o empregador avalie quais serão os dados requeridos ao candidato para que não haja descumprimento das normas legais. (CALCINI; ANDRADE, 2021, p. 01-02)

Justifica-se, portanto, o exame apartado dos principais dentre estes efeitos da LGPD na fase prévia do contrato de trabalho.

3.1.1 Cautela na coleta de dados

Como salientado acima, na fase anterior à vigência do contrato de trabalho, a LGPD já possui efeitos. Isto porque nesta fase, em consonância com os fundamentos e princípios da LGPD, examinados acima, é proibida a coleta de dados que possam representar qualquer critério discriminatório entre os candidatos, como a solicitação de exames de gravidez, toxicológico, de sangue; o atestado de antecedentes criminais; a análise de crédito.

A demanda deste tipo de documentos representaria inefável violação à Lei 9.029/95 e aos artigos 5º, *caput* e 7º, XXX da CF/88, que vedam qualquer forma de discriminação nas relações em geral e trabalhistas no Brasil.

Valéria Reani apresenta essa vedação às práticas discriminatórias na fase pré-contratual, nos seguintes termos:

Um dos princípios basilares de LGPD é o da não discriminação. Ele determina que uma pessoa não pode ser discriminada, de modo que a prejudique, com base nos seus dados pessoais. Ainda, a LGPD confere ao titular — a pessoa física a quem os dados se referem —, o direito de ter acesso a todos os dados que uma entidade, privada ou pública, tem sobre ela. Assim, o cidadão poderia verificar realmente quais dados sobre ele a empresa tinha em mãos e o que fez com tais dados após o uso dos mesmos.

A LGPD, de forma objetiva, reforça, por exemplo, o que o direito trabalhista já consolidou na Consolidação das Leis do Trabalho, no capítulo específico para proteção do trabalho da mulher, aonde consta expressamente a vedação da discriminação. (REANI, 2020, p. 03-04)

Nesse sentido, a empresa não poderá coletar dados com viés discriminatório dos candidatos ao emprego, por não poderem servir de fundamento à admissão, devendo, ademais, dar inteira ciência ao candidato ao emprego dos dados que estão sendo coletados e tratados.

Há, contudo, exceções expressamente previstas em normas trabalhistas esparsas. Uma delas concerne ao exame toxicológico do motorista profissional, passível de

exigência, nos termos do artigo 168, §6º da CLT.

Outrossim, o atestado de antecedentes criminais é exigível do vigilante, na forma dos artigos 12 e 16, VI, da Lei n. 7.102/1983 c/c art. 4º, I da Lei n. 10.826/2003.

Fora dessas hipóteses excepcionais, entretanto, é absolutamente incompatível com a LGPD a exigência deste tipo de documento, pois configura hipótese discriminatória.

Conveniente mencionar, ainda, tema objeto de acalorada cizânia: as redes sociais dos candidatos. De fato, a possibilidade ou não de uso dos dados nelas contidos para seleção enseja fortes dúvidas e questionamentos.

A melhor forma de harmonizar a LGPD com este uso dos dados oriundos das redes sociais dos candidatos é aquela que priorize a extração unicamente de dados relacionados à experiência profissional do candidato, sem uso de dados privados.

Além disso, somente dados tornados espontaneamente públicos pelo seu titular podem ser utilizados, sem acesso a redes restritas do candidato, pois este uso igualmente violaria a LGPD.

Isto porque este uso de dados da vida privada ou de rede restrita do candidato frequentemente se insere em hipótese de discriminação, vedada pela LGPD, além de violar direitos fundamentais dele, como a intimidade e a vida privada.

3.1.2 Mitigação dos riscos e destino dos dados

Em linhas gerais, a empresa deve respeitar, na fase pré-contratual, ao realizar o processo de seleção de candidatos, o princípio da minimização da coleta de dados, coletando-se somente os dados estritamente necessários ao processo seletivo.

Além disso, é fortemente recomendável que a empresa elabore um documento pelo qual o candidato ao emprego indique o seu consentimento expresso com a coleta e a utilização dos seus dados pela possível contratante.

Desse modo, a empresa seguramente logrará mitigar significativamente o risco de realizar a coleta indevida de dados pessoais dos candidatos.

Outrossim, a empresa deverá informar claramente aos candidatos não selecionados a política de utilização dos dados que foram fornecidos, além do destino dos dados e documentos daqueles que não foram selecionados.

Ela deve, assim, desfazer-se daqueles dados, uma vez rejeitado o candidato ao emprego, pois cessada a finalidade do seu tratamento, nos termos do artigo 15 da LGPD, salvo se existente a possibilidade de contratação futura, ainda que não formalizada de imediato, fato que deve ser devidamente informado ao candidato.

3.2 LGPD no curso do contrato

Presentes desde a fase pré-contratual, os efeitos da LGPD no curso do contrato de trabalho são igualmente variados. Nesse diapasão, o tratamento de dados pessoais dos trabalhadores deve ser realizado de acordo com os parâmetros já examinados acima da LGPD, nos termos do seu artigo 7º.

Dada a relevância e a tutela de direitos fundamentais da LGPD, seus efeitos são imediatos sobre todos os contratos de trabalho: os contratos novos deverão ser realizados de acordo com os novos parâmetros da LGPD, já sendo formatados nesses novos moldes; os contratos em curso deverão ser adequados, ajustando o tratamento de dados dos antigos empregados às diretrizes da nova lei.

Este ajuste no tratamento dos dados pessoais dos empregados deve seguir uma

diretriz geral de cautela e finalidade, como observa Fabrício Lima Silva no seguinte trecho de artigo sobre o tema:

Diante desse contexto, pode-se verificar que o novo sistema imposto pela LGPD, embora tenha trazido várias balizas para o tratamento dos dados pessoais, não impediu que tais dados continuassem sendo coletados e utilizados na seara trabalhista.

A nova legislação inaugurou um modelo de responsabilidade e de conscientização sobre novos parâmetros para proteção da privacidade em nosso país.

Assim, antes de se procurar obter o consentimento a qualquer custo, com a utilização de açodados aditivos contratuais, melhor seria que as empresas efetuassem um inventário dos dados tratados em suas atividades corriqueiras, procurando encontrar as bases legais justificadoras do tratamento.

E, se inexistente base legal diversa do consentimento, deveriam analisar, com base na proporcionalidade, se existente a efetiva necessidade de tratamento e a adequação às finalidades apresentadas, diante da inexistência de outros meios menos intrusivos para consecução do mesmo objetivo. Se não preenchidos tais requisitos, o dado deveria ser eliminado.

Por fim, somente no caso de efetiva necessidade de tratamento, uma vez cumprido o teste de proporcionalidade, deveria ser obtido o consentimento do empregado, tomando todas as cautelas devidas para que a vontade seja manifestada livremente e com a devida documentação. (SILVA, 2021, p. 05-06)

Convém examinar, assim, de forma apartada, os campos de incidência mais relevantes destes efeitos da LGPD no curso do contrato de trabalho.

3.2.1 Documentos mantidos pela empresa

A empresa, em função do contrato de trabalho mantido com o empregado, tem de manter uma série de documentos dele, contendo dados pessoais, por vezes sensíveis. Deve, portanto, tratá-los em consonância com a LGPD.

Pode-se mencionar, inicialmente, a ficha de registro, na qual é comum a existência de dados pessoais e de dados sensíveis, a exemplo da filiação a sindicato.

Nesse aspecto, a LGPD prevê expressamente a necessidade de tratamento desses dados com a limitação de acesso, com consentimento expresso do empregado ou por interesse público e para fins específicos (art. 11).

Aliás, conveniente reiterar que a obtenção do consentimento do empregado, apesar de ser uma conduta desejável, não constitui uma obrigação para qualquer tipo de tratamento de dados pessoais dele, eis que existem situações que prescindem desta

anuência expressa, especialmente as necessárias para o cumprimento de obrigação legal ou para a execução do contrato (na forma do artigo 7º, II e V da LGPD).

Leandro Araújo trata do tema da seguinte forma:

É preciso ficar claro que nem sempre é preciso o «consentimento» do titular (pessoa natural) para o tratamento de dados. Embora o primeiro contato com a matéria remeta o raciocínio a tal exigência, certo é que referida hipótese só deve ser utilizada quando da ausência e/ou impossibilidade de enquadramento de todas outras. E a razão parece ser óbvia: o consentimento pode ser revogado a qualquer tempo (artigo 8º, parágrafo 5º), o que coloca o controlador em uma situação delicada.

Tratando exclusivamente de relações de trabalho, conclui-se que o empregador e/ou contratante, pode se valer, como regra (sem prejuízo de avaliação caso a caso), da previsão contida no artigo 7º, incisos II e V (para dados pessoais), e artigo 11, inciso II, alíneas “a” e “d” (para dados pessoais sensíveis), isto é, quando o tratamento deriva de obrigação legal, ou, ainda, quando necessário para execução do contrato. Portanto, regular o tratamento de dados pessoais sem que a haja a necessidade de colher o expreso consentimento do titular nesse particular. (ARAÚJO, 2020, p. 03)

Nesse diapasão, a realização de exames médicos periódicos, com previsão legal, independe da anuência do empregado, antes ou após a LGPD.

Todavia, não podem ser solicitados exames que possam expor a saúde do trabalhador a fim de causar-lhe discriminação, sem qualquer vínculo efetivo com o trabalho, a exemplo dos exames de HIV, gravidez ou câncer.

Isso para se salvaguardar o respeito a preceitos constitucionais (especialmente a dignidade e a intimidade) e à LGPD (para evitar o desrespeito ao requisito da finalidade dos dados pessoais).

Além disso, atestados médicos entregues pelo empregado contendo CID deverão ser mantidos sob sigilo pelo empregador, por se tratar de dado sensível. O procedimento da anonimização é fortemente recomendável, neste caso.

Por fim, o registro da jornada de trabalho, desde o advento da Portaria nº 1.510/2009, do extinto Ministério do Trabalho, pode ser realizado por meio de controle de ponto biométrica.

Sucedo que a biometria constitui um dado pessoal sensível, na forma do artigo 5º, II da LGPD. Nesse sentido, a empresa deve ter toda a cautela no armazenamento dessa biometria registrada nos controles de ponto do seu empregado, com acesso restrito, somente devendo utilizá-la para a sua específica finalidade.

3.2.2 Vigilância dos empregados

A vigilância de empregados, fortemente potencializada pelas novas tecnolo-

gias, pode ocorrer por meio de variadas ferramentas (e-mails, redes sociais, dispositivos funcionais, dispositivos pessoais, geolocalização).

A LGPD não proíbe o acesso a e-mails ou dispositivos funcionais dos empregados, abstratamente analisando a questão.

Entretanto, a informação deverá ser clara, indicando que a vigilância ocorre, dispondo do propósito e finalidade da coleta, assim como deverá ter a ciência do funcionário quanto aos limites do acesso da empresa aos seus dados pessoais e o tratamento que será destinado a esses dados, ainda que não se exija seu consentimento (art. 7º, IX).

Cumprido salientar, ademais, que esta vigilância deve respeitar a intimidade e a vida privada do empregado, não podendo ocorrer em locais reservados (vestiários, sanitários) ou com ferramentas privadas do empregado (emails pessoais, redes sociais restritas, entre outras).

Tércio Souza destaca esse cuidado que a empresa deve ter com a intimidade dos seus empregados, à luz dos preceitos da LGPD, da seguinte forma:

O direito à privacidade foi reconhecido pelo Constituinte como direito fundamental de todos. Em um mundo tão conectado, não parece haver dúvidas de que tal direito à privacidade encontra-se a cada dia sujeito às suas mais variadas compreensões.

Coube ao legislador apresentar, através da LGPD, mas não apenas, uma delimitação geral acerca da preservação da privacidade e dos tratamentos de dados pessoais, atribuindo àqueles responsáveis pela custódia de tais informações, os ônus decorrentes desta mesma guarda.

O acesso a dados pessoais, pelo empregador, configura-se em verdadeira obrigação legal. Serve como instrumento à própria operacionalização da relação de trabalho, mas a sua guarda e tratamento, a partir de então, explicitamente passa a estar adstrita à condições adequadas de uso e guarda, as quais descumpridas, parecem poder violar a privacidade do empregado e ocasionar danos da natureza moral, a serem apuradas em sua existência e extensão, caso a caso.

Sem prejuízo das demais questões fiscalizatórias, concluímos que a LGPD encaminha outras obrigações, inclusive atinentes ao dever de indenizar, para aqueles que descuidem-se da gestão dos dados inerentes às relações de trabalho, e que em razão de tais descuidos, violem a privacidade e intimidade das pessoas físicas cujos dados encontrem-se protegidos por aquela Lei. Nos parece que tais repercussões não podem ser ignoradas, nem que tais obrigações possam ser relevadas. (SOUZA, 2020, p. 09-10)

Desse modo, o monitoramento interno e externo do ambiente da empresa é permitido, mas deverá ser justificado e com a ciência do empregado, zelando pela transparência e necessidade, com informação clara e respeito aos princípios da LGPD, em especial a finalidade deste monitoramento.

Conveniente examinar, ademais, o teletrabalho, no qual é permitido e mesmo necessário o controle, pelo empregador, das ferramentas de trabalho do teletrabalhador, como computador ou telefone, inclusive pelo uso de câmeras, eis que o trabalho é executado à distância.

Estas ferramentas do teletrabalho são, aliás, elementos de configuração da própria subordinação do empregado (na forma do artigo 6º, parágrafo único da CLT).

Todavia, esse controle deve se limitar ao trabalho executado, não podendo englobar elementos estranhos a ele, como a atividade de membros da família do empregado ou detalhes da residência do empregado, que eventualmente fiquem visíveis durante a prestação de serviços do empregado.

Isso porque, repise-se, tal controle representaria violação a preceitos constitucionais (sobretudo dignidade e intimidade) e ao requisito da finalidade da Lei Geral de Proteção de Dados Pessoais.

3.3 LGPD na fase pós-contratual

Mesmo na fase pós-contratual a LGPD demanda cautela por parte da empresa, pois o tratamento de dados do antigo empregado deve ser realizado em consonância com os seus preceitos.

Isso se dá pelo fato de que a LGPD, expressamente, estipula ser necessária a informação de finalização do uso de dados, seja por determinação legal, seja por solicitação do titular do direito.

Ocorre que, no caso das relações trabalhistas, há obrigações de guarda de documentos que decorrem de imposição legal, o que afasta a possibilidade de eliminação imediata destes dados do empregado, ainda que haja solicitação expressa de sua parte.

Por conseguinte, a empresa pode manter os dados pessoais gerais do empregado sob guarda, pelo prazo prescricional, de até dois anos após a ruptura contratual (art. 7º, XXIX da CF/88), para eventual utilização em reclamação trabalhista futura.

Ressalvam-se, todavia, os dados referentes a pedidos submetidos a prazos diferenciados de prescrição – como os referentes a doença ocupacional, cujo marco prescricional somente se inicia com a ciência inequívoca da enfermidade - ou, ainda, imprescritíveis, como os referentes à própria declaração do vínculo empregatício, cuja guarda não está, portanto, limitada ao prazo prescricional trabalhista ordinário, como salientam Rodolpho Pamplona e Vicente Vasconcelos no trecho seguinte:

No caso do direito do trabalho além das obrigações decorrentes das imposições legislativas, as empresas poderão recusar-se a eliminar dado, mantendo o arquivamento de documentação dos ex-empregados, durante o prazo prescricional de 02 (dois) anos, observado o critério da prescrição quinquenal nos termos do artigo 11 da CLT, para eventuais defesas em futuros passivos trabalhistas, além

da obrigação de guarda de informações para compartilhamento com convênios de saúde em caso de aposentadoria ou desligamento sem justa causa, dentre outras, tal como provocado por Leandro Sampaio Correa de Araújo, para os casos que não foram esclarecidas pelo legislador que, por exemplo “envolvam doenças e/ou acidentes, pois o marco prescricional tem como ponto de partida o efetivo conhecimento do titular (diagnóstico e extensão dos danos) ou quando do evento morte (titular), sendo os herdeiros menores, caso em que não é deflagrado de imediato o prazo prescricional”, ou ainda na demandas de natureza declaratória, imprescritíveis pela própria natureza, tal como numa hipotética situação na qual um ex-funcionário requeira o fornecimento de dados para fins previdenciários ou do próprio PPP (Perfil Profissiográfico Previdenciário), que certamente demandarão autorização de ampliação do período de guarda pelo empregador, para salvaguardá-lo perante as exigências da LGPD. (PAMPLONA FILHO; CONI JUNIOR, p. 29).

A regra geral permanece, contudo, a de que, após o prazo prescricional bienal, findando a finalidade da sua guarda, devem ser descartados estes documentos do antigo empregado.

Deve ser apontado, outrossim, que a empresa não poderá compartilhar, mesmo no prazo prescricional, estes dados sob guarda, ainda que não haja oposição expressa do empregado nesse sentido, por não se atender à sua finalidade específica de guarda este compartilhamento.

3.4 Responsabilidade da empresa

O exame detalhado dos efeitos da LGPD no contrato de trabalho demonstra, de forma inegável, a sua relevância na seara laboral.

Será necessário, por conseguinte, que se passe a adotar diversos ajustes no tratamento de informações dos empregados pelo empregador, para salvaguardar seus dados gerais e, especialmente, os sensíveis.

Conclui-se, assim, que o descumprimento deste dever ensejará, inefavelmente, o direito do empregado a reparações variadas, em especial a indenização por danos morais, de acordo com os parâmetros contidos na própria LGPD, mais especificamente nos seus artigos 42 a 44.

Nos termos do artigo 42 da LGPD, o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

A fim de assegurar a efetiva indenização ao titular dos dados, o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador.

Por outro lado, os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente.

Por sua vez, o artigo 43 da LGPD estipula que os agentes de tratamento só não serão responsabilizados quando provarem que não realizaram o tratamento de dados pessoais que lhes é atribuído; que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Ademais, na forma do artigo 44 da LGPD, o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: o modo pelo qual é realizado; o resultado e os riscos que razoavelmente dele se esperam; as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Responde, ainda, pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas na LGPD, der causa ao dano.

Há, igualmente, previsão do trâmite da ação de reparação por danos, pelos parágrafos 2º a 4º do artigo 42 da LGPD, com possibilidade de inversão do ônus da prova a favor do titular dos dados quando o juízo entender verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

Urge destacar, por derradeiro, a existência de acalorada cizânia doutrinária acerca da modalidade de responsabilização da empresa pelo descumprimento das diretrizes da LGPD, se subjetiva ou objetiva.

Iuri Pinheiro e Vólia Bomfim analisam a questão da seguinte forma:

Os artigos 42 a 45 da Lei 13.709/18 tratam da responsabilidade civil patrimonial e extrapatrimonial dos agentes de tratamento de dados (controlador e operador).

Há forte tendência doutrinária em se adotar apenas a responsabilidade subjetiva, com culpa presumida e, via de consequência, em afastar o entendimento de responsabilidade civil objetiva do empregador, por aplicação do artigo 42 e incisos II e III do artigo 43 da LGPD, que expressamente isenta de responsabilidade aquele que não violou a lei. A exceção se faz às relações de consumo, pois excluídas pelo artigo 45 da Lei 13.709/18.

A tese tem amparo, também, no fato de a reparação de dano decorrente de responsabilidade objetiva estar regulada genericamente no Código Civil, lei de mesma hierarquia que a LGPD. Logo, a lei posterior pode revogar a anterior de mesma hierarquia, ou a especial revogar a geral, como é o caso.

Entretanto, mesmo antes do Código Civil (parágrafo

único do art. 927) a jurisprudência já vinha alargando o conceito de “culpa”, cujo requisito é necessário para o dever de indenizar. A culpa presumida nasce da premissa do dever de que todos temos de não prejudicar ninguém e praticar atos com segurança. Ainda que não se confunda com a culpa presumida, a atividade de risco é mero desdobramento dessa tese, pois a pessoa que explora economicamente a atividade de risco deve ser responsabilizada pelos prejuízos materiais e morais daí decorrentes.

Por isso e considerando que a LGPD (lei especial) não trouxe a culpa como elemento necessário para configuração de responsabilidade, defendemos que, em tese, é possível a aplicação da responsabilidade objetiva. (PINHEIRO; BOMFIM, 2020, p. 19-20)

Efetivamente, os dispositivos examinados acima da LGPD não dispõem expressamente em nenhum dos sentidos, mas acreditamos ser mais razoável a interpretação que sustenta a responsabilidade objetiva, em função do completo domínio que a empresa possui – ou deveria possuir – no tratamento de dados pessoais dos seus empregados, ato unilateral e realizado por ferramentas que lhe pertencem.

Nesse sentido, qualquer violação aos deveres impostos pela LGPD decorreria, necessariamente, do desrespeito às suas diretrizes, devendo implicar, por conseguinte, a responsabilidade da empresa pelos danos sofridos pelo seu empregado, salvo prova por ela produzida de alguma excludente relacionada a este desrespeito.

Será necessária, contudo, sedimentação doutrinária e jurisprudencial para melhor conclusão sobre o tema.

4. LGPD e a Justiça do Trabalho

A LGPD, voltada à salvaguarda de dados pessoais, não poderia deixar de influenciar o processo judicial, incluindo aquele tramitando na Justiça do Trabalho.

Isto porque, ao veicular uma quantidade considerável de dados pessoais, das partes e eventualmente de terceiros (como paradigmas de pleito de equiparação salarial, testemunhas, dentre outros), o processo trabalhista demanda um cuidado especial por parte dos envolvidos.

Nesse sentido, convém examinar os principais efeitos da LGPD na Justiça do Trabalho, como se fará a seguir.

4.1 LGPD e publicidade

A publicidade é um princípio fundamental do processo, no Brasil, nos termos do artigo 93, IX da CF/88, que a impõe a todos os julgamentos dos órgãos do Poder Judiciário, salvo nos casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação.

Nota-se, assim, que a LGPD, como lei ordinária, deve naturalmente se adequar aos preceitos constitucionais, dentre os quais o princípio da publicidade.

Todavia, essa regra geral do processo, que remanesce intacta, deve ser exami-

nada, após o advento da LGPD, à luz do reforço da contradição apontada no final do dispositivo transcrito: o direito ao sigilo dos intervenientes processuais deve ser resguardado com estrito rigor, sempre que justificado.

Nesse sentido, dados pessoais dos intervenientes podem ser disponibilizados, em respeito à publicidade, mas somente nos estritos limites da necessidade, adequação e finalidade.

Essa cautela envolve todos os responsáveis pelo tratamento dos dados desses intervenientes, a saber: juízes, advogados, servidores, peritos, dentre outros.

Não se trata, portanto, de ocultar indiscriminadamente nomes e dados dos intervenientes, medida extrema e que menoscabaria, inefavelmente, o princípio constitucional da publicidade.

Em vez disso, o uso desses dados deve atender a finalidades específicas, sem exposição desprovida de interesse efetivo, em especial por um excesso de zelo em juntar e expor documentos e atos desnecessários para o deslinde do feito.

4.2 LGPD e provas digitais

As provas digitais seguramente integrarão o futuro da dilação probatória no Brasil, ao lado das provas já utilizadas atualmente.

As novas tecnologias permitem um alcance imenso das suas novas ferramentas, em especial as de geolocalização ou as de captura de áudio e vídeo.

Nos demais ramos do Judiciário, em especial na seara criminal, o uso de provas digitais já vem se tornando habitual. Na seara laboral, ainda que incipiente, o seu uso tende a se generalizar rapidamente, dada a eficácia desses novos meios de prova.

É fundamental, por conseguinte, buscar a harmonização entre esse futuro uso abundante das provas digitais e os preceitos da LGPD.

Isso porque, por meio das novas ferramentas digitais, é possível se obter a geolocalização de partes e terceiros, como testemunhas, a qualquer tempo – do presente ou do passado –, podendo tal busca levar à publicização de situações constrangedoras, em determinadas hipóteses.

Desse modo, para se assegurar o respeito à LGPD, deve-se utilizar essas provas digitais com cautela, com respeito aos princípios legais já mencionados da finalidade, adequação e necessidade, além dos princípios constitucionais da intimidade, da vida privada e do contraditório e ampla defesa.

Em casos extremos, de provas digitais que capturem situações constrangedoras dos envolvidos – como no caso de assédio moral ou sexual –, esses dados devem ser juntados aos autos com todo o cuidado possível, de preferência com acautelamento sob sigilo.

Ademais, todos os dados tratados por meio das provas digitais, sejam eles ordinários ou sensíveis, demandam o necessário equilíbrio entre a necessidade de instrução processual, eventualmente invasiva nas searas privadas de partes e terceiros, com a guarda responsável dessas informações coletadas, especialmente pelo alcance quase ilimitado das provas digitais.

Considerações finais

O estudo realizado no presente artigo demonstrou a amplitude dos efeitos da LGPD na seara laboral: desde as diferentes fases do contrato de trabalho até a

questão central da publicidade dos atos judiciais, assim como a atualíssima temática das provas digitais.

Por se tratar de lei muito recente, o alcance destes efeitos ainda está longe de se estabelecer de forma nítida, somente a sedimentação jurisprudencial futura sendo capaz de fixar, de maneira clara, todos os impactos que as relações de trabalho e a Justiça do Trabalho sofrerão da nova lei de proteção de dados.

Todavia, o que já é possível afirmar é a necessidade de uma mudança de cultura, na era digital em que se vive no século XXI: a invasão da privacidade, com publicização e comercialização dos dados pessoais de terceiros, sem o consentimento ou sequer a ciência delas, tornou-se prática generalizada neste mundo virtual.

É fundamental, por conseguinte, valer-se dos princípios e diretrizes da LGPD para se impor, na seara laboral, objeto do presente estudo, limites a esta possível invasão de dados pessoais dos empregados, impondo às empresas o dever de tratar estes dados de forma prudente e cautelosa, sob pena de responsabilização, inclusive por meio de eventual indenização por danos morais causados aos trabalhadores.

11. EFICÁCIA ESPACIAL DA LGPD: DOCTRINA DOS EFEITOS E SUA APLICAÇÃO NO TRATAMENTO TRANSFRONTEIRIÇO DE DADOS NAS RELAÇÕES DE TRABALHO

LGPD TERRITORIAL EFFECTIVENESS: DOCTRINE OF EFFECTS AND ITS APPLICATION IN CROSS-BORDER DATA PROCESSING IN LABOR RELATIONS

RAPHAEL MIZIARA¹

Resumo

O presente artigo revisita a teoria geral da eficácia espacial normativa, o princípio da territorialidade e sua inserção nos foros do Direito Digital. Em seguida, enfrenta as disposições da Lei Geral de Proteção de Dados brasileira – Lei n.º 13.709 de 2018 – relativas ao tema de sua eficácia territorial. Dentre elas, destaca-se o estudo da aplicação territorial da norma brasileira em quatro casos: i) operações de tratamento realizada no território nacional; ii) atividades de tratamento tenham por objetivo a oferta ou o fornecimento de bens ou serviços no território nacional; iii) a atividade de tratamento tenha por objetivo o tratamento de dados de indivíduos localizados no território nacional; iv) os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional. Por fim, parte-se para análise mais detalhada da opção feita pela LGPD quanto à chamada Doutrina dos Efeitos ou do Impacto Territorial, especialmente a partir de situações envolvendo as relações de trabalho subordinado.

Palavras-chave: Lei Geral de Proteção de Dados – Doutrina dos Efeitos ou do Impacto Territorial – Eficácia normativa espacial – Direito do Trabalho.

Abstract

This article revisits the general theory of normative territorial effectiveness, the principle of territoriality and its insertion in the Digital Law forums. Then, it faces the provisions of the Brazilian General Data Protection Law – Law number 13.709 of 2018 – relating to the issue of its territorial effectiveness. Among them, the study of the territorial application of the Brazilian rule stands out in four cases: i) treatment operations carried out in the national territory; ii) treatment activities have as their objective the offer or supply of goods or services in the national territory; iii) the processing activity has as its objective the processing of data from individuals located in the national territory; iv) the personal data subject to the processing have been collected in the national territory. Finally, part of a more detailed analysis of the option made by the LGPD regarding the so-called Doctrine of Effects or Territorial Impact, especially in situations involving subordinate labor relations.

Keywords: General Data Protection Law – Doctrine of Effects or Territorial Impact – Territorial normative effectiveness – Labor Law.

¹ Doutorando em Direito do Trabalho pela Faculdade de Direito da Universidade de São Paulo (USP). Mestre em Direito do Trabalho e das Relações Sociais pela UDF. Especialista em Direito do Trabalho pela *Universidad Castilla-La Mancha* (UCLM – Espanha). Advogado. Professor em cursos de graduação e pós-graduação em Direito.

1. Introdução

“Os homens criam as ferramentas, as ferramentas recriam os homens”. Com esse assertivo pensamento, o canadense Marshall McLuhan – um dos principais teóricos da comunicação e criador do termo “aldeia global”² – talvez não tivesse dimensão, à época, do tamanho impacto social que a ferramenta internet hoje causa nas relações sociais.

A conexão à rede mundial de computadores permite que um indivíduo, localizado em um determinado lugar do globo terrestre, possa acessar sites hospedados em diferentes locais do mundo. Informações e oportunidades oriundas dos mais diversos e variados países podem ser acessadas em segundos, ao mesmo tempo e por diferentes pessoas.

O mundo atual, em boa medida, constitui-se em uma realidade sem fronteiras físicas, no qual a internet relativizou os limites geográficos, provocando uma verdadeira desestruturação do espaço e, muitas vezes, do próprio tempo. A interconexão entre porções descontínuas do espaço terrestre institui uma nova categoria espacial, comumente denominada de ciberespaço.

No chamado ciberespaço é possível que um ato, praticado em determinado Estado, irradie efeitos sobre o território de outro. Basta imaginar uma postagem ofensiva publicada por um indivíduo situado na França, em um blog hospedado em servidor situado na Austrália, que atinja a honra de um cidadão residente e domiciliado no Brasil. Em hipóteses como a exemplificada surgem os chamados conflitos espaço-normativos e instaura-se certa controvérsia acerca da lei material aplicável para solução do caso.

A sociedade em rede, cada vez mais interconectada³, expõe progressivamente a insuficiência dos tradicionais métodos do Direito Internacional, Público e Privado, como fórmula para solução de seus conflitos, inclusive os normativos e de jurisdição. Tais métodos foram tradicionalmente formulados a partir de uma sociedade com fronteiras territoriais geográficas e físicas bem delimitadas, realidade cada vez mais distante.

Com efeito, a pulverização das fronteiras territoriais, provocadas sobretudo pelo fluxo virtual e internacional de dados propiciado pela internet, desafia as seculares e tradicionais normas sobre a aplicação das leis no espaço. Um dos maiores desafios colocados hoje à regulação da internet e dos fatos digitais reside na compatibilização entre sua natureza transfronteiriça e o exercício da soberania digital pelos Estados nacionais.⁴

Não se trata de um debate apenas teórico, uma vez que abrangidos conflitos de ordem prática, cuja resolução e desdobramentos terão impacto decisivo sobre

2 McLUHAN, Marshall. *Understanding media: the extensions of man*. New York: Mentor Press, 1964. p. 103.

3 Para se ter ideia da dimensão do afirmado, observe que no Brasil, por exemplo, a população no ano de 2016 era de 206 milhões de habitantes e os dispositivos conectáveis à internet somavam 244 milhões. Cinco anos depois, já no ano de 2021, a população teve um tímido crescimento para 213 milhões de habitantes, enquanto os dispositivos conectáveis à rede mundial de computadores teve um aumento exponencial para 424 milhões, conforme dados extraídos da 32ª pesquisa anual do uso de TI da FGVcia. Este fenômeno de *capilaridade tecnológica* é chamado de *computação ubíqua* ou *pervasiva*.

4 CARVALHO, Lucas Borges de. *Soberania digital: legitimidade e eficácia da aplicação da lei na internet*. In: *Revista brasileira de direito*. Vol. 14, n. 2, maio-agosto, 2018, p. 213-235.

o futuro das relações digitais, em especial no que concerne à proteção de direitos online, além da estabilidade jurídica necessária para a realização de investimentos econômicos e para a promoção de inovação no setor de tecnologia.⁵

Os avanços tecnológicos, não se nega, proporciona novas possibilidades de concretização de direitos fundamentais, todavia, também suscitam novos riscos de sua violação. Além disso, considerando que os espaços digitais em geral são controlados por agentes econômicos dotados de alta capacidade de coleta, armazenamento e processamento de dados pessoais a intensificação do fluxo comunicacional na internet aumenta as possibilidades de violação de direitos de personalidade e, até mesmo, do direito fundamental ao trabalho.⁶

Mesmo direitos fundamentais de igualdade e isonomia são colocados em risco pelo uso de algoritmos e de ferramentas de data analytics, que, promovendo a classificação e estereotipação discriminatória de grupos sociais, são utilizados por empresas e governos automatizem processos de tomadas de decisões estratégicas para a vida social, como a alocação de oportunidades de acesso a emprego, negócios e outros bens sociais.⁷

Diante desse cenário, a principal pergunta a ser feita e que deve guiar as discussões em torno do assunto é: qual a lei material aplicável nas questões envolvendo proteção de dados em condutas praticadas no ambiente digital trabalhista transnacional? Nesta perspectiva, mostra-se importante trazer o debate para as relações de trabalho subordinado.

Imagine-se situação na qual uma determinada empresa oferte, por meio de seu website, um processo de candidatura global para determinada vaga de trabalho. Ciente da notícia, uma pessoa, localizada em território brasileiro, resolve acessar o site da empresa e preencher formulário de candidatura ao emprego. O candidato ao emprego, titular dos dados que estão sendo coletados, percebe que o formulário exige como condição de candidatura dados flagrantemente desnecessários, à luz da LGPD. Nesta hipótese, indaga-se: poderá o candidato ao emprego ajuizar ação perante a justiça brasileira invocando a aplicação – eficácia espacial – da LGPD ao caso?

O hipotético exemplo acima é apenas um dos inúmeros que surgirão dentro daquilo que chamado de Direito do Trabalho Digital, caracterizado pelo impacto da internet e da inteligência artificial na conformação e no redimensionamento das relações trabalhistas.

Desde já, esclareça-se que o ponto central objeto de investigação no presente estudo relaciona-se com a eficácia espacial da norma brasileira de proteção de dados e não com as questões processuais afetas à jurisdição.

E estudo revisita a teoria geral da eficácia espacial normativa, o princípio da territorialidade e sua inserção nos foros do Direito Digital. Em seguida, enfrenta as disposições da Lei Geral de Proteção de Dados brasileira – Lei n.º 13.709 de 2018 – relativas ao tema de sua eficácia territorial. Dentre elas, destaca-se o estudo

5 *Ibidem*.

6 MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. *Constitucionalismo digital e jurisdição constitucional*: uma agenda de pesquisa para o caso brasileiro. In: *Revista brasileira de direito*. Vol. 16, n. 1, janeiro-abril, 2020, p. 1-33.

7 *Ibidem*.

da aplicação territorial da norma brasileira em quatro situações:

- i) operações de tratamento realizada no território nacional;
- ii) atividades de tratamento tenham por objetivo a oferta ou o fornecimento de bens ou serviços no território nacional;
- iii) a atividade de tratamento tenha por objetivo o tratamento de dados de indivíduos localizados no território nacional;
- iv) os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional.

Por fim, o estudo parte para análise mais detalhada da opção feita pela LGPD quanto à chamada Doutrina dos Efeitos ou da Teoria do Impacto Territorial.

2. Eficácia espacial da norma, princípio da territorialidade e Direito Digital

Cada Estado é soberano para regular as condutas praticadas em seu espaço geográfico. A norma estatal tem potencial para incidir dentro do território daquele Estado que a criou. Fala-se, neste caso, em eficácia territorial ou espacial. A eficácia espacial designa, pois, a aplicação ou execução da norma jurídica dentro de um determinado espaço territorial.

Disso resulta logicamente a clássica regra de que o império das normas jurídicas tem por confins os do território no qual se exerce o poder de onde emanou, de modo que, assim como cada Estado pode exigir o reconhecimento exclusivo do seu direito no seu território, da mesma forma Estado algum pode pretender que as normas sejam reconhecidas fora das suas fronteiras.⁸ Trata-se do princípio da territorialidade.

Ocorre que, há muito tempo, percebeu-se que a aplicação rigorosa da territorialidade e do conceito de soberania seria um obstáculo às relações internacionais. E, modernamente, pode-se dizer que a ideia fundante de tal princípio é, na maioria das vezes, incompatível com a nova realidade virtual que encampa as relações sociais.

É também preciso ter em mente que o problema da eficácia territorial da norma é, antes, um problema hermenêutico ou de aplicação do direito. Outrossim, é preceito preliminar e fundamental da hermenêutica o de que a interpretação varia conforme a área do direito. Em outras palavras, é necessário sempre levar em conta o caráter especial da norma e a matéria de que é objeto, e indicar o ramo de Direito a que ela pertence, visto variarem o critério de interpretação e as regras aplicáveis em geral, conforme a espécie jurídica de que se trata.

Com efeito, a teoria orientadora do exegeta não pode ser única e universal, a mesma para todas as leis, imutáveis no tempo; além dos princípios gerais, observáveis a respeito de quaisquer normas, há outros especiais, exigidos pela natureza das regras jurídicas, variável conforme a fonte de que derivam, o sistema político a que se acham ligadas e as categorias diversas de relações que disciplinam. Aquele que não partir desses pressupostos, essenciais à boa hermenêutica, incidirá em erros graves e frequentes.⁹

Desse modo, a nova realidade virtual a que o Direito do Trabalho e a sociedade como um todo estão envoltos, impõem a adaptação de antigas máximas e a criação

8 RUGGIERO, Roberto de. *Instituições de direito civil*: introdução e parte geral. Volume I. Campinas: Bookseller, 1999. p. 239.

9 MAXIMILIANO, Carlos. *Hermenêutica e aplicação do direito*. 19. ed. Rio de Janeiro: Forense, 2006. p. 247.

de outras. Nessa ordem de ideias é que se mostra a necessidade de se repensar o princípio da territorialidade dentro do Direito Digital.

Muitas vezes, como adverte a doutrina, não é possível determinar qual o território em que aconteceram as relações jurídicas, os fatos e seus efeitos, sendo difícil determinar qual norma aplicar utilizando os parâmetros tradicionais.¹⁰ Isso se dá porque a sociedade digital rompeu barreiras e o mundo virtual construiu um novo território, já designado de ciberespaço, dificilmente demarcável.¹¹

No Brasil, a Lei n.º 12.965 de 2014, o Marco Civil da Internet (MCI), contemplou cláusulas gerais e princípios de conformação de direitos individuais no ciberespaço que servem de baliza hermenêutica aos atores sociais e profissionais do direito em geral. Mais recentemente, a Lei n.º 13.709 de 2018 (LGPD) também trouxe regras sobre a aplicação da lei brasileira para fatos ocorridos no estrangeiro, como adiante se demonstrará.

3. Lei Geral de Proteção de Dados e a sua eficácia territorial

Ao disciplinar a eficácia espacial da LGPD, o artigo 3º da Lei n.º 13.709 de 2018 estabeleceu que a Lei se aplica a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I – a operação de tratamento seja realizada no território nacional;

II – a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional ou;

III – os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Como se observa, a LGPD elegeu como **elemento de conexão** para aplicação material da lei o **território nacional**. Desse modo, se qualquer das operações de tratamento (inciso I), inclusive a coleta (inciso III) for realizada no **território nacional**, a LGPD deverá ser aplicada. De igual modo, também deverá ser aplicada se a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no **território nacional** (inciso II). Esclareceu o § 1º do mesmo dispositivo que se consideram coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

As hipóteses de aplicabilidade da lei brasileira acima descritas são independentes entre si, ou seja, basta que o fato se enquadre em somente uma delas para que a LGPD seja aplicável ao agente de tratamento dos dados pessoais.

O único caso no qual não se aplicará a LGPD mesmo quando a operação de tratamento for realizada no território nacional é a hipótese de tratamento de dados previsto no **inciso IV, caput, do artigo 4º da LGPD**, qual seja, quando os dados forem provenientes de fora do território nacional e não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros

10 PECK, Patrícia. *Direito digital*. 7. ed. São Paulo: Saraiva, 2021. p. 78.

11 *Idem*. p. 79.

ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.

Pretende-se, nos subtópicos seguintes, analisar individualmente as hipóteses normativas previstas nos incisos I a III do, do artigo 3º da LGPD, especialmente a partir de aplicações nas relações subordinadas de trabalho.

3.1 Operação de tratamento realizada no território nacional (artigo 3º, inciso I, da LGPD)

O artigo 5º, inciso X, da LGPD estatui, em rol exemplificativo, que tratamento de dados é toda operação realizada com dados pessoais, como as que se referem a *coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração*. São inúmeros núcleos verbais, todos eles espécies do gênero tratamento.

Se qualquer das práticas acima ocorrer em território nacional, terão incidência as disposições da Lei Geral de Proteção de Dados Brasileira, independentemente do meio (físico ou digital), do país de sua sede do controlador ou do país onde estejam localizados os dados.

Imagine-se uma hipótese na qual uma empresa brasileira realiza a contratação de um teletrabalhador residente e domiciliado no Uruguai e que prestará o seu trabalho a partir do seu país. Se a empresa brasileira armazena os dados do trabalhador uruguaio no Brasil, seja em meio físico ou digital, tais dados devem ser tratados de acordo com as disposições da LGPD, ainda que o serviço seja prestado remotamente e mesmo que o trabalhador nunca tenha vindo ao Brasil.

Outra situação que pode ocorrer, dentre várias outras, é a seguinte: uma empresa italiana, que contrata um cidadão japonês, residente e domiciliado na África, que tem seu servidor estabelecido no Brasil e aqui armazena os dados dos seus trabalhadores. Também neste caso a legislação de proteção de dados aplicável será a brasileira.

3.2 Atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços a indivíduos localizados no território nacional (artigo 3º, inciso II, primeira parte, da LGPD)

Aplica-se a legislação brasileira de proteção de dados a qualquer operação de tratamento quando a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional.

Trata-se do chamado *targeting criterion*,¹² pelo qual aplica-se a norma brasileira se a atividade de tratamento que tenha por objetivo a oferta ou o fornecimento de bens ou serviços a indivíduos localizados no território nacional, independentemente da localização geográfica do agente de tratamento.

A legislação europeia de proteção de dados tem disposição semelhante à brasileira. Ao disciplinar o seu âmbito de aplicação territorial, o artigo 3º, item 2, alínea “a”, do *GDPR – General Data Protection Regulation* (Regulamento EU n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016) prevê que o “regu-

12 GEIST, Michael. *The shift toward “targeting” for internet jurisdiction*. In: TIERER, Adam D. *Who rules the net? Internet governance and jurisdiction*. Washington: Cato Institute, 2003. p. 91-118.

lamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com: a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento”.

Para a *fattispecie* prevista no inciso II, pode-se pensar na hipótese de uma agência de empregos, situada fora do Brasil, mas que oferece serviços de recolocação no mercado para trabalhadores brasileiros.

3.3 A atividade de tratamento tenha por objetivo o tratamento de dados de indivíduos localizados no território nacional (artigo 3º, inciso II, segunda parte, da LGPD)

A leitura atenta do inciso II, do artigo 3º, da LGPD revela que o texto legal contempla duas hipóteses de incidência da legislação brasileira de proteção de dados, quais sejam:

1) quando a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços a indivíduos localizados no território nacional (artigo 3º, inciso II, primeira parte, da LGPD);

ii) quando a atividade de tratamento tenha por objetivo o tratamento de dados de indivíduos localizados no território nacional (artigo 3º, inciso II, segunda parte, da LGPD).

Percebe-se que a legislação brasileira, no tocante ao seu âmbito de aplicação territorial, é mais ampla do que a o Regulamento Geral de Proteção de Dados europeu que, em seu artigo 3º, item 2, assim prevê:

Art. 3º [...] 2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:

a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento; **b)** O controle do seu comportamento, desde que esse comportamento tenha lugar na União.

Como se nota, a legislação europeia somente se aplicará em relação ao tratamento de dados pessoais de titulares residentes no território da União, quando as atividades de tratamento estejam relacionadas com i) a oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento; ou, ii) o controle do seu comportamento, desde que esse comportamento tenha lugar na União.

Interpretando referido dispositivo, o *EDPB – European Data Protection Board* já enfrentou o seguinte caso sobre a aplicação do Regulamento Geral de Proteção de Dados: uma empresa privada com sede em Mônaco processa dados pessoais de seus empregados para pagamento de salário. Inúmeros funcionários são franceses e outros residentes na Itália.

Neste caso, entendeu o *EDPB* que, em que pese o processamento pela empresa se relacionar a titulares de dados na França e na Itália, não ocorreu no contexto de uma oferta de bens ou serviços. Por isso, para o *EDPB*, dados tratados para a gestão de recursos humanos, incluindo o pagamento de salários por uma empresa

de um país terceiro não foi considerado serviço na acepção do n. 2, alínea “a”, do artigo 3º do GDPR, dispositivo que coincide com o disposto no artigo 3º, inciso II, primeira parte, da LGPD, acima analisado.¹³

Ocorre que a LGPD, como já afirmado, **tem previsão mais ampla de incidência material do que a GDPR**, para também abarcar a atividade de tratamento que tenha *por objetivo* o tratamento de dados de indivíduos localizados no território nacional (artigo 3º, inciso II, segunda parte, da LGPD), independente de qualquer outra condicionante, como faz o Regulamento europeu.

Na situação acima, se uma empresa privada com sede em Mônaco processa dados pessoais de seus empregados para pagamento de salário e dentre os empregados alguns estão situados em território brasileiro, o caso se amoldará perfeitamente à hipótese normativa do artigo 3º, inciso II, segunda parte, da LGPD, pois a atividade de tratamento tenha por objetivo o tratamento de dados de indivíduos localizados no território nacional.

3.4 Os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional (artigo 3º, inciso III, da LGPD)

A coleta é uma das espécies de tratamento, de modo que a hipótese do inciso III, do artigo 3º, da LGPD já está abarcada pelo texto inscrito no inciso I, do artigo 3º, da LGPD, que prevê a aplicação da norma brasileira quando “a operação de tratamento seja realizada no território nacional”.

Tal redundância não passou despercebida pela doutrina:

[...] primeiramente houve atecnia do inciso primeiro ao não delimitar a aplicação da Lei ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento do agente do tratamento situado no Brasil, mas sim prever o cumprimento da Lei em qualquer “operação de tratamento realizada em território nacional”, culminando na abrangência, também, quando dados pessoais são somente coletados no Brasil.

Portanto, seria coerente corrigir o inciso I, nos moldes anteriormente exposto, deixando clara a aplicação territorial com base no “critério do estabelecimento” e suprimir, por completo, o inciso III, pois, assim, a aplicação extraterritorial se daria não meramente quando da coleta de qualquer dado pessoal em território nacional, mas, sim, quando, comprovadamente, de acordo com os testes elencados antes, o agente de tratamento estrangeiro tenha como objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional.¹⁴

13 EDPB – European Data Protection Board. *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*, de 16.11.2018, p. 16.

14 VAINZOF, Rony. *Comentários ao artigo 3º da LGPD*. In: MALDONADO; Viviane Nóbrega; OPI-CE BLUM, Renato (coords.). *Lei Geral de Proteção de Dados Pessoais comentada* [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

Fato é que, se o dado foi coletado em território nacional, independentemente da nacionalidade ou localização do titular ou do agente de tratamento, deverá a LGPD ser aplicada. Nesse caso, a conduta de coletar efetivamente ocorre no território brasileiro, devendo a LGPD reger não só a coleta dos dados, mas todo e qualquer operação decorrente da referida coleta.

4. LGPD e a Doutrina dos Efeitos ou Teoria do Impacto Territorial

Retomando o exemplo hipotético lançado na parte introdutória, imagine-se situação na qual uma determinada empresa oferte, por meio de seu website, um processo de candidatura global para determinada vaga de trabalho. Ciente da notícia, uma pessoa, localizada em território brasileiro, resolve acessar o site da empresa e preencher formulário de candidatura ao emprego. O candidato ao emprego, titular dos dados que estão sendo coletados, percebe que o formulário exige como condição de candidatura dados flagrantemente desnecessários, à luz da LGPD. Nesta hipótese, indaga-se: *poderá o candidato ao emprego ajuizar ação perante a justiça brasileira invocando a aplicação – eficácia espacial – da LGPD ao caso?*

A solução está na conhecida **doutrina dos efeitos ou teoria do impacto**. Inicialmente desenvolvida nos foros do Direito Internacional, a mencionada teoria passou a ser bastante aplicada no direito digital. Especificamente, a teoria tem origem no Direito norte-americano e, em resumo, prega a aplicação do ordenamento jurídico interno a fatos praticados fora das fronteiras de um Estado, mas que geram efeitos dentro do território nacional. Em outras palavras, a aplicação da teoria permite a aplicação da lei brasileira a fatos ocorridos na internet (fora de suas fronteiras), mas que produzem efeitos dentro do território brasileiro.

No caso, o website está hospedado fora do território nacional e a empresa sequer tem sede ou filial no Brasil. Contudo, o evento “*exigência de dados desnecessários*” produz efeitos dentro do território brasileiro, atraindo a incidência da Lei Geral de Proteção de Dados brasileira, nos moldes das hipóteses previstas no artigo 3º, inciso II, da LGPD.

As opções legislativas previstas no inciso II, do artigo 3º, da LGPD, se fundam na ideia de que as normas que regem a proteção de dados objetivam a tutela da ordem jurídica do local no qual a conduta do agente de tratamento possa causar potenciais efeitos.

Nesse sentido, a legislação aplicável a determinadas condutas prima pelo **local dos efeitos de potencial lesão** ao ordenamento jurídico existente, não se importando com o local do agente de tratamento que busca explorar determinado mercado internacional.¹⁵ Desse modo, o fundamental para que se estabeleça a aplicação substancial da norma são os potenciais efeitos locais da conduta.

O artigo 4º, item 23, da GDPR define o chamado **tratamento transfronteiriço** de dados pessoais. É o que se dá com **a)** o tratamento de dados pessoais que ocorre no contexto das atividades de estabelecimentos em mais do que um Estado-Membro de um responsável pelo tratamento ou um subcontratante na União,

15 VAINZOF, Rony. *Comentários ao artigo 3º da LGPD*. In: MALDONADO; Viviane Nóbrega; OPI-CE BLUM, Renato (coords.). *Lei Geral de Proteção de Dados Pessoais comentada* [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

caso o responsável pelo tratamento ou o subcontratante esteja estabelecido em mais do que um Estado-Membro; ou **b**) o tratamento de dados pessoais que ocorre no contexto das atividades de um único estabelecimento de um responsável pelo tratamento ou de um subcontratante, mas que **afeta substancialmente, ou é suscetível de afetar substancialmente, titulares de dados em mais do que um Estados-Membro.**

Logo, em casos de tratamento transfronteiriço de dados de trabalhadores brasileiros, a LGPD elegeu como critério de aplicação substancial da legislação brasileira, a ideia consubstanciada na **doutrina dos efeitos** ou do **impacto territorial**, como se infere das hipóteses contempladas no inciso II, do artigo 3º, da LGPD.

Tal solução normativa, embora em menor extensão, já era prevista no Marco Civil da Internet (artigo 11, § 2º, do MCI), tendo sido inclusive acolhida pelo Superior Tribunal de Justiça – STJ:

RECURSO ESPECIAL. INTERNET. JURISDIÇÃO. SOBERANIA DIGITAL. PREQUESTIONAMENTO. AUSÊNCIA. MARCO CIVIL DA INTERNET. ALCANCE. APLICAÇÃO DA LEGISLAÇÃO BRASILEIRA. PERTINÊNCIA DA JURISDIÇÃO NACIONAL. [...] 4. Quando a alegada atividade ilícita tiver sido praticada pela internet, independentemente de foro previsto no contrato de prestação de serviço, ainda que no exterior, é competente a autoridade judiciária brasileira caso acionada para dirimir o conflito, pois aqui tem domicílio a autora e é o local onde houve acesso ao sítio eletrônico onde a informação foi veiculada, interpretando-se como ato praticado no Brasil. Precedente. 5. É um equívoco imaginar que qualquer aplicação hospedada fora do Brasil não possa ser alcançada pela jurisdição nacional ou que as leis brasileiras não sejam aplicáveis às suas atividades. 6. Tem-se a aplicação da lei brasileira sempre que qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet ocorra em território nacional, mesmo que apenas um dos dispositivos da comunicação esteja no Brasil e mesmo que as atividades sejam feitas por empresa com sede no estrangeiro. (REsp 1.745.657/SP, Rel. Ministra Nancy Andrighi, 3ª Turma, julgado em 03/11/2020, DJe 19/11/2020)

Com efeito, de acordo com referido pensamento teórico, acolhido legislativamente, um Estado pode ter jurisdição e aplicar sua lei material, em situações resultantes de atividades iniciadas fora de suas fronteiras, quando as atividades têm uma ligação substancial com esse Estado – por exemplo, visando os trabalhadores nesse Estado ou causando danos/efeitos nesse Estado.

Tal opção teórica muito se assemelha ao conhecido **princípio jurídico do Centro da Gravidade**, de Otto Gierke, que foi inicialmente desenvolvido como **Teoria da Sede do Fato**, por Savigny. Tal teoria aponta o direito material a ser aplicado ao problema subjacente ao fato misto, ou seja, aquele que ocorreu em mais de um lugar, como geralmente se dá no tratamento transfronteiriço de dados pessoais de trabalhadores.

Se um fato gera efeitos em vários países ao mesmo tempo, em diversas ordens jurídicas, estaremos diante de um fato misto ou multinacional, e qualquer juiz será competente desde que, no país em que ele se situe, o **fato gere efeitos**. Ocorre que, apesar de tal fato gerar efeitos em várias ordens jurídicas, Savigny sustenta que ele só tem uma sede jurídica (um único centro de gravidade, “*para qual o pêndulo pende*”). Isso se dá porque em apenas em um país o fato gera mais efeitos, ainda que isso seja difícil de perceber.

No direito do trabalho isso se aplica frequentemente em relação aos marítimos. O trabalho do marítimo, desenvolvido em navio registrado sob bandeira brasileira, é disciplinado pela legislação brasileira (artigos 248 a 252, da CLT). Todavia, quando um marítimo brasileiro ou um estrangeiro residente no Brasil (art. 5º, caput, CF/88) é contratado para laborar, dentro e fora do Brasil, em favor de armadores estrangeiros, sua situação jurídica pode vir a ser regida por dois ou mais ordenamentos jurídicos, o que configuraria a hipótese de conflito de leis no espaço.

O centro de gravidade é onde acontece a maior irradiação de efeitos e o juiz deste local é mais competente que os outros; além disso, ele aplicará o seu direito (lei material) vigente na sede do fato. E, pela lógica do sistema, em qualquer lugar que se ajuizar a ação, o juiz aplicará o direito da sede do fato.

Nesses casos, a situação jurídica deve ser disciplinada pelo ordenamento jurídico que exerça maior influência sobre a relação jurídica, afastando-se os de menor relevância. Nesta situação, o princípio do centro de gravidade – chamado no direito norte americano de “**most significant relationship**” –, por ter surtido efeitos no Brasil, possibilita a aplicação da LGPD, conforme explicado acima.

Conclusões

A desestruturação do espaço e do tempo propiciada pelas novas tecnologias de informação e comunicação causa significativos impactos nas relações de trabalho subordinado. O denominado tratamento transfronteiriço de dados pessoais é situação cada vez mais comum e as legislações de proteção de dados, também neste aspecto, refletem sua disciplina normativa no Direito do Trabalho.

Demonstrou-se que para proteger os dados de trabalhadores a LGPD prevê pelo menos quatro hipóteses nas quais terá eficácia territorial. São elas: i) quando a operação de tratamento for realizada no território nacional (artigo 3º, inciso I, da LGPD); ii) quando a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços a indivíduos localizados no território nacional (artigo 3º, inciso II, primeira parte, da LGPD); iii) quando a atividade de tratamento tenha por objetivo o tratamento de dados de indivíduos localizados no território nacional (artigo 3º, inciso II, segunda parte, da LGPD); e, por fim, iv) quando os dados pessoais objeto do tratamento tenham sido coletados no território nacional (artigo 3º, inciso III, da LGPD).

Especificamente quanto às segunda e terceira hipóteses, observou-se que a LGPD acolheu a chamada doutrina dos efeitos, também conhecida como teoria do impacto territorial, como se infere das hipóteses contempladas no inciso II, do artigo 3º, da LGPD, já que nestas situações se aplicará a legislação brasileira a fatos praticados fora das fronteiras estatais, na medida em que eles geram efeitos dentro do território nacional.

Isso se dá, em boa medida, porque a LGPD, ao disciplinar o seu âmbito de aplicação territorial (artigo 3º, especialmente o seu inciso II), possui um âmbito de incidência mais amplo do que o Regulamento Geral de Proteção de Dados europeu, quem também disciplina o tema em seu artigo 3º.

O inciso II, do artigo 3º, da LGPD revela que o texto legal contempla duas hipóteses de incidência da legislação brasileira de proteção de dados dos empregados, quais sejam: i) quando a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços a indivíduos localizados no território nacional (artigo 3º, inciso II, primeira parte, da LGPD); ii) quando a atividade de tratamento tenha por objetivo o tratamento de dados de indivíduos localizados no território nacional (artigo 3º, inciso II, segunda parte, da LGPD).

Ambas as situações são passíveis de aplicação na proteção de dados de trabalhadores, como no caso em que uma empresa privada com sede em Mônaco processa dados pessoais de seus empregados para pagamento de salário e dentre os empregados alguns estão situados em território brasileiro. Tal exemplo se amolda à hipótese normativa do artigo 3º, inciso II, segunda parte, da LGPD, pois a atividade de tratamento tenha por objetivo o tratamento de dados de indivíduos localizados no território nacional. De igual modo, também se aplicará a LGPD na hipótese em que uma agência de empregos, situada fora do Brasil, oferece serviços de recolocação no mercado para trabalhadores brasileiros.

REFERÊNCIAS

CARVALHO, Lucas Borges de. Soberania digital: legitimidade e eficácia da aplicação da lei na internet. In: Revista brasileira de direito. Vol. 14, n. 2, maio-agosto, 2018.

EDPB – European Data Protection Board. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), de 16.11.2018.

GEIST, Michael. The shift toward “targeting” for internet jurisdiction. In: TIERER, Adam D. Who rules the net? Internet governance and jurisdiction. Washington: Cato Institute, 2003.

IBGE. Projeção da população do Brasil e das Unidades da Federação. Disponível em: <<https://www.ibge.gov.br/apps/populacao/projecao/index.html>> Acesso em: 13.11.2021.

MAXIMILIANO, Carlos. Hermenêutica e aplicação do direito. 19. ed. Rio de Janeiro: Forense, 2006.

McLUHAN, Marshall. Understanding media: the extensions of man. New York: Mentor Press, 1964.

MEIRELLES, Fernando de Souza. 32ª pesquisa anual do uso de TI da FGVcia. Disponível em: <<https://easp.fgv.br/producao-intelectual/pesquisa-anual-uso>>

-ti> Acesso em: 13.11.2021.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. In: Revista brasileira de direito. Vol. 16, n. 1, janeiro-abril, 2020.

PECK, Patrícia. Direito digital. 7. ed. São Paulo: Saraiva, 2021.

RUGGIERO, Roberto de. Instituições de direito civil: introdução e parte geral. Volume I. Campinas: Bookseller, 1999.

VAINZOF, Rony. Comentários ao artigo 3º da LGPD. In: MALDONADO; Viviane Nóbrega; OPICE BLUM, Renato (coords.). Lei Geral de Proteção de Dados Pessoais comentada [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

12. PRINCÍPIOS NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: DO NÚCLEO COMUM AOS DESAFIOS DE CONCRETIZAÇÃO

PRINCIPLES IN GENERAL PERSONAL DATA PROTECTION LAW: FROM THE COMMON CORE TO THE CHALLENGES OF REALISATION

JULISE LEMONJE¹

Resumo

A Lei Geral de Proteção de Dados Pessoais (LGPD), responsável por posicionar diretrizes, deveres e direitos no que toca à proteção de dados pessoais, também apresenta um rol de princípios que orienta a tratativa da matéria em âmbito nacional. Tendo em vista a novidade da temática, assim como a simultânea referência a princípios já existentes no ordenamento jurídico brasileiro, faz-se relevante a compreensão das bases, conteúdo e desafios dos princípios elencados no artigo 6º da Lei Geral de Proteção de Dados Pessoais (LGPD). O artigo, portanto, a partir de pesquisa bibliográfica em literatura científica especializada, objetiva apresentar e discutir a aplicação dos princípios que regem a matéria. Para tanto, inicia-se pela elaboração de noções introdutórias sobre a teoria geral dos princípios, traçando conceitos e funções dos princípios. Em seguida, são tecidas considerações a respeito do núcleo comum dos princípios em proteção de dados pessoais, que tende a convergir em sua tratativa internacional. Reflete-se, ademais, acerca da identificação de expressões destes princípios em normativas anteriores no contexto legislativo nacional. Após, é exposto o conteúdo dos princípios positivados no caput e incisos do artigo 6º da Lei n. 13.709/2018, traçando-se considerações sobre a sua relação com outros dispositivos da normativa e oportunidades de concretização. Por fim, discutem-se os desafios à realização dos princípios previstos no artigo 6º da Lei Geral de Proteção de Dados Pessoais em atenção à cultura e protagonismo do titular de dados pessoais.

Palavras-chave: Lei Geral de Proteção de Dados Pessoais. Princípios na Proteção de Dados Pessoais. Teoria Geral dos Princípio.

Abstract

The General Personal Data Protection Law, responsible for establishing guidelines, duties and rights with regard to the protection of personal data, also presents a list of principles that guide the handling of the matter at the national level. Considering the novelty of the theme, as well as the simultaneous reference to principles that already exist in the Brazilian legal system, it is important to understand the bases, content and challenges of the principles listed in article 6 of General Personal Data Protection Law. The article, thus, based on bibliograph-

¹ Mestranda em Direito pela PUCRS. Especializanda em Direito do Trabalho pela UFRGS. Advogada e Psicóloga. Bolsista PRO-Stricto PUCRS. juliselemonje@hotmail.com

ical research in specialized scientific literature, aims to present and discuss the application of the principles that govern the subject. Therefore, it starts with the elaboration of introductory notions about the theory of legal principles, tracing concepts and functions of the principles. Then, considerations are made about the common core of principles in the protection of personal data, which tends to converge in its international approach. It also reflects on the identification of expressions of these principles in previous regulations in the national legislative context. Afterwards, the content of the principles affirmed in the caput and items of article 6 of Law n. 13.709/2018, with considerations on its relationship with other provisions of the regulation and opportunities for implementation. Finally, the challenges to the realization of the principles foreseen in article 6 of the General Personal Data Protection Law are discussed, taking into account the culture and the protagonism of the title-holder of personal data.

Keywords: General Personal Data Protection Law. Principles in personal data protection. Theory of legal principles

1. Noções introdutórias: teoria geral dos princípios

A Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018) apresenta um rol de princípios em seu artigo 6º, caput e incisos, responsável por orientar a tratativa da matéria em âmbito nacional. Tendo em vista a novidade da temática no ordenamento jurídico brasileiro, faz-se relevante o estudo e compreensão da base principiológica da normativa em estudo. O presente artigo, portanto, trata dos princípios da Lei Geral de Proteção de Dados Pessoais (LGPD), em atenção às funções dos princípios no ordenamento jurídico, a sua inspiração em tratativas internacionais e aos desafios para a sua concretização em contexto nacional.

Ao tratar dos princípios que regem a proteção de dados pessoais em âmbito nacional, especialmente do rol positivado no artigo 6º da Lei Geral de Proteção de Dados Pessoais, faz-se imprescindível a compreensão do conceito e da função dos princípios no ordenamento jurídico. Freitas (2010), ao abordar a interpretação sistemática do direito, reconhece que além de jamais anularem-se mutuamente – ainda que possam ser ponderados –, os princípios apresentam-se enquanto linhas mestras que conduzem o intérprete, especialmente quando este se depara com antinomias jurídicas.

Nesse sentido, os princípios guardam uma natureza fundante, atuando tanto na manutenção de uma ordem interna quanto na adequação valorativa (NEGREIROS, 1998). Ainda quanto à conceituação dos princípios, Bobbio (1995, p. 158) entende que se tratam de “normas fundantes generalíssimas do sistema, as normas mais gerais”.

Alexy (2011, p. 90), por sua vez, amparado em Dworkin, supera a tradicional classificação de princípios que se restringe a diferenciá-los de regras tão somente em decorrência de características como maior abstração e generalidade. Assim, o autor extrapola tal concepção e entende que princípios configuram-se como mandamentos – contemplando tanto permissões quanto proibições – de otimização, isto é, devem ser realizados em maior medida possível dentro das possibilidades existentes:

O ponto decisivo na distinção entre regras e princípios é que princípios são normas que ordenam que algo seja realizado na maior medida possível dentro das possibilidades jurídicas e fáticas existentes. Princípios são, por conseguinte, mandamentos de otimização, que são caracterizados por poderem ser satisfeitos em graus variados e pelo fato de que a medida de vida de sua satisfação não depende somente das possibilidades fáticas, mas também das possibilidades jurídicas. (grifos originais)

Ainda no que tange à diferenciação entre princípios e regras, importa revisitar a teoria dos princípios de Humberto Ávila. O autor – que, como um realista metodológico, entende que a norma jurídica é produto da atividade de interpretação de textos jurídicos, estando conectada à atividade do intérprete – reconhece que os princípios enquadram-se no gênero norma jurídica, contando com seus atributos, quais sejam: “incidência, caráter deontico (prescritividade) e vinculatividade aos seus destinatários” (MELLO, 2020, p. 294).

Desta forma, assim como as regras, os princípios encontram-se endereçados à prescrição de comportamentos – todavia, apresentam relevantes contrastes quanto ao modo como justificam a sua aplicação, como contribuem para a decisão e como orientam o comportamento. Quanto à justificação para a sua aplicação, enquanto as regras são descritivas e avalia-se a correspondência entre a situação factual construída e o texto, os princípios são pautados pelo elemento finalístico, fundamentando a sua aplicação a partir da identificação de uma correspondência entre a conduta exigida e o estado ideal de coisas que se busca alcançar (ÁVILA, 2011, p. 73-5).

No que se refere ao modo como contribuem para a decisão, os princípios não são geradores de uma solução específica, contribuindo de forma complementar e parcial à análise do caso. Ademais, ao prescreverem o comportamento, enquanto as regras descrevem a conduta a ser adotada, estipulando obrigações, restrições e proibições, os princípios apontam a um “estado ideal de coisas” que merece ser alcançado, configurando-se como normas finalísticas (ÁVILA, 2011, p. 76-7):

[...] os princípios são normas imediatamente finalísticas, já que estabelecem um estado de coisas para cuja realização é necessária a adoção de determinados comportamentos. Os princípios são normas cuja qualidade frontal é, justamente, a determinação da realização de um fim juridicamente relevante, ao passo que características dianteira das regras é a previsão do comportamento.

Por conseguinte, entende-se que os princípios guiam a interpretação do direito, devendo-se almejar a sua realização em maior medida possível, conforme ensina Alexy. Ademais, de acordo com os postulados de Humberto Ávila, assim como as regras, os princípios também estão voltados à prescrição de comporta-

mento, apresentando, para isso, um estado ideal de coisas que se deve buscar. A partir dessas concepções, passa-se à análise dos princípios que guiam a proteção de dados pessoais e que, por consequência, devem orientar a busca de um cenário ideal de tutela das informações da pessoa natural identificada ou identificável (ÁVILA, 2011, p.76-7).

2. Núcleo comum de princípios em proteção de dados pessoais

Os princípios previstos na Lei Geral de Proteção de Dados Pessoais (LGPD), em seu artigo 6º, além de fornecerem uma unidade sistêmica à disciplina no Brasil, apresentam, com frequência, uma forte carga substancial (MENDES; DONEDA, 2018). Mendes e Doneda (2018) apontam, nesta senda, que a previsão principiológica da normativa é acompanhada de um caráter didático, tendo em vista a novidade da matéria em âmbito legislativo nacional.

Em que pese a legislação específica acerca da proteção de dados pessoais seja uma novidade no ordenamento jurídico brasileiro, Oliveira e Lopes (2019) observam que alguns elementos dos princípios previstos no artigo 6º da LGPD já despontavam em preocupações positivadas em outras normativas - a título de exemplo, no Código de Defesa do Consumidor (Lei n. 8.078/1990), na Lei de Arquivos Públicos (Lei n. 8.159/1991), na Lei do Habeas Data (Lei n. 9.507/1997), na Lei do Cadastro Positivo (Lei n. 12.414/2011), na Lei de Acesso à Informação (Lei n. 12.572/2011) e no Marco Civil da Internet (Lei n. 12.965/2014). Desta forma, identifica-se que o processo de formação de um sistema de proteção já se encontrava em desenvolvimento quando da edição da LGPD (OLIVEIRA; LOPES, 2019).

Ademais, importa observar que os princípios previstos no artigo 6º da LGPD, embora se insiram em nosso ordenamento com características próprias, retomam uma “tradição já amadurecida em outros países” (MENDES; DONEDA, p. 474). Nesse sentido, observa-se que também os princípios previstos na LGPD inserem-se no fenômeno denominado de convergência – isto é, o movimento de evolução normativa internacional da matéria alinha-se no que tange as suas principais diretrizes e formas (BENNET, 1992).

Nesta senda, as FIPP’s – Fair Information Practice Principles –, datadas de 1973, repercutiram enquanto estrutura de diretrizes para as discussões acerca da privacidade, sendo desenvolvidas pelo Comitê de Aconselhamento sobre Sistema de Dados Automatizados do governo estadunidense (BIONI, 2019). Sobre suas repercussões, Bioni (2019) reconhece que, embora tenham tais princípios tenham alçado maior consistência a partir das guidelines da OCDE na década de 1980, as FIPP’s já pautavam a preocupação com a carga participativa do titular ao longo do fluxo de tratamento:

[...] as FIPPs desenharam um arquétipo cujo centro gravitacional girava em torno de princípios e direitos para conformar essa diretriz normativa de que o indivíduo deveria autodeterminar as suas informações pessoais.

Atento à existência de uma “espinha dorsal” que já vem orientando iniciativas internacionais há décadas, Doneda (2011) também destaca que a origem comum desse núcleo encontra importante respaldo na Convenção de Strasbourg – Convenção n. 108 do Conselho da Europa para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais² –, de 1981, bem como nas Guidelines da OCDE – Diretivas para Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais³ –, de 1980, que buscavam fomentar um ambiente regulatório comum.

Observa-se que, embora a LGPD atualize o rol – atentando a preocupações que passam a receber maior atenção em normativas posteriores, como no caso do princípio da não discriminação –, muitos dos princípios positivados no artigo 6º renovam a abordagem deste tronco comum. De tal sorte que, a partir da leitura da parte dois das Guidelines da OCDE, verifica-se a previsão dos seguintes princípios: Collection Limitation Principle; Data Quality Principle; Purpose Specification Principle; Use Limitation Principle; Security Safeguards Principle; Openness Principle; Individual Participation Principle; e Accountability Principle. Por conseguinte, os princípios que passam a ser apresentados encontram respaldo tanto no núcleo comum identificado pela doutrina, quanto em elementos que já despontavam em legislação nacional esparsa.

3. Princípios na LGPD

No que tange à positivação de princípios na Lei Geral de Proteção de Dados (LGPD), o artigo 6º estabelece, logo em seu caput⁴, a referência expressa ao princípio da boa-fé; orientador, portanto, de todas as relações estabelecidas entre os titulares e os agentes envolvidos no tratamento de seus dados pessoais. Assim, a proteção de dados explícita que as relações recíprocas entre as partes devem reger-se com base na confiança⁵.

Em seguida, a LGPD inicia o rol de princípios pela previsão do princípio da finalidade⁶, responsável por vincular todo o tratamento de dados à finalidade para a qual fora coletada a informação – qual seja, a finalidade informada ao titular de dados quando da obtenção do consentimento. Assim, a normativa restringe eventuais transferências de dados e demanda que qualquer alteração na finalida-

2 CONSELHO DA EUROPA. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. Acesso em: 15 maio 2021.

3 ORGANIZAÇÃO PARA COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Disponível em: <https://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm>. Acesso em: 16 maio 2021.

4 Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios. In: BRASIL. Lei Geral de Proteção de Dados (LGPD), de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 maio. 2021.

5 Sobre breve histórico da boa-fé, tanto na condição de cláusula geral quanto de princípio, ver ROSENVALD, Nelson. O princípio da boa fé. Revista do Tribunal Regional Federal 1ª Região, Brasília, v. 15, n. 10, p. out. 2003.

6 I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; In: BRASIL op. cit.

de esteja submetida à necessidade de novo consentimento, haja vista o teor dos artigos 8º, § 4º, e 9º, § 2º, da Lei em estudo. Ainda no que se refere ao princípio da finalidade, Ruaro (2017, p. 410) destaca que, na medida em que impede o uso de dados por terceiros não legitimados, o princípio em comento vincula-se profundamente à autodeterminação informativa, ofertando aos titulares de dados a faculdade de vetar o uso de suas informações pessoais de maneira desconexa da finalidade informada.

A partir do conhecimento e ênfase acerca da finalidade da coleta, a LGPD também estabelece, no segundo inciso do artigo 6º – princípio da adequação⁷ –, que durante todo o tratamento de dados pessoais deverá se ter em vista a adequação e a proporcionalidade em relação à finalidade informada. Da mesma forma, o volume e o conteúdo dos dados tratados deve ater-se à necessidade para que se alcance a finalidade que sustentou o consentimento da coleta, haja vista o princípio da necessidade⁸. Diante disso, faz-se imprescindível a promoção de revisões nas estruturas de armazenamento de dados das entidades que manejam informações de pessoas naturais identificadas ou identificáveis, para que sejam mantidos tão somente os dados necessários, bem como para que se eliminem dados extras ou que já alcançaram a finalidade informada e não se mostram mais indispensáveis (OLIVEIRA; LOPES, 2019).

Logo após, a LGPD expressa o princípio do livre acesso⁹, dispondo que o titular tem o direito de acessar os bancos de dados que armazenam suas informações. Sublinha-se que, além de facilitado, este acesso deve ser não oneroso – isto é, gratuito (MACIEL, 2019). Pondera-se, contudo, que o livre acesso, assim como o princípio da transparência, deverá respeitar o segredo comercial e industrial, conforme previsão dos artigos 9º, II, e 19, II, da Lei n. 13.709/2018.

A partir do livre acesso, faz-se possível a retificação de dados coletados incorretamente ou desatualizados, alinhando-se também ao princípio da qualidade dos dados, previsto no inciso V do artigo 6º da LGPD¹⁰. Nesse sentido, Sarlet (2013, p. 433) arrola, enquanto posição jurídica vinculada à proteção de dados pessoais, “o direito à retificação e, a depender do caso, à exclusão de dados pessoais armazenados em bancos de dados”. Destaca-se que, o direito do titular de dados de ter suas informações, além de corretas, também atualizadas, constrói-se a partir da perspectiva de identidade do sujeito, que merece ter seus dados submetidos a tratamento correspondendo, de forma fidedigna, à realidade (BIONI, 2019).

Tanto o livre acesso quanto a qualidade dos dados relacionam-se ao princípio

7 II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; In: BRASIL op. cit.

8 III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; In: Ibidem.

9 IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; In: BRASIL. op. cit.

10 V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; In: BRASIL. op. cit.

previsto no inciso VI do rol em análise, qual seja, o princípio da transparência¹¹. Este princípio garante, durante todo o tratamento dos dados – e não somente em sua coleta – que as informações disponibilizadas aos titulares sejam claras e de fácil compreensão, além de exatas. Por conseguinte, conecta-se à utilização de uma linguagem que possa ser apreendida pelo cidadão médio, não dependendo de conhecimentos técnicos para que se assimile o que está sendo informado.

A seguir, a normativa traz o princípio da segurança¹², dizendo respeito à proteção contra acessos não autorizados e ao extravio de dados pessoais. Observa-se que a concretização do referido princípio é abordada pela LGPD a partir do artigo 46, quando se passa a tratar da segurança e das boas práticas em proteção de dados pessoais.

A matéria articula-se, ademais, com o princípio da prevenção¹³, voltado à mitigação dos riscos existentes. A realização do princípio da prevenção encontra profunda relação com o desenvolvimento de ferramentas que, em sua concepção, estejam endereçadas à tutela da privacidade, conforme destacam Mendes e Doneda (2018). Acrescenta-se que a prevenção também se respalda na promoção de programas de governança e de uma cultura de proteção, haja vista que os riscos minimizam-se na medida em que os atores que manejam os dados pessoais constroem uma melhor compreensão sobre a temática e seus impactos (MACIEL, 2019).

A LGPD prevê, ainda, o princípio da não discriminação¹⁴, atentando-se a novas demandas e ao potencial discriminatório do tratamento de dados pessoais. Embora todo e qualquer tratamento de dados deva se dar sob o manto do princípio que veda sua aplicação discriminatória, a preocupação com o princípio da não discriminação acentua-se quando do tratamento de dados pessoais sensíveis – quais sejam, aqueles que, conforme conceituação do artigo 5º, II, da LGPD, envolvam origem racial ou étnica, orientação sexual, opinião política, convicção religiosa, filiação sindical, ou informação de saúde, genética e biométrica de pessoa natural.

Por fim, a Lei registra o princípio da responsabilização e prestação de contas¹⁵, impondo que os agentes de tratamento, além de cumprir a norma que regulamenta a proteção de dados pessoais, devem estar aptos a prestar contas e demonstrar sua atenção ao ordenamento vigente, tanto à Autoridade Nacional de Proteção de Dados (ANPD) quanto ao titular de dados. Em atenção ao modelo de responsabilidade accountability e ao articular o teor da LGPD com o do Regulamento Geral de Proteção de Dados (RGPD) europeu, Limberger (2020) enfatiza uma perspec-

11 VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; In: BRASIL op. cit.

12 VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; In: op cit.

13 VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

14 IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; In: BRASIL op. cit.

15 X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. In: BRASIL op. cit.

tiva de “responsabilidade pró-ativa”, não sendo necessária a ocorrência de um incidente para que o agente de tratamento tenha que demonstrar a conformidade de suas práticas com a regulamentação vigente.

A partir da apresentação dos princípios expressamente previstos no artigo 6º da LGPD, vislumbra-se a “preocupação do legislador com a participação do indivíduo no fluxo de suas informações” (TEFFÉ, 2020, p. 5). Ademais, nota-se que há uma integração formal e material dos princípios com os demais dispositivos da normativa, sendo possível identificar as reverberações destes mandamentos ao longo do texto da Lei n. 13.709/2018¹⁶, por meio de obrigações, direitos e restrições, que se encontram endereçados à elevação coletiva da autodeterminação informativa.

Acrescenta-se, ainda no que tange as considerações finais acerca da concretização dos princípios arrolados na normativa em estudo, que sua realização no plano material encontra-se vinculada ao desenvolvimento de dispositivos que apresentam uma arquitetura voltada à facilitação da gestão de dados pelos titulares – extrapolando-se, conforme investigado por Bioni (2019) ao tratar de tecnologias usablefriendly e das PETs (Privacy-Enhancing Technologies), a mera perspectiva de contratualização do consentimento. Além disso, ressalta-se a importância, visando-se o alcance do estado ideal apresentados pelos princípios que regem o tratamento de dados pessoais, da atuação da ANPD e da promoção de uma cultura de proteção de dados pessoais¹⁷, para que os titulares possam se apropriar de sua autonomia e exercer a autodeterminação informativa que lhes é garantida.

Considerações finais

A partir da publicação da Lei n. 13.709/2018, a proteção de dados pessoais – entendidos como informações de pessoas naturais identificadas ou identificáveis – passou a ser regida por legislação específica que, dentre outros fundamentos, diretrizes e obrigações, arrola expressamente os princípios que orientam qualquer relação de tratamento de dados pessoais em âmbito nacional. Diante disso, o presente trabalho objetivou abordar os princípios previstos no artigo 6º, caput e incisos, da LGPD, tecendo breve análise acerca de sua origem, função no ordenamento jurídico e conteúdo.

Para tanto, iniciou-se o presente estudo revisitando-se as principais concepções de princípios na doutrina clássica. Extrapolando-se a perspectiva de caracterização dos princípios tão somente como normas mais gerais e abstratas, destacou-se entendimento de Alexy no sentido de que os princípios devem ser realizados em maior medida possível. Ademais, a partir dos ensinamentos de Humberto Ávila, examinou-se as principais distinções entre princípios e regras, especialmente no

¹⁶ Para articulação dos demais dispositivos da LGPD com o seu artigo 6º, consultar OLIVEIRA, Marco Aurélio Belizze; LOPES, Isabela Maria Pereira. Capítulo 2. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZAO, Ana; OLIVA, Milena Donato (Org.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 1a ed. São Paulo: Thompson Reuters Brasil, 2019. p.53-82.

¹⁷ Sobre desafios para a implementação da LGPD, consultar MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor (Thomson Reuters), v. 120, p. 469-483, nov./dez. 2018.

que tange ao modo como orientam comportamentos, como se aplicam e como se justificam.

Em seguida, examinou-se que os princípios arrolados na LGPD, além de já terem despontado em legislação nacional esparsa, amparam-se em um tronco comum de diretrizes que vem orientando a regulamentação da matéria – especialmente visando um ambiente regulatório uniforme – em âmbito internacional. Recebem, portanto, significativa influência das FIPP's, da Convenção 108 do Conselho Europeu e das guidelines da OCDE.

Por fim, foram apresentados os princípios previstos no caput e nos incisos do artigo 6º, da LGPD, articulando-os com literatura científica especializada e outros dispositivos da própria normativa em estudo. Fez-se possível identificar, a partir desta análise, que os princípios privilegiam a participação do titular de dados no decorrer de todo o tratamento de suas informações identificadas ou identificáveis, assim como dialogam com outros dispositivos da LGPD, vislumbrando-se oportunidades de concretização de tais postulados. Embora a realização dos princípios expressamente previstos no artigo 6º encontre amparo nas próprias obrigações, proibições e restrições da Lei, torna-se imprescindível a promoção de uma cultura de proteção e a diligente atuação da ANPD para a efetivação de tais mandamentos e o seu respectivo alcance em maior medida possível.

REFERÊNCIAS

ALEXY, Robert. Teoria dos Direitos Fundamentais. 2a ed. São Paulo: Malheiros, 2011.

ÁVILA, Humberto. Teoria dos Princípios: da definição à aplicação dos princípios jurídicos. 12a ed. São Paulo: Malheiros, 2011.

BENNETT, Colin. Regulating Privacy: data protection and public policy in Europe and the United States. Ithaca: Cornell University, 1992.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e o limite do consentimento. Rio de Janeiro: Forense, 2019.

BOBBIO, Norberto. Teoria do ordenamento jurídico. 6a. ed. Brasília: Editora Universidade de Brasília, 1995.

BRASIL. Lei Geral de Proteção de Dados (LGPD), de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 maio. 2021.

CONSELHO DA EUROPA. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. Acesso em: 15 maio 2021.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico, v. 12, n. 2, p. 91-108, jul./dez. 2011.

FREITAS, Juarez. A Interpretação Sistemática do Direito. 5a ed. São Paulo: Malheiros Editores, 2010.

LIMBERGER, Têmis. Informação em rede: uma comparação da Lei Brasileira de Proteção de Dados Pessoais e o Regulamento Geral de Proteção de Dados Europeu. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti

(Org.). Direito Digital: direito privado e internet. Indaiatuba: Editora Foco, 2020.

MACIEL, Rafael Fernandes. Princípios para o tratamento de dados pessoais. In: Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais. RM Digital Education, 2019. [livro digital]. Disponível em: <https://materiais.rmdigital.education/livro-lgdp-rafaelmaciel>. Acesso em: 20 abr. 2021.

MARTINS-COSTA, Judith. De Princípios, Regras, Ficções e Presunções. In: MITIDIERO, Daniel; ADAMY, Pedro (Org.). Direito, Razão e Argumento: a reconstrução dos fundamentos democráticos e republicanos do direito público com base na teoria do direito. São Paulo: Malheiros, 2020.

MELLO, Cláudio Ari. O Realismo Jurídico e a “Teoria dos Princípios” de Humberto Ávila. In: MITIDIERO, Daniel; ADAMY, Pedro (Org.). Direito, Razão e Argumento: A Reconstrução dos Fundamentos Democráticos e Republicanos do Direito Público com base na Teoria do Direito. São Paulo: Malheiros, 2020. p. 293-317.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor (Thomson Reuters), v. 120, p. 469-483, nov./dez. 2018.

NEGREIROS, Teresa. Fundamentos para uma interpretação constitucional do princípio da boa-fé. 1. ed. Rio de Janeiro: Renovar, 1998.

OLIVEIRA, Marco Aurélio Belizze; LOPES, Isabela Maria Pereira. Capítulo 2. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização

pela Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZAO, Ana; OLIVA, Milena Donato (Org.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 1a ed. São Paulo: Thompson Reuters Brasil, 2019. p. 53-82.

ORGANIZAÇÃO PARA COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Disponível em: <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsofPersonalData.htm>. Acesso em: 16 maio 2021.

ROSENVALD, Nelson. O princípio da boa fé. Revista do Tribunal Regional Federal 1ª Região, Brasília, v. 15, n. 10, p. out. 2003.

RUARO, Regina Linden. A tensão entre o direito fundamental à proteção de dados pessoais e o livre mercado. Revista de Estudos e Pesquisas Avançadas do Terceiro Setor (REPATS), Brasília, v. 4, n. 1, p. 389-423, Jan/Jun. 2017.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. Curso de Direito Constitucional. 2a ed. São Paulo: Revista dos Tribunais, 2013.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. Civilistica. Rio de Janeiro, a. 9, n. 1, 2020. Disponível em:

<http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/>. Acesso em: 02 maio 2021.

13. DADOS PESSOAIS: O QUE SÃO? QUEM OS DETÊM? COMO E POR QUE OS COLETA?

*PERSONAL DATA: WHAT ARE THEY? WHO HAS THEM?
HOW AND WHY TO COLLECT?*

FRANCIANO BELTRAMINI¹

Resumo

Objetivo: O presente trabalho tem como finalidade compreender, o que são os dados pessoais previstos na Lei Geral de Proteção de Dados (LGPD), quem os detém; como e por que essas informações são captadas. Para tanto, os objetivos propostos neste estudo são os seguintes: (i) expor genericamente o que é a LGPD, as suas origens e os seus objetivos; (ii) apresentar o conceito legal de dados pessoais, dados pessoais sensíveis, tratamento de dados e alguns de seus desdobramentos; (iii) investigar qual a importância dos dados pessoais nos dias atuais, e, assim, entender por que eles são captados; (iv) buscar compreender como os dados pessoais são captados e quem são os grandes detentores dessas informações. Metodologia: O método científico empregado é dedutivo. Registra-se a utilização da técnica de pesquisa bibliográfica e documental, posto que as respostas aos objetivos traçados neste artigo são buscadas a partir de referências teóricas já publicadas em livros especializados, em artigos científicos e na legislação brasileira. Resultados: Conforme bem destaca o economista italiano Luigi Zingales o século XXI será caracterizado pela análise de dados, havendo a partir destes, grandes e importantes mudanças em todos os aspectos que se relacionam com a vida humana. Assim sendo, o presente artigo buscou compreender o que são os dados pessoais tutelados pela LGPD, bem como qual a importância dessas informações, como elas são coletada e quem são os maiores detentores desses que são considerados a commodity do novo milênio.

Palavras-chave: LGPD. Dados pessoais. Autonomia privada. Privacidade.

Abstract

Objective: The purpose of this paper is to understand what are the personal data provided for in the General Data Protection Law (LGPD), which holds them; how and why this information is captured. For this purpose, the objectives proposed in this study are: (i) to expose generically what the LGPD is, its origins and objectives; (ii) present the legal concept of personal data, sensitive personal data, data processing and some of its consequences; (iii) investigate the importance of personal data today, and, therefore, understand why they

¹ Mestrando em Direito Empresarial e Cidadania do UNICURITIBA e pesquisador do CNPq, integrante do grupo de pesquisa "Impacto do regramento da proteção de dados nas relações do trabalho" do PPGD da UNICURITIBA. franciano.beltramini@gmail.com. Curriculum Lattes: <http://lattes.cnpq.br/4288905831001490>. ORCID: <https://orcid.org/0000-0003-1185-0230>

are captured; (iv) seek to understand how personal data are captured and who are the major holders of this information Methodology: The scientific method used is deductive. The use of the bibliographic and documentary research technique is registered, since the answers to the objectives outlined in this paper are sought from theoretical references already published in specialized books, scientific articles and Brazilian legislation. Results: As the Italian economist Luigi Zingales points out, the 21st century will be characterized by data analysis, encompassing major and important changes in all aspects related to human life. Therefore, this article sought to understand what the personal data protected by the LGPD are, as well as the importance of this information, how it is collected and who are the biggest holders of those that are considered the commodity of the new millennium.

Keywords: LGPD. Personal data. Private autonomy. Privacy.

1. Introdução

A ideia por traz deste artigo surgiu a partir da leitura do livro de João Ubaldo Ribeiro, cujo o título é: “Política quem manda, por que manda, como manda”, em que o saudoso romancista baiano trata de temas da Ciência Política e Direito.

Além de famoso escritor, integrante da Academia Brasileira de Letras, João Ubaldo foi também Jornalista, Bacharel em Direito, Mestre em Ciência Política e Professor universitário. Assim sendo, escreveu o referido livro para fins acadêmicos, mas com uma linguagem clara e acessível, sem perder a profundidade e o raciocínio crítico que lhe são peculiares.

O referido Autor conclui a obra de Ciência Política com o capítulo intitulado “quem manda e como manda”, em que, de maneira bastante assertiva, conclui o seguinte: “Não importa o que lhe digam, quem manda é quem está levando vantagem”(RIBEIRO, 2010, pg. 173).

Assim sendo, voltando ao tema proposto para o presente estudo – dados pessoais – será realizado um movimento inicial para apresentar o conceito de dado pessoal previsto na Lei Geral de Proteção de Dados, bem como algumas peculiaridades sobre o tema previstos na legislação brasileira.

Buscar-se-á na seção seguinte compreender melhor quem são os maiores detentores dos dados pessoais, como eles os captam e por que, a partir de reflexões de alguns dos maiores pensadores da atualidade que buscam entender e significar as expressivas mudanças que a atual civilização vive neste momento histórico.

O método científico empregado é dedutivo, mediante o qual se estabelecem grandes formulações dogmáticas, como, por exemplo, a LGPD, dados pessoais, dignidade da pessoa humana e, posteriormente, buscar a estratificação destes temas mediante a análise do que vem a ser os dados pessoais sensíveis, tratamento de dados, autodeterminação e autonomia privada, etc.

Ainda, acerca da questão metodológica; registra-se a utilização da técnica de pesquisa bibliográfica e documental, posto que as respostas aos objetivos traçados neste artigo serão buscadas a partir de referências teóricas já publicadas em livros especializados, em artigos científicos e na legislação brasileira

Após a realização dos movimentos listados, buscar-se-á correlacionar os dados

peçoais, denominado por alguns como o “novo petróleo” com as profundas mudanças que se observa no limiar desse novo milênio.

2. Os dados pessoais na LGPD

De acordo com o economista Luigi Zingales (2015, pg. 17), enquanto o século XX caracterizou-se pelas ideologias, o século XXI caracterizar-se-á pela análise de dados.

Ao partir do destaque realizado pelo economista italiano sobre a grande importância dos dados pessoais, muitos Estados mundo afora têm editado as suas legislações com o propósito de regulamentar o uso dos dados pessoais pelas corporações públicas e privadas.

Neste diapasão, merece ser mencionado o Regulamento Geral sobre a Proteção de Dados (RGPD – Regulamento (UE) 2016/679) que, de acordo com Selma Carlotto (2020, pg.11), é o regulamento do Direito Europeu que trata sobre a privacidade e a proteção de dados pessoais a todos os indivíduos residentes na União Europeia e no Espaço Econômico Europeu. Referido regulamento aplica-se a todas as empresas que operem no Espaço Econômico Europeu, independentemente do seu Estado de origem.

A referência à regulamentação europeia serve tão somente para informar que esta foi a fonte de inspiração da legislação brasileira que, em 14 de agosto de 2018, foi sancionada pelo Presidente da República.

Trata-se da Lei Geral de Proteção de Dados Pessoais (LGPD) (Lei nº. 13.709/2018), que recebeu alterações através da Lei nº. 13.853/2019. Em relação à LGPD, é importante consignar que se trata de lei promulgada a partir de amplo debate público iniciado nos idos de 2010², que deu origem a uma legislação sofisticada e bastante estruturada, contendo a explicitação de conceitos, princípios e fundamentos que auxiliam os operadores jurídicos a aplicar os seus termos.

Nesta linha argumentativa, é importante destacar que no art. 1º, da LGPD, o legislador consignou que o objetivo da lei é proteger o direito fundamental à liberdade e à privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural. Assim sendo, observa-se que a lei objetiva a implementação de direitos fundamentais previstos na Constituição da República Federativa do Brasil (CRFB).

Sobre a LGPD, Patrícia Peck Pinheiro (2018. Kindle, posição 178-183) explicita que:

A Lei n. 13.709/2018 é um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas como para as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica. É uma regulamentação que traz princípios, direitos e obrigações relacionados ao uso de um

2 JINKINGS, Daniella. Governo vai debater criação de marco legal para proteção de dados pessoais no Brasil. Rede Brasil Atual. 1 dez. 2010. Disponível em: <https://www.redebrasilatual.com.br/cidada-ria/2010/12/governo-vai-debater-criacao-de-marco-legal-para-protacao-de-dados-pessoais-no-brasil>. Acesso em: 6 mar. 2021:

dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas.

Do fragmento acima colacionado, extrai-se que se trata de nova legislação que trará profundas modificações nas instituições públicas e privadas que, em suas relações com os indivíduos, fazem uso de dados pessoais, sendo este, em uma sociedade digital, um dos ativos mais valiosos.

Nesta perspectiva, é costumeiro ouvir que os dados pessoais são o “novo petróleo” ou a “commodity do novo milênio”, devendo destacar-se que, ao contrário do petróleo e das commodities, os dados pessoais são inesgotáveis.

Reitera-se que se trata de legislação robusta, que institui no Brasil a estrutura normativa necessária para propiciar a construção de uma cultura de proteção de dados a partir da explicitação dos fundamentos da disciplina de proteção de dados, de um sem-número de conceitos próprios da área, de princípios específicos e direitos e obrigações que regulamentam o uso dos dados pessoais.

A título exemplificativo, colaciona-se o disposto no art. 2º, da LGPD, que estabelece quais são os fundamentos que disciplinam a proteção de dados pessoais:

Art. 2º. A disciplina da proteção de dados pessoais tem como fundamentos:

- I - o respeito à privacidade;
- II - a autodeterminação informativa;
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV - a inviolabilidade da intimidade, da honra e da imagem;
- V - o desenvolvimento econômico e tecnológico e a inovação;
- VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Em relação aos fundamentos previstos na lei, Patrícia Peck Pinheiro (2018, Kindle, posição 607-612) esclarece o seguinte:

A proteção aos direitos fundamentais é bastante evidente no art. 2º da LGPD, que pode ser relacionado ao texto constitucional brasileiro no que concerne ao conteúdo, haja vista que a Constituição Federal Brasileira é pautada na proteção aos direitos fundamentais. Entre os artigos constitucionais destacáveis, pode-se citar: art. 3º, I e II; art. 4º, II; art. 5º, X e XII; art. 7º, XXVII; e art. 219.

Conforme se depreende da leitura do citado artigo, que é ratificado com o fragmento doutrinário colacionado acima, os fundamentos da legislação que disciplina a proteção dos dados pessoais têm íntima relação com os direitos fundamentais previstos no art. 5º. da Carta Maior, bem como outros valores de envergadura constitucional.

Ademais, apresenta-se nesta seção três conceitos trazidos na LGPD que são necessários ao bom entendimento da questão em análise na presente resenha, quais sejam: o dado pessoal; o dado pessoal sensível e o dado anonimizado.

Referidos conceitos constam nos primeiros incisos do art. 5º. e seguem abaixo transcritos:

Art. 5.º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento

De acordo com a lei, é dado pessoal qualquer informação relacionada à pessoa natural que a identifique diretamente ou que indiretamente possa identificá-la.

Destaca-se, ainda de acordo com a disposição legal, os dados da pessoa jurídica não são protegidos pela LGPD, uma vez que o inciso I, do art. 5º. faz expressa menção ao dado que se relaciona à pessoa natural. Neste sentido, a lei traz o conceito de dados anonimizados, ou seja, os que não permitem a identificação do titular no momento do tratamento que, por esse motivo, não se aplica a salvaguarda da lei.

Em relação ao dado pessoal, Selma Carolo (2020, p. 48) apresenta alguns exemplos que permitem uma melhor compreensão e identificação dos dados pessoais diretos e indiretos:

São dados pessoais diretos os que identificam a pessoa natural de maneira inequívoca e sem a necessidade de informações adicionais, tais como: RG, CPF, OAB, título de eleitor e são considerados dados pessoais indiretos, aqueles que necessitam de informações adicionais para identificar o titular dos dados, como: profissão, geolocalização, sexo, idade estado civil, hábitos de consumo, endereço, entre outros.

Do explicitado acima, extrai-se que se trata de algo bastante abrangente, que envolve informações pessoais permissivas da identificação direta, bem como informações mais genéricas que conjuntamente com outros dados permitem a identificação do titular.

Em relação aos dados pessoais sensíveis, Stefano Rodotà (2008, pg. 96) já em 2008, ou seja, 10 anos antes da publicação da lei em comento, defendera a existência de um núcleo duro no direito à privacidade que envolvesse informações pessoais com uma maior necessidade de sigilo, tendo em conta o seu potencial discriminatório, conforme extrai-se do seguinte fragmento:

[...] a classificação desses dados na categoria de dados sensíveis, particularmente protegidos contra os riscos da circulação, deriva de sua potencial inclinação para serem utilizados com finalidades discriminatórias

Em similar perspectiva, Selma Carolo (2020, p. 26) esclarece que a LGPD apresenta como um dos seus princípios fundamentais a não discriminação e implementa esse comando realizando a diferenciação dos dados pessoais com os dados pessoais sensíveis, conforme se depreende do seguinte fragmento da sua doutrina:

A Lei Geral de Proteção de Dados, Lei 13.709/2018 tem como princípio basilar o da não discriminação, nos termos do art. 6, inciso IX, de forma expressa e ao diferenciar os dados pessoais sensíveis que são os de maior potencial discriminatório

Assim sendo, diante da segmentação dos dados pessoais e dos dados pessoais sensíveis, bem como do princípio da não discriminação, o legislador elaborou os mecanismos necessários à proteção de informações, cuja circulação podem gerar maior risco de discriminação.

Sobre os dados pessoais sensíveis, de acordo com o que consta na lei, são as informações da pessoa natural que tratam sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como os dados referente à saúde; à vida sexual, à genética ou à biometria.

A título de exemplo, as informações referentes à saúde e à genética de uma determinada pessoa, que estão armazenadas nos bancos de dados de hospitais, dos planos de saúde e dos laboratórios, têm um potencial de impedir que uma seguradora ou empresa de plano de saúde aceite determinado cliente de maneira abusiva, gerando, assim, uma discriminação.

Em uma abordagem um pouco diferente, merece o destaque os dados biométricos que foram detalhados no art. 2º.³, inciso II, do Decreto nº. 10.046/2019, que

³ Art. 2º. Para fins deste Decreto, considera-se:

[...]

II - atributos biométricos - características biológicas e comportamentais mensuráveis da pessoa natu-

institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

Em essência, trata-se das características biológicas e comportamentais que permitem a identificação única e exclusiva de uma pessoa natural para o reconhecimento automatizado.

Nesta senda, a lei cita a palma da mão, as impressões digitais dos dedos, a retina ou a íris dos olhos, o formato da face e a maneira de andar. Referidos dados, por estarem vinculados à individualidade humana, identificam cada ser humano como único e insubstituível, não podendo ser alterados, como, por exemplo, uma senha ou telefone que, caso chegue ao alcance de alguém mal intencionado, poderia gerar incômodos e perturbações. Sendo esse, um motivo a mais para classificar os dados biométricos com um grau de proteção mais elevado.

Patrícia Peck Pinheiro (2018. Kindle, posição 930-933) destaca o tratamento excepcional que o dado sensível demanda, tendo em conta que tutelam valores de maior envergadura, previstos no texto constitucional, nos seguintes termos:

Os dados sensíveis merecem tratamento especial porque em algumas situações a sua utilização mostra-se indispensável, porém o cuidado, o respeito e a segurança com tais informações devem ser assegurados, haja vista que – seja por sua natureza, seja por suas características – a sua violação pode implicar riscos significativos em relação aos direitos e às liberdades fundamentais da pessoa.

Neste aspecto convém esclarecer que o tratamento de dado é um conceito jurídico explicitado no inciso X⁴, do art. 5º., da LGPD, de maneira que o art. 11 da referida lei apresenta os requisitos especiais que devem ser observados para o tratamento de dado pessoal sensível.

Consigna-se que, ao comparar-se o art. 7º., que estabelece os requisitos para o tratamento de dados pessoais (comuns), com o art. 11, que estabelece os requisitos para o tratamento de dados pessoais sensíveis, observa-se que estes possuem requisitos mais rigorosos para o tratamento de informações que são consideradas sensíveis.

Neste sentido, entende-se que não convém aos fins pretendidos na presente pesquisa colacionar os referidos dispositivos de lei para facilitar a realização de comparações, mas, exemplificadamente, informar; enquanto o art. 7º. determina que o tratamento do dado pessoal somente poderá ocorrer quando houver o consentimento do titular, ao passo que o art. 11 estabelece que o tratamento do dado pessoal sensível somente poderá ocorrer quando o titular ou seu representante

ral que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar;

4 Art. 5º Para os fins desta Lei, considera-se:

[...]

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

legal consentir de forma específica e destacada para finalidades intrínsecas.

Ao referir-se a tratamento de dados, importa fazer a correlação com a denominada mineração de dados que, segundo Carlos Nelson Konder (2013, pg. 373), pode ser compreendida como:

[...] técnicas de mineração de dados (data mining) permitem, dentro do amplo manancial de informações já disponíveis da rede – fornecidas pelos titulares devido aos mais variados motivos e nos mais diversos contextos –, a seleção daquelas úteis e valiosas e sua reconstrução sob nova formatação

É por intermédio da mineração de dados que as corporações elaboram perfis dos usuários por meio de rastreamento, que ocorre à revelia dos seus titulares de informações pessoais relativas às suas predilecências, como, por exemplo, os interesses de consumo, a opinião política, a orientação sexual, e as convicções religiosas, entre outros, com finalidades das mais variadas e, muitas vezes, pouco republicanas; ou seja, pautadas em interesses pessoais em detrimento do bem-estar geral.

Os elementos acima apresentam, em linhas gerais, os conceitos e alguns delineamentos do que a LGPD estabeleceu sobre os dados pessoais; na seção seguinte será analisado quem são os grandes detentores dos dados pessoais, como e porque os capta.

3. Quem são os grandes detentores dos dados pessoais, como e por que coletam e armazenam essas informações

A ideia por traz deste estudo surgiu a partir da leitura do livro de João Ubaldo Ribeiro, cujo título é: “Política quem manda, por que manda, como manda”, em que o saudoso romancista baiano trata de temas da Ciência Política e Direito.

Para quem não sabe, além de famoso escritor integrante da Academia Brasileira de Letras, João Ubaldo foi também jornalista, bacharel em direito, mestre em ciência política e professor universitário. Assim sendo, escreveu o referido livro para fins acadêmicos, mas com uma linguagem clara acessível, sem perder a profundidade e o raciocínio crítico que lhe são peculiares.

Na referida obra de não ficção, João Ubaldo apresenta sua concepção sobre política e um sem-número de temas que possuem íntima relação com o exercício de poder, como, por exemplo, os conceitos de nação, soberania, ditaduras, democracia, partidos políticos, dentre tantos outros. Conclui a obra com capítulo intitulado “quem manda e como manda”, onde de maneira bastante assertiva João Ubaldo (2010, pg. 173) conclui o seguinte “Não importa o que lhe digam, quem manda é quem está levando vantagem”

Assim sendo, voltando ao tema proposto a presente resenha – dados pessoais – após realizarmos o movimento inicial onde foi apresentado o conceito que a lei brasileira e algumas peculiaridades estabelecidas nela relativa aos dados pessoais, busca-se nessa seção compreender melhor quem são os maiores detentores dos dados pessoais, como eles os captam e por quê.

Para efeitos didáticos, inicia-se invertendo a ordem estabelecida por João Ubaldo para buscar compreender qual a importância dos dados pessoais na atualidade, como eles são captados e quem são seus maiores detentores na hodiernamente.

Passamos, a seguir, a compreender qual a importância dos dados pessoais neste momento histórico e, com isso por que de eles serem captados. Neste sentido Yuval Hoah Harari (2018, pg. 107) destaca o seguinte:

Se quisermos evitar a concentração de toda a riqueza e de poder nas mãos de uma pequena elite, a chave é regulamentar a propriedade dos dados. Antigamente a terra era o ativo mais importante no mundo, a política era o esforço por controlar a terra, e se muitas terras acabassem se concentrando em poucas mãos – a sociedade se dividia em aristocracia e pessoas comuns. Na era moderna, máquinas e fábricas tornaram-se mais importantes que a terra, e os esforços políticos focam no controle desse meio de produção. Se um número excessivo de fábricas se concentrasse em poucas mãos – a sociedade se dividiria entre capitalistas e proletários. Contudo no século XXI, os dados vão suplantam tanto a terra quanto a maquinaria como o ativo mais importante, e a política será o esforço por controlar o fluxo de dados. Se os dados se concentrarem em muito poucas mãos - o gênero humano se dividirá em espécies diferentes.

Conforme destacado pelo professor israelense, assim como a política teve de debruçar-se para regulamentar e controlar o uso da terra – que foi o ativo econômico mais precioso na antiguidade – posteriormente, o mesmo ocorreu com os meios de produção (máquinas e fábricas) – que foram os ativos econômicos mais preciosos na Idade Moderna. Neste tempo, urge a atual sociedade enveredar esforços para regulamentar o uso dos dados pessoais.

Nesta perspectiva histórica, Jeremy Rifkin (2016, pg. 159) esclarece que:

A Primeira Revolução Industrial eliminou a escravidão e o trabalho servil. A Segunda Revolução Industrial encolheu drasticamente o trabalho artesanal e a agricultura. A Terceira Revolução Industrial está provocando o fim da mão de obra em massa assalariada no setor de manufatura e serviços, e o fim do trabalho profissional especializado na maior parte das áreas do conhecimento.

TI, informatização, automação, megadados, algoritmos, IA incorporados à Internet das Coisas estão reduzindo rapidamente o custo marginal da mão de obra de produzir e entregar uma ampla gama de produtos e serviços.

Do fragmento acima colacionado, é possível concluir que se está em meio a uma mudança sem precedentes na história da civilização humana, em que a tecnologia da informação e os seus consectários pautarão os novos tempos, sendo os dados pessoais o combustível que moldará esse futuro.

Compreendida a importância dos dados pessoais na atualidade, passa-se a buscar compreender como os principais agentes econômicos da área de tecnologia agem para captar os dados pessoais.

Neste prisma, Yuval Hoah Harari (2018, pg.107) destaca o seguinte:

A corrida para obter dados já começou, liderada por gigantes como Google, Facebook e Tencent. Até agora, muitos deles parecem ter adotado o modelo de negócio dos “mercadores da atenção”. Eles capturam nossa atenção fornecendo-nos gratuitamente informações, serviços e entretenimento, e depois revendem nossa atenção aos anunciantes. Mas provavelmente visam a muito mais do que qualquer mercador de atenção anterior. Seu verdadeiro negócio não é vender anúncios. E sim, ao captar a nossa atenção eles conseguem acumular imensa quantidade de dados sobre nós, o que vale mais do que qualquer receita de publicidade. Nós não somos seus clientes – somos seu produto.

O fragmento acima colacionado apresenta o modo de ação de grandes transnacionais, que estão na vanguarda em coletar e tratar dados pessoais. Em essência, o modus operandi dos denominados “mercadores de atenção” consiste em disponibilizar de maneira gratuita serviços, informações e entretenimento para captar a atenção e os dados pessoais dos seus usuários para posteriormente vender as informações às empresas que têm interesse de anunciar os seus produtos aos usuários que, em algum momento, buscaram ou demonstraram predileções aos seus produtos.

Assim sendo, há inicialmente a perspectiva publicitária que, registra-se, é de veras assertiva, dado que aproxima o interessado e potencial cliente ao fornecedor de produtos e serviços por meio de constantes publicidades vinculadas às mais diversas plataformas, sítios da internet e canais que a utilizam.

Harari destaca contudo, que o verdadeiro negócio das empresas desse mercado não é vender anúncios, mas obter e acumular grandes quantidades de dados dos seus usuários, para que estes passem a ser o produto dessas multinacionais, em total desconhecimento dos usuários, visto que entregam gratuitamente os seus dados pessoais às grandes corporações do setor.

Aprofunda este debate, o recém traduzido e publicado livro intitulado “A era do capitalismo de Vigilância”, da autora Shoshana Zuboff. Nas primeiras páginas do denso estudo realizado pela professora estadunidense (2021, pg. 13), apresenta oito diferentes definições para o termo capitalismo de vigilância, por ela cunhado:

1. Uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para

práticas comerciais dissimuladas de extração, previsão e vendas; 2. Uma lógica econômica parasítica na qual a produção de bens e serviços é subordinada a uma nova arquitetura global de modificação de comportamento; 3. Uma funesta mutação do capitalismo marcada por concentrações de riqueza, conhecimento e poder sem precedentes na história da humanidade; 4. A estrutura que serve de base para a economia de vigilância; 5. Uma ameaça tão significativa para a natureza humana no século XXI quanto foi o capitalismo industrial para o mundo natural nos séculos XIX e XX; 6. A origem de um novo poder instrumentário que reivindica domínio sobre a sociedade e apresenta desafios surpreendentes para a democracia de mercado; 7. Um movimento que visa impor uma nova ordem coletiva baseada em certeza total; 8. Uma expropriação de direitos humanos críticos que pode ser mais bem compreendida como um golpe vindo de cima: uma destituição da soberania dos indivíduos.

As oito definições apresentadas por Zuboff apresentam concepções diferentes e complementares ao termo capitalismo de vigilância e explicitam de maneira expressa os reais interesses de quem detém e faz o tratamento dos dados pessoais. Não se trata mera de venda de espaços publicitários com anúncios dirigidos a eventuais interessados, mas sim de um eficiente sistema de arquitetura global que influencia e manipula o comportamento humano com o propósito de beneficiar os seus próprios interesses.

A partir da captura de dados pessoais e do tratamento destas informações pelas corporações com matriz na área da tecnologia, referido sistema subverte o processo natural de tomada de decisão; uma vez que ao invés de simplesmente prever o comportamento ele o induz, sem que as pessoas sequer percebam a manipulação.

O denominado “capitalismo de vigilância” desrespeita a dignidade humana ao não observar a “soberania dos indivíduos” que, dentre outros atributos da personalidade humana, pode-se dizer, ofende a autodeterminação e a autonomia privada.

Torna-se importante consignar que, de acordo com Ingo Wolfgang Sarlet (2015, pág. 296-297), a dignidade humana é um fim em si mesmo, não um meio para alcançar outros fins, não podendo ser admitida qualquer instrumentalização do ser humano; ou seja, o uso arbitrário desta ou daquela vontade.

É de conhecimento geral que no meio acadêmico que o conceito jurídico e filosófico de dignidade da pessoa humana é amplo e profundo, permitindo um sem número de ilações e abordagens sobre as suas dimensões, mas, no intuito de desenvolver o argumento vinculado à proposta da presente resenha, colaciona-se um fragmento da doutrina do jurista Thadeu Weber (2105, pg. 930), que explicita o seguinte:

A condição de ser pessoa impõe tratamento e proteção rigorosamente iguais para todos. A realização da li-

berdade como autodeterminação parte dessa condição de igualdade. Ter direito ao respeito à dignidade significa ter o direito de ser respeitado como pessoa enquanto pessoas ou pelo fato de ser homem.

Do explicitado acima, extrai-se que, para a existência do respeito à dignidade, é necessário observar a igualdade de todos e a realização da liberdade compreendida por meio do conceito de autodeterminação.

Joaquim de Souza Ribeiro (2003, pg. 19) esclarece que a autodeterminação é um conceito pré-jurídico, que atribui a cada ser humano o valor de gerir a sua vida e decidir livremente as suas preferências.

Com vinculação quase umbilical ao conceito de autodeterminação, há o conceito de autonomia privada que, segundo o Autor citado (2003, pg. 21), “é um processo de ordenação que faculta a livre constituição e modelação das relações jurídicas pelos sujeitos que nelas participam”

Infere-se do acima exposto, que é possível concluir que a autodeterminação é um gênero do qual decorre a autonomia privada: a liberdade externalizada através das relações jurídicas, onde a pessoa natural dita regras e vincula-se aos seus efeitos.

A conceituação jurídica neste ato explicitada ratifica as citações de Harari e Zubbof, no sentido de que o usuário das grandes corporações de matriz tecnológica não é visto como cliente, mas sim como produto dessas transnacionais, na medida em que reduz o ser humano à condição de mero instrumento.

Sobre este fator, Yuval Noah Harari(2018, págs. 110-111) atenta para a grande questão a ser respondida na atualidade:

Assim, fariamos melhor em invocar juristas, políticos, filósofos e mesmo poetas para que voltem a atenção para essa charada: como regular a propriedade de dados? Essa talvez seja a questão mais importante de nossa era. Se não formos capazes de responder essa pergunta logo, nosso sistema sociopolítico pode entrar em colapso. As pessoas já estão sentindo a chegada do cataclismo

O pensador hebreu conclui fazendo uma chamada às mentes pensantes da atualidade, asseverando que a questão mais importante da atual geração é regular a propriedade dos dados, sob pena de, não o fazendo, permitir o colapso do sistema sociopolítico.

Para finalizar esta seção, retoma-se a conclusão do livro de João Ubaldo; o Autor, com uma síntese genial ratifica que “Não importa o que lhe digam, quem manda é quem está levando vantagem”

Neste sendeiro, ao compreender-se que os dados pessoais são o maior ativo financeiro dos dias atuais, fácil é concluir-se: quem os detiver será quem estará levando a maior vantagem.

Confirma esta constatação a informação publicada na Revista Forbes⁵, reco-

5 Revista Forbes. Disponível em: <https://forbes.com.br/listas/2020/07/as-marcas-mais-valiosas-do-mundo-em-2020/#foto5>. Acesso em: 8 mar. 2021.

nhecida mundialmente por publicar a relação das maiores fortunas do Planeta.

Ao analisar-se o topo da lista das marcas mais valiosas no ano de 2020, observa-se que as cinco corporações mais valiosas da atualidade são empresas que atuam na área da tecnologia, e que, cada uma a seu modo, conseguiu desenvolver produtos e serviços que aliam tecnologia à captura de dados.

Assim, não por acaso, Apple; Google, Microsoft, Amazon e Facebook são as multinacionais mais valiosas na atualidade.

Considerações finais

Tendo como inspiração as lições de João Ubaldo Ribeiro, que em capítulo derradeiro de sua obra intitulada “Política quem manda, por que manda, como manda” assevera de maneira bastante assertiva o seguinte: “Não importa o que lhe digam, quem manda é quem está levando vantagem.”

O presente artigo, empresta a ideia de João Ubaldo, mas a transplanta para o tema dos dados pessoais.

Assim sendo, na primeira seção foi apresentado o conceito de dado pessoal previsto na Lei Geral de Proteção de Dados, bem como algumas peculiaridades sobre este tema previstos na legislação brasileira.

Na seção seguinte, foram apresentados conceitos e reflexões de grandes pensadores da atualidade que estão buscando entender e significar as expressivas e profundas mudanças que a humanidade vive neste momento histórico.

Nesse sentido, foram apresentados conceitos e reflexões de Yuval Noah Harari, Jeremy Rifkin e Shoshana Zuboff, dentre outros, que destacam a importância dos dados pessoais, como e por que o denominado “novo petróleo” é capturado e processado pelas empresas que atuam na área de tecnologia.

Assim sendo, conclui-se que regular a propriedade dos dados pessoais, inserindo-se a forma como este é captado e tratado, é o maior desafio da atual geração. Trata-se de questão que deve ser respondida de maneira premente e adequada para não permitir o colapso do sistema sociopolítico.

REFERÊNCIAS

BRASIL. Lei nº. 13.709, de 2018. Lei Geral de Proteção de Dados (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 15 jan. 2021.

CARLOTO, Selma. Lei Geral de Proteção de Dados: enfoque nas relações de trabalho. – São Paulo: LTR, 2020

JINKINGS, Daniella. Governo vai debater criação de marco legal para proteção de dados pessoais no Brasil. Rede Brasil Atual. 1 dez. 2010. Disponível em: <https://www.redebrasilatual.com.br/cidadania/2010/12/governo-vai-debater-criacao-de-marco-legal-para-protacao-de-dados-pessoais-no-brasil>. Acesso em 6 fev. 2021.

HARARI, Yuval Noah. 21 lições para o século 21 – 1. ed. São Paulo: Companhia das Letras, 2018

KONDER, Carlos Nelson. Privacidade e corpo: convergências possíveis. Pensar - Revista de Ciências Jurídicas da Universidade de Fortaleza(UNIFOR), v.

18, 2013, p. 352-398. Disponível em: <https://periodicos.unifor.br/rpen/issue/view/323>. Acesso em: 12/10.2021.

PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação (Kindle), 2018.

RIBEIRO, João Ubaldo. Política quem manda, por que manda, como manda. 1. ed. Rio de Janeiro: Objetiva, 2010.

RIBEIRO, Joaquim de Sousa. O problema do contrato: as cláusulas contratuais gerais e o princípio da liberdade contratual. Coimbra: Almedina, 2003

RIFKIN, Jeremy. Sociedade com custo marginal zero – 1. ed. - São Paulo: M. Books, 2016

RODOTÀ, Stefano. A vida na sociedade da vigilância (coord. Maria Celina Bodin de Moraes). Rio de Janeiro: Renovar, 2008

SARLET, Ingo Wolfgang. Notas sobre a dignidade (da pessoa) humana no âmbito da evolução do pensamento ocidental. In: Draiton Gonzaga de Souza; Francisco Jozivan Guedes de Lima (orgs.). Filosofia e Interdisciplinaridade. Porto Alegre: Editora Fi, 2015.

ZINGALES, Luigi. Um capitalismo para o povo – Reencontrando a chave da prosperidade americana. São Paulo: BEI Comunicação, 2015

ZUBOFF, Shoshana. A Era do Capitalismo de Vigilância. A luta por um futuro humano na nova fronteira do poder – 1. ed., Rio de Janeiro: Intrínseca, 2021.

WEBER, Thadeu. Dignidade Humana e Liberdade em Hegel. In: Draiton Gonzaga de Souza; Francisco Jozivan Guedes de Lima (orgs.). Filosofia e Interdisciplinaridade. Porto Alegre: Editora Fi, 2015.

14. A CRIANÇA COMO TITULAR E DESTINATÁRIA DA PROTEÇÃO DE DADOS PESSOAIS FRENTE À CULTURA FRATERNA

GERALDA MAGELLA DE FARIA ROSSETTO¹
E JOSIANE ROSE PETRY VERONESE²

Resumo

O presente estudo tem como objetivo apresentar a criança como titular e destinatária da proteção de dados pessoais. Nesse sentido, dois outros principais aspectos serão levados em consideração: um, examinar a Lei Geral de Proteção de Dados Pessoais, como fundamento e razão da proteção da criança no tema dos dados pessoais; e, dois, contrapor alguns aspectos que se apresentam desafiadores: na mesma medida em que a geração da criança tem se apresentado cada vez mais habilidosa em relação às ferramentas digitais, de outro modo, a criança não tem ampla compreensão quanto aos riscos do ambiente digital, justificando, em relação a tais desafios, sejam verificados quais os mecanismos vão protegê-la na sua condição de titular e destinatária da proteção de dados pessoais, da mesma forma que, também, deve ser concentrados esforços para não empurrá-la prematuramente para uma preparação para o trabalho. A ideia é protegê-la do trabalho infantil e da “cultura do quarto” em prol da cultura fraterna. Assim, recorre-se ao método dedutivo, centrado em uma pesquisa bibliográfica e qualitativa, e, por destacar e problematizar as principais contribuições normativas e de autores que se dedicam ao tema.

Palavras-chave: Lei Geral de Proteção de Dados Pessoais; trabalho infantil; Criança; cultura fraterna.

Abstract

The following paper aims to put forth the children are the bearers and recipients of the personal data protection. In this sense, two other main aspects will be taken into consideration: (1) to examine Brazil's General Personal Data Protection Law as the basis and reason for children protection in the subject of personal data; and (2) to contrast some aspects that present themselves as challenging: to the same extent as each generation of children has shown itself to be more and more skillful in dealing with digital tools, on the other hand, children lack the discernment regarding the risks of the digital environment, justifying, in relation to such challenges, that the mechanisms which are going to protect

1 Doutorado em Direito pela UFSC. Mestrado em Direito pela UNISINOS. Advogada. Procuradora Federal aposentada. Pesquisadora do Direito e Fraternidade; do DataLab e do NEJUSCA. E-mail: geraldamagella@gmail.com

2 Professora Titular da disciplina “Direito da Criança e do Adolescente” da UFSC. Mestre e Doutora em Direito pela UFSC, pós-doutorado pela PUC Serviço Social/RS e em Direito pela UnB. Coordenadora do NEJUSCA e do Núcleo de Pesquisa Direito e Fraternidade/ UFSC. jpetryve@uol.com.br

them in their condition of bearers and recipients of the personal data protection be verified, in the same way that concentrated effort must be undertaken in order not to force them prematurely into a preparation for work. The idea is to protect the them from child labor and of the “culture of the bedroom” in favor of the fraternal culture. As such, this paper resorts to the deductive method, centered on a bibliographical and qualitative research, and to highlighting and problematizing the main normative contributions and those of authors who are dedicated to the subject.

Keywords: General Personal Data Protection Law; child labor; children; fraternal culture.

1. Introdução

O ambiente digital parece mesmo ter se tornado o “país” comum de todos, inclusive da criança. A demanda por pertencimento e habilitação a favor de estar e ser o “povo-internet” é de significativa agenda no mundo todo, com vertiginosa produção de dados, especialmente os pessoais. Traduzir a proteção de dados pessoais na perspectiva da criança e de sua infância, levando-se em consideração a sua condição de portadora de direitos (titular e destinatária), tanto quanto, a qualidade contida na legislação pertinente, como, também, em face dos desafios que se apresentam na world wide web.

Com efeito, o tema proposto diz respeito a um assunto que afeta, cada vez mais, praticamente todos os aspectos de vida para milhões de crianças em todo o mundo e, também, para todos os habitantes: a tecnologia digital disposta na sociedade em rede e em interconectividade.

A adoção da temática, pretende ser uma contribuição ao tema do trabalho às avessas: de forma que a criança não seja “empurrada” para as esferas do trabalho infantil. É preciso pensar em uma hora certa, e em mecanismos de proteção nesse sentido. A ideia é proteger a criança desse contexto extremamente complicado que é o trabalho infantil.

É fato que a criança precisa ser resguardada do mundo do trabalho – por sua evidente susceptibilidade - mas não se pode negar a importância de prepará-la para estar em condições de assumir esse futuro encargo, equivalente a munir de aptidões que virão com o tempo. A “nota” nesse sentido é resguardá-la para não ser exposta prematuramente. Nesse sentido, a internet precisa ser parceira na esfera do ambiente digital e não sua concorrente em termos educacionais e formativos; ser canal e não instrumento para propagar a desgraça no sentido de antecipar redes de trabalho infantil; ser portal de boas notícias e não de disseminação de violências e de ilicitudes que minam a infância, comprometem a qualidade da vida e a confiança na continuidade das gerações.

Convém que todos estejamos unidos a favor de suas bênçãos em prol da humanidade e não de suas desgraças e “matanças” de direitos, a minar o tecido social, a ordem política e tornar-se ameaça concreta ao bem-estar. Porque, para melhor e para pior, a tecnologia digital é um fato de nossas vidas, de modo irreversível, a confirmar: se a tecnologia digital já mudou o panorama mundial – o que não dizer desse fato: quanto mais e mais crianças ficam online em todo o mundo, é

certo que, cada vez mais vai mudando a infância, de forma que, inobstante siga na história humana a cultura do trabalho infantil, e, com o ambiente virtual, já são percebidas o voltar-se da criança para uma cultura de estar plugada, ininterruptamente, do que dá conta a “cultura do quarto”³. Para contrapor a essas duas culturas, o estudo sugere uma terceira: a cultura fraterna, cujo sentido diz respeito a estar em fraternidade: um especial compromisso, uns com os outros, comunidade e sociedade, instituições e Estado, família e pessoas, uma qualidade especial que precisamos dispor a favor de reconhecimento de direitos.

Ademais, antes de sugerir medidas e apontar desafios e até possíveis soluções, considera-se fundamental compreender quais são as características e as dificuldades trazidas pela tecnologia digital e pelas mídias sociais em termos de dados pessoais. É dizer, é importante entender como as redes funcionam para, então, reunir elementos que devem ser considerados ao se enfrentar o fenômeno do ambiente digital e sua alta produção de dados pessoais no tema da criança, e, de tal munus, não escapa ninguém, exatamente porque, a sociedade, o Estado e a família, todos são chamados a intervir. Aliás, no caso do trabalho, um outro elemento parece nos atingir: trata-se da própria reestruturação do capitalismo, para o qual, a esfera tecnológica é uma ferramenta básica.

Por último, a referência neste estudo quanto à “criança”, segue a adoção de quem é titular e destinatária de direitos; no caso, a criança é o ser humano até a idade de dezoito anos, segundo o que estabelece a Convenção sobre os Direitos da Criança (ONU, 1989), a qual foi recepcionado pelo Estatuto da Criança e do Adolescente (1990).

Munida dessas considerações, recorre-se ao método dedutivo, por meio de uma pesquisa bibliográfica e qualitativa, e, na sequência, começa-se por destacar e problematizar algumas principais contribuições de autores, sem, contudo, cair no propósito de elaborar um manual de resposta ou solução ao tema e, sim, apresentar os desafios quanto a proteção de dados pessoais em face da criança, tendo por pano de fundo as questões que desafiam a proteção de dados pessoais, tendo a criança como razão e fundamento.

2. Um panorama sobre o direito à proteção de dados pessoais: um olhar na direção da infância

Para que se possa seguir com este estudo, esclareça-se a distinção necessária, quanto à criança e quanto à infância. Em termos etários, já fora dito anteriormente, mas aqui repisa-se: criança é a pessoa com idade até 18 anos incompletos, enquanto que, a infância é o período inicial vivido por ela. De forma específica. A adoção do conceito de criança, encontra-se recepcionada no Estatuto da Criança e do Adolescente, e sendo regra específica, aos seus dispositivos devem seguir os demais.

³ “Estudos na área de Psicologia Social indicam que, com o amplo acesso à tecnologia digital, houve uma mudança radical no comportamento dos jovens no que se refere aos espaços de diversão: a proliferação da “cultura do quarto fechado” em detrimento da “cultura da molecada da rua”. Para se divertirem, os mais novos, acompanhados ou não, têm preferido o uso do espaço privado, principalmente o quarto. Mas, ainda que na companhia de amigos em um mesmo ambiente, é comum vermos crianças e adolescentes interagindo mais com seus celulares do que uns com os outros”. (RÝCKER, 2021).

Nessa linha, segundo o Estatuto da Criança e do Adolescente (BRASIL, 2021b):

Art. 2º Considera-se criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade.

Segundo a Convenção sobre os Direitos da Criança (BRASIL, 2021g):

Artigo 1. Para efeito da presente Convenção, considera-se como criança todo ser humano com menos de 18 anos de idade, salvo quando, em conformidade com a lei aplicável à criança, a maioridade seja alcançada antes.

A esse respeito:

O Estatuto da Criança e do Adolescente trouxe este primeiro e pioneiro conteúdo, qual seja, a universalização de Direitos: todas as pessoas com menos de 18 anos de idade devem ser contempladas por esta norma. Sendo que o Estatuto da Criança e do Adolescente, no que o difere da Convenção sobre os Direitos da Criança, de 1989, estabelece uma distinção cronológica (não de direitos) entre criança – pessoas de até 12 anos de idade incompletos e o adolescente, entre 12 e 18 anos incompletos. (VERONESE, 2020, p. 13).

Com efeito, quanto à criança, a referência ao longo deste é adotada tendo em consideração que o titular de direitos é a criança até a idade de 18 anos incompletos. Portanto, a referência é quanto a categoria da criança e em relação ao adolescente, conjuntamente.

A infância diz respeito ao período, o dado histórico, geográfico e de pertencimento aos dias que se contam. É o momento vivido e convivido pela criança na altura de seus primeiros dias e que seguem nos anos em que se forma e se desenvolve. No caso deste, o olhar que é depositado nessa referida temática, diz respeito a criança sujeito e titular constituente de direitos, no processo de sua infância.

Além disso, as expressões “criança” e “infância”, ambas, detêm relação com o tempo, sendo que a primeira diz respeito a sua própria identidade; a outra, ao seu pertencimento na escala dos dias; é a geografia e a sua história. No mais, ambas estão na linha de vida da criança, e dizem respeito a ela: uma na forma do ser; a outra do estar. É dito que não há criança sem infância, mas será que há infância sem criança?

Tendo a criança como titular e destinatária de direitos, propriamente quanto a questão de direitos e de suas acepções, tais como a proteção, promoção e defesa, de que são regras as esferas e funções da (re)construção jurídica, o que é o caso da matéria dos dados pessoais, e, em tal fundamento, convém as seguintes explicações.

Onde quer que esteja, a criança do século XXI respira tecnologia, além de navegar em um ambiente digital, para o qual, a geração que a educou, somente deparou com o mundo word wide web, quando já adulta, ou seja, o risco que a criança da Geração Z e Alpha⁴ enfrenta, no sentido de ter comprometida sua privacidade, é verdadeiramente gigante, de forma que, “A construção de uma nova cultura baseada na comunicação multimodal e no processamento digital de informações cria um hiato geracional entre aqueles que nasceram antes da Era da Internet (1969) e aqueles que cresceram em um mundo digital” (CASTELLS, 2020, p. 11).

Em relação ao adulto, a questão nem sempre se inverte, em que pese sua experiência da vida, a habilidade com a internet pode não ser seu forte. Porém, a criança requer a medida e a concessão da proteção integral, o que é indiscutível, a dar conta de uma balizada proteção de sua privacidade.

Borelli dá conta do seguinte desenho do monitoramento contínuo que envolve as atividades online das crianças: utilizando um estudo de comportamentos de privacidade de apps Android, uma equipe de estudiosos e cientistas da computação dos EUA e do Canadá concluiu – dos 5.855 aplicativos incluídos no estudo, 281 coletaram dados de contato ou de localização sem pedir permissão dos pais; 1.100 compartilhavam informações com terceiros, enquanto 2.281 pareciam violar os Termos de Serviço do Google, com compartilhamento indevido para o mesmo destino do ID; aproximadamente 40% dos aplicativos transmitiam informações sem medidas de segurança adequadas, e 92% dentre os 1280 aplicativos do Facebook não usavam corretamente os sinalizadores do código de rede social para limitar o uso da criança de até 13 anos. (2018, p. 141-142).

Além do mais, sob o ponto de vista jusfundamental, é regra de ouro em termos de proteção de dados pessoais, que todos os seus respectivos titulares tenham o direito de acesso aos seus dados pessoais, inclusive aqueles produzidos no ambiente digital - portanto, dados informatizados – podendo, para tanto, em seu interesse, exigir que o mesmo seja objeto de retificação, atualização e o direito de conhecer a finalidade a que se destinam. Em relação à criança, a regra é mesmo igualmente criteriosa, e um pouco mais.

Munida dessas considerações é de se reconhecer que os dados pessoais é tema de pauta e de expressão da agenda contemporânea. Em relação à criança, quer em decorrência de sua vulnerabilidade e de estar em desenvolvimento, quer por conta de sua fragilidade enquanto usuária da internet, alguns dados reforçam essa susceptibilidade: segundo aponta o Fundo das Nações Unidas para a Infância, antes da pandemia, as crianças já representavam um terço dos usuários da internet (UNICEF, 2021a), o que é um dado a inferir no advento e no pós-covid, porque, se de um lado a criança é constantemente exposta ao ambiente digital, de outro, é certa a influência da tecnologia digital – e especialmente da internet – que foi potencializada nos dois últimos anos 2020 e 2021 e, certamente, ensejará aumento crescente pela necessidade com que está sendo demandada. Isso porque, segundo registra a UNICEF, o debate sobre seu impacto cresceu mais alto: é uma bênção para a humanidade, oferecendo oportunidade ilimitada de comunicação e comércio, aprendizagem e livre expressão? Ou é uma ameaça ao nosso caminho da vida,

4 Geração Z: nascidos entre 1990 e 2010; Geração Alpha: nascidos a partir de 2010.

minando o tecido social, mesmo a ordem política, e ameaçadora nosso bem estar? (UNICEF, 2021a)⁵.

A resposta para essas questões, sejam quais forem, revelam algo incontestável: o fato de que nossas identidades estão sendo moldadas pela disposição conectiva, e não somente pela dinâmica da igualdade e das diferenças – não somente pela dinâmica do assistencialismo e, sim, pela acessibilidade em que é possível plasmar junto às tecnologias digitais, dentre as quais a internet, é provavelmente, o elemento mais importante, desencadeador de aspectos incrementadores ou disruptivos, “porque para melhor e para pior, a tecnologia digital é um fato de nossas vidas” (UNICEF, 2021a), que podem dar conta de nossas escolhas e de nossa identidade, sobretudo em termos de dados pessoais, a influenciar e impactar a infância, a geração presente e a geração futura.

Além do mais, na sociedade em rede, conforme revela Mendes, a disciplina da proteção de dados pessoais, tem como finalidade, tutelar a personalidade do indivíduo contra os riscos decorrentes do tratamento desses dados. Não se protege os dados em si, mas a pessoa que é a titular desses dados. (2019, p. 32). Em específico, quanto à criança, a responsabilidade não pode restar a cargo de um único segmento, seja este social, político, familiar, e, até mesmo, depender do aspecto legislativo. Esse processo necessita estar ancorado em compromisso e dever, o que fornece um viés de proteção, de promoção e de defesa de direitos, conforme consta do texto constitucional especialmente na redação do artigo 227⁶, e incorporado pelo Estatuto da Criança e do Adolescente, a fornecer fundamento para assegurar a proteção da criança – também do adolescente e do jovem - como prioridade absoluta; atribui responsabilidade compartilhada entre Estado, família e sociedade; e dentre outros direitos, estabeleceu o direito à educação e à privacidade. Em relação a esse aspecto, que não se encontra sozinho, é importante a vinculação com outros mecanismos protetivos, tais como, no cenário brasileiro, as disposições contidas na Convenção sobre os Direitos da Criança (BRASIL, 2021g), ratificada pelo Brasil em 1990 e outros mais documentos regulativos, especialmente, tendo-se em conta o trânsito dos dados em mais de um país.

Essa “arquitetura” coloca em rede e alinhamento outros mais segmentos da sociedade, na medida de seus propósitos, tais como,

O setor privado - especialmente na tecnologia e telecomunicações indústrias - tem uma responsabilidade especial e uma capacidade única de moldar o impacto da tecnologia digital nas crianças. O poder e a influência do privado setor deve ser aproveitado para avançar padrões éticos de toda a indústria sobre dados e privacidade, bem como outras práticas que beneficiar e proteger as crianças

5 Em tradução literal.

6 Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão. (Redação dada Pela Emenda Constitucional nº 65, de 2010) (BRASIL, 2021a).

online. Os governos podem promover o mercado estratégias e incentivos que fomentam inovação e competição entre prestadores de serviços para ajudar a reduzir o custo de se conectar à internet, assim expandindo o acesso para os desfavorecidos crianças e famílias. Empresas de tecnologia e internet devem tomar medidas para evitar suas redes e serviços sejam usados por criminosos para coletar e distribuir crianças sexuais abusar de imagens ou cometer outras violações contra crianças⁷. (UNICEF, 2021a).

Para que se possa ter clareza quem é a pessoa titular dos dados - usuário(a) e destinatário(a) da referida proteção – e, em tal decorrência, convém deixar claro quem é a “criança” - e a tradução de seus direitos – no específico aspecto da esfera e alcance da proteção de dados pessoais.

Com efeito, tendo em consideração o tema dos dados pessoais na perspectiva da criança, é importante que se leve em conta os seguintes pontos: i) esboço histórico e, nos dias atuais, as principais leis que regulamentam a matéria; ii) conceito étario para efeitos da LGPD; iii) o significado e o alcance da proteção dos direitos, inclusive em termos legislativo, tendo a criança como sujeito desses direitos, em especial, na esfera de dados pessoais; para tanto, na última parte, passamos a contrapor as questões que estão a desafiar a proteção de dados pessoais, especialmente tendo-se em conta a prioridade absoluta e as implicações em relação a retomada de questões que tais em face dos desafios apresentados – semelhantes ao desenrolar do trabalho infantil -, tendo como parâmetro a criança na condição de titular e destinatária de direitos voltados à proteção de dados pessoais.

Inicialmente, em termos jurídicos e alcance do reconhecimento de direitos da criança, alusiva à matéria da proteção de dados pessoais, temos o seguinte quadro evolutivo da normatização referente ao tema, o qual é indicado sem a intenção de esgotar o seu viés legislativo. Senão, veja-se.

Em termos de esboço histórico na contemporaneidade: ainda que a temática dos dados e a privacidade sejam categorias presentes na história humana, é a sua vinculação com a internet e o mundo das redes que vai conferir, de modo específico, o destaque à proteção de dados pessoais, que, no caso, requer ser examinado em conjunto com a privacidade que se dissemina na internet, quase que, uma não privacidade, qual seja, um salto em sua redefinição: de um efeito negativo de ser deixado em paz para um controle dos dados pessoais, o forjar da identidade pessoal.

Como resultado e efeito de processo político e de participação democrática, em 1988, no Brasil, a Constituição Federal, contempla alguns aspectos pertinentes a essa nova concepção que os dados passaram a exigir. São ilustrativos, o art. 5º, no que se refere a vida privada, a intimidade, a honra e a imagem das pessoas. (BRASIL, 2021a).

Quanto às principais leis que sustentam o tema, há as primeiras leis europeias, produzidas na década correspondente aos anos 1970-1980, de forma que o marco zero, foi a lei criada em Hesse, na Alemanha, na década de 1970; a Lei de Dados da

⁷ Em tradução literal.

Suécia (1973), o Estatuto da Proteção de Dados da Alemanha (1977). São Leis de primeira geração. (MENDES, 2019, p. 38).

A Convenção sobre os Direitos da Criança, de 1989, promulgada pelo Decreto nº 99.710, de 21 de novembro de 1990, dispõe, em seu artigo 40, 2, letra b, dentre outros aspectos, que os Estados Partes reconhecem e assegura as disposições pertinentes dos instrumentos internacionais, os Estados Partes assegurando, quanto a criança, “VII) ter plenamente respeitada sua vida privada durante todas as fases do processo” (BRASIL, 2021g).

O Estatuto da Criança e do Adolescente, Lei 8.069, de 13 de julho de 1990 (BRASIL, 2021b), reconhece o estágio peculiar de desenvolvimento característico da infância e adolescência⁸, fato que coloca crianças e adolescentes em posição de vulnerabilidade presumida, a justificar a proteção especial e integral que devem receber.

Em 2013, a Lei nº 12.965, de 23 de abril de 2014, ou Lei do Marco Civil da Internet (MCI) (BRASIL, 2021d), veio a estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil, ocasião em que introduziu de forma específica a questão da privacidade online no Brasil. Foi a primeira lei a regulamentar o uso da internet no país, tendo introduzido conceitos como a neutralidade de rede e a liberdade de expressão e definidas quais são as obrigações dos órgãos públicos no fornecimento de internet.

Em relação a criança, o MCI pontua que:

Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente.

Parágrafo único. Cabe ao poder público, em conjunto com os provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e fornecer informações sobre o uso dos programas de computador previstos no caput, bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes. (BRASIL, 2021d).

A Lei nº 13.257, de 08 de março de 2016, Marco Legal da Primeira Infância, corrobora a Doutrina da Proteção Integral e a regra constitucional da absoluta prioridade. Referida lei contempla especificidades em relação aos direitos e as garantias de crianças até seis anos completos. Em seu artigo 3º, a mesma dispõe sobre “o dever do Estado de estabelecer políticas, planos, programas e serviços para a primeira infância que atendam às especificidades dessa faixa etária, visando a garantir seu desenvolvimento integral”. (BRASIL, 2021e).

Com o Regulamento Geral de Proteção de Dados da União Europeia (GDPR

⁸ Também em relação ao jovem, conforme consta do art. 227, da CF, de 1988 (BRASIL, 2021a).

– General Data Protection Regulation, EU 679/2016), com vigência em 2018, há a consagração da proteção de dados pessoais, de forma definitiva. Em relação à União Europeia, Willemin considera que “a GDPR favorece os países-membros da UE com a aplicação de uma idade mínima” (2020, p. 582). No caso, a GDPR confere aos países membros da UE que observem a seguinte adoção para o consentimento: “que o consentimento seja dado para, no mínimo, maiores de 16 anos. Abaixo dessa idade, o consentimento do processamento deve ser autorizado pelos pais ou responsáveis” (WILLEMIN, 2020, p. 582), ou seja, “a GDPR favorece os países-membros da UE com a aplicação de uma idade mínima para consentimento, desde que não seja inferior a 13 anos” (WILLEMIN, 2020, p. 582).

Nos Estados Unidos, em que pese a ausência de um regramento geral para todo o país – o que há são normativos federais, tais como a HIPAA – Health Insurance Portability and Accountability Act; FCRA – Fair Credit Reporting Act; ECPA – Electronic Communications Privacy Act; e, em termos estaduais, a CCPA (California Consumer Privacy Act), a qual entrou em vigência em 2020 (LIMA, 2020, p. 502).

Em relação à criança, a COPPA – Children’s Online Privacy Protection Act, tem abrangência federal nos Estados Unidos da América. De forma que, segundo a COPPA (2021), o Congresso americano promulgou a Lei de Proteção da Privacidade das Crianças Online em outubro de 1998. Esta Lei instruiu a Comissão a estabelecer regras limitadas que regem a recolha quanto aos dados pessoais de crianças com 12 anos ou menos⁹. Ato seguinte, a Comissão promulgou a Regra de Proteção da Privacidade das Crianças Online, que entrou em vigor em 21 de abril de 2000. A Lei e a Regra serão intercambiavelmente referenciadas como “COPPA”¹⁰.

Assim, desde a aprovação da Lei de Proteção da Privacidade das Crianças Online (COPPA), os sítios da Web têm razões legais para não recolherem informações pessoais de crianças com idade de 12 anos ou menos – o que é, até então, um “progresso” significativo na proteção da segurança e da privacidade das crianças na Internet (COPPA, 2021)¹¹.

No Brasil, a privacidade e a proteção de dados pessoais estão assentadas no direito constitucional à intimidade e à vida privada previsto no art. 5º, X, da Constituição Federal. Imbuídos desses fundamentos, e inspirada na GDPR, nasce a Lei 13.709, de 14 de agosto de 2021, ou Lei Geral de Proteção de Dados Pessoais, a qual, em relação à criança (e também ao adolescente) contempla algumas regras, sem, contudo, fazer referência, de modo explicativo quanto ao adolescente.

A LGPD estabeleceu os princípios norteadores da proteção de dados pessoais, incluindo seus princípios básicos: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas no art. 6º (BRASIL, 2021f).

Considerando que, por força constitucional, a criança usufrui de proteção ju-

9 Há textos referindo a idade “inferior a 13 anos”, para deixar clara a proteção relativa à criança com idade de 12 anos ou menos. Nesse sentido, a regulamentação da COPPA proíbe a coleta de dados pessoais da criança com idade inferior a 13 anos sem o consentimento dos pais.

10 Em tradução livre, das autoras.

11 Em tradução livre, das autoras.

rídica especial que a assiste e, em tal razão, deve ter seus direitos assegurados em absoluta prioridade.

Vale ressaltar que a distribuição da matéria, em relação à criança, está prevista em dois momentos: um, a regra geral das hipóteses do art. 7º; dois, o melhor interesse, que é seu ponto chave, conferindo sua imprescindibilidade a todo e qualquer tratamento de dados pessoais, no caso da criança (e do adolescente), cujas disposições estão especificadas no art. 14, da LGPD (BRASIL, 2021f).

É fato que alguns desses dispositivos encontram-se ancorados na moderna concepção e regulamentação que a matéria vem recebendo. Assim como o GDPR, alguns dos principais pontos da LGPD reconhecem: o direito para o titular acessar, editar ou solicitar a exclusão de seus dados, recolhimento autorizado (com exceção em casos específicos), maior cuidado com dados sensíveis, portabilidade de dados e sanções administrativas, penalidades ou multas, no caso de descumprimento.

Em síntese, na contemporaneidade, além da Constituição Federal, três leis guardam pertinência direta, tanto em termos de atualidade, e como dispositivo da disciplina de dados pessoais, tendo a criança como núcleo chave deste breve estudo: trata-se do GDPR – Regulamento Geral de Proteção de Dados da União Europeia (General Data Protection Regulation - EU 679/2016), da COPPA (Ato de Proteção Online à Criança), da LGPD – Lei Geral de Proteção de Dados Pessoais (Lei 13.709, de 14 de agosto de 2018) e, como não poderia deixar de ser, é importante também alguns especiais dispositivos contidos no Estatuto da Criança e do Adolescente, Lei 8.069, de 13 de julho de 1990, além da Constituição Federal, de 1988. Os três últimos, no caso do Brasil, são os mais destacados e essenciais.

É fato que, pelo lugar que ocupa, a criança encontra-se em uma tal conotação, cuja exposição direta ao ambiente virtual necessita de acentuado nível protetivo. Se ela não recebe determinadas camadas em seus pontos de dados, significa que, no futuro, ela não terá acesso aos principais direitos. Pior, poderá estar exposta até ao trabalho precoce. É sobre essas temáticas as considerações seguintes.

3. A proteção de dados pessoais da criança: fundamentos e desafios em face da Lei Geral de Proteção de Dados Pessoais e suas implicações – um locus para a cultura fraterna.

A LGPD representa um importante passo na demanda de direitos da sociedade da informação: impulsionar um nível aprofundado de proteção dos pequenos, naquilo que concerne aos seus dados pessoais e retirar dessa estatística mecanismos facilitadores de direitos.

Nessa dinâmica, as privações de direitos saltam aos olhos, enquanto que a proteção de direitos parece mesmo passar despercebida para aqueles que não usufruem de privações – que podem ser de toda ordem¹². Um olhar sobre a infância dá conta de que são muitas as privações, e, curiosamente, na medida em que

12 A UNICEF (2021b), em relatório intitulado “Pobreza na Infância e na Adolescência”, apresenta os seguintes pontos a respeito dos quais são traduzidos percentuais de privação de direitos - educação, informação, proteção contra o trabalho infantil, moradia, água e saneamento, de forma que, “Compreender cada uma dessas dimensões é essencial para desenhar políticas públicas capazes de reverter a pobreza na infância e na adolescência” (UNICEF, 2021b).

catalogamos direitos, elas tendem a alargar. Há, nessa dinâmica, um paradoxo e que ninguém saia por aí defendendo os “não direitos” sob a justificativa de que, assim, inexistirão privações. A lógica é exatamente oposta. Reconhecer direitos é uma das melhores formas de conferir consciência e importância no sentido de promover uma cultura de reconhecimento de direitos, segundo uma dinâmica de proteção, promoção e defesa de direitos de que dão conta, de forma específica, a legislação a respeito dessa temática¹³.

A realidade sobre as privações retrata o seguinte quadro, no Brasil:

As privações de direito também afetam de forma diferente cada grupo de meninas e meninos brasileiros. Moradores da zona rural têm mais direitos negados do que aqueles da zona urbana. Crianças e adolescentes negros sofrem mais violações do que meninas e meninos brancos. Moradores das regiões Norte e Nordeste enfrentam mais privações do que os do Sul e do Sudeste. E, conforme crescem, crianças e adolescentes vão experimentando um número maior de privações. (UNICEF, 2021b).

Em termos tecnológicos, indicados na qualidade da “informação”, a UNICEF apresenta o seguinte quadro ilustrativo desses dados de privação de direitos, retirados da cena brasileira, visando “dar destaque a problemas graves que afetam meninas e meninos e colocam em risco seu bem-estar”: SEM PRIVAÇÃO: Criança 10-17 anos que acessou a internet nos últimos três meses; PRIVAÇÃO INTERMEDIÁRIA Criança 10-17 anos que não teve acesso à internet nos últimos três meses, mas tem uma televisão em casa; e PRIVAÇÃO EXTREMA: Criança 10-17 anos que não utilizou a internet nos últimos três meses nem tem televisão em casa. (UNICEF, 2021b), ocasião em que, faz um alerta: 61% das meninas e dos meninos brasileiros vivem na pobreza – sendo monetariamente pobres e/ou estando privados de um ou mais direitos; quase 27 milhões de crianças e adolescentes (49,7% do total) têm um ou mais direitos negados; os mais afetados são meninas e meninos negros, vivendo em famílias pobres monetariamente, moradores da zona rural e das Regiões Norte e Nordeste. (UNICEF, 2021b).

Seja como for, “A ausência de um ou mais desses direitos coloca meninas e meninos em situação de ‘privação múltipla’, uma vez que os direitos de crianças e adolescentes são indivisíveis”. (UNICEF, 2021b).

13 Representativo da mais alta proteção de direitos: no Brasil, o Estatuto da Criança e Adolescente, Lei 8.069, de 1990. A Constituição Federal, de 1988, da qual decorre o direito à proteção integral estabelecido pelo art. 227. Na esfera internacional, a Convenção sobre os Direitos das Crianças adotada pela ONU em 1989, com vigência no ordenamento brasileiro a partir de 1990, cujo tratado internacional de proteção de direitos humanos contempla, no preâmbulo, o princípio da liberdade, proclamado na Carta das Nações Unidas, o qual estabelece que nenhuma criança será objeto de interferências arbitrárias ou ilegais em sua vida particular (art. 16.1), com direito à proteção da lei contra essas interferências ou atentados (art. 16.2). Também, o art. 19 da Convenção Americana de Direitos Humanos prevê que “toda criança tem direito às medidas de proteção que a sua condição de menor requer por parte da sua família, da sociedade e do Estado”.

No cenário internacional, Borelli (2018, p. 141), apresenta o seguinte quadro da criança no ambiente digital:

Notavelmente, crianças estão acessando a internet cada vez mais cedo. Um relatório elaborado em Madri, pela Comissão espanhola da Unicef, em 2018, revelou que jovens entre 15 e 16 anos atualmente tiveram o primeiro acesso à internet por volta dos 10 anos, ao que, os que hoje estão com 9 ou 10 anos de idade, iniciaram a vida digital aos 7 anos. Entre os espanhóis, 95% dos jovens entre 10 e 15 anos utilizam regularmente a internet. Ainda, conforme o texto divulgado pela ONU, diariamente, mais de 175 mil crianças acessam a internet pela primeira vez no mundo.

Através do relatório “Pobreza na Infância e na Adolescência”, a UNICEF apresenta os seguintes dados a respeito da categoria denominada “Informação”:

Entre meninas e meninos brasileiros de 10 a 17 anos, 25,7% não tiveram acesso à internet nos últimos três meses antes da coleta da Pnad 2015, sendo considerados privados de informação. 24,5% não acessaram à internet, mas têm televisão em casa, estando em privação intermediária. E 1,3% não acessou a rede e não tem televisão em casa, estando em privação extrema. Entre eles, 500 mil meninas e meninos não têm acesso a nenhum meio de comunicação em casa: rádio, televisão ou internet. Crianças e adolescentes negros são 73% do total de meninas e meninos privados de informação. A proporção de crianças e adolescentes privados de informação no Norte é três vezes a do Sudeste. (UNICEF, 2021b).

De igual forma, no mesmo documento, a UNICEF (2021b) apresenta os seguintes dados a respeito da educação:

No Brasil, 20,3% das crianças e dos adolescentes de 4 a 17 anos têm o direito à educação violado. 13,8% estão na escola, mas são analfabetos ou estão em atraso escolar, estando em privação intermediária. E 6,5% estão fora da escola, em privação extrema. A garantia do direito à educação varia por regiões. No Norte, a proporção de crianças e adolescentes privados de educação é o dobro do que no Sudeste. Há 545 mil meninas e meninos negros de 8 a 17 anos analfabetos, versus 207 mil brancos. O analfabetismo e o atraso escolar afetam 53% mais meninos

do que meninas. E quem vive no quintil mais pobre da população tem quatro vezes mais privação do que os do quintil mais rico.

Por onde se pode buscar, as informações são de que os jovens são os mais plugados, mas certamente, os mais comprometidos em uma “cultura de quarto”¹⁴, ou seja, são a faixa etária mais conectada, enquanto que, segundo a UNICEF, um terço daqueles que acessam a internet são crianças (UNICEF, 2021a), mas não se pode esquecer que elas são o elo frágil dessa rede – não somente por estarem em processo de desenvolvimento, ou porque representam um público consumidor e de interesse para o mercado, e sim, pela condição de que, contra a criança está sendo forjado um nível de exposição de afetação em várias ordens e de chamamento contrário aos seus interesses, típicos de violação de seus direitos – e, nessa perspectiva, convém dar a elas um nível protetivo de alta performance, seja linguística, seja em termos educacionais e culturais, seja em proporção comunicativa e informativa, como, também, performativa quanto a um cansaço de exposição constante ao ambiente virtual, semelhante ao que pode conter os mecanismos de questões tais, como a exposição ao trabalho em tenra idade. Já se antevê que o acesso para muitas crianças está tomando características de ordem pessoal, privada e menos supervisionada.

Essas situações que podem ser examinadas sob várias dimensões, inclusive na qualidade de dívida fraternal e de proporcionar uma política compensatória¹⁵ – porque as crianças, mais do que ninguém, são epígonas dessa especial cultura em fraternidade, ou cultura fraterna, a merecer novas considerações frente a esse estado de coisas, exatamente porque assumimos uns com os outros uma espécie de dívida, um pacto transgeracional de que é forte a lição de Hans Jonas (2006). Nessa linha, as questões jurídicas da proteção de dados pessoais, tendo a criança como titular e destinatária desses direitos é mesmo um convite portentoso sobre questões dessa natureza.

Sob tal prisma e, em termos de proteção de dados pessoais de titularidade da criança, os temas seguintes merecem atenção e cuidado. São eles: i) a compreensão desse especial grupo, notadamente, em termos de vulnerabilidades; ii) as implicações e os desafios que questões que tais estão a apresentar, sobretudo em termos de

14 A expressão é utilizada, conforme exposto em nota, na introdução, por “cultura de quarto” e não “cultura de quarto fechado”. O significado diz respeito à “tendência crescente que empurra os jovens, cada vez mais, para o espaço do seu quarto. Este empurrão toma várias formas: o do tempo lá passado (a dormir, mas também a socializar com outros jovens) e o do conjunto de tecnologias de mediação que o jovem tem à sua disposição. A televisão no quarto, o rádio no quarto, o leitor de CDs no quarto, o computador no quarto, a consola no quarto – uma série de equipamentos recreativos, de trabalho e mediáticos que são levados (ou, ao nível da casa, replicados) para o quarto”. (CARDOSO, 2021).

15 No julgamento do Recurso Ord. em MS n. 26.071/DF, Relator Ministro Ayres Britto, constou: “Nesse rumo de ideias, nunca é demasiado lembrar que o preâmbulo da Constituição de 1988 erige a igualdade e a justiça, entre outros, “como valores supremos de uma sociedade fraterna, pluralista e sem preconceitos”. Sendo certo que reparar ou compensar os fatores de desigualdade factual com medidas de superioridade jurídica é política de ação afirmativa que se inscreve, justamente, nos quadros da sociedade fraterna que a nossa Carta Republicada idealiza a partir das suas disposições preambulares” (DJ 1º.2.2008) (STF, 2021b).

cultura fraterna e, nessa esfera, dois outros temas são pertinentes – ambos, devem ser examinados pela concepção positiva e negativa, um plus que decorre desse estado de coisas, relacionados à cultura do trabalho infantil fora de casa e a “cultura do quarto” a dar conta da garantia de prioridade e as implicações desse especial aspecto, ensejador do reconhecimento da cultura de dados pessoais, que no caso, enfrenta o mesmo paradoxo do reconhecimento de direitos no seu conjunto. Senão, veja-se.

Quanto ao contido no “item i”, referida condição de vulnerabilidade, via de regra, comporta um particular desenho em que, crianças são protagonistas e vítimas de aspectos que lhes são essenciais, dominados por questões econômicas e de pertencimento, cuja moeda, a pobreza é posta à prova da oportunidade e da inclusão. No ambiente digital, mais do que a pobreza, a exclusão digital é posta a prova, na medida em que, por variadas razões, até econômicas, a criança poderá restar em situação de absoluta irrelevância.

A seu modo a UNICEF, por meio de seu relatório, que fora levado a público no ano de 2018, pontua que a pobreza na infância e na adolescência tem múltiplas dimensões, que vão além do dinheiro. Ela é o resultado da interrelação entre privações, exclusões e as diferentes vulnerabilidades a que meninas e meninos estão expostos, a impactar o seu bem-estar. (UNICEF, 2021b). Trata-se, pois, de uma pobreza que vai além da pobreza monetária e se alonga em privações múltiplas (inclusive de direitos), consolidadas nos dados seguintes:

Os resultados mostram que, dos 61% de crianças e adolescentes brasileiros que vivem na pobreza, 49,7% têm privações múltiplas. Muitas dessas meninas e desses meninos estão expostos a mais de uma privação simultaneamente. Em média, elas e eles tiveram 1,7 privação. Há 14,7 milhões de meninas e meninos com apenas uma, 7,3 milhões com duas e 4,5 milhões com três ou mais. Neste grupo, existem 13,9 mil crianças e adolescentes que não têm acesso a nenhum dos seis direitos analisados pelo estudo, estão completamente à margem de políticas públicas. No conjunto de aspectos analisados, o saneamento é a privação que afeta o maior número de crianças e adolescentes (13,3 milhões), seguido por educação (8,8 milhões), água (7,6 milhões), informação (6,8 milhões), moradia (5,9 milhões) e proteção contra o trabalho infantil (2,5 milhões). (UNICEF, 2021b).

Em destaque, o fundamento da miserabilidade, da pobreza¹⁶, ou, em apertada síntese, da vulnerabilidades em que se encontram as crianças, sobretudo, a par de

16 Sob a perspectiva da pobreza, sobretudo a condição de vulnerabilidade das crianças e adolescentes, habitantes da rua, há um fundamento levado a razão de decidir, tal como se vê do trecho seguinte: “Entendimento em sentido contrário poderia dar azo a apreensões sem fundamento constitucional, em violação ao devido processo legal (art. 5º, LIV) e qualquer tipo de controle. Serviriam, ainda, para a implementação de uma política higienista que, em vez de reforçar a tutela dos direitos dos menores, restringiria ainda mais o nível de fruição de direitos, amontoando crianças em unidades institucionais sem qualquer cuidado ou preocupação com o bem-estar desses indivíduos”. (STF, 2021a).

várias resoluções e de recomendações levadas a termo e conforme consta da atribuição do Conselho Nacional dos Direitos da Criança e do Adolescente – CONANDA (BRASIL, 2021c), estão entre os motivos recepcionados na qualidade de vulnerabilidade, cujo comando o Estado Nação toma em defesa dos direitos da criança.

Porém, não se pode esperar que o próprio fundamento contenha em si grave equívoco, um direito manifestamente regressivo, redundante que deponha contra o sistema de garantia dos direitos e da proteção integral das crianças, e, em tal razão, não esteja apto a refletir o atual paradigma do sistema de garantia de direitos, cujo fundamento maior é a expressão da proteção integral.

Quanto às questões expostas no “item ii”, sob a dinâmica de implicações e desafios que tais questões despertam, à volta com a proteção de direitos, significa dar conta de uma imperiosa vocação que pende a favor da cultura fraterna. Nessa perspectiva, dois outros temas são pertinentes – um plus que decorre desse estado de coisas: o primeiro, relacionado à cultura do trabalho infantil fora de casa, que contrapõe a “cultura do quarto”; o segundo, ensejador do reconhecimento da cultura de dados pessoais. Ora, a cultura de dados pessoais e o reconhecimento de direitos pertencem ao mesmo paradoxo: a tradução de seus imperativos normativos. Dar conta deles, significa vencer a gramática de seus marcos interpretativos.

Essa situação – de ausência de direitos – ou de direitos mal distribuídos e com dificuldade de reconhecimento, pode ser agravada com o cerceamento dos direitos ou de direitos culturalmente perseguidos, que necessitam ser objeto de entrega ou de acesso. Um importante instrumento de acessibilidade diz respeito à política de compensação - esse remédio reparador de direitos, a dar conta de uma conexão de direitos, uma tal compensação, reparando e elevando referida condição, com a qual se homenageia a insuperável máxima do compromisso da proteção dos direitos humanos, a ressignificar e dar o alerta ao Estado, a suas instituições, à família, ao ser humano, aos titulares e não titulares de direitos – especialmente os que virão a ser. Em termos de dados pessoais a máxima é de priorizar o reconhecimento desses direitos que estão sendo construídos.

Em relação ao cenário que tem como matriz a esfera tecnológica, que é onde vamos encontrar a criança e sua especial vulnerabilidade, Rosling apresenta um quadro alentador a respeito do mundo e suas dinâmicas, senão, veja-se: em todos os países de baixa renda do mundo 60% das meninas terminam o ensino fundamental; a maioria da população mundial vive em países de renda média; nos últimos vinte anos, a proporção da população mundial vivendo em extrema pobreza, caiu pela metade; a expectativa de vida no mundo hoje é de 70 anos; existem hoje no mundo 2 bilhões de crianças entre 0 a 15 anos de idade e até 2100, de acordo com a ONU haverá 2 bilhões (esse número permanecerá estável); em 2100 a população mundial terá crescido em mais de 4 bilhões, sendo o principal motivo o fato de que haverá mais adultos, com idade de 15 a 74 anos; ao longo dos últimos 100 anos, o número de mortes anuais por conta de desastres naturais diminuiu pela metade; 80% de crianças de 1 ano de idade no mundo já foram vacinadas de alguma doença; em média, no mundo todo, homens de 30 anos passaram dez anos na escola, e as mulheres, na mesma idade, passaram 9 anos; 80% das pessoas no mundo têm acesso a eletricidade de algum modo; e especialistas em clima global

acreditam que, nos próximos cem anos, a temperatura média irá esquentar. (ROSLING et al, 2019, p. 13-15).

Esse quadro apresentado por Rosling et al (2019) fornece pontos alentadores, mas não se pode desconsiderar que o volume de dados, quanto a esfera tecnológica, tem outras conotações e muitas dizem respeito a preocupações, sobretudo por conta da acirrada vigilância e comercialização que os dados estão a implicar.

Quanto ao ambiente digital, precisamos ter em conta que a “inteligência artificial (IA) procura preparar os computadores para fazer o tipo de coisas que a mente é capaz de fazer” (BODEN, 2020, p. 13). Além desses aspectos, “Algumas dessas coisas (como o raciocínio) são definidas normalmente como “inteligentes”. Outras (a visão por exemplo), não” (BODEN, 2020, p. 13). Porém, um aspecto é fundamental: “todas envolvem habilidades psicológicas – percepção, associação, previsão planejamento, controle motor – que permitem que os seres humanos e os animais alcancem seus objetivos” (BODEN, 2020, p. 13). De tal decorre a influência dessas questões com as das crianças.

Em todo o mundo, crianças estão online, e os adultos também. Mas elas, de modo preponderante – e não necessariamente os adultos - precisam de cuidados e atenção especial em uma dinâmica de dispensar proteção a favor das crianças, sempre; enquanto que, para os adultos, a proteção, que também deve e requer estar presente, mas sabendo que usufruem grau de maturidade, as conotações a eles dispensadas, são de outra ordem, em conformidade e simetria, mas não em altas e especiais “doses” protetivas como deve ser em relação à criança. Se imaginarmos a população pela perspectiva de estarem ou não online, os números começam a acenar que o percentual maior é daqueles que estão online em comparação com a população total. Estima-se que, em relação às crianças e adolescentes estão sendo construídas estatísticas de pesada vigilância, associada a usuários da Internet na sociedade em rede, sem esquecer que as crianças estão acessando a internet em idades cada vez mais jovens.

Em uma linha: os aplicativos estão monitorando diariamente as crianças que passam a ser, em uma linguagem virtual, um Access Point. Via de regra, usam uma análise automática de comportamento, cujo prejuízo primeiro ultrapassa a mensagem da privacidade, além de implicar em muitas outras questões, tais como “educação” para a violência, publicidade enganosa, exposição indevida da imagem e de localização, comercialização sem controle, etc. Essa constatação dá conta de que o tratamento de dados pessoais, por si só, é um tema importante. E o que dizer sobre o tratamento de dados pessoais de crianças e adolescentes?

A resposta para situações como essas, podem encontrar várias considerações. Contudo, alguns pontos de tratamento de dados pessoais não podem passar em vão. Os dados da criança não podem ser compartilhados com terceiros e nem para outras finalidades. Essa compreensão, ainda que submetida a pseudoanonimização, continua a ser personally identifiable (dados pessoais), eis que, nessa condição, alguém segue possuindo uma chave – mesmo que codificada – que possibilita a reversão do procedimento e, conseqüentemente a sua exposição sem tempo para terminar. Portanto, uma medida parcial, reversível e até mesmo provisória. Uma medida capaz de reduzir – e não “apagar” – a capacidade de associação de um con-

junto de dados com a identidade do titular dos dados, cujas implicações podem, dentre outras, ser substituídas por uma condição definitiva – resultante da ação do tratamento. Ou seja, o prejuízo pode ser ad infinitum e comprometer muitos pontos de dados pessoais, além de violar direitos fundamentais da personalidade, por exemplo, e, também direitos em construção no mundo todo, como é o caso dos dados pessoais, os quais no atual estágio, muitas vezes, sem cultura formada, custam a receber reconhecimento, agendas e demandas.

Em relação à criança, questões que tais podem ferir direitos agora e no futuro, direitos que nem sequer foram alvos de reconhecimento no momento atual e que, em dias próximos, poderão ser, e que, podem, inclusive, impulsionar micro fábricas de cansaço, semelhante ao compromisso de trabalho, para os quais as crianças não estão preparadas e nem devem estar pelo grau de desenvolvimento natural a que suas tenras vidas suportam. Em outras palavras, há necessidade de preservar os direitos fundamentais, a garantir que “o desenvolvimento tecnológico se torne um elemento que aprimore o desenvolvimento da personalidade e as condições econômicas e sociais dos indivíduos e coletividades, e não o contrário”. (SOUZA e LEMOS, 2021, p. 16).

Acerca do trabalho infantil propriamente dito, levado a termo por meio de alguma atividade, no Brasil, segundo dados da OIT, que amparada no último censo do IBGE, pontua a existência de mais de 3.406.000 crianças em algum tipo de ocupação. (OIT, 2021). Mas esse triste retrato seguiu contando outra “história”, e, dessa forma, entre os anos de 1992 e 2015, cerca de 5,7 milhões de crianças e adolescentes deixaram de trabalhar no Brasil, culminando com uma redução de 68% (OIT, 2021). Haverá razões para comemorar?

Sempre há. Porém, na ideia da vida que segue, na referência da PNAD, em 2019, esse “público” pontua dados gigantes: “referentes ao ano de 2019, ainda há 1,7 milhões em situação de trabalho infantil no país, sendo 66% de meninos e 34% de meninas” (OIT, 2021). Contados por faixa etária, os dados são mesmo reveladores: “21,3% tinham de 5 a 13 anos; 25,0%, 14 e 15 anos e a maioria, 53,7%, tinha 16 e 17 anos de idade” (OIT, 2021). Relativo ao exercício de ocupação considerada perigosa: “40,0% do total em situação de trabalho infantil” (OIT, 2021). Esse dado parece conter uma simples alusão, mas não. Se esses números são complicados, quando às voltas com o indesejado trabalho infantil, i.é., para as crianças eles podem passar a ser reveladores de violência, e não só isso, podem comprometer o seu desenvolvimento. Portanto, esses dados “avassaladores” precisam ser revistos, a anunciar outra história na paisagem da infância, sobretudo outra dinâmica de proteção de direitos.

Trazidas para as questões tecnológicas – a criança é um grande e especial público nesse sentido¹⁷ - não estão ainda adequadamente vivenciadas ou experimen-

¹⁷ Na qualidade de usuária da internet e com proximidade direta da criança junto ao ambiente digital, tenhamos em consideração que, tendo a criança como titular e destinatária de proteção de direitos, contrariamente aos seus interesses, pesa a existência de condições violadoras de seus direitos e que estão a reforçar uma possível presença de susceptibilidades. Segundo confirma a UNICEF - as crianças ocupam a seguinte estatística: um terço dos usuários da internet são crianças (UNICEF, 2021a). Esse dado pode ser bem maior nos dias atuais, em que o uso do ambiente digital e da tecnologia como um todo foram potencializados, inclusive em decorrência da presença da COVID19.

tadas (exatamente porque diz respeito a direitos em construção), e, exatamente por isso, seu alcance ainda está sendo avaliado. Até onde se pode mirar, suas consequências e condições, quiçá sua classificação, porque pertencentes a uma revolução tecnológica (modificando a maneira como os dispositivos se conectam), que é também social (com modificações nas relações, inclusive de trabalho) e jurídica (porque há direitos em construção) – carecem de reconhecimento e de estudos.

No que respeita a criança e sua convivência próxima com o ambiente digital, sua condição parece ensejar mecanismos mercadológicos (seja de consumo, seja de publicidade, seja de exposição a níveis laborativos) – presente e futuro – o que sugere a qualidade de contrapor a sua condição de estar em desenvolvimento, inclusive de personalidade. Esses aspectos, por si, fornecem uma lógica em termos de proteção de dados pessoais, a dar conta de que as empresas, instituições e toda a sociedade (aqui também convém incluir a família) deverão urgentemente buscar uma agenda de governança de dados tendo a criança como foco primeiro dessa especial proteção.

Aliás, as questões tecnológicas, quando postas em relação ao trabalho infantil, denotam situações para as quais há um campo vazio, em gerúndio, que estão acontecendo, e como tal, novidadeiras, ao largo de recepção e de proteção. Trata-se, pois, de uma cultura que está sendo forjada e que, no caso da criança, já sabemos onde essa história vai parar e qual é o seu terrível final: milhões de crianças longe das escolas, dos brinquedos, do que verdadeiramente importa para esse especial momento de desenvolvimento, inclusive de sua personalidade.

Não por acaso, “se torna essencial que essa experimentação e inovação ocorram no mesmo passo em que novas iniciativas de proteção também sejam desenvolvidas” (ALMADA, 2021), com modificações no cotidiano da sociedade tecnológica.

Com efeito, em relação à criança, essa posição de sociedade de risco, não pode vir ao encontro dos interesses dos pequenos e, com razão, está a necessitar de novas agendas, a dar conta de anunciar esses desafios e a denunciar suas implicações e consequências, que, por ora, cabe à prevenção e à precaução - de outro modo, teremos irrompido em destituição de relações de vidas, em quebra de continuidade de modelos sociáveis seguros, com afetação do desenvolvimento da criança e de sua personalidade. Essa “tomada de pé” da situação é urgente, a menos que, tenhamos comprometido o futuro de nossas crianças.

Via de regra, trata-se da “cultura do trabalho fora de casa”, o que é uma contradição, pois sabemos que a tecnologia, no mais das vezes, em termos atuais, em que seguimos frente a uma pandemia, e ainda que assim não estivéssemos, em relação à criança, a ideia, em termos de ambiente digital, é a “cultura do quarto”. Como se sabe, a tecnologia, parece mesmo estar imiscuída nesse circuito.

Sob tal prisma, o tratamento de dados, relacionados a crianças, de um modo geral, traduzem dupla realidade, uma cultura do microtrabalho infantil – inobstante forjado na internet, relaciona-se a um modelo psicológico de trabalho firmado na “cultura do quarto”, em contraponto ao que ecoa fora de casa. Qual deles é pior, não importa, porque ambos são prejudiciais quando posto no exagero. Necessitamos estar atentos a corrigir essa dupla situação – a do trabalho infantil – tradicional e já reconhecido; e o novo modelo de expressão de trabalho, a qual

podem estar sendo submetidas milhares de crianças em uma peça tecnológica inarredável – e, curiosamente, para a qual, nem mesmo tivemos tempo de perceber, de reconhecer e de pesquisar.

Desse adiantado estado de coisas, sobressai a importância da proteção de dados pessoais, que, no caso da criança, vem com essa “pegada” inusitada de vários efeitos. Sobre esse contexto, a regra do art. 5º, da Lei 13709, de 2018, traça as especificidades do tratamento de dados pessoais. (BRASIL, 2021f).

Não por outra razão, o dia a dia não cansa de oferecer exemplos dos mais reconditos significados, desde a exposição da imagem (que pode ficar em exibição eterna), da política de privacidade não lida, ou de uma política de privacidade (que é o filtro da proteção de dados pessoais) que não consegue passar sua resposta, sendo evidente o prejuízo, principalmente em relação aos vulneráveis, justificando a governança de dados pessoais nesse sentido, no qual há muitas questões a serem avançadas. Trata-se de um compromisso fraterno, para o qual temos muito que cooperar, relacionar e comunicar uns com os outros, uma verdadeira cultura de fraternidade, ou cultura fraterna.

A respeito do primeiro ponto, um aspecto é deveras significativo considerar, conforme lembra Borelli (2018, p. 141) no sentido de que, uma das formas principais de se “obter informações sobre quais dados pessoais serão coletados para uso do serviço que se pretende utilizar, como serão tratados, com quem serão compartilhados e a forma de armazenamento é lendo sua política de privacidade”

Ocorre que,

[...] definitivamente, termos de uso e políticas de privacidade não estão entre as coisas que mais atraem o internauta. Pelo contrário há quem diga que uma das maiores mentiras deste século é “li e concordo”, já que ninguém (ou quase ninguém), de verdade, lê os referidos termos. (BORELLI, 2018, p. 141).

Além do mais, frente a sua posição de vulnerabilidade, é uma situação que requer ainda mais atenção e cuidado, a começar pelo próprio significado de vulnerabilidade, que, na lição de Montanaro, em empréstimo quanto ao conjunto de diretrizes da norma ISO/IEC 27001: 2005, representa uma fraqueza de um ativo ou de um grupo de ativos que pode(m) ser explorada(s) por uma ou mais ameaças. (2019, p. 314).

Bem por isso, o processamento de dados pessoais, desse especial público, necessita de adequada conformidade e simetria, levando-se em conta o seu melhor e legítimo interesse. Outro ponto: pela posição de vulnerabilidade a que pertencem, a criança necessita estar adequadamente sob o arco constitucional protetivo desses regimentos, e, também, necessita estar acobertada, na lição de Montanaro, o triângulo de ouro, composto por pessoas, processos e tecnologia, de forma a gerir vulnerabilidades. (2019, p. 315).

Além do mais, a influência da tecnologia digital - e especialmente da Internet – aumentou o debate em torno de seu impacto e de seu crescimento vertiginoso.

Ainda que o fato de colocar todos em rede ilimitada de comunicação imediata, permitir educação onde quer que a criança esteja, traduzir aprendizagem e livre expressão, é esperado que a mesma não seja canal para disseminar a desgraça no sentido de antecipar redes de trabalho infantil, de ser portal de comércio e de tráfico de criança, e de disseminação de ilicitudes de toda ordem, tais como as práticas do cyberbullying (perseguição virtual), do grooming (aliciamento), do sexting (envio de pornografia), do profiling (criação de acesso e de perfil do usuário) a dar causa e razão a um risco de alta gravidade, quer, porque a grande maioria das pessoas ainda ignoram a sua existência; quer, porque o acesso e a utilização dos dados pessoais para a criação de perfil representa riscos reais, tanto no campo pessoal, quanto profissional, e até mesmo com feições políticas, estendendo-se para além do individual, em razão do grande poder de influência que isso confere a quem detém essas informações. Incorporado a uma linha do tempo, esse tipo de prática, poderá, em um futuro próximo, gerar diversas outras implicações dentre as quais, a afetação do trabalho, que sobrevive tanto de uma formação de habilidades, competências e condições técnicas e até formativas, poderá ter sua perspectiva violada em redes que demandam o aliciamento, a negativa de educação e de violação de confiança intergeracional.

A respeito da criação de perfis, Willemin (2020, p. 575) pontua que:

Qualquer forma de tratamento automatizado de dados pessoais que consiste na utilização de dados pessoais para avaliar certos aspectos pessoais relativos a uma pessoa singular, em particular para analisar ou prever aspectos relativos ao desempenho dessa pessoa singular no trabalho, em sua situação econômica, saúde, preferências pessoais, interesses, confiabilidade, comportamento, localização ou movimentos.

Há ainda, uma última categoria, certamente a mais perigosa de todas, presente por associação dessas, ou de cunho único: trata-se de fake news, cuja disseminação é um risco evidente ao indivíduo e a toda organização relacional e social. Seus efeitos podem ser sentidos imediatamente ou em um futuro próximo e tardio, a comprometer as relações de toda uma geração, exatamente, porque o seu objetivo último é exatamente mudar um comportamento. Quando se tem em conta, tratar-se de criança, cuja personalidade está em formação e em processo de desenvolvimento, a presença e combinação desses elementos representam exposição danosa a sua liberdade de expressão, exatamente pela suscetibilidade presente na criança e nas implicações decorrentes de muitos desses “fatos”.

Corroborando, há muitos modos pelos quais, tratar questões de tecnologia, levando-se em conta o fato de as crianças estarem em Digital World, implicam em perspectivas, boas ou más, que não depende só de um comando, mas também de um propósito e até de um projeto. A tecnologia digital já mudou a vida das crianças e as chances de vida - e o futuro será marcado por essa proximidade, de forma que, se aproveitada de modo correto e universalmente acessível, a tecnologia di-

gital pode ser uma virada comunicacional: o acesso e a proteção de direitos, uma lógica inclusiva para muitas crianças, que estarão conectadas e habilitadas em um mundo digital de oportunidades. Porém, se os dados pessoais de meninos e meninas não receberem a adequada proteção, é certa a onda de pontos de direitos que estarão violados e perdidos nas estatísticas e não será o tratamento que irá conferir novas e boas perspectivas.

Considerações finais

Quando, situações como as que foram neste apresentadas - inauguradas em termos legislativos do Direito brasileiro pela LGPD - deparam-se com os interesses e direitos da criança, é preciso um esforço criterioso para conferir arquitetura protetiva a esses específicos direitos e não afetar outros mais direitos.

Seja como for, lançar na defesa da cultura de proteção de dados, tendo como propósito a promoção dos direitos da criança frente a LGPD, refletindo sobre a importância de proteger imediatamente os direitos, tem a ver com uma tarefa paradoxal, porque se trata de direitos que estão sendo reconhecidos, bem por isso, direitos de um público que carece de acirrada proteção e definição de sua proteção.

A menos que o acesso a tecnologia digital, incluindo a proteção de dados pessoais sejam razoavelmente garantidos e dispostos em conformidade e simetria, o ambiente virtual pode criar novas divisões com impedimentos ao exercício do potencial das crianças, ou até mesmo de ter comprometido esse período áureo de desenvolvimento. Em relação ao conjunto de seus direitos é preciso levar em conta a sua condição de indivisibilidade e, como tal, a violação desses direitos colocam as crianças, em privação múltipla de direitos, uma ode de contribuição inversa, a favor da violência. Nessa linha, ampliar o reconhecimento sobre os direitos, entender os riscos e mecanismos de meninos e meninas não terem acesso a tais direitos, prevenir e responder à violência, são balizas fecundas em face de garantias que crianças tenham acesso à informação e proteção no exercício de seus direitos.

Significativa é a agenda de proteção de dados pessoais. Disposta em contraponto à criança, convém destacar que o direito mais exposto, quando se tem em conta a proteção de dados pessoais, o mesmo diz respeito à privacidade e aos direitos fundamentais, e, nessa linha, muitos outros direitos poderão estar sendo violados - um aspecto delicado, diz respeito às implicações e aos desafios ocasionados. Uma específica contingência tem a ver com o trabalho infantil, na medida em que, o ambiente digital, incluindo as questões tecnológicas podem favorecer a ambientação de condições semelhantes ao stress gerado por demandas do trabalho, e que pode expor as crianças a uma agenda cotidiana, nada ideal a sua formação.

Bem por isso, investir no monitoramento e na geração de dados e de evidências são essenciais para entender o cenário das questões digitais, das violências desencadeadas e tomar medidas para enfrentá-las. Vindas de onde vier, cada uma dessas questões pluga no que é decisivo para mudar o cenário digital atual e, em contrapartida, proteger os direitos das crianças.

É significativo uma atuação rápida, a aquilatar os riscos online: na mesma proporção em que esses riscos podem tornar as crianças vulneráveis, mais suscetíveis à exploração (tanto quanto a exposição desenfreada, o trabalho infantil, abuso

e outras ameaças mais sutis para seu bem-estar), este estudo defende uma larga atuação a favor de acirrada proteção dos direitos baseado em menos “cultura de quarto” e mais “cultura fraterna”, a proporcionar maior cooperação para proteger as crianças dos danos de um mundo mais conectado - enquanto aproveita as oportunidades da era digital para beneficiar todas as crianças.

Quando se interconecta as esferas tecnológicas e o ambiente virtual na esfera de dados pessoais, o primeiro recado é se colocar na dianteira da proteção desses dados. Agir, em desconformidade, não levando a termo a proteção de dados pessoais, no atual momento, equivale a violar direitos fundamentais de milhares de pessoas, qual seja, em uma lógica antiga de proteção de direitos, traduzida pela dinâmica de proteger não o que falta, mas o que existe, quanto a proteção de dados pessoais, trata-se mesmo de dupla equivalência, do que falta e do que existe em termos de defesa de direitos, os quais devem estar em simetria protetiva e promocional. Levando-se em consideração a criança, os cuidados desses direitos e a governança de seus dados pessoais, os mesmos necessitam de mais atenção e prioridade, seguindo uma tomada de posição: defender e promover direitos equivale a protegê-los em sua essencialidade.

Mais do que ter momentos de individualidade – conforme pode estar sugerindo a “cultura do quarto”, a ombreira da porta pode estar marcando um espaço diferente, um ponto de alternância de relações estressantes, compromissos infundáveis, muito semelhantes ao mundo do trabalho e, em tal razão, o ambiente virtual precisa de urgente avaliação, sobretudo porque, além da recolha e coleta de dados que já está sendo enfrentada por força da LGPD, há, essa dinâmica para a qual a psicologia social e as demais ciências precisarão conferir atenção. A receita, por ora, pode passar pela substituição de seus efeitos para os da cultura fraterna, que é onde os envolvidos no processo assumem suas responsabilidades de forma cooperativa, irmanados da vontade de acertar.

REFERÊNCIAS

ALMADA, Giovanna Michelato; FREITAS, Cinthia Obladen de Almendra. A internet dos brinquedos e a proteção de dados pessoais das crianças sob a legislação brasileira. Disponível em: <https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1286>. Acesso em: 19 out. 2021.

BODEN, Margaret A. Inteligência Artificial: uma brevíssima introdução. Tradução Fernando Santos. São Paulo: Editora UNESP, 2020.

BORELLI, Alessandra. O tratamento de dados de crianças no âmbito do General Data Protection Regulation (GDPR). In: Viviane Nóbrega Maldonado; Renato Ópice Blum (coordenação). Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia. p. 139-167.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15. out. 2021.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/18069.htm. Acesso em: 12.10.2021.

BRASIL. Lei nº 8.242, de 12 de outubro de 1991. Disponível em: <http://www>.

planalto.gov.br/ccivil_03/leis/l8242.htm. Acesso em:

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 16 out. 2021.

BRASIL. Lei nº 13257, de 08 de março de 2016, Marco Legal da Primeira Infância. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13257.htm. Acesso em: 17 out. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 13.10.2021.

BRASIL. Convenção sobre os Direitos da Criança. Decreto nº 99.710, de 21 de novembro de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d99710.htm. Acesso em: 15 out. 2021.

CARDOSO, Daniel S. A cultura do quarto e o uso excessivo da internet. Resultados nacionais do inquérito eu Kids online. Disponível em: https://www.academia.edu/10612494/a_cultura_do_quarto_e_o_uso_excessivo_da_internet_resultados_nacionais_do_inqu%3%89rito_eu_kids_online. Acesso em: 17 out. 2021.

CASTELLS, Manuel. A Sociedade em Rede. Tradução Roneide Venancio Majer. 22ª edição. Rio de Janeiro – São Paulo: Paz & Terra, 2020.

COPPA. Protecting Children's Privacy Under (COPPA): A Survey on Compliance. Federal Trade Commission - April 2002. In: COPPA Children's Online Privacy Protection Act. Federal Trade Commission. Disponível em: <https://www.ftc.gov/>. Acesso em: 17 out. 2021.

HENRIQUES, Isabella; PITA, Marina; HARTUNG, Pedro. A Proteção de Dados Pessoais de Crianças e Adolescentes. Tratado de Proteção de Dados Pessoais. Coordenadores Danilo Doneda et al. 2. Reimpressão. Rio de Janeiro: Forense, 2021, p. 199-225.

JONAS, Hans. O princípio responsabilidade: ensaio de uma ética para a civilização tecnológica. Tradução Marijane Lisboa, Luiz Barros Montez. Rio de Janeiro: Contraponto, Ed. PUC-Rio, 2006.

LIMA, Caio César Carvalho. Cookies e proteção de dados: análise teórica e prática para os setores público e privado. In: Denise de Souza Luiz Francoski; Fernando Antonio Tasso. A Lei Geral de Proteção de Dados Pessoais: aspectos práticos e teóricos relevantes no setor público e privado. p. 491-538. MONTANARO, Domingo. Gest. de Vulnerabilidades. Viviane Nóbrega Maldonado (coordenação). Lei Geral de Proteção de Dados Pessoais: manual de implementação. São Paulo: Thomson Reuters Brasil, 2019, p. 313-338.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 2ª. tiragem. São Paulo: Saraiva, 2019.

OIT – Organização Internacional do Trabalho: Observatório da Prevenção e da Erradicação do Trabalho Infantil – Proteção Integral guiada por dados. Disponível em: <https://smartlabbr.org/trabalhoinfantil/>. Acesso em: 18 out. 2021.

ROSLING, Hans; ROSLING Ola; e RÖNNLUND, ANNA Rosling. Fact Ful-

ness: o hábito libertador de só ter opiniões baseadas em fatos. Tradução de Vitor Paolozzi. 1ª. ed. Rio de Janeiro: Record, 2019.

RÝCKER, Josiane. Da “cultura do quarto fechado” para a vida das crianças e dos adolescentes?. Disponível em: <https://minhaslcoes.com.br/pucrs-inverno-2018/>. Acesso em: 18 out. 2021.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. Marco Civil da Internet: construção e aplicação. Juiz de Fora: Editar Editora Associada Ltda., 2016. p. 16.

STF. Ação Direta de Inconstitucionalidade 3.446 - DF. Disponível em: <http://portal.stf.jus.br/processos/downloadPeca.asp?id=15343882020&ext=.pdf>. Acesso em: 23 out. 2021a.

STF. Recurso Ordinário em MS 26071-1 DF. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=506599>. Acesso em: 23 out. 2021b.

UNICEF. The State of the World ‘s Children 2017 – Children in a digital world. Unicef, 2017. Disponível em: <https://www.unicef.org/bulgaria/media/421/file/State%20of%20the%20world's%20children%20-%20children%20in%20a%20digital%20age.pdf>. Acesso em: 15 out. 2021.

UNICEF. Pobreza na Infância e na Adolescência. Disponível em: https://www.unicef.org/brazil/media/156/file/Pobreza_na_Infancia_e_na_Adolescencia.pdf. Acesso em: 22 out. 2021.

VERONESE, Josiane Rose Petry. Estatuto da Criança e do Adolescente – 30 anos – entre avanços e omissões. In: Estatuto da Criança e do Adolescente – 30 anos: grandes temas, grandes desafios. Rio de Janeiro: Lumen Juris, 2020, p. 11-22.

WILEMIN, Andrea. Aspectos importantes e diferenciados entre a GPDR e a LGPD. In: Denise de Souza Luiz Francoski; Fernando Antonio Tasso. A Lei Geral de Proteção de Dados Pessoais: aspectos práticos e teóricos relevantes no setor público e privado. p. 571-587.

15. AMBIENTE DIGITAL E A PROTEÇÃO DOS DADOS PESSOAIS DA CRIANÇA E DO ADOLESCENTE

IVANI CONTINI BRAMANTE¹

Resumo

A Carta Federal traz o princípio da proteção integral da criança e do adolescente a cargo do Estado e de toda sociedade. A Lei 13.709/18 (LGPD), em seu artigo 14, traz as regras relativas ao tratamento de dados pessoais das crianças e adolescentes e comanda a aplicação do princípio do melhor interesses e da legislação pertinente. A questão radica em saber o alcance, a profundidade e extensão da proteção legal dos dados pessoais da criança e do adolescente, bem como as respectivas responsabilidades dos agentes de tratamento dos dados pessoais e também dos pais no exercício do dever-poder parental. Em se tratando dos pequenos e incapazes titulares de dados pessoais, o desiderato do artigo 14 da LGPD vem no sentido do equilíbrio, de um lado, assegurar o livre desenvolvimento da sua personalidade no ambiente digital, e de outro, a proteção verificável em cada condição ostentada pela criança e pelo adolescente como: (i) usuário da Internet e das mídias sociais; (ii) trabalhador e ou empregado; (iii) dependente dos pais para fins dos direitos individuais, políticos, econômicos, sociais e culturais. Portanto, mister se faz desvendar, no diálogo das fontes normativas, o alcance e conteúdo do comando de integração legislativa protetiva, pertinentes à tutela da criança e do adolescente, bem como os diversos níveis de responsabilidades.

Palavras-Chave: Proteção à criança. LGPD.

Abstract

The Constitution brings the principle of full protection of children and adolescents and a position of the State and of the entire Society. Law 13.709/18 (LGPD), in its article 14, brings the rules relating to the processing of personal data of children and adolescents and commands the application of the principle of best interests and the relevant legislation. The issue is to know the scope, depth and extent of the legal protection of the personal data of children and adolescents, as well as the respective responsibilities of the personal data processing agents, as well as of the parents in the exercise of parental duty-power. In the case of small and incapable holders of personal data, the aim of article 14, of the LGPD, comes in the sense of balance, on the one hand, to ensure the free development of their personality in the digital environment; and on the other, verifiable protection in each condition displayed by children and adolescents as: (i) Internet and social media users; (ii) worker and/or employee; (iii) dependent on the parents for the purposes of individual, political, economic, social and

¹ Desembargadora federal do Trabalho. Professora da Faculdade de Direito de São Bernardo do Campo. Doutora pela PUC/SP. Especialista em Relações Coletivas Comparadas pela OIT/Torino/Itália.

cultural rights Therefore, it is necessary to unveil, in the dialogue of normative sources, the scope and content of the protective legislative integration command, relevant to the protection of the child and the adolescent, as well as the different levels of responsibilities.

Keywords: Child protection. LGPD,

1. Introdução: A era digital e os riscos ao desenvolvimento da personalidade da geração centennials

As novas tecnologias da era digital trazem inúmeros benefícios do novo mundo de conectividade em massa e transnacional. De outro lado, potencializam os riscos e as nocividades para as crianças e os adolescentes no desenvolvimento da personalidade, a chamada geração “Z” ou “Centennial”, nascida nos idos 1997, que só conhecem o ambiente virtual como meio socializador.

A comunidade online de crianças e adolescentes, sabidamente vulnerável, sofre uma exposição silenciosa midiática que escapa à fiscalização dos responsáveis legais, pois os seus dados pessoais são coletados, compartilhados e armazenados, para além do conhecido vazamento e uso ilegal. A criança e o adolescente não possuem maturidade, autonomia e capacidade de controle, nas telas das parafernalias telemáticas, do tempo dispendido e tampouco do conteúdo acessado.

Estudos revelam que o uso da Internet, sem filtro, influencia negativamente no desenvolvimento biopsicossocial da criança e do adolescente, exemplificando: desestímulos de outras diversões ou atividades ao ar livre, interação com a família, amigos, passeios; queda do rendimento escolar, maior dificuldade para dormir, prejuízo da criatividade, dores musculares posturais, aumento de peso pela falta de atividades físicas, irritação nos olhos, dependência, compulsão, ansiedade, danos cerebrais, sem contar os danos na desproteção dos dados pessoais sensíveis.

Em boa hora vem a lume a Lei 13.079/18, cujo objeto é a proteção de dados pessoais da pessoa natural, incluídas a criança e o adolescente, notadamente vulneráveis, que conclama novas reflexões e cuidados.

2 Normativas de proteção de dados pessoais da criança e do adolescente

2.1 A identificação da integração da legislação pertinente para desvendar da maioridade digital. Teoria das incapacidades e maioridade digital brasileira.

O artigo 1º, da Convenção das Nações Unidas sobre os Direitos da Criança (Resolução 44/25 de 20 de novembro de 1989), estabelece que criança é todo o ser humano menor de 18 anos, salvo se, nos termos da lei que lhe for aplicável, atingir a maioridade mais cedo.

A Lei 13.709/18 (LGPD) traz as seguinte diretrizes:

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

Registem-se as inúmeras críticas ao texto da LGPD (Lei 13.709/18), chegando a ser cunhada de lei da “desproteção”, pois, à primeira vista, parece que traz uma maioria digital aos 13 anos, porque exige para a criança e dispensa para o adolescente o consentimento dos pais ou responsáveis legais.

Assim, surge a questão de alta indagação jurídica e muitos debates dizem respeito à maioria digital. Uma corrente defende a aplicação do Código Civil, em que a personalidade encontra maturidade aos 18 anos; outros indicam a idade de 16 anos, com base na legislação aplicável a criança e adolescente; outra aponta que a maioria digital se dá aos 13 anos, com base na legislação estrangeira.

Em uma leitura apressada, vê-se que o caput do artigo 14 comanda princípio do melhor interesse para a criança (ECA, art.2º- até 12 anos) e adolescentes, mas de forma contraditória, nos demais parágrafos, omite a figura do adolescente (ECA, art. 2ª - acima de 13 anos), pois faz referência ao consentimento dos pais somente para a criança.

A leitura da Lei 13.709/18, artigo 14 e seus parágrafos, não pode ser interpretada de modo isolado, mas no contexto da compatibilidade constitucional, da legislação internacional e nacional protetiva da criança e adolescente, bem assim, com o corpo unitário da lei que traz os princípios gerais do respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

No Brasil, em geral, há uma preocupação crescente na proteção da criança, com a adoção do princípio constitucional da proteção integral.

Ainda, o artigo 227 da CF/88 e o artigo 4º do ECA asseguram o direito à liberdade e a convivência familiar e comunitária, significando que a criança e o adolescente não poderão ser afastados do ambiente virtual, que faz parte do seu desenvolvimento, sob pena da sua exclusão desse grupo social.

Por tal motivo, a Lei 13.709/18 adotou o princípio holístico, da integridade do Direito, ao comandar que no tratamento de dados pessoais sejam aplicadas as legislações específicas e pertinentes à proteção do menor. Assim, devem ser observadas as medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal e os princípios gerais de proteção dos direitos dos titulares menores de idade, inseridos na ordem jurídica nacional e internacional, pois a Carta Federal não exclui outros princípios compatíveis com seu texto (art. 5º, § 2º, CF/88).

Desta feita, é possível traçar os limites dos poderes estabelecidos e contratuais, fundados nos princípios da dignidade da pessoa humana e valor social do trabalho, incluídos os direitos à vida, saúde, de personalidade, de intimidade e vida privada, não discriminação, que se apresentam como limites dos limites, e que demarcam a função econômica-sócio-ambiental-consumerista-tecnológica-informacional da empresa e a função social do contrato (artigos 1º, III e IV; 5º, caput e inciso X, incisos XXII e XXIII; 170, caput e incisos III, IV, V, VI; 218, 219,CF/88).

2.2 Teoria das incapacidades e maioridade digital brasileira

Nos EUA, o título 16, parte 312.2 da COPPA (Children's Online Privacy Protection Act, de 1998), traz diretriz de que: criança significa um indivíduo com menos de 13 anos e há proibição de atos ou práticas desleais ou enganosas em conexão com a coleta, uso e ou divulgação de informações pessoais das crianças na Internet.

A General Data Protection Regulation – GDPR (art.8º e n. 2º) estabelece que apenas será lícito tratar dados pessoais de uma criança, sem consentimento dos pais ou responsáveis, se ela tiver, ao menos, 16 anos. Entrementes, autoriza os Estados Membros da União Europeia a estabelecer uma idade inferior a 16 anos, sem autorização do responsável legal específica, desde que essa idade inferior não seja inferior a 13 anos.

No Brasil, vigoram regras diferentes quanto à maioridade digital, diante da teoria das incapacidades e vulnerabilidades, e o princípio da proteção integral da criança e adolescente, adotados pela Carta Federal, artigo 227, no Estatuto da Criança e Adolescente - ECA (Lei 8069/90), no Estatuto do Jovem (Lei 12.852/13), no Marco Civil da Internet (Lei 12.965/20) e no Código Civil (arts. 2º e 3º, 11 a 21 e 1634 a 1638).

Diferentemente dos Estado Unidos e da Europa, no Brasil o sistema de capacidade civil em geral vem estruturado no Código Civil (artigos 3º e 4º) e estabelece que a pessoa até 16 anos é incapaz; entre 16 e 18 anos, a capacidade é relativa; a partir de 18 anos, a capacidade é absoluta.

O Estatuto da Criança e Adolescente (ECA, Lei 8.069/90) traz os princípios da proteção integral e da preferência tutelar à criança e ao adolescente. Considera-se criança a pessoa até (12) doze anos de idade incompletos, e adolescente aquela entre (12) doze e (18) dezoito anos de idade. Nos casos expressos em lei, aplica-se excepcionalmente este Estatuto às pessoas entre (18) dezoito e (21) vinte e um anos de idade (art. 2º e § único).

A criança e o adolescente gozam de todos os direitos fundamentais inerentes à pessoa humana, sem prejuízo da proteção integral. Assim, são assegurados por lei ou por outros meios todas as oportunidades e facilidades, a fim de lhes facultar o desenvolvimento físico, mental, moral, espiritual e social, em condições de liberdade e de dignidade.

Os direitos aplicam-se a todas as crianças e adolescentes, sem discriminação de nascimento, situação familiar, idade, sexo, raça, etnia ou cor, religião ou crença, deficiência, condição pessoal de desenvolvimento e aprendizagem, condição econômica, ambiente social, região e local de moradia ou outra condição que diferencie as pessoas, as famílias ou a comunidade em que vivem (art. 3º, e § único, ECA).

A Lei 12.852/13, Estatuto da Juventude, traz a regra de que são consideradas jovens as pessoas com idade entre 15 (quinze) e 29 (vinte e nove) anos de idade (art.1º). Ainda deixa claro que aos adolescentes com idade entre 15 (quinze) e 18 (dezoito) anos aplica-se a Lei nº 8.069/90, do Estatuto da Criança e do Adolescente, e de forma excepcional o Estatuto da Juventude, quando não conflitar com as normas de proteção integral do adolescente (art. 1º § 2º).

No Brasil, em matéria de proteção de dados pessoais, uma vez identificada a

integração da legislação pertinente de proteção da criança e adolescente, é factível desvendar da maioridade relativa digital aos 16 anos, e a maioridade absoluta aos 18 anos. Assim, os maiores de 18 anos poderiam fornecer consentimento válido sem representação parental.

A conclusão para correta interpretação vem no sentido de que o artigo 14, caput, da LGPD comanda a aplicação integrada “da legislação pertinente à proteção da criança e do adolescente”.

Portanto, não se trata de uma “omissão eloquente da figura do adolescente”, mas a remissão legal ao diálogo das fontes, e aplicação integrada pelos ditames do princípio da proteção integral da criança e adolescente, enraizados na Carta Federal (art. 227), no ECA (Lei 8069/90), no Estatuto do Jovem (Lei 12.852/13), no Marco Civil da Internet (Lei 12.965/20) e no Código Civil (arts. 2º e 3º, 11 a 21 e 1634 a 1638).

E na técnica do diálogo das fontes, de integração da legislação protetiva geral da criança e adolescente na proteção de dados pessoais pela aplicação do princípio do melhor interesse, resulta a interpretação de que: (i) para as crianças a lei reservou uma maior proteção e devem ser observados o princípio do melhor interesse e a integração da “legislação pertinente de proteção à criança”; ainda do consentimento “extraordinário” específico, destacado, livre e inequívoco do responsável legal; (ii) para o adolescente devem ser observados o princípio do melhor interesse e a integração da “legislação pertinente de proteção ao adolescente” que exige “um consentimento ordinário”.

2.3 Compatibilização das regras de identidade e consentimento digital com as normas contatuais e negócios jurídicos

Na era digital surge a seguinte questão: navegar na Internet e fornecer dados pessoais, conectados com o direito fundamental constitucional da proteção da privacidade e intimidade, é um ato da vida civil? É um negócio jurídico?

Hodiernamente, surge uma nova “teoria das incapacidades na Internet” que sopesa como assegurar a prática de atos da vida civil, a inserção social dos vulneráveis, menores de idade, deficientes, idosos, curatelados no contexto global da era digital. Ainda, e concomitante, como efetivar o livre desenvolvimento da sua personalidade e também permitir de forma segura o tratamento de dados pessoais, de acordo com a vontade inerente à sua idade, capacidade e discernimento.

No âmbito da LGPD, as orientações não abordam a questão de saber se é lícito ao menor ou ao incapaz celebrar contratos. Entretanto, a lei determina a aplicação “da legislação pertinente” aos requisitos de autorização parental em relação a menores. Portanto, a Lei 13.709/18 não interfere no direito contratual e/ou na teoria das incapacidades. De modo que permanecem hígidas as disposições que regulam a validade, a formação ou os efeitos dos contratos em relação ao menor de idade e a harmonização das disposições nacionais de direito contratual, pois os regimes jurídicos podem ser aplicados simultaneamente.

No Brasil, a LGPD traz os requisitos para obtenção do consentimento válido para a utilização de dados acerca de criança e adolescente e faz parte de um quadro jurídico de integração da legislação pertinente da proteção da criança e adolescente (art. 14, LGPD).

3. O consentimento parental extraordinário para a criança e o consentimento parental ordinário para o adolescente. Hipóteses de dispensa do consentimento parental no tratamento de dados da criança. Vedação e permissão para compartilhamento

O cumprimento da Lei 13.709/18 (LGPD) deve ser integrado com as demais legislações protetivas pertinentes à tutela da criança e do adolescente (art. 14, LGPD). Para perquirir a legislação pertinente aplicável, uma conduta correta será verificar qual condição ostenta a criança e o adolescente: (i) usuário da Internet e das mídias sociais; (ii) ou trabalhador e/ou empregado; (iii) ou dependente dos pais para fins de benefícios sociais etc.

A Lei 13.709/18 (LGPD), em seu artigo 14, comanda genericamente o tratamento de dados da criança e do adolescente, seu melhor interesse, e manda aplicar a legislação pertinente em todos os seus termos. Deste modo, o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal, e sendo adolescente misteres faz um consentimento ordinário na forma do ECA e Estatuto do Jovem, sem descuidar das regras da capacidade previstas no Código Civil.

Destarte, é possível afirmar, com segurança, que no tratamento de dados pessoais da criança e do adolescente exige-se um consentimento parental extraordinário para a criança e um consentimento parental ordinário para o adolescente.

Quanto às hipóteses de dispensa do consentimento parental e vedação e permissão para compartilhamento, o artigo 14, § 3º, da LGPD autoriza a coleta de dados pessoais da criança, sem o consentimento, para a finalidade e necessidade de contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento; ou para sua proteção.

Há apenas três hipóteses de dispensa do consentimento parental, em relação ao tratamento dos dados do menor de idade, ditadas pela lei: (i) prevista no artigo 14, § 3º, LGPD, para proteção da criança; (ii) prevista no artigo 14, § 3º, LGPD, quando a coleta do dado for necessária para contatar os pais ou responsáveis. Ainda assim, a lei deixa claro que, na primeira hipótese, há uma política de descarte imediato, o dado coletado poderá ser utilizado apenas 1 (uma) vez e não poderá ser armazenado pelo controlador; (iii) prevista de modo geral, no artigo 11, alíneas “e” e “f”, da LGPD, quanto aos dados sensíveis, para proteção à vida ou tutela da saúde incluída a figura do menor de idade.

Embora a dicção do artigo 14, § 3º, da LGPD estabeleça que os dados da criança em nenhum caso poderão ser repassados a terceiros sem o consentimento, é defensável a excepcionalidade do compartilhamento de dados de crianças, na hipótese da proteção relativa à vida e saúde, prevista no artigo 11, letra “e” e “f”, LGPD, para fins de atendimento médico e exames laboratoriais, sob pena de desproteção.

A declaração de consentimento deve ser livre, de forma escrita, clara, objetiva, indicar o seu alcance de forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas. Haverá vício do consentimento se a escolha não é verdadeira ou livre, ou se o titular não puder recusar nem retirar o consentimento sem ser prejudicado.

4. Teoria do consentimento qualificado

4.1 Os riscos da utilização isolada do consentimento como base legal na relação trabalhista

Sabe-se que na relação trabalhista, com a pessoa maior de idade, há uma relação de subordinação e que há possibilidade da revogação do consentimento a qualquer tempo.

A questão mais se complica quando se trata de menor de idade. Considera-se menor para os efeitos trabalhistas o trabalhador de 14 até 18 anos. As regras que tratam da idade mínima para ingressar no mercado de trabalho, bem como os cuidados que devem ser observados ao contratar o menor, se conectam com a compatibilização com a educação e escolaridade fundamental.

Há normas internacionais ratificadas que compõem o nosso ordenamento jurídico a respeito do trabalho da criança e adolescente. Por exemplo, a Convenção n.º 138, da OIT, que trata sobre a Idade Mínima de Admissão ao Emprego, e a Recomendação n.º 146 da OIT. Ainda, a Convenção 182, que trata das piores formas de trabalho infantil, ratificada através do Decreto n.º 3.597/ 2000.

O trabalho artístico do menor exige não só a autorização dos pais, mas também que autoridade judiciária competente conceda alvará judicial com permissão para que crianças e adolescentes participem de espetáculos públicos (art. 149, II do ECA).

As condições de trabalho do aprendiz, maior de 14 (quatorze) e menor de 24 (vinte e quatro) anos estão definidas e delimitadas no art. 62 do ECA, e no artigo 428 da CLT, que exigem a inscrição em programa de aprendizagem e formação técnico-profissional metódica, compatível com seu desenvolvimento físico, moral e psicológico. A idade máxima de 24 anos não se aplica a aprendizes portadores de deficiência (art. 428, § 5º, CLT).

4.2 Consentimento parental obrigatório no tratamento de dados da criança e do adolescente para fins de trabalho

É factível o tratamento de dados pessoais da criança e adolescente para fins de: (i) contratação do trabalho do menor para o trabalho artístico; trabalho do aprendiz; trabalho do estagiário; e trabalho como empregado (art. 3º, CLT); (ii) e para fins de dependência dos seus pais na declaração do imposto sobre a renda e para fins de gozo de benefícios previdenciários, planos de saúde e benefícios sociais.

Nos termos do artigo 14 da LGPD, o consentimento dos pais é obrigatório no tratamento de dados em geral, o que inclui para fins de relação de trabalho do menor de idade. As empresas que possuem colaboradores menores de idade precisam dar atenção especial no tratamento dos dados pessoais, que deverá ser realizado com base no seu melhor interesse e, mediante o consentimento obrigatório, específico e em destaque, dado por pelo menos um dos pais ou representante legal. Registre-se que os riscos são potenciados, relacionados ao termo “livre consentimento”, que pressupõe além da ausência de desequilíbrio entre as partes aliado ao quesito idade.

A contratação, bem como a rescisão contratual de trabalhador com idade inferior a 18 anos, deve ser realizada mediante a aplicação de procedimentos específicos, conforme prevê a legislação trabalhista, pois é obrigatória a presença e a

assinatura de seu representante legal na contratação e no termo de homologação, exceto para os emancipados nos termos da lei civil.

Em suma, na contratação e na rescisão trabalhista do menor:

- (i) é mister obter o consentimento do poder familiar (art. 14, LGPD);
- (ii) o consentimento deve ser fornecido “por escrito ou por outro meio que demonstre a manifestação de vontade do titular”, e caso seja fornecido por escrito, deve “constar de cláusula destacada das demais cláusulas contratuais” (art. 8º, caput e § 1º, da LGPD);
- (iii) ao responsável legal do menor é facultado pleitear a extinção do contrato de trabalho, desde que o serviço possa acarretar-lhe prejuízos de ordem física ou moral (art. 408, CLT);
- (iv) a retenção e descarte dos dados pessoais da criança deve ter em conta que a prescrição não corre contra os menores de 18 anos, tendo início apenas com o advento da maioridade (arts. 2º e 3º, CC, e 440, da CLT).
- (v) registrem-se as hipóteses de dispensa do consentimento: para fins de proteção da criança e para localização dos pais, caso em que os dados devem ser utilizados uma única vez, sendo vedado o compartilhamento com terceiros; e portanto o descarte dos dados deve ser imediato (art. 14, § 3º, LGPD).

5. Responsabilidades do poder parental: fiscalização digital e abandono digital

Na forma dos arts. 1.630 a 1.638 do Código Civil, os filhos estão sujeitos ao poder familiar, conjunto de deveres e obrigações dos pais em relação aos filhos menores não emancipados e aos bens destes, decorrentes da relação de parentesco existente entre eles, visando ao bom desenvolvimento, ao bem-estar e à proteção dos filhos².

No contexto da era digital, surge o dever parental de fiscalização digital dos filhos menores, sob pena de configuração de negligência e/ou abandono digital e perda do poder parental (art. 1.638, CC). Portanto, cumpre aos pais cuidar do desenvolvimento da personalidade dos filhos menores de idade, incluída a proteção e segurança da privacidade e intimidade e dos dados pessoais da criança e do adolescente, e ainda evitar que os filhos sejam agentes de práticas ilegais na Internet.

6. Responsabilidade dos agentes de tratamento de dados pessoais da criança e adolescente

6.1 Dever de precaução

No Brasil, a maioria digital é tratada de modo diferente em cotejo com os Estados Unidos e a Europa. Entretanto, como norte de interpretação da Lei 13.079/18 (LGPD), acerca do procedimento da coleta do consentimento para o tratamento de dados pessoais da criança e adolescente, é recomendável a adoção das diretrizes da General Data Protection Regulation (GDPR), os artigos 8.º, n.º 2, com 5.º, n.º 1, alínea “c” e ainda as diretrizes do título 16, parte 312.2 e 312.5, da Children’s Online Privacy Protection Act, de 1998 - COPPA.

Os artigos 5º, inciso XII e 14, § 5º, da LGPD, estatuem que o controlador deve

2 CARVALHO FILHO, Milton Paulo de. Comentário ao art. 1.630. In: PELUSO, Cezar (coord.). **Código Civil comentado: doutrina e jurisprudência**. 5 ed. Barueri, SP: Manole, 2011. p. 1837.

realizar todos os esforços razoáveis para verificar que o consentimento foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis. Ainda, entram em cena os princípios da transparência, do livre acesso às informações sobre os detalhes do tratamento de dados, de maneira “simples, clara e acessível” ao usuário, principal tutelado, de acordo com as características da criança, bem como aos seus responsáveis legais.

6.2 Dever de minimização de dados (data minimization)

O artigo 14, § 4º, da LGPD estabelece que os controladores não deverão condicionar a participação dos titulares criança e adolescentes em jogos, aplicações de Internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade. Constitui um dever do agente de tratamento de dados observar a “data minimization”, porque não deve conduzir a um tratamento de dados excessivos.

A lei se preocupa com a interação entre criança e os jogos de Internet e comanda a aplicação do princípio da finalidade e adequação. Logo, não poderão exigir os dados pessoais da criança além daqueles estritamente necessários para a participação em jogos ou outras atividades.

Há consonância com a Resolução nº 163/2014 do Conselho dos Direitos da Criança e do Adolescente (CONANDA), que determina “ser considerado abusivo o direcionamento de publicidade à criança com intenção de persuadi-la para o consumo de qualquer produto ou serviço”.

6.3 Dever de categorização dos riscos

O dever de precaução do controlador atrai as medidas procedimentais válidas de categorização dos riscos: (i) de verificação da idade do titular dos dados; (ii) de obtenção do consentimento parental; (iii) de modo proporcional à natureza e aos riscos das atividades de tratamento, e à luz da tecnologia disponível.

No caso de baixo risco, pode ser adequado exigir que o novo subscritor do serviço revele o seu ano de nascimento ou preencha um formulário onde declara (não) ser menor e verificar se a responsabilidade parental por correio eletrônico pode ser suficiente. No caso de alto risco, pode ser adequado solicitar mais provas, para que o responsável pelo tratamento possa verificar e conservar as informações. Na dúvida, deve-se considerar que são necessárias maiores verificações e busca de outras alternativas.

6.4 Dever de informação no tratamento dos dados da criança e adolescentes

No tratamento dos dados pessoais da criança, o art. 14, § 2º, da LGPD, estabelece que os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 da lei.

Em suma, o artigo 5º, inciso XII, da Lei 13.079/18 (LGPD) impõe a obrigação do controlador do dados de manter a publicidade das informações sobre os dados coletados e empregar todos os esforços razoáveis para conferir se o consentimento foi dado realmente pelo responsável do menores de idade em geral.

7. Responsabilidades dos pais e da sociedade

O artigo 227 da Constituição Federal comanda o conjunto mínimo de deveres cometidos à família, a fortiori ao poder familiar, em benefício do filho, enquanto

criança e adolescente, a saber: o direito à vida, à saúde, à alimentação (sustento), à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar. São deveres jurídicos corresponsáveis a direitos cujo titular é o filho.³ Por isso, o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos da legislação pertinente (art. 14, LGPD).

Logo, o tratamento de dados pessoais da criança e do adolescente tem como condição *sine qua non* o consentimento prévio dos pais ou responsáveis, seja um consentimento extraordinário específico e destacado para a criança, seja um consentimento ordinário e genérico para adolescente, e sempre sujeito a confirmação.

Sinalize-se que pode ser dispensado o consentimento parental prévio somente no contexto de serviços de prevenção ou aconselhamento oferecidos diretamente a uma criança e de proteção do interesse, vida, saúde, segurança da criança (art. 11, letra “e” e “f” e art. 14, §3º, LGPD).

A educação digital é uma obrigação dos pais e um desafio do poder parental frente às novas tecnologias. Há, por assim dizer, um dever-poder dos pais, de fiscalização digital dos filhos, para evitar a invasão da privacidade dos filhos, sob pena de configurar a negligência digital. A expressão “abandono digital” foi criada por Patrícia Peck Pinheiro para ilustrar a negligência dos pais com relação à segurança dos filhos no ambiente virtual.

Na hipótese da configuração da conduta faltosa do pai ou da mãe, no que tange à proteção de dados pessoais dos menores, justifica decretação da perda do poder familiar (arts. 1.638 do CC, e 24 c/c 22 do ECA), cuja natureza é bifronte porque configura mais uma proteção aos filhos menores do que uma medida punitiva.

Num cenário ainda mais abrangente, cumpre ao poder público e à sociedade auxiliarem neste papel nas escolas, campanhas públicas etc.

Quando o tratamento de dados pessoais da criança se dá na condição de usuário, surgem os deveres e responsabilidades dos agentes de tratamento de dados, bem como dos pais, no exercício do poder parental. Ainda, se faz necessária a atuação dos organismos nacionais competentes.

Conclusão

As crianças merecem proteção especial quanto aos seus dados pessoais, diante da falta de maturidade e vulnerabilidade.

No Brasil, considera-se criança a pessoa até (12) doze anos de idade incompletos, e adolescente aquela entre (12) doze e (18) dezoito anos de idade, e jovem idade entre 15 (quinze) e 29 (vinte e nove) anos de idade.

Por isso, é possível concluir que a Lei 13.709/18 exige um consentimento parental extraordinário para a criança e um consentimento parental ordinário para o adolescente (art. 14, caput e § 1º, LGPD; artigo 3º e 4º, arts. 1630/1638, CC).

No tratamento de dados da criança e do adolescente é mister verificar qual condição ostenta a criança e adolescente: (i) usuário da Internet e das mídias sociais; (ii) ou trabalhador e/ou empregado; (iii) ou dependente dos pais para fins

3 LÔBO, Paulo. Do poder familiar. *Revista Jus Navigandi*, Teresina, ano 11, n. 1057, 24 maio 2006. Disponível em: <http://jus.com.br/artigos/8371>. Acesso em: 20 ago. 2021.

de benefícios sociais etc. Em qualquer relação, há obrigação de cumprimento da LGPD integrada com as demais legislações protetivas, pertinentes à tutela da criança em cada área (art. 14, LGPD).

O responsável pelo tratamento deve envidar todos os esforços adequados para verificar que o consentimento foi dado ou autorizado pelo titular das responsabilidades parentais da criança, tendo em conta a tecnologia disponível, e manter públicas as informações sobre os dados coletados (art. 5º, inciso XII e 14, § 5º, da LGPD).

Dentre os vários deveres ao controlador temos: dever de precaução; dever de busca da certeza do consentimento parental; dever de obtenção da confirmação da idade e do consentimento parental; dever de categorização dos riscos; dever de informação; dever de minimalização dos dados. A lei abomina o tratamento excessivo de dados, e comanda a aplicação do princípio da minimização (artigo, 14 § 4º, da LGPD). Deste modo, é abusivo o direcionamento de publicidade à criança com intenção de persuadi-la para o consumo de qualquer produto ou serviço.

No âmbito do poder parental, registre-se o desafio de buscar um equilíbrio entre a autonomia do menor e o dever de fiscalização digital dos filhos, sem invasão da privacidade e sem incorrer em uma negligência digital (arts.1.638 do CC).

O consentimento dos pais é obrigatório no tratamento de dados pessoais do menor de idade para fins de: (i) contratação do trabalho do menor para o trabalho artístico; trabalho do aprendiz; trabalho do estagiário; e trabalho como empregado (art. 3º, CLT); (ii) para fins de dependência dos seus pais na declaração do imposto sobre a renda e para fins de gozo de benefícios previdenciários, bem como planos de saúde e defesa de direitos perante o Judiciário; (iii) é mister obter o consentimento do poder familiar de forma livre, informado e específico e inequívoco, pela qual o titular concorda com o tratamento de seus dados pessoais do menor e para uma finalidade determinada (art. 5º, XII, e 14, LGPD); o consentimento deve ser fornecido “por escrito ou por outro meio que demonstre a manifestação de vontade do titular”, e caso seja fornecido por escrito deve “constar de cláusula destacada das demais cláusulas contratuais” (art. 8º, caput e § 1º, da LGPD); (iv) a retenção e descarte dos dados pessoais da criança deve ter em conta que a prescrição não corre contra os menores de 18 anos, tendo início apenas com o advento da maioridade (artigo 440, da CLT).

Registrem-se apenas três hipóteses de dispensa do consentimento parental para tratamento dos dados do menor de idade: proteção em geral da criança; dificuldade para contatar os pais ou responsáveis e para proteção à vida ou tutela da saúde (art. 11, alíneas “e” e “f” e art. 14, 3º, LGPD).

Mister se faz a colaboração dos pais, responsáveis legais, e organismos nacionais competentes, tais como o Poder Executivo, a ANPD (Autoridade Nacional de Proteção de Dados), Ministério Público, Defensoria Pública e demais órgãos de defesa da criança, adolescentes, jovens e sindicatos na defesa dos interesses da criança e adolescente.

Cabe a propositura das ações individuais ou coletivas, sempre que necessárias, em defesa dos direitos e interesses de menores e incapazes, decorrentes das relações de trabalho, bem como na proteção de dados pessoais como usuário (art. 8º, III, CF/88; art. 127/129, CF/88; LC 75/93; Lei 7347/85 arts.1.638 do CC, e 24; art.

22, ECA e art. 22 da Lei 13;709/18).

Nada obsta, tudo recomenda e urge que a Autoridade Nacional de Proteção de Dados (ANPD) traga diretrizes acerca do tema, com indicação de procedimentos de prevenção e precaução, para cumprimento de uma Política das Boas Práticas no Tratamento de Dados da Criança e Adolescente.

16. RESPONSABILIDADE CIVIL NA LGPD

CIVIL RESPONSIBILITY IN THE LGPD

LARA ISABEL MARCON SANTOS¹

Resumo

Este estudo tem por objetivo analisar a responsabilidade civil de agentes de tratamento de dados pessoais instituída pela LGPD (Lei 13.709/18), bem como as hipóteses de exclusão da responsabilidade, bem como seus reflexos no ordenamento jurídico pátrio. Serão abordadas questões relacionadas aos aspectos relativos ao direito do trabalho nas fases pré-contratual, execução do contrato e término da relação jurídica.

Palavras-Chave: LGPD. Dados pessoais. Responsabilidade civil. Relações de trabalho.

Abstract

This study aims to analyze the civil liability of personal data processing agents established by the LGPD (Law 13.709/18), as well as the hypotheses of exclusion of liability, as well as its consequences in the national legal system. Issues related to labor law aspects related to the pre-contractual phases, contract execution and termination of the legal relationship will be addressed.

Keywords: LGPD. Personal data. Civil responsibility. Work relationships.

1 INTRODUÇÃO

O presente trabalho tem como objetivo analisar a responsabilidade civil no que se refere à proteção de dados pessoais nas relações de trabalho, através da inserção da Lei 13.709/18, também denominada Lei Geral de Proteção de Dados (LGPD).

Numa visão geral, esta norma foi editada para regulamentar as relações estabelecidas entre os titulares e os controladores e operadores dos dados, com objetivo claro de proteger dados de pessoas naturais frente ao grande avanço tecnológico, de modo a instituir um órgão administrativo, a Agência Nacional de Proteção de Dados, para regulamentar e fiscalizar as relações jurídicas que se enquadram neste contexto.

A questão levantada no presente artigo refere-se a um dos mais relevantes debates atuais em torno da Lei Geral de Proteção de Dados – LGPD, ou seja, seria objetiva ou subjetiva a responsabilidade civil dos agentes de tratamento de dados privados?

A lei não dispõe de modo claro sobre esta questão e há um grande debate doutrinário quanto à natureza da responsabilidade civil estabelecida na LGPD.

¹ Advogada. Especialista em Direito Humanos pela Universidade de Coimbra, Portugal. Especialista em Direito Processual Civil e em Direito do Trabalho pela ESA/SP. laramarconsantos@gmail.com

O risco de lesão a direitos no tráfego de dados pessoais é uma realidade que encontramos frequentemente noticiada nas mídias, evidenciando o vazamento de informações pessoais sensíveis.

Todas as atividades de tratamento de dados pessoais levadas a efeito pelo empregador, denominado pela norma como controlador, como a coleta, uso, armazenamento, compartilhamento e até a exclusão dos dados pessoais precisam estar de acordo com as normas da LGPD, sob pena de acarretar, entre outras penalidades, a responsabilização civil.

2. Breves considerações sobre a LGPD

A sociedade vive numa constante evolução em relação à tecnologia e ao mercado de dados, estas inovações estão cada vez mais presentes em nossos dias e têm importância significativa em nosso cotidiano. Não se vive mais sem a tecnologia digital.

De fato, as novas tecnologias deixam o homem em situação extremamente vulnerável, havendo necessidade de um posicionamento marcante e forte quanto à legislação com o objetivo de proteger os direitos da personalidade.

Por outras palavras, Ivani Contini Bramante (2021, p. 25) diz que:

(...) é factível a situação de vulnerabilidade do homem frente às novas tecnologias, assim, a busca da proteção da pessoa humana em todas as normas do ordenamento jurídico à vista do princípio da unidade-funcionalidade do Direito e da supremacia da Constituição ensancha o constante apelo às normas (princípios e regras) constitucionais, por conta da constitucionalização dos direitos civis e políticos.

A Constituição Federal, em seu artigo 218, dispõe que o Estado promoverá e incentivará o desenvolvimento científico, a pesquisa, a capacitação científica e tecnológica e a inovação.

Ainda traz à baila a regra que estabelece tratamento prioritário do Estado em relação à pesquisa científica básica e tecnológica, tudo com o objetivo de estabelecer o bem público e o progresso da ciência, tecnologia e inovação.

Em contraponto, a própria Constituição Federal, em seu artigo 3º, traça as diretrizes de uma sociedade justa, fraterna e solidária, sem discriminação ou desigualdades.

De fato, uma das intenções da lei é facilitar a ciência, a pesquisa e a inovação tecnológica, a atuação e o fluxo dos negócios das *startups*, máxime na seara do tratamento de dados; a outra intenção é compatibilizar e proteger os direitos civis e políticos, incluídos os direitos de personalidade frente às inovações tecnológicas (CALCINI, 2021, p. 95).

A Lei Geral de Proteção de Dados (LGPD - Lei n.º 13.709/2018) estabeleceu, pela primeira vez no ordenamento jurídico brasileiro, um conjunto de normas – regras e princípios – que regulamentam o tratamento de dados pessoais em todas as atividades e setores da economia.

O objetivo da Lei é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural². A lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado.

Dado pessoal corresponde à informação relacionada a pessoa natural identificada ou identificável (art. 5º, inciso I), e dado pessoal sensível são os dados pessoais sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

É certo que a Lei Geral de Proteção de Dados - Lei 13.708/18, é uma lei geral, cuja esfera na justiça do trabalho necessita de compatibilização com princípios já existentes que regem o direito do trabalho.

No direito do trabalho, nota-se que desde o processo seletivo para contratação de trabalhador até o armazenamento de dados pessoais daqueles que foram contratados e o término da relação de emprego surgem diversos fatos que necessitam da aplicabilidade das normas estabelecidas na LGPD.

A LGPD institui de modo principiológico a responsabilização e prestação de conta³, e, salvo exceções, o não cumprimento da norma de modo eficaz e contundente acarreta deveres quanto à responsabilidade civil.

Neste sentido, constata-se que:

Prever a responsabilização e a prestação de contas como princípio demonstra a intenção da Lei em alertar os controladores e os operadores de que são eles os responsáveis pelo fiel cumprimento de todas as exigências legais para garantir todos os objetivos, fundamentos e demais princípios nela estabelecidos. E não basta somente pretender cumprir a Lei, é necessário que as medidas adotadas para tal finalidade sejam comprovadamente eficazes. Ou seja, os agentes deverão, durante todo ciclo de vida de tratamento de dados sob sua responsabilidade, analisar a conformidade legal e implementar os procedimentos de proteção dos dados pessoais de acordo com a sua própria ponderação de riscos. (MALDONADO e BLUM, 2019, p.166-167).

Denota-se então o ônus do controlador, bem como daqueles que figuram como operadores, de responderem por seus atos na medida de suas ações e omissões.

2 Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

3 X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

3. Da responsabilidade civil na LGPD

Inicialmente destaca-se que a responsabilidade civil está regulamentada na Seção III do Capítulo VI da Lei Geral de Proteção de Dados – Lei 13.709/2018, nomeada de “Da Responsabilidade e do Ressarcimento de Danos”.

A doutrina brasileira tem, nesse primeiro momento, centrado a sua atenção para responder essencialmente à seguinte indagação: se o regime da responsabilidade é objetivo ou subjetivo.

Há muitos debates acerca da natureza e responsabilidade civil na Lei Geral de Proteção de Dados (BRAMANTE, 2021, pag. 87).

A LGPD estabelece entre os artigos 46 a 54 quais são as condutas a serem implementadas pelos agentes de tratamento de dados de pessoas naturais, entre elas, dispõe sobre o tratamento de dados para segurança, sigilo e boas práticas de governança.

As regulamentações trazidas nos artigos 42 e 44 da lei em questão têm dividido a doutrina entre qualificar a responsabilidade civil objetiva e subjetiva.

A responsabilidade civil nasce do exercício da atividade de proteção de dados que viola a “**legislação de proteção de dados**”. De fato, o legislador reconheceu que a proteção de dados é um microsistema, com normas estabelecidas em diversas leis específicas, sendo a LGPD a sua base estrutural.

A interpretação do artigo 42, *caput*, deve ser realizada em conjunto com o artigo 44, parágrafo único da Lei 13.709/18⁴.

O art. 42⁵ da LGPD contém uma cláusula geral de responsabilidade, imputando a obrigação de indenizar ao controlador ou operador que, descumprindo a legislação de proteção de dados, causar dano patrimonial ou extrapatrimonial aos titulares dos dados pessoais violados.

O art. 42 da LGPD aponta as condutas a serem observadas: (i) não fornecer a segurança que o titular dele pode esperar; (i) deixar de observar a legislação. De modo que a simples omissão na adoção de medidas de segurança para o tratamento adequado dos dados, bem como o descumprimento das obrigações impostas na lei, independente de causar efetivo dano, ensacha a responsabilidade pelas multas. E havendo dano surge a responsabilidade de reparação de dano material e moral. (BRAMANTE, 2021, pág. 88).

Assim, este artigo traz à baila o dever de indenizar “em razão do exercício de atividade de tratamento de dados pessoais”, impondo assim deveres de conduta de precaução e prevenção, sinalizando o fato de que trata-se de uma atividade de ris-

4 Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

5 Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

co, via de consequência compatível com a responsabilidade civil objetiva, prevista no artigo 927 do Código Civil⁶.

De forma similar ao regime implantado pelo Código de Defesa do Consumidor - CDC (Lei 8.078/90), a LGPD estabeleceu a solidariedade dos agentes que causaram a lesão (art. 42, § 1º, I e II) e, para abrandar a relação entre controladores, operadores e titulares de dados pessoais, concedeu a possibilidade de ocorrer a inversão do ônus da prova sempre por critério judicial (art. 42, § 2º), o que, a rigor científico, implica um sistema de presunção legal do dano sofrido pela titular de dados lesado:

Não existe propriamente uma inversão do ônus dos encargos probatórios quando o juiz aplica o art. 6º, VIII, do CDC. [...] Ao contrário, o que verdadeiramente ocorre quando se aplica o art. 6º, VIII, do CDC é que o juiz passa a presumir que os fatos ocorreram de acordo com a narrativa do autor consumidor (presunção *juris tantum*), de modo que o réu fornecedor conserva os mesmíssimos ônus probatórios que possuía antes da 'inversão' (art. 333, II, do CPC), permanecendo com a necessidade de fazer prova de que os fatos descritos na petição inicial não ocorreram ou ocorreram de forma diversa do alegado pelo consumidor, podendo comprovar, ainda, a existência de fatos impeditivos, modificativos ou extintivos do direito afirmado pelo consumidor. (NOVAKOSKI, 2006, p. 10-11)

De outro lado, o art. 44 da LGPD define o conceito de tratamento irregular de dados, quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: a) o modo pelo qual é realizado; b) o resultado e os riscos que razoavelmente dele se esperam e c) as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Já o art. 46, por sua vez, estabelece o dever dos agentes de tratamento em adotar medidas de segurança, técnicas e administrativas, visando a proteção de dados pessoais.

Dessa forma, é possível identificar as situações que ensejam a aplicabilidade da responsabilidade civil na LGPD: a) violação de normas **jurídicas**, do microsistema de proteção de dados e b) violação de normas **técnicas**, voltadas à segurança e proteção de dados pessoais.

Diante do quanto exposto, denota-se que a LGPD traz duas espécies de responsabilidade, sendo uma a responsabilidade objetiva pelo mero tratamento irregular dos dados, configurando nesta hipótese o dano moral *in re ipsa*, independente-

⁶ Art. 927 - Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

mente⁴ do efetivo dano material. Já na modalidade de responsabilidade subjetiva, por culpa e dolo no caso de haver dano material ao titular dos dados pessoais.

O art. 45 da LGPD, último da Seção III da lei, ressalva que as situações de lesão a direito de consumidor ou pessoa a ele equiparada continuam sujeitas à disciplina do microsistema de relações de consumo instituído pelo CDC (Lei 8.078/90).

4. Excludentes da responsabilidade do agente de tratamento de dados

No dispositivo do artigo 43, a LGPD trata das hipóteses de exceção da responsabilidade dos agentes de tratamento, quando provarem que i) não realizaram o tratamento dos dados pessoais; ii) se o realizaram, não violaram as normas de proteção de dados pessoais; ou iii) que o dano foi causado por terceiro ou pelo próprio titular (art. 43, I a III).

Recente julgado proferido pelo Egrégio Tribunal de Justiça do Estado de São Paulo, nos autos do processo 1025180-52.2020.8.26.0405, reconheceu a incidência da hipótese de excludente de responsabilidade do agente de tratamento de dados.

EMENTA: Ação de indenização por dano moral. Apropriação por terceiros de dados pessoais do consumidor, extraídos dos cadastros de concessionária de energia elétrica.

Ocorrência versada nas Leis nºs 12.414/2011, 12.965/2014 e 13.709/2018. Responsabilidade dos controladores e operadores que é objetiva, mas dela se eximem se não houve violação à legislação de proteção de dados ou o dano decorreu de culpa exclusiva de terceiro.

Artigo 43 da LGPD. Caso em que inexistia base para se reconhecer que a empresa deixou de adotar medida de segurança recomendada pela Ciência ou determinada pela ANPD de modo a com isso ter dado causa a que terceiros tivessem acesso àqueles dados. Ação improcedente. Recurso não provido. (TJ/SP – Relator Desembargador ARANTES THEODORO, 36ª Câmara de Direito Privado)

À semelhança da disciplina adotada pelo CDC, a LGPD estabeleceu que o tratamento de dados será irregular quando contrariar a disciplina legal (art. 44, *caput*) ou, também, quando não fornecer a segurança legitimamente esperada pelo respectivo titular (art. 44, I a III)⁷.

No âmbito trabalhista, para beneficiar-se das hipóteses de exclusão de responsabilização, ficará a cargo da empresa um controle elaborado de todo o ciclo de dados, incluindo mapeamento, procedimentos, políticas internas e gestão de contratos com a classificação adequada do tratamento, tudo em conformidade com o art. 7º, V, LGPD.

⁷ Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

- o modo pelo qual é realizado;
- o resultado e os riscos que razoavelmente dele se esperam;
- as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

5. Inversão do ônus da prova

O tema de sua relevância vem disposto no artigo 42, § 2º, que admite a inversão do ônus da prova, a critério do juiz, a favor do titular de dados, desde que verossímil a alegação, haja hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular for excessivamente onerosa. Há normas sobre a redistribuição/inversão do ônus da prova em outras leis: uma muito semelhante no art. 373, § 1º do CPC⁸ e outra no art. 6º, VIII do CDC⁹, aplicável nas ações de natureza consumerista.

Além da inversão do ônus probatório, o reconhecimento da hipossuficiência do titular também se verifica no fato de que a responsabilidade civil da LGPD seja da modalidade objetiva, onde não há discussão sobre a culpa do agente.

Desta monta, é passível de se concluir que o regime jurídico de responsabilidade civil estabelecido traz significativa proteção em favor do titular dos dados. Ainda que o regime seja o de responsabilidade civil subjetiva, a culpa e autoria do agente de tratamento de dados são presumidas e, adicionalmente, pode haver a inversão do ônus da prova quanto aos demais pressupostos da responsabilidade civil.

6. Considerações finais

De certo, entende-se que a Lei Geral de Proteção de Dados trouxe verdadeiro avanço na legislação em busca de uma maior proteção aos dados pessoais dos titulares, com extensão a todas as áreas do direito.

Em que pese já existisse previsão legal de norma em âmbito nacional tratando de proteção de informações e dados, como é o caso da Lei 12.737/12, Lei 12.414/11 e Lei 12.965/14, a LGPD estabelece normas específicas e amplas sobre a proteção de dados pessoais.

Estar em conformidade com a norma é um verdadeiro diferencial ao mundo corporativo empresarial, pois a nova legislação determina aos controladores de dados pessoais que se adequem à nova visão de proteção o que definitivamente corrobora com atitude de boas práticas de governança, gerando assim segurança aos funcionários da empresa e clientes, bem como demonstrando ao mercado que a estrutura empresarial em segurança da informação é moderna, confirmando um “olhar para o futuro”.

Por outro lado, como não poderia ser diferente, cabe à norma estabelecer sanções para os casos daqueles que descumprirem com o quanto disposto na Seção III do Capítulo VI da Lei Geral de Proteção de Dados – Lei 13.709/2018, nomeada “Da Responsabilidade e do Ressarcimento de Danos”.

8 Art. 373. O ônus da prova incumbe:

§ 1º Nos casos previstos em lei ou diante de peculiaridades da causa relacionadas à impossibilidade ou à excessiva dificuldade de cumprir o encargo nos termos do *caput* ou à maior facilidade de obtenção da prova do fato contrário, poderá o juiz atribuir o ônus da prova de modo diverso, desde que o faça por decisão fundamentada, caso em que deverá dar à parte a oportunidade de se desincumbir do ônus que lhe foi atribuído.

9 Art. 6º São direitos básicos do consumidor:

VIII - a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências;

A doutrina brasileira tem, nesse primeiro momento, centrado a sua atenção para responder essencialmente à seguinte indagação: o regime da responsabilidade é objetivo ou subjetivo? A doutrina não é uniforme sobre essa referida indagação.

Denota-se que a LGPD traz duas espécies de responsabilidade, sendo uma a responsabilidade objetiva pelo mero tratamento irregular dos dados, configurando nesta hipótese o dano moral *in re ipsa*, independentemente do efetivo dano material. Já na modalidade de responsabilidade subjetiva, por culpa e dolo no caso de haver dano material ao titular dos dados pessoais.

Já o dispositivo contido no artigo 43 da LGPD trata das hipóteses de exceção da responsabilidade dos agentes de tratamento, quando provarem que: i) não realizaram o tratamento dos dados pessoais; ii) se o realizaram, não violaram as normas de proteção de dados pessoais; ou iii) que o dano foi causado por terceiro ou pelo próprio titular (art. 43, I a III).

REFERÊNCIAS

BRASIL. **Código Civil. Lei nº10.406, de 10 de janeiro de 2002.** Brasília, DF. Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em: 22 out. 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 22 out. 2021.

BRASIL. **Lei Geral de Proteção de Dados. Lei nº 13.709, de 14 de agosto de 2018.** Brasília, DF. Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L3709.htm. Acesso em: 22 out. 2021.

BRASIL. **Marco Civil da Internet. Lei nº12.968, de 06 de maio de 2014.** Brasília, DF. Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12968.htm. Acesso em: 22 out. 2021

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 22 out. 2021.

BIONI, Bruno; DIAS, Daniel. **Responsabilidade civil na proteção de dados pessoais:** construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. *Civilistica.com*. Rio de Janeiro, a. 9, n. 3, 2020. Disponível em: <<http://civilistica.com/responsabilidade-civil-na-protecao-de-dados-pessoais/>>. Data de acesso: 22 out. 2021.

BRAMANTE, Ivani Contini. **Proteção de dado pessoais na relação de trabalho.** São Paulo: Editora Juruá, 2021.

CALCINI, Ricardo. **LGPD e Compliance Trabalhista.** Leme (SP): Editora Mizuno, 2021.

MALDONADO, V. N.; BLUM, R. O. **LGPD: Lei Geral de Proteção de Dados comentada.** 1. ed. São Paulo: Revista dos Tribunais, 2019.

17. PROVAS DIGITAIS, LEI GERAL DE PROTEÇÃO DE DADOS E PRINCÍPIO DA PUBLICIDADE PROCESSUAL

DIGITAL EVIDENCE, GENERAL DATA PROTECTION LAW AND PRINCIPLE OF TRANSPARENCY IN THE JUDICIAL PROCESS

EROTILDE RIBEIRO DOS SANTOS MINHARRO¹⁰

As relações digitais, que dispensam da fadiga de cultivar uma amizade, uma reciprocidade estável e até um consenso que amadurece com o tempo, têm aparência de sociabilidade, mas não constroem verdadeiramente um «nós»; na verdade, habitualmente dissimulam e ampliam o mesmo individualismo que se manifesta na xenofobia e no desprezo dos frágeis. A conexão digital não basta para lançar pontes, não é capaz de unir a humanidade. ENCÍCLICA FRATELLI TUTTI – PAPA FRANCISCO.

Resumo

O presente artigo verifica se, de acordo com a Lei 13.709/2018, o Poder Judiciário Trabalhista Brasileiro deve cuidar de dados pessoais apenas com relação a seus servidores, terceirizados e estagiários, ou se tem responsabilidade também para com seus jurisdicionados. Procurar-se-á interpretar o art. 7º, III, da LGPD à luz de outros ordenamentos jurídicos existentes sobre o tema. Se o entendimento for no sentido de que o Estado-Juiz tem responsabilidade para com os jurisdicionados e demais cidadãos que de alguma forma participam do processo, analisar-se-á a possibilidade ou não de compatibilizar o uso das provas digitais no direito processual trabalhista, o princípio da autodeterminação informativa (previsto na LGPD) e o princípio da publicidade processual.

Palavras-Chave: LGPD. Provas digitais. Autodeterminação informativa. Princípio da publicidade processual.

Abstract

This article verifies whether, according to the 13.709/2018 Act, the Brazilian Labor Judiciary Branch must handle personal data only in relation to its employees, outsourced workers and interns, or whether it is also responsible for its jurisdictions. An attempt will be made to interpret art. 7, III, of the LGPD in light of other existing legal systems on the subject. If the understanding is that the

¹⁰ Doutora e mestre em Direito do Trabalho e Seguridade Social pela USP. Professora de Direito Processual do Trabalho e de Compliance nas Relações Trabalhistas e Previdenciárias da Faculdade de Direito de São Bernardo do Campo. Juíza Titular da 2ª VT de São Caetano do Sul.
e-mail: erotilde.minharro@direitosbc.br

State-Judge has responsibility towards the jurisdictions and other citizens who somehow participate in the process, it seeks to analyze whether it is possible or not to reconcile the use of digital evidence in labor procedural law, the principle of informative self-determination (provided for in the LGPD) and the principle of procedural publicity.

Keywords. LGPD. Digital evidence. Informative self-determination. Principle of procedural advertising.

1. Introdução

As novas tecnologias permitem, além daqueles documentos que comumente já eram juntados aos autos, que possam ser carregadas outros tipos de provas, impregnadas de dados sensíveis, como, por exemplo, mensagens de áudio, vídeo e texto que foram trocadas em um ambiente restrito, fotografias com EXIF's que exibem detalhes da localização, endereços residenciais, endereços de IP, IMEIs etc. Ao lado desta nova realidade, desde agosto de 2020 passou a vigorar a LGPD (Lei 13.709/2018), que estabelece os cuidados que entes públicos e privados devem ter com relação a dados pessoais. Para contrastar, há a regra constitucional relativa à publicidade processual. Será que tudo o que é apurado pelo Poder Judiciário e colacionado aos autos tem mesmo de ir para a rede mundial de computadores?

O objetivo deste artigo é o de demonstrar a necessidade de ponderação de valores, com o objetivo de equacionar o dilema que envolve o princípio da publicidade processual, o princípio da autodeterminação informativa e o direito de se obter a verdade substancial por meio das provas digitais.

2. Da publicidade processual

Nos termos do art. 93, IX, da Constituição Federal, “todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação; (...)”. Como se vê, na esfera processual, a publicidade é a regra e o segredo é a exceção.

Entretanto, o princípio da publicidade processual não é absoluto, pois o próprio art. 5º, LX, da Constituição Federal de 1988 estabelece que a lei poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem, daí ser possível sopesar o princípio da publicidade processual com o da autodeterminação informativa. Senão vejamos:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no país a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

LX - a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem;

Os atos processuais são públicos, todavia tramitam em segredo de justiça os processos: (...)

III - em que constem dados protegidos pelo direito constitucional à intimidade;

Assim, mister se faz analisar cada caso concreto para saber se, naquela situação específica, estamos ou não diante de dados pessoais passíveis de proteção e sopesar acerca da necessidade ou não de levar referidos dados ao conhecimento do público em geral. Entendo que neste momento o magistrado deve se perguntar: qual a utilidade de se fornecer estes dados de pessoa natural para o público? O não fornecimento deste dado pessoal prejudica a transparência que o Poder Judiciário deve imprimir em seus atos? O fornecimento destes dados pessoais presta-se apenas à satisfação da curiosidade humana? Tais perguntas são as primeiras balizas para que se perceba até que ponto a privacidade dos dados pessoais está sendo desnecessariamente exposta pela Justiça.

3. Informatização processual, publicidade processual e a proteção de dados da pessoa natural no pode judiciário

A Lei 11.419/2006, que dispõe sobre a informatização do processo judicial, estabelece que os documentos digitalizados juntados em processos eletrônicos estarão disponíveis para acesso, por meio da rede externa, apenas para visibilidade das respectivas partes processuais, pelos advogados, independentemente de procuração nos autos, pelos membros do Ministério Público e pelos magistrados, sem prejuízo da possibilidade de visualização nas secretarias dos órgãos julgadores, à exceção daqueles que tramitarem em segredo de justiça, respeitadas suas regras, o que denota que – desde os primórdios da informatização processual – já havia a preocupação do poder público em expor os dados pessoais dos litigantes apenas na medida em que isso fosse absolutamente necessário.

Convém registrar que foi a Lei 13.793/2019 que alterou a norma supra citada para expressamente permitir o acesso de qualquer advogado aos atos do processo eletrônico (mesmo que não represente nenhum dos sujeitos processuais), ressalvados aqueles protegidos pelo segredo de justiça, que só podem ser consultados por advogado com procuração nos autos. Antes da vigência desta norma, apenas os advogados com procuração nos autos podiam acessá-los livremente.

A Lei 12.527/2011 (Lei de Acesso à Informação), por seu turno, subordina o Poder Judiciário às suas regras (art. 1º) e fixa, no artigo 25, que “é dever do Estado controlar o acesso e a divulgação de informações sigilosas produzidas por seus órgãos e entidades, assegurando a sua proteção”. Logo, o Poder Judiciário, como um dos poderes do Estado, deve zelar para que não sejam vazadas ao público externo informações pessoais desnecessárias.

O Marco Civil da Internet (Lei 12.965/2014), por sua vez, arrola a proteção da privacidade e dos dados pessoais como dois de seus princípios basilares. Nesta

senda, o art. 22 estabelece regras para que a parte interessada possa, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de Internet. Como se vê, a possibilidade de expedição de ofício para as operadoras a fim de instruir o feito com provas digitais não é exclusividade do âmbito penal, podendo ser utilizada também no juízo cível (que inclui a seara trabalhista).

O diploma legal em apreço traça limites para a prerrogativa supra e determina, sob pena de inadmissibilidade, que o requerimento da parte seja cumulativamente fundado em indícios da ocorrência do ilícito, que haja justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória e que contenha o período ao qual se referem os registros.

Segundo o art. 23 da referida norma, fornecidos os dados, caberá ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

Diante dos termos explícitos da norma em cotejo, não vejo, pois, como o Poder Judiciário possa se furtar à responsabilidade de cuidar dos dados pessoais das pessoas naturais no que se refere às informações fornecidas pelas operadoras relativamente a dados e metadados colhidos na rede mundial de computadores e trazidos aos autos para formação do conjunto probatório. A meu ver, tais documentos devem se revestir do sigilo documental.

Cite-se, ainda, que o parágrafo 1º, do art. 4º, da Resolução 121/2010 do CNJ também aborda este tema e estabelece que – em se tratando de processos trabalhistas – as consultas públicas dos sistemas de tramitação e acompanhamento processual dos Tribunais e Conselhos, disponíveis na rede mundial de computadores, devem permitir a localização e identificação dos dados básicos de processo judicial, observados os seguintes critérios: número atual ou anteriores, inclusive em outro juízo ou instâncias; nomes dos advogados; registro junto à Ordem dos Advogados do Brasil.

Notem que no processo do trabalho não se identifica o feito na rede mundial de computadores pelo nome das partes nem tampouco por seu CPF, com o intuito de evitar discriminações em razão do exercício regular do direito de ação, devendo – pois – a Justiça do Trabalho cuidar para que referida Resolução seja rigorosamente cumprida.

A Resolução 215/2015 do CNJ, que dispõe sobre a divulgação de dados processuais eletrônicos na Internet, em seu art. 32, limita o acesso público a informações pessoais relativas à intimidade, à vida privada, à honra e à imagem detidas pelo Poder Judiciário e determina que tais dados serão de acesso restrito a agentes públicos legalmente autorizados e às pessoas a que se referirem, independentemente de classificação de sigilo, pelo prazo máximo de 100 (cem) anos a contar da data de sua produção. Em seguida estabelece, no art. 33, que o tratamento das informações pessoais deve ser realizado de forma transparente e com respeito à

intimidade, à vida privada, à honra e à imagem das pessoas, bem como às liberdades e garantias individuais.

No contexto deste artigo, vale trazer à colação a Resolução 332/2020 do CNJ que, em seu art. 8º, esclarece que “transparência” para fins do mencionado diploma consiste na divulgação responsável, considerando a sensibilidade própria dos dados judiciais. Pode-se, pois, ter este preceito como regra de atuação na seara de divulgação de dados pessoais: o Poder Judiciário não pode divulgar os dados pessoais de pessoas naturais de maneira displicente, tem que fazê-lo de forma responsável.

Por fim, tem-se a Recomendação CNJ 73/2020 (adoção de medidas preparatórias e iniciais para a adequação às disposições contidas na Lei Geral de Proteção de Dados Pessoais), que, em suas considerações preambulares, deixou claro que o Poder Judiciário entende necessária não só a proteção dos dados pessoais de seus servidores, terceirizados, estagiários e magistrados, mas que também é necessária a proteção da privacidade e dos dados pessoais de jurisdicionados e outros sujeitos identificados ou identificáveis nos atos processuais.

Pelas razões acima expostas, constata-se que mesmo antes da Lei 13.709/2018 os órgãos do Poder Judiciário já demonstravam o cuidado com os dados que seriam expostos ao público em geral relativamente aos jurisdicionados e cidadãos envolvidos nos processos judiciais. Portanto, mesmo que referida norma permita o tratamento de dados pelos juízes, desembargadores, servidores etc., este tratamento não pode expor mais do que o necessário à concretização da publicidade dos atos processuais.

4. Há dados pessoais que devam ser protegidos no processo do trabalho?

Nos processos trabalhistas há inúmeros dados pessoais e dados pessoais sensíveis que – quanto expostos – tornam a pessoa física extremamente vulnerável a fraudadores, estelionatários, empresas que colocam o nome do reclamante em listas sujas, pessoas interessadas na compra de créditos por valores irrisórios etc.

Sem falar em dados médicos atrelados a laudos, conversas íntimas em aplicativos de mensagens e outras situações que nem sempre convém ser expostas na rede mundial de computadores.

À guisa de exemplo, há caso concreto de empresas que “garimpam” informações sobre precatórios a serem liberados e, de posse de dados fornecidos nos próprios portais do Poder Judiciário, com nome e CPF dos credores, conseguem localizá-los e convencê-los de que o dinheiro demorará muito a ser liberado (o que não é verdade, porque nesta altura já há previsão da data da liberação de valores) para, assim, levá-los a ceder o crédito por 20% ou 30% do valor original, causando-lhes prejuízos irreparáveis.

Por isso, é preciso buscar meios de proteger os dados pessoais das pessoas naturais mesmo no âmbito do Poder Judiciário.

Insisto que, dependendo do caso concreto, advogados e magistrados, sempre que necessário, devem fazer uso do mecanismo de sigilo de peças processuais.

Para lembrar: segredo de justiça é o sigilo integral dos autos para a proteção do interesse público, do interesse social ou da intimidade da pessoa, e impõe a ve-

dação da divulgação da existência do próprio processo. Já no sigilo, afasta-se a publicidade externa apenas para um ou alguns atos do processo. Por exemplo, quando se apresenta a declaração de imposto de renda nos autos, apenas o arquivo que contém esses dados fica anexado como sigiloso (VALENTE CARDOSO, 2020).

Assim, deve haver a preocupação em não tornar visíveis documentos que tragam dados sensíveis do trabalhador.

No TRT-2, exemplificativamente, as gravações das audiências ficam em sigilo porque trazem dados sensíveis das partes e das testemunhas. Os interessados, se quiserem, podem participar (ao vivo) das audiências que são públicas e possuem um link de acesso no portal, mas as gravações ficam restritas às partes, advogados em geral, servidores que manuseiam o processo e magistrados vinculados à Unidade Judicial. A saber:

PORTARIA GP/CR N° 04/2020 – Art. 2º O acesso para juntada de arquivos de áudio e vídeo ao Acervo Eletrônico PJe, bem como para a posterior visualização dos arquivos, será permitido apenas ao(s) advogado(s), procurador(es) e partes envolvidas no processo, mediante a utilização de identidade digital da pessoa física, em meio eletrônico (e-CPF) e a indicação do processo eletrônico ao qual o arquivo deve ser associado.

Destarte, protegem-se trabalhadores e testemunhas da curiosidade e maldades alheias. quivos de áudio e vídeo ao Acervo

5. O que diz a LGPD

Para o inciso III, do art. 7º, da Lei 13.709/2018, o tratamento de dados pessoais poderá ser realizado pela administração pública, para o uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos, daí porque o Poder Judiciário necessita utilizar dados pessoais (ainda que sensíveis) no seu dia a dia, a fim de executar sua tarefa precípua de dar a cada um o que é seu com celeridade e justiça.

Neste ponto, a maior parte da doutrina diz que ao ingressar com ações judiciais ou defender-se nelas o cidadão concede seu consentimento para o tratamento de tais dados.

Portanto, o Poder Judiciário pode tratar de dados pessoais de pessoas naturais. Isto é fato incontestável.

Porém, não pode se olvidar do cuidado em não expor estes dados de maneira a prejudicar jurisdicionados, testemunhas e todas as pessoas naturais que de alguma forma estão com seus dados alocados nos autos.

Tudo isso é esclarecido pelo art. 21, da Lei 13.709/2018, que estabelece que os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Em outras palavras: a exposição de reclamantes e testemunhas a listas sujas faz com que o jurisdicionado tenha medo de exercer o seu direito de ação ou de defesa.

A autorização dada pelo art. 7º, inciso III, da LGPD para que o Poder Judiciário trate dos dados de pessoas naturais não lhe dá carta branca para divulgar estes dados de maneira irresponsável. Como vimos no item anterior, várias são as normas que impõem limites às divulgações de dados pessoais de pessoas naturais, mas o art. 21 da própria Lei 13.709/2018 traça de maneira indubitável os contornos da atuação do magistrado.

6. Como é na Europa?

Historicamente, o GDPR começou a ser desenhado na Europa no início do século 20.

Logo após a Primeira Guerra Mundial, houve um censo religioso na Alemanha, com finalidade legítima de saber a religião da população idosa local e, assim, possibilitar que o Estado fizesse funerais dignos e de acordo com a crença dos falecidos que não tinham familiares vivos no país. Esta finalidade absolutamente legítima, entretanto, foi desvirtuada pelo Governo de Adolf Hitler, que se utilizou de tais dados e da tecnologia de Hollerith (futura IBM) para obter mais rapidamente informações sobre quem eram e onde estavam os judeus na Alemanha, subjugando-os. (SABBATINI, 2001).

Finda a Segunda Grande Guerra, estas feridas fizeram com que o povo europeu cuidasse para que seus dados não ficassem expostos (nem mesmo para o Estado ou pelo Estado).

Na década de 1970 - várias normas de proteção de dados pessoais de primeira geração, como a lei de dados da Suécia (1973), o estatuto de proteção de dados do Land alemão de Rheinland-Pfalz (1974) e a lei federal de proteção de dados da Alemanha (1977).

Nos EUA, foi editado, em 1970, o Fair Credit Reporting Act e, em 1974, o Privacy Act. Em 1976, Portugal foi o primeiro país a estabelecer em sua Constituição o direito fundamental à autodeterminação informativa (art. 35). Em 1981 foi promulgada a Convenção nº 108, do Conselho da Europa que, mais tarde, serviu de base para a Diretiva 95/46/CE, de 1995.

Finalmente, em 2018, entrou em vigor o GDPR, que traz o regramento da proteção de dados pessoais para os cidadãos europeus nos dias atuais.

No item 20 de seus “considerandos”, o GDPR diz que muito embora seus artigos sejam aplicáveis às atividades dos tribunais e autoridades judiciais, a competência das autoridades de controle não abrange o tratamento de dados pessoais efetuados pelos tribunais no exercício de sua função jurisdicional, a fim de assegurar a independência do Poder Judiciário no exercício de sua função jurisdicional na tomada de decisões.

A partir desta assertiva, começou a se formar no Brasil um entendimento de que a Lei 13.709/2018, a exemplo da lei europeia, não poderia atingir o Poder Judiciário em sua função judicante.

Ocorre que o texto do GDPR não exclui o Poder Judiciário de zelar pelos dados pessoais das pessoas físicas dos jurisdicionados, diz apenas que a supervisão desta tutela deverá, se possível (grifos meus), ser confiada a órgãos específicos do sis-

tema judiciário de cada Estado-Membro. E arremata afirmando que estes órgãos específicos devem ser capazes de assegurar o cumprimento das regras do GDPR e sensibilizar os membros do sistema judicial para as suas obrigações ao abrigo do presente regulamento, regular e tratar reclamações em relação a tais operações de processamento de dados. (grifei)

Repita-se, o regulamento europeu não autoriza ao Poder Judiciário tratar os dados pessoais de maneira irresponsável, ao contrário, deixa clara a obrigação de as autoridades judiciais respeitarem o princípio da privacidade e as regras do GDPR. O que o regulamento faz é apontar a preferência de se confiar a órgãos do próprio sistema judiciário de cada país a supervisão e aplicação das penalidades pelas infrações ao GDPR que possam ocorrer no exercício da atividade judicante.

Ao encontro do nosso entendimento, em 23 de março de 2019 foi publicada na França a Lei 2019-222, que no art. 33 reforça a ideia de que os debates judiciais são públicos, mas os dados pessoais podem ser anonimizados para garantir o direito à privacidade dos cidadãos envolvidos nos processos.

O próprio Tribunal de Justiça da União Europeia estabeleceu regras para a proteção de dados pessoais no âmbito das publicações relativas a processos judiciais em tramitação naquele órgão, fazendo-o nos seguintes termos:

Em conformidade com as obrigações que lhe incumbem, o Tribunal de Justiça tem a preocupação, no exercício das suas funções jurisdicionais, de conciliar o princípio da publicidade da justiça e da informação dos cidadãos com a proteção de dados pessoais das pessoas singulares mencionadas nos processos entrados.

Quando uma parte considerar necessário que alguns dos seus dados pessoais não sejam divulgados no âmbito das publicações relacionadas com um processo entrado no Tribunal de Justiça, pode dirigir-se a este último para se for caso disso requerer que lhe seja concedido o anonimato no âmbito desse processo.

Na Europa, o que são públicos são os debates, não os dados das pessoas naturais.

A Lei 13.709/2018 não fez nenhuma observação quanto a isentar o Poder Judiciário do respeito às regras de proteção de dados pessoais das pessoas naturais, daí por que, até que advenha legislação em contrário, há que se cumprir o disposto no art. 21 da referida norma, a saber: *os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.*

No Brasil, vejo a possibilidade de pseudoanonimização (ou pseudonimização) dos dados pessoais e, assim, preservar a publicidade processual e o direito à auto-determinação informativa simultaneamente. Para tanto, mister se faz a “sensibilização” dos membros dos diversos órgãos do Poder Judiciário (conforme sugere o considerando n. 20 do GDPR), o incentivo a boas práticas na proteção de dados dos jurisdicionados e cidadãos que tenham seus dados tratados em atividades ju-

dicantes e treinamento a todos os servidores, magistrados, estagiários e terceiros que lidam com este tipo de dados.

Segundo Machado e Doneda, “o procedimento de “pseudonimização consiste em substituir um atributo (tipicamente um atributo único) em um registro por outro; seria um processo de mascaramento ou disfarce (disguising) de identidade, que afeta principalmente identificadores diretos”. (MACHADO, 2020).

O art. 4º do Regulamento Geral de Proteção de Dados (GDPR) diz que “pseudonimização” é o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

Seria facilmente possível, por exemplo, qualificar as testemunhas em apartado, atribuir-lhes iniciais aleatórias ou números, deixar esta qualificação em sigilo e escrever na ata, sentença ou acórdão apenas as iniciais aleatórias ou a numeração atribuída.

Outro exemplo de boa prática, nos acordos judiciais, é não colocar os dados bancários e o CPF do credor na ata que vai para publicação, estes dados não interessam ao público.

Práticas simples, não onerosas, que respeitam o princípio da publicidade e o da autodeterminação informativa simultaneamente. Os atos processuais continuariam sendo públicos, apenas os dados pessoais estariam protegidos. Gestos simples que trariam maior segurança a todos.

Ressalte-se, ainda, que se deve a todo custo evitar o chamado efeito “mosaico”, ou seja, a pseudoanonimização ou pseudonimização não pode levar, por meio de simples ilações, à identificação do titular de dados.

7. Provas digitais

Provas digitais deixam rastros e metadados. O Poder Judiciário tem o dever de se preocupar e evitar de expor estes dados que podem ser raspados por site legítimos de análise jurisprudencial.

Ao determinar uma exportação de mensagens do WhatsApp ou ao trazer aos autos EXIF's de fotografias digitais devemos, a meu ver, colocar tais documentos em sigilo e na hora de elaborar a ata ou a sentença pseudoanonimizar os dados pessoais dos jurisdicionados.

Por exemplo, atuando como magistrada, mesmo antes do advento da LGPD, nunca coloquei os dados bancários nas atas de audiências referentes aos acordos firmados, porque entendo que seria uma exposição desnecessária da vida íntima do trabalhador que ficaria vulnerável a crackers.

Assim, ao utilizarmos das novas tecnologias com o objetivo de facilitar a obtenção da verdade substancial, não podemos esquecer do direito à autodeterminação informativa dos cidadãos.

8. Considerações finais

A Constituição estabelece a publicidade dos ATOS processuais e não a publici-

dade dos DADOS PESSOAIS, motivo pelo qual os tribunais devem tratar referidos dados com extremo cuidado.

Os Tribunais têm o direito de tratar de dados pessoais no exercício de sua função institucional (art. 7º, III, da LGPD), mas não podem tratá-los de maneira displicente. Devem cuidar para não os expor, especialmente quando envolver dados sensíveis, em outras palavras, “(...) *cada Tribunal deverá ter o cuidado de não expor informações desnecessárias e que possam comprometer/constranger a pessoa, mesmo que o processo não siga em segredo de justiça*” (Nelson Nery Júnior e Rosa Maria de Andrade Nery). (ZANETTI, 2021).

Inúmeros são os dados pessoais, em seara trabalhista, que devem ser preservados da publicidade. Por exemplo, o número da conta corrente onde será depositado o valor do acordo do trabalhador, o laudo médico com suas doenças e condições físicas, lista de recebimento de precatórios etc.

A LGPD veio imprimir uma nova mentalidade quanto a tratamento de dados pessoais. Os dados pertencem aos titulares que têm o direito à autodeterminação informativa. A Lei 13.709/2018 não isentou explicitamente o Poder Judiciário de respeitá-la em sua inteireza, ainda que no exercício de suas atividades judicantes. Convém lembrar que o GDPR tampouco isentou o Poder Judiciário local de respeitar a privacidade dos dados pessoais de pessoas naturais, apenas estabeleceu que – quando possível – a fiscalização do cumprimento do regulamento em seara judicante seria feita pelo sistema do próprio judiciário.

A França e o Tribunal Europeu viram na anonimização uma forma de solucionar este dilema, com reforço de que na Europa os debates são públicos e os dados são privados.

No Brasil também devemos buscar mecanismos para conciliar o princípio da publicidade processual com o da autodeterminação informativa que, de todo modo, não são contraditórios.

Enquanto não vier em nosso país nenhuma regulamentação formal quanto à atuação do Poder Judiciário no âmbito da proteção de dados, convém usarmos de boas práticas, sensibilização e muito treinamento a fim de evitar exposições desnecessárias das pessoas naturais.

Dentre as boas práticas, está a pseudoanonimização do nome das partes e das testemunhas no documento que vai para a Internet (ata de audiência, sentença, acórdão, por exemplo). A ata vai para a rede mundial de computadores com nomes fictícios e os nomes reais estão certificados nos autos do processo e lacrados com o sigilo processual. Assim, por exemplo, a qualificação das testemunhas poderia vir em documento em apartado que ficaria em sigilo.

O Poder Judiciário já se preocupa com a questão da proteção de dados há tempos, conforme demonstram todos os normativos mencionados no item 3 deste artigo, e a LGPD veio impulsionar ainda mais esta preocupação. As provas digitais vieram aumentar os riscos e com isso a necessidade de ampliar os cuidados. É possível aprimorar os meios protetivos e o diálogo pode levar a soluções práticas, simples, baratas e eficazes.

A capacidade humana de se colocar no lugar do outro, e perceber a angústia que ele pode estar sentindo por ter sido colocado em perigo físico, digital ou social, cria

as pontes necessárias para que eventuais percalços na aplicação das regras de proteção de dados pessoais sejam transpostos. Pensar juntos nos une. A troca de ideias, as boas práticas, a sensibilização e os treinamentos são nossos grandes aliados.

OS ATOS PROCESSUAIS SÃO PÚBLICOS, OS DADOS PESSOAIS SÃO PROTEGIDOS.

REFERÊNCIAS:

LOI 2019-222. Disponível em <https://www.legifrance.gouv.fr/jorf/id/JORFARTI000038261761>. Acesso em: 23 set. 2021.

GENERAL DATA PROTECTOR REGULATION. Disponível em: <https://www.galvaoesilva.com/lei-gdpr-em-portugues/>. Acesso em: 23 set. 2021.

MACHADO, Diego. **Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados**. Disponível em: https://www.academia.edu/38168713/Prote%C3%A7%C3%A3o_de_dados_pessoais_e_criptografia_tecnologias_criptogr%C3%A1ficas_entre_anonimiza%C3%A7%C3%A3o_e_pseudonimiza%C3%A7%C3%A3o_de_dados. Acesso em: 22 set. 2021.

SABBATINI, Renato. **Hitler e a IBM**. Disponível em: <http://www.renato.sabbatini.com/correio/cp010215.html>. Acesso em: 23 set. 2021.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Disponível em: https://docs.google.com/viewerng/viewer?url=https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-11/tra-doc-pt-div-c-0000-2015-201508723-05_00.pdf. Acesso em: 22 set. 2021.

VALENTE CARDOSO, Oscar. **Lei Geral de Proteção de Dados e Publicidade Processual**. Disponível em: [https://jus.com.br/artigos/84273/lei-geral-de-protecao-de-dados-e-publicidade-processual#:~:text=\(a\)%20sigilo%20integral%20dos%20autos,de%20quaisquer%20atos%20nele%20praticados](https://jus.com.br/artigos/84273/lei-geral-de-protecao-de-dados-e-publicidade-processual#:~:text=(a)%20sigilo%20integral%20dos%20autos,de%20quaisquer%20atos%20nele%20praticados). Acesso em: 21 set. 2021.

ZANETTI, Dânton. **Proteção de dados pessoais e publicidade processual: um contrassenso?** Disponível em: <https://www.conjur.com.br/2021-abr-15/zanetti-protecao-dados-pessoais-publicidade-processual>. Acesso em: 22 set. 2021.

18. O DESCARTE DE DISPOSITIVOS TECNOLÓGICOS FRENTE À LGPD

THE DISPOSAL OF TECHNOLOGICAL DEVICES AGAINST THE LGPD

VALÉRIA REANI RODRIGUES GARCIA¹¹
E MANUEL DAVID RODRIGUES MASSENO¹²

Resumo

Este trabalho contém uma reflexão breve acerca do impacto jurídico resultante do descarte de ferramentas tecnológicas, sobretudo em ambiente laboral. O contexto social e econômico é o da pandemia causada pelo covid-19, ao qual se junta a entrada em vigor da Lei Geral de Proteção de Dados. Em especial, serão facultadas indicações práticas destinadas a minimizar os riscos para a Privacidade e a Proteção de Dados Pessoais no momento do descarte de dispositivos eletrônicos.

Palavras-Chave: Descarte. Proteção de dados. Obsolescência tecnológica.

Abstract

This paper contains a brief reflection on the legal impact resulting from the disposal of technological tools, especially in the work environment. The social and economic context is that of the pandemic caused by covid-19, to which the entry into force of the General Data Protection Law is added. In particular, prac-

11 Advogada com curso de extensão em “Strategic Thinking” pela University of Albany (State University of New York). Especialista em Direito e Privacidade de Dados Pessoais pela UNL – Universidade Nova Lisboa – Portugal. Curso Avançado Contratos Digitais e a LGPD na PUC Paraná. Curso Information Security Management Professional Based on Iso/IEC 27001 Exin. Curso Avançado USP-FEA—LGPD/GDPR – DPO- Data Protection Officer. Especialista em Direito Digital e Compliance pela Faculdade Damásio Educacional. Especialista em Gestão Empresarial pela PUCC – Pontifícia Universidade Católica de Campinas e em Direito do Trabalho e Direito Processual do Trabalho pela Escola Superior de Advocacia – ESA/SP. Coordenadora Pedagógica, Científica e Docente dos cursos de Direito Digital e Inovação da ESA – Escola Superior de Advocacia de Santos, Santo André e Campinas. Escritora colunista de sites jurídicos; autora das obras *Direito Digital – Debates Contemporâneos*, 2019; *Compliance Digital*, 2020, ambas pela Thonsom Reuters, e *LGPD Aplicada*, 2021, pela Editora GenJuridico; presidente da Comissão Especial de Privacidade e Proteção de Dados Pessoais, 2020 até então, e vice-presidente da Comissão de Direito Digital, ambos os cargos de indicação na OAB Campinas, e Membro Convidada do Instituto Nacional de Proteção de Dados –INPD.

12 Professor Adjunto e Encarregado da Proteção de Dados do IPBeja – Instituto Politécnico de Beja, em Portugal; Membro das Coordenações do Laboratório UbiNET – Segurança Informática e Cibercrime e do MESI – Mestrado em Engenharia de Segurança Informática, também no IPBeja; pertence à EDEN, Rede de Especialistas em Proteção de Dados da Europol (Agência Europeia de Polícia); integra o Grupo de Estudos de Direito Digital e Compliance da FIESP – Federação das Indústrias do Estado de São Paulo; faz parte das Comissões de Direito Digital da Seção de Santa Catarina e da Subseção de Campinas, assim como da Comissão de Inovação, Gestão e Tecnologia da Subseção de Guarulhos, todas da Ordem dos Advogados do Brasil.

tical indications will be provided to minimize the risks to privacy and protection of personal data at the time of disposal of electronic devices.

Keywords: Disposal. Data protection. Technological obsolescence.

1. O contexto geral

O desenvolvimento tecnológico demanda uma produção crescente de equipamentos, ferramentas e acessórios que, através de mudanças e atualizações constantes, tornam obsoletas as versões anteriores, tornando (quase) indispensável o consumo contínuo de novos modelos e o descarte dos antigos.

As principais novidades e inovações surgem na informática, telefonia celular, comunicação e entretenimento, possibilitando um rápido avanço e diversificação das capacidades de memória, velocidade, armazenamento e transmissão de dados, captação e transmissão de sinais de modo preciso e instantâneo.

Através da publicidade, é estimulada a compra de novidades tecnológicas e os consumidores são impulsionados à substituição dos celulares, computadores, impressoras, TVs, vídeo games, câmeras digitais, MP3, notebooks, tablets. Em todos está inerente a obsolescência, quase sempre planejada, funcional ou proveniente de desgastes do uso cotidiano, inclusive peças de substituição e consertos.

Ao longo da história, outras pandemias já assolaram o planeta e causaram transformações significativas na sociedade. As formas de consumo e de relação e as inovações tecnológicas, também visando a sobrevivência, são exemplos do que podemos esperar.

Como constatamos, as últimas décadas do século 20 foram marcadas pela tecnologia digital, sem que tivessem sido ponderadas as questões relacionadas com as respectivas segurança e resiliência. Agora, em um cenário crítico, é preciso repensar as estratégias e inovar, inclusive nas ferramentas já disponíveis, para que se adequem às necessidades sociais.

Para muitos estudiosos, o coronavírus acelera uma série de mudanças que já estavam em andamento. Exemplo disso é a educação a distância (EaD):

“A pandemia covid-19 mudou permanentemente os padrões de uso de dispositivos por funcionários e consumidores. Com o trabalho remoto se transformando em trabalho híbrido, a educação doméstica se transformando em educação digital e os jogos interativos migrando para a nuvem, os tipos e o número de dispositivos que as pessoas precisam, têm e usam continuarão a aumentar”, aponta o diretor sênior de pesquisa da Gartner, Ranjit Atwal¹³.

Perante uma realidade nova, pelo menos para a grande maioria das pessoas, se deu o recurso aos dispositivos já disponíveis, em especial os smartphones. Efetivamente, esta ferramenta passou a ser fundamental para se comunicar e compartilhar momentos durante o distanciamento e isolamento social.

2. Os riscos

Porém, a integração da vida pessoal e profissional, juntamente com uma força

13 ABRANET - Covid-19 dispara consumo de PCs, tablets e celulares no mundo. Disponível em: <https://www.abranet.org.br/Noticias/Covid-19-dispara-consumo-de-PCs,-tablets-e-celulares-no-mundo-3332.html?UserActiveTemplate=site&UserActiveTemplate=mobile%252Csite%252Cmobile#.YIhFey3OpsM>

de trabalho muito mais dispersa, requer flexibilidade na escolha do dispositivo. Os trabalhadores estão cada vez mais usando uma combinação de dispositivos de propriedade da empresa e seus próprios dispositivos pessoais executados no Chrome, iOS e Android (o denominado BYOD, acrônimo em inglês de “Traga Seu Próprio Dispositivo”), o que está aumentando a complexidade do serviço e suporte de TI.

A conectividade já era um desafio para muitos usuários que trabalhavam remotamente. Mas, à medida que a mobilidade retorna à força de trabalho, a necessidade de equipar os funcionários com as ferramentas certas para trabalhar em qualquer lugar se torna crucial. Conseqüentemente, a demanda por laptops 4G/5G conectados e outros dispositivos aumentará conforme a justificativa de negócios aumenta, apesar das atuais dificuldades no fornecimento de chips, também resultante da pandemia.

Conforme dados da ABRANET (Associação Brasileira de Internet), em 2022, a base global instalada de dispositivos deverá atingir 6,4 bilhões de unidades, um aumento de 3,2% em relação a 2021. Embora a mudança para o trabalho remoto tenha destacado o declínio dos desktops, o uso de tablets e laptops aumentou.

Este cenário contribuiu para a aceleração da obsolescência do consumo programado dos respectivos dispositivos, uma vez que os produtos são fáceis de comprar, mas são desenhados para não durar. Como efeito, os consumidores são obrigados a descartar os produtos adquiridos em um prazo muito menor e substituí-los por novos, cuja durabilidade ainda será potencialmente menor. Além do prejuízo ao consumidor, essa ação causa um impacto negativo ao meio ambiente, pelo uso de recursos naturais, energia e geração de resíduos.

Outrossim, além do impacto ambiental, ressaltamos que estudo citado aponta que 90% dos dispositivos descartados contêm dados confidenciais.

Aliás, novo experimento realizado pela empresa de cibersegurança Kaspersky sobre revenda de eletrônicos¹⁴ mostra que os utilizadores, empresariais e não empresariais, antes de avançarem para o descarte ou a venda de seus equipamentos eletrônicos usados, precisam estar atentos aos dados neles contidos.

Os pesquisadores descobriram também ser possível extrair dados de 74% dos dispositivos usando o método de esculpimento¹⁵ de arquivos (*file carving*, em inglês), o qual recupera arquivos em mídias de armazenamento. Os dados variaram de compromissos de calendários e anotações de reuniões, fotos e vídeos pessoais, documentos fiscais, informações bancárias, credenciais de login a dados médicos.

“Este experimento tem como objetivo principal alertar as pessoas sobre sua responsabilidade em relação a proteção de seus dados pessoais”, avalia Fabio Assolini, analista sênior de segurança da Kaspersky no Brasil.

3 Que fazer?

Portanto, sendo um consumidor, e por isso mesmo “titular de dados pesso-

14 BRASIL. Lei Geral de Proteção de dados. Lei 13.709 de 2018. Brasília, DF: Presidência da República. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 out. 2021.

15 Esculpimentp de arquivos (*file carving*) é o processo de remontar arquivos de computador a partir de fragmentos na ausência de metadados do sistema de arquivos.

ais”, antes de doar, vender ou mandar para reciclagem, convém fazer uma limpeza efetiva na máquina ou no gadget do dispositivo, retirando todos os seus arquivos, deixando-os livres para outros usuários, de forma segura e protegendo seus dados e mantendo sua privacidade conforme condutas abaixo¹⁶:

Fazer o backup;

Retirar o cartão SIM (o cartão SIM é o da sua operadora, aquele que te permite fazer ligações, enviar SMS e conversar pelo Whatsapp ou Telegram; parece óbvio que, antes de vender celular usado, é necessário retirá-lo, mas é normal esquecer essa parte);

Remover ou limpar o cartão SD ou MicroSD (é no cartão SD ou MicroSD que ficam armazenadas as suas fotos e vídeos, além de alguns áudios do Whatsapp, gifs, músicas e alguns aplicativos; se você for vender o celular sem um dispositivo do tipo, é só retirá-lo abrindo a tampa do celular ou a gaveta híbrida para chip e cartão);

Criptografar os dados; depois de cuidar de todos os componentes externos do celular, chegou a hora de pensar na parte interna; a primeira etapa consiste em criptografar os dados do celular para evitar que dados gravados na memória consigam ser acessados por hardwares especializados; para fazer isso, basta ir às configurações do seu aparelho, escritas como “Configurar” ou “Configurações”, depois clicar em “Segurança” e depois em “Criptografar dispositivo” ou “Criptografar telefone”¹⁷.

Fazer o reset do aparelho: depois de realizar o backup, tem de salvar seus dados e desvincular suas contas, pois você já pode resetar o aparelho e deixá-lo, ao novo proprietário, como veio de fábrica.

Nesse cenário, é preciso avaliar a importância do descarte correto e responsável de aparelhos tecnológicos por parte dos consumidores e sobretudo pelas empresas, cujos ativos de TI são itens físicos e virtuais que formam uma rede corporativa.

No que concerne à responsabilidade corporativa quanto a dados pessoais, é fundamental que sejam identificados e avaliados os dados que estiverem armazenados nos diversos dispositivos listados a seguir:

Pendrive, HD externo e demais dispositivos móveis para armazenamento;

Placa-mãe (CPU), memória RAM, processador, Hard Disk (HD) e demais componentes de um computador;

Tablets, telefones celulares e smartphones;

Mouse, teclado, monitores e outros periféricos;

Softwares e sistemas operacionais instalados em um computador;

Switches, servidores e demais equipamentos;

Impressoras conectadas à rede.

Gerenciar esses ativos significa por em prática diversas ações administrativas com o objetivo final de garantir a segurança dos dados (impacto da Lei Geral de Proteção aos Dados – LGPD, Lei nº 13.709/2018) e a conformidade com a lei de

16 Cuidados antes de descartar o celular ou vender. Disponível em <https://www.promobit.com.br/blog/quais-cuidados-se-deve-tomar-antes-de-vender-celular-usado/>. Acesso em: 25 abr. 2021

17 Kaspersky sobre revenda de eletrônicos. Disponível em <https://computerworld.com.br/plataformas/estudo-aponta-que-90-dos-dispositivos-descartados-contem-dados-confidenciais/>. Acesso em: 27 abr. 2021.

resíduos sólidos (leis estaduais que regulam o descarte de eletrônicos).

No que tange à segurança dos dados, vale lembrar que a LGPD estabelece regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, impondo mais proteção e penalidades para o não cumprimento.

Especificamente, Segurança e Governança, previstas em seus artigos 49 e 50, incluem a gestão de incidentes e de riscos, o mapeamento de dados, o DPO/Encarregado, assim como a gestão do descarte de ativos de TI.¹⁸ (6).

Assim, na hora de organizar os ativos e escolher um fornecedor para o descarte dos dispositivos, é prudente que sejam analisados os pontos abaixo:

- 1) se este tem um histórico em relação à manipulação correta de dados e quanto à segurança dos ativos de TI, garantindo a privacidade e a conformidade com todas as normativas e leis;
- 2) se os processos de manipulação de ativos são seguros e claramente demonstrados pelo fornecedor para garantir o fiel cumprimento do disposto na LGPD;
- 3) se atende aos requisitos de segurança de dados corporativos, também em conformidade com a LGPD;
- 4) de que maneira são apagados os dados;
- 5) se efetua a reciclagem dos equipamentos obsoletos ou danificados, adotando boas práticas de segurança de informação;
- 6) sendo esse serviço subcontratado, se adotam as mesmas medidas dos itens anteriores;
- 7) quando os ativos saem da instalação corporativa, obter a garantia contratual de que os dados pessoais serão devidamente protegidos, de forma a garantir a reputação corporativa e marca, assim como a conformidade à LGPD sob pena de responsabilidade solidária na hipótese de vazamento de dados;
- 8) garantir a transparência das operações do fornecedor;
- 9) garantir a realização de auditorias de clientes e as inspeções de instalações;
- 10) ter o conhecimento quanto ao tipo de mídia de armazenamento de dados que eles podem destruir;

Em suma, saber se os serviços e a logística estão em conformidade com a LGPD.

Sugerimos que um checklist seja parte integrante do contrato de prestação de serviços entre a corporação e o fornecedor com cláusulas específicas de Privacidade e Proteção de dados pessoais, conforme a LGPD, de forma a garantir as boas práticas previstas na respectiva legislação, bem como a efetiva proteção aos dados pessoais contidos nos ativos descartados ou vendidos. Essa prática proporciona ao gestor uma previsão de como podem controlar e mitigar os riscos.

Vale lembrar que no âmbito de promoção da Segurança da Informação, os processos e os procedimentos devem assegurar a disponibilidade, integridade e

18 Para mais aprofundamentos sobre estas questões, ver Masseno, M. D., Martins, G. M., & Faleiros Júnior, J. L. de M. (2020). *A Segurança na Proteção de Dados: entre o RGPD Europeu e a LGPD Brasileira*. Revista do CEJUR/TJSC: Prestação Jurisdicional, 8(1), e346. Disponível em: <https://doi.org/10.21902/rctjsc.v8i1.346>

confidencialidade de todas as formas de informação ao longo de todo o ciclo de vida do dado.

4. Concluindo

Existem diversas particularidades que precisam ser analisadas, sendo que o principal objetivo deste trabalho é que deverão ser garantidas, sobretudo nas organizações, a segurança e a sustentabilidade do processo de descarte de ferramentas tecnológicas, sob a responsabilidade dos gestores corporativos e em conformidade com a Lei Geral de Proteção de Dados, nunca esquecendo as regras relativas aos resíduos e ao meio ambiente.

Por isso mesmo, é prudente testar, conferir e revisar a checklist para ver se ela realmente atende às demandas relacionadas à conformidade da organização com os critérios legais, sobretudo em matéria de Proteção de Dados.

Na realidade, conseguir alcançar um nível de maturidade quanto à sensibilização e conscientização de privacidade e proteção de dados, em todo processo de gestão de ativos de TI, é algo que leva tempo e requer que seja agregada à cultura organizacional desde a alta administração a todos os colaboradores.

Finalmente, ressaltamos que a responsabilidade da proteção de dados pessoais é de todos nós.

REFERÊNCIAS

BRASIL. **Lei Geral de Proteção de dados. Lei nº 13.709 de 2018**. Brasília, DF: Presidência da República. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 out. 2021.

HARARI, Yuval Noah. **Notas sobre a pandemia: E breves lições para o mundo pós coronavírus**. São Paulo: Companhia das Letras, 2020.

TOMASEVICIUS FILHO, Eduardo. *A Política Nacional de Resíduos Sólidos e a Lei Geral de Proteção de Dados Pessoais*. Disponível em <https://www.conjur.com.br/2020-ago-14/tomasevicius-filho-politica-nacional-residuos-solidos-l-gpd>. Acesso em: 25 out. 2021.

19. PROTEÇÃO DE DADOS PESSOAIS NAS RELAÇÕES DE TRABALHO

PROTECTION OF PERSONAL DATA IN LABOR RELATIONS

LAURA MEDINA MARTINS MOREIRA¹⁹
E DIOGO ANTONIO PEREIRA MIRANDA²⁰

Resumo

O presente trabalho faz uma análise da proteção de dados pessoais nas relações de trabalho, através da inserção da Lei 13.709/18, também denominada Lei Geral de Proteção de Dados (LGPD), no ordenamento jurídico brasileiro. Para isso o estudo partiu de uma apreciação inicial sobre os principais aspectos da referida lei, passando então a verificar os aspectos relativos às fases pré-contratual, contratual e pós-contratual, momento no qual se fez necessário analisar os principais aspectos de convergências entre a inovação legislativa e o direito do trabalho, bem como foi realizado estudo no tocante à jurisprudência já existente sobre o tema. Por fim, entende-se que houve avanço na legislação, bem como maior proteção aos dados pessoais, inclusive com possibilidade de aplicação de sanções que até então não eram previstas na legislação brasileira. No entanto, é necessário que sejam realizados estudos mais aprofundados sobre o tema para que não se criem situações de injustiça aos envolvidos.

Palavras-Chave: Lei Geral de Proteção de Dados. Relações de Trabalho. Privacidade. Fases contratuais.

Abstract

The present work analyzes the protection of personal data in labor relations, through the insertion of Law 13.709/18, also known as the General Data Protection Law (LGPD), in the Brazilian legal system. Initial analysis of the main aspects of that law, then proceeding to verify the aspects relating to the pre-contractual, contractual and post-contractual phases, at which time, it was necessary to analyze the main aspects of convergence between legislative innovation and the law of work, as well as an analysis was carried out regarding the existing jurisprudence on the subject. Finally, it is understood that there was progress in legislation, as well as greater protection of personal data, including the pos-

19 Mestranda em Direito pela PUC-RS. Pós-Graduada em Direito do Trabalho pela UFRGS. Pós-Graduada em Direito do Trabalho e Direito Processual do Trabalho pela PUC-RS. Bacharel em Direito pela Universidade Católica de Pelotas. Advogada trabalhista em Porto Alegre/RS. E-mail: laurammoreira@outlook.com.

20 Mestrando em Direito pela PUC-RS. Especialista em Direito e Processo do Trabalho pela PUC-RS. Bacharel em Direito pela PUC-RS. Advogado trabalhista em Porto Alegre/RS. E-mail:diogo@sturmer.com.br.

sibility of applying sanctions that were not previously provided for in Brazilian legislation. However, it is necessary that more in-depth studies be carried out on the theme, so that situations of injustice are not created for those involved.

Keywords: General Data Protection Law. Work relationships. Privacy. Contract phases.

1. Introdução

O presente artigo trata sobre a proteção de dados pessoais nas relações de trabalho.

A pesquisa se justifica diante da relevância do tema e de seus impactos tanto na privacidade dos obreiros quanto em posterior contrapartida econômica, sendo que há inúmeros processos que tratam sobre o tema, principalmente após a positividade advinda pela Lei Geral de Proteção de Dados.

O problema do presente artigo é verificar de que forma a Lei Geral de Proteção de Dados foi inserida no contexto brasileiro e se há avanço e efetividade na proteção de dados pessoais.

Entre as principais hipóteses do presente artigo estão: a) houve avanço, uma vez que a legislação não trazia regras específicas, sendo suficiente para a proteção dos dados atualmente; b) houve avanço, mas a lei não cumpriu na integralidade com os propósitos nos quais foi inserida no direito brasileiro.

O principal objetivo do artigo é verificar as mudanças advindas com a referida lei e o impacto que geraram dentro das relações de emprego. Nos objetivos específicos, destacou-se: analisar a jurisprudência sobre o tema; a forma como está sendo aplicada no direito do trabalho; por fim, se houve avanço na proteção dos dados.

Para tanto, parte-se, primeiramente, da análise macro acerca da Lei Geral de Proteção de Dados, conceituando-a, passando pelos institutos e princípios que a fundamentam; após, são analisados os pontos que a vinculam com as relações de trabalho.

Para tanto, são analisadas as formas de tratamento de dados nas fases pré-contratual, contratual e pós-contratual de uma relação de trabalho, em especial a proteção advinda nessas fases no tocante à seleção dos empregados, de não discriminação, monitoramento por câmeras, manutenção de dados após a extinção do contrato, entre outros.

2. Breves considerações acerca da Lei Geral de Proteção de Dados

A Lei 13.709/18, também denominada Lei Geral de Proteção de Dados (LGPD), tem como inspiração o Regulamento Geral Europeu de Proteção de Dados, tendo trazido ao ordenamento jurídico pátrio o cuidado na proteção das informações, uma vez que, até então, não havia regulamentação específica sobre o tema²¹.

Portanto, a LGPD dispõe sobre o tratamento de dados pessoais, até mesmo meios digitais, sejam eles de pessoa natural ou pessoa jurídica (direito público ou privado), tendo como foco a proteção dos direitos fundamentais de liberdade e de privacidade e do livre desenvolvimento da personalidade da pessoa natural²².

21 MARCOLINO, Beatriz Aparecida; DA SILVEIRA, Daniel Barile. *A Lei Geral de Proteção de Dados e as relações de trabalho: o Compliance como alternativa*. Revista Juris UniToledo, v. 5, n. 04, 2020.

22 RAMOS, Lara Castro Padilha; GOMES, Ana Virgínia Moreira. *Lei geral de proteção de dados pessoais e seus reflexos nas relações de trabalho*. Scientia Iuris, v. 23, n. 2, p. 127.

O artigo 1º da referida lei traz a sua finalidade, consistente nos “direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”, ou seja, não faz distinção quanto à relação jurídica na qual se dará o tratamento dos dados pessoais²³.

Entende-se também como fundamento da Lei Geral de Proteção de Dados a proteção à inviolabilidade da intimidade, da honra e da imagem, conforme preceitua o artigo 2º da referida legislação²⁴.

Destacam-se, também, outros princípios assegurados pela referida lei, quais sejam: “finalidade, adequação, necessidade, livre acesso, qualidade de dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas”²⁵.

O conceito de dado pessoal é trazido pelo artigo 5º da LGPD, no qual o define como qualquer informação que identifique precisamente ou torne identificável uma pessoa natural, ou seja, nome, domicílio, contatos telefônicos, infrações penais, administrativas, entre outros²⁶.

Outro aspecto que merece ponderação é a perspectiva transnacional da origem dos dados pessoais, tanto é que o artigo 3º giza que poderá ser aplicada em transações operadas em território nacional ou quando os indivíduos que forneceram ou receptaram os dados estiverem no Brasil²⁷.

A lei traz, em diversas oportunidades, o termo “tratamento”: o uso da expressão se dá em relação às operações realizadas com os dados pessoais, entre elas a coleta, a transmissão, o arquivamento de informações, entre outras²⁸.

Assim, os agentes que realizam o tratamento dessas informações, dados pessoais, são distinguidos pela legislação como: controlador – responsável por determinar o tratamento de dados; operador – aquele que faz a efetiva coleta dos dados, sendo que ambos são responsáveis pela segurança das informações, tomando os devidos cuidados para que não haja acessos não autorizados e, em caso de infrações à lei, poderão responder por sanções administrativas²⁹.

O artigo 52 da LGPD dispõe sobre as penalidades aplicáveis aos que desobedecerem a legislação, sendo elas: advertência e adoção de medidas corretivas; multa de até 2% do faturamento da pessoa jurídica – limite de R\$ 50 milhões por infração; publicação da infração; bloqueio e eliminação dos dados em questão; multa diária e, por fim, indenização ao titular dos dados³⁰.

23 CASSAR, Vólia Bomfim; PINHEIRO, Iuri. *A Lei de Proteção de Dados e seus Impactos nas Relações de Trabalho*. Revista LTr, São Paulo: LTr, ano 84, n. 11, nov. 2020. p. 1338.

24 DOS SANTOS, Flávia Alcassa. *A lei geral de proteção de dados pessoais (LGPD) e a exposição de dados sensíveis nas relações de trabalho*. Revista do TRT da 10ª Região, v. 24, n. 2, p. 145-151, 2020.

25 RAMOS, Lara Castro Padilha; GOMES, Ana Virgínia Moreira. *Lei geral de proteção de dados pessoais e seus reflexos nas relações de trabalho*. Scientia Iuris, v. 23, n. 2, p. 127.

26 Idem.

27 FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. *Privacidade e lei geral de proteção de dados pessoais*. Revista de Direito Brasileira, v. 23, n. 9, p. 284-301, 2020.

28 Idem.

29 Idem.

30 Idem.

3 Tratamento de dados na fase pré-contratual de uma relação de trabalho

Após a realização de breves considerações acerca da Lei Geral de Proteção de Dados, observa-se a sua inserção dentro do direito do trabalho pátrio, uma vez que existe grande fluxo de dados e informações nas relações de trabalho, a começar pela fase pré-contratual, nos quais destacam-se os processos seletivos e a admissão dos trabalhadores³¹, ou seja, é necessário que se tenha contato prévio entre as duas partes, no qual se dá a seleção através de currículos e entrevistas³².

O processo de seleção, obrigatoriamente, traz consigo a coleta e o tratamento de dados pessoais dos interessados por determinada vaga de emprego. Para tanto, a LGPD, através do seu artigo 7º, V, faculta a utilização de tais dados, quando necessário para a execução do contrato, ou até mesmo de procedimentos preliminares para a sua confecção, devendo ser parte o titular dos dados e a seu pedido³³.

Assim, com o advento da LGPD, as empresas precisam solicitar o consentimento expresso daqueles que se candidataram para as vagas, bem como informar sobre a forma pela qual aqueles dados serão utilizados durante o recrutamento, avaliação e seleção, sendo que qualquer uso dos dados para fins diversos devem ser informados ao interessado pela vaga, o qual deverá consentir³⁴. Veja-se, também:

Exemplificativamente, pode-se citar, no momento que antecede a celebração do contrato de trabalho, a adoção de práticas discriminatórias no processo de seleção, quando se exigem informações de foro íntimo do candidato, expressamente vedadas pela CLT, conforme o artigo 373-A da CLT, que disciplina que é vedado publicar ou fazer publicar anúncio de emprego no qual haja referência ao sexo, à idade, à cor ou situação familiar, salvo quando a natureza da atividade a ser exercida, pública e notoriamente, assim exigir³⁵.

Portanto, existem diversas proteções que antecedem a celebração do contrato trabalhista, algumas já eram inclusive previstas na Consolidação das Leis do Trabalho, sendo a LGPD mais um marco, agora na proteção dos dados de trabalhadores e/ou candidatos a vagas de emprego.

Destaca-se que, em não sendo o candidato selecionado para referida vaga, a

31 CASSAR, Vólia Bomfim; PINHEIRO, Iuri. *A Lei de Proteção de Dados e seus Impactos nas Relações de Trabalho*. Revista LTr, São Paulo: LTr, ano 84, n. 11, nov. 2020. p. 1338

32 MARCOLINO, Beatriz Aparecida; DA SILVEIRA, Daniel Barile. *A Lei Geral de Proteção de Dados e as relações de trabalho: o Compliance como alternativa*. Revista Juris UniToledo, v. 5, n. 04, 2020.

33 SANKIEVICZ, Alexandre; PINHEIRO, Guilherme Pereira. *Aspectos da Proteção de dados nas relações de trabalho*. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (Orgs.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021, p. 510.

34 Idem.

35 RUARO, Regina Linden; HAINZENREDER JÚNIOR, Eugênio. *Proteção da privacidade no contrato de trabalho: da normatização legal a situações de conflitos*. Espaço Jurídico Journal of Law [EJLL], [S. l.], v. 16, n. 2, p. 601–636, 2015. DOI: 10.18593/ejll.v16i2.5051. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/5051>. Acesso em: 3 jul. 2021.

empresa deverá eliminar os dados pessoais obtidos, devendo guardá-los somente em casos de obrigação legal. Ademais, em atenção aos princípios da necessidade, da adequação e da finalidade, fica proibido que as empresas solicitem informações excessivas ou irrelevantes, considerando o cargo que está sendo oferecido, devendo ser retirado, portanto, do formulário, perguntas sobre dados bancários, já que importam somente para aqueles que forem efetivamente contratados³⁶.

Os dados excessivos também poderiam ser: “*aplicação de testes genéticos, exames toxicológicos, questionamentos sobre orientação sexual e opinião política em casos de seleção de empregados*”³⁷.

As empresas precisam tomar medidas para fins de proteger os dados pessoais armazenados durante o processo de seleção, através de medidas técnicas e administrativas, evitando-se acessos não autorizados (artigo 46 da LGPD), ou seja, os dados encaminhados pelos candidatos devem estar restritos àqueles que forem de fato responsáveis pelo recrutamento³⁸.

Por fim, merece cuidado, por parte dos recrutadores, a eventual coleta de dados sensíveis dos candidatos e a sua utilização para fins de políticas de ação afirmativa, já que somente podem ser usados para este fim³⁹.

4. Tratamento de dados na fase contratual de uma relação de trabalho

A fase contratual de uma relação de trabalho certamente é a que mais envolve o armazenamento e o tratamento de dados pessoais. É importante que se ressalte que a LGPD se aplica não só às relações de emprego, com carteira assinada, mas também às relações de trabalho em geral, como contratos autônomos, por exemplo.

Aqui, o tratamento inicia no próprio contrato (de trabalho ou de prestação de serviços). Os contratos existentes e não adequados à LGPD precisam ser aditados e os novos devem respeitar a inserção de cláusulas não gerais, mas destacadas e específicas de coleta de dados⁴⁰, especificando a base legal, quais os dados serão tratados, qual a sua destinação, o período pelo qual serão tratados e se haverá transferência para terceiros.

Para uma maior segurança, é importante que seja destinado um campo específico na própria cláusula para assinatura do empregado, com o fim de demonstrar o inequívoco consentimento, conforme estabelece o artigo 8º da LGPD. Ou até mesmo a criação de anexos contratuais inteiramente para esse fim.

36 SANKIEVICZ, Alexandre; PINHEIRO, Guilherme Pereira. *Aspectos da Proteção de dados nas relações de trabalho*. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (Orgs.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021, p. 510.

37 RAMOS, Lara Castro Padilha; GOMES, Ana Virgínia Moreira. *Lei geral de proteção de dados pessoais e seus reflexos nas relações de trabalho*. Scientia Iuris, v. 23, n. 2, p. 139.

38 SANKIEVICZ, Alexandre; PINHEIRO, Guilherme Pereira. *Aspectos da Proteção de dados nas relações de trabalho*. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (Orgs.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021, p. 510.

39 Idem.

40 CARLOTO, Selma. *Lei Geral de Proteção de Dados com enfoque nas relações de trabalho*. São Paulo: LTr, 2020. p. 104.

Uma ressalva merece ser feita: o consentimento, apesar de constar no inciso I do artigo 7º da LGPD como uma autorizadora para tratamento de dados pessoais, na esfera trabalhista merece uma atenção especial. Apesar de ser importante e necessário se buscar o consentimento do empregado nos dados que serão tratados, por fins de segurança o consentimento não pode ser a primeira base legal de tratamento nas relações de trabalho, diante do risco da alegação de “consentimento forçado” por conta da subordinação jurídica entre empregado/empregador. É que o inciso XII do artigo 5º da LGPD afirma que o consentimento deve ser “a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”. O desequilíbrio de poder em uma relação de emprego pode trazer dúvidas quanto a essa liberdade⁴¹.

Não há, na LGPD, nenhuma disposição sobre essa disparidade entre poderes e o seu efeito sobre o consentimento. Entretanto, na Europa, no Considerando 43⁴² do Ato Inicial Legal que deu origem ao Regulamento Geral sobre a Proteção de Dados (RGPD)⁴³, há expresse esclarecimento de que o consentimento não pode servir de fundamento jurídico válido para o tratamento de dados pessoais quando houver, na relação, um desequilíbrio manifesto.

Além disso, o consentimento pode ser retirado a qualquer momento pelo titular dos dados, conforme artigo 8º, § 5º e artigo 15º, inciso III da LGPD. Logo, se o dado for realmente necessário, ele precisa estar embasado também em outra hipótese legal, e não apenas no consentimento.

Afora o consentimento, há hipóteses em que o empregador possui respaldo legal para o tratamento dos dados de seus empregados, não havendo, pois, necessidade de autorização por parte do trabalhador. Essa autorização legal está prevista no artigo 7º da LGPD. Como exemplo, tem-se o inciso II, que autoriza o tratamento “para o cumprimento de obrigação legal ou regulatória pelo controlador”. No campo prático, se traduz no envio de dados do empregado para o eSocial (Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas), sistema obrigatório a todos os contratos de emprego.

O inciso V, por sua vez, traz “quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados”. Aqui, o campo prático é traduzido no tratamento

41 CARLOTO, Selma. *Lei Geral de Proteção de Dados com enfoque nas relações de trabalho*. São Paulo: LTr, 2020. p. 92.

42 “A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução.”

43 Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>. Acesso em: 06 jul. 2021.

de dados e informações relativas ao salário, assim como dos dados relativos à conta bancária dos empregados para que os salários possam ser pagos.

Como último exemplo, e talvez o mais polêmico, o inciso IX, que indica a possibilidade do tratamento “quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais”. Aqui se poderiam incluir, por exemplo, o monitoramento ambiental, por câmeras, e o monitoramento de e-mails.

É recomendado que o empregador, quando pretender suscitar o legítimo interesse, cuide para aplicar esses conceitos de forma proporcional e menos intrusiva possível, justamente para que não se ultrapasse um direito fundamental do titular. Nesse sentido, Selma Carloto e Livia Clozel⁴⁴:

O que for necessário para prosseguir interesses legítimos do responsável pelo tratamento deverá ser ponderado em relação aos direitos e liberdades fundamentais do titular e é o resultado do teste da ponderação que determina se o artigo 7º, inciso IX, poderá ser invocado pelo controlador como fundamento jurídico para o tratamento.

Com relação ao monitoramento por câmeras, entende-se possível o monitoramento ambiental feito por equipamentos comuns, sem capacidade de reconhecimento facial e nem ligado a softwares para esse fim. O monitoramento, pois, com o fim de resguardo do patrimônio e de preservar a integridade física das pessoas que circulam pelo ambiente, sem fins de fiscalização, e diante da impossibilidade da realização por outros meios, deve ser declarado legítimo. Evidentemente, pois, que essa situação deve ser comunicada aos empregados e devem ser resguardados ambientes íntimos, como banheiros e vestiários⁴⁵. Nesse sentido está inclinada a jurisprudência do Tribunal Superior do Trabalho (TST)⁴⁶.

Com relação ao monitoramento de e-mails, igualmente entende-se ser possí-

44 CARLOTO, Selma; CLOZEL, Livia. *LGPD e o Direito à Privacidade dos Trabalhadores*. In: TOMASEVICIUS FILHO, Eduardo (coord.). *A Lei Geral de Proteção de Dados Brasileira: Uma Análise Setorial* (Volume 1). São Paulo: Almedina, 2021. p. 251.

45 RUARO, Regina Linden; HAINZENREDER JÚNIOR, Eugênio. *Proteção da privacidade no contrato de trabalho: da normatização legal a situações de conflitos*. Espaço Jurídico Journal of Law [EJLL], [S. l.], v. 16, n. 2, p. 601–636, 2015. DOI: 10.18593/ejll.v16i2.5051. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/5051>. Acesso em: 3 jul. 2021.

46 “AGRAVO DE INSTRUMENTO - MINISTÉRIO PÚBLICO DO TRABALHO – INSTALAÇÃO DE CÂMERAS DE VÍDEO – DIREITO DE APRENDER E DE ENSINAR 1. O uso do poder diretivo do empregador atendeu a critérios de razoabilidade, tendo em vista que a instalação de câmeras de vídeo teve por fim a proteção do estabelecimento de ensino e das pessoas que lá se encontram, sejam alunos, sejam funcionários da instituição, com o intuito de evitar furtos e roubos. 2. Além disso, os direitos previstos no artigo 206, II, da Constituição de 88, quais sejam, “liberdade de aprender, ensinar, pesquisar e divulgar o pensamento, a arte e o saber”, não são vulnerados ou ameaçados pela instalação de câmeras de vídeo na portaria, na tesouraria e no estacionamento de instituição de ensino. Agravo de Instrumento a que se nega provimento” (AIRR-183040-84.2003.5.05.0011, 3ª Turma, Relatora Ministra Maria Cristina Irigoyen Peduzzi, DEJT 10/08/2006).

vel, desde que seja informado ao empregado, de forma bastante clara e explícita, que a propriedade da ferramenta do e-mail é da empresa e que há um ambiente monitorado. A existência de uma política clara de uso de dados coletados nessa caixa postal corporativa não deverá trazer problemas legais ao empregador⁴⁷. A jurisprudência do TST⁴⁸ nesse ponto também se inclina para essa legalidade no monitoramento, desde que respeitadas essas condições, pela prevalência do poder diretivo do empregador, que nada mais é do que a sua prerrogativa de organizar o processo e o procedimento de trabalho em um estabelecimento empresarial⁴⁹. O poder diretivo do empregador não é absoluto, gize-se, mas, tanto nesse caso como no monitoramento por câmeras, possui prevalência caso as precauções mencionadas acima sejam tomadas pelo empregador.

Ao fim e ao cabo, na esteira da ideia de Kirstie Ball, o monitoramento é uma necessidade e um elemento comum no ambiente de trabalho. Os empregados, desde que cientificados, já esperam por isso para fins de avaliação de performance, por exemplo, e isso é uma boa prática de gestão, desde que não se extrapole o limite do razoável ou necessário (monitoramento para além do ambiente de trabalho), não se pratique um controle excessivo no tempo utilizado pelo empregado em seu trabalho e, por fim, que não afete os níveis existentes de controle, autonomia e confiança entre as partes⁵⁰.

Quando se trata de dados pessoais sensíveis⁵¹, um cuidado ainda maior deve ser tomado pelo empregador na análise e aplicação do artigo 11º da LGPD. Esse artigo também traz a possibilidade de tratamento de dados para o cumprimento de obrigação legal (inciso II, “a”), tal como ocorre com os dados pessoais normais. Nesse caso, se enquadra, por exemplo, o tratamento de dados de saúde obrigatórios, como atestados médicos, exames admissionais, demissionais e periódicos. Além desses, a biometria (imagens faciais ou impressões digitais, por exemplo),

47 PINHEIRO, Patrícia Peck. *Direito digital*. 6. ed. rev., atual. e ampl. São Paulo: Saraiva, 2016. p. 244.
48 “RECURSO DE REVISTA. ACÓRDÃO REGIONAL PUBLICADO NA VIGÊNCIA DA LEI Nº 13.015/2014 E ANTERIORMENTE À LEI Nº 13.467/2017. 1. PROVA ILÍCITA. “E-MAIL” CORPORATIVO. ACESSO E UTILIZAÇÃO DO CONTEÚDO DAS MENSAGENS DOS EMPREGADOS PELO EMPREGADOR. POSSIBILIDADE. NÃO CONHECIMENTO. I. Consoante entendimento consolidado neste Tribunal, o e-mail corporativo ostenta a natureza jurídica de ferramenta de trabalho. Daí porque é permitido ao empregador monitorar e rastrear a atividade do empregado em e-mail corporativo, isto é, checar as mensagens, tanto do ponto de vista formal (quantidade, horários de expedição, destinatários etc.) quanto sob o ângulo material ou de conteúdo, não se constituindo em prova ilícita a prova assim obtida. II. Não viola os arts. 5º, X e XII, da Constituição Federal, portanto, o acesso e a utilização, pelo empregador, do conteúdo do “e-mail” corporativo. III. Acórdão regional proferido em consonância ao entendimento desta Corte Superior. IV. Recurso de revista de que não se conhece. [...]

(RR-1347-42.2014.5.12.0059, 4ª Turma, Relator Ministro Alexandre Luiz Ramos, DEJT 26/06/2020).

49 DELGADO, Mauricio Godinho. *Curso de Direito do Trabalho*. 12. ed. São Paulo: LTr, 2013. p. 666.

50 BALL, Kirstie. *Workplace surveillance: an overview*. Labor History, 51: 1, p. 87-106. DOI: <https://doi.org/10.1080/00236561003654776>. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/00236561003654776>. Acesso em: 1 jul. 2021. p. 89.

51 Conforme Art. 5º, II da LGPD: “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”.

que hoje é largamente utilizada no ambiente de trabalho, sendo mais comum sua utilização para controle de acesso a ambientes seguros e controlados e para controle de jornada de trabalho.

Com a autorização do artigo 74, § 2º da CLT, no sentido de que o controle de jornada se dê de forma digital, a utilização da biometria é o meio mais seguro e eficaz de registro de horário⁵², o que justifica a sua coleta e tratamento.

Fora das hipóteses dos artigos 7º e 11º da LGPD, todo e qualquer dado, para ser coletado e tratado, necessita de expressa autorização do titular, no caso, o empregado, como, por exemplo, o envio dos dados do empregado a empresas de previdência privada e operadoras de plano de saúde e a utilização de dados para fins de avaliação de produtividade entre empregados, com *rankings* e tabelas comparativas. Para essa comparação ser publicizada é necessário o consentimento dos envolvidos.

5. Tratamento de dados na fase pós-contratual de uma relação de trabalho

A fase pós-contratual é a que sucede o fim do contrato de trabalho ou rescisão de um contrato de emprego. O término do tratamento dos dados está previsto no artigo 15º da LGPD. No âmbito trabalhista, o fim do contrato não é o fim do tratamento dos dados. Por isso, o artigo 16º da LGPD traz exceções para a manutenção desses dados. São quatro hipóteses: I - cumprimento de obrigação legal ou regulatória pelo controlador; II - estudo por órgão de pesquisa; III - transferência a terceiro ou; IV - uso exclusivo do controlador.

Ainda que obviamente todas as hipóteses sejam possíveis, certamente a mais importante é a do inciso I, que possui, como exemplo prático, a guarda de documentos para defesa em uma eventual reclamação trabalhista.

Ainda que o usual seja o prazo prescricional de dois anos para as reclamações trabalhistas em geral, há exceções como, por exemplo: 1) existência de absolutamente incapazes no falecimento de um empregado ou menores de 18 anos, hipótese em que não há prescrição (artigo 440 da CLT); 2) doenças ocupacionais, cujo prazo prescricional se dá a partir do exame pericial que comprovar a enfermidade ou verificar a natureza da incapacidade (Súmula 230 do STF) e 3) reconhecimento de vínculo de emprego e anotação da CTPS, que possui natureza declaratória e é imprescritível, conforme artigo 11 da CLT.

Por esse motivo, é possível que seja estabelecido, e comunicado, aos empregados, que os dados serão tratados por mais de dois anos ou, até, por tempo indeterminado. É necessária essa comunicação para que o ex-empregado esteja ciente de que seus dados serão armazenados pela empresa e por qual motivo eles permanecerão nos bancos de dados da empresa após a extinção contratual.

6. Conclusão

O estudo em análise buscou, em um primeiro momento, enaltecer a importância do tema, trazendo as principais modificações geradas pelo advento da Lei 13.709/18, também denominada Lei Geral de Proteção de Dados (LGPD), partin-

52 CASSAR, Vólia Bomfim; PINHEIRO, Iuri. *A Lei de Proteção de Dados e seus Impactos nas Relações de Trabalho*. Revista LTr, São Paulo: LTr, ano 84, n. 11, nov. 2020. p. 1346.

do-se do seu conceito, fundamentos e princípios a ela relacionados.

Após, entendeu-se por examinar a sua aplicação nas relações de trabalho, dividindo-se pelas fases pré-contratual, contratual e pós-contratual, nas quais identificou-se os principais aspectos dela decorrentes.

Apesar da divisão proposta, viu-se que o fluxo de dados pessoais, tanto sensíveis como não sensíveis, é muito alto e ocorre em absolutamente todas as fases de uma relação de trabalho. Desde o anúncio de uma vaga de emprego até o fim de uma relação de trabalho, há dados envolvidos, muitos dos quais necessários para a segurança do empregador, necessários para que o próprio empregado atinja determinado objetivo e, mais, necessários para o próprio desenvolvimento do trabalho.

A LGPD é instrumento necessário para resguardar os dados do empregado e para manter a segurança da empresa, ao mesmo passo em que reprime avanços indesejados e a utilização de forma indevida desses dados coletados. Resguardo esse, gize-se, que era incipiente até então. Não se desconhece que a grande maioria das empresas não está adequada à LGPD, mas a regulamentação é necessária e exige comprometimento das partes envolvidas, já que, mais do que nunca, os dados necessitam de proteção, dado o seu valor mercadológico.

Ao final, conclui-se, portanto, que houve avanço na legislação, bem como maior proteção aos dados pessoais dos trabalhadores, inclusive com possibilidade de aplicação de sanções que até então não eram previstas na legislação brasileira. Há, entretanto, espaço para aperfeiçoamento.

Para tanto, não se pode olvidar que é imprescindível que sejam realizados maiores estudos sobre o tema, de modo que não sejam gerados prejuízos à privacidade dos empregados e nem perpetuado um rigor punitivista excessivo às empresas.

REFERÊNCIAS

BALL, Kirstie. *Workplace surveillance: an overview*. **Labor History**, 51: 1, p. 87-106. DOI: <https://doi.org/10.1080/00236561003654776>. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/00236561003654776>. Acesso em: 1 jul. 2021.

CARLOTO, Selma. **Lei Geral de Proteção de Dados com enfoque nas relações de trabalho**. São Paulo: LTr, 2020.

CARLOTO, Selma; CLOZEL, Livia. LGPD e o Direito à Privacidade dos Trabalhadores. In: TOMASEVICIUS FILHO, Eduardo (coord.). **A Lei Geral de Proteção de Dados Brasileira: Uma Análise Setorial (Volume 1)**. São Paulo: Almedina, 2021.

CASSAR, Vólia Bomfim; PINHEIRO, Iuri. A Lei de Proteção de Dados e seus Impactos nas Relações de Trabalho. **Revista LTr**, São Paulo: LTr, ano 84, n. 11, nov. 2020.

DELGADO, Mauricio Godinho. **Curso de Direito do Trabalho**. 12. ed. São Paulo: LTr, 2013.

DOS SANTOS, Flávia Alcassa. A lei geral de proteção de dados pessoais (LGPD) e a exposição de dados sensíveis nas relações de trabalho. **Revista do Tribunal Regional do Trabalho da 10ª Região**, v. 24, n. 2, p. 145-151, 2020.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e lei geral de proteção de dados pessoais. **Revista de Direito Brasileira**, v. 23, n. 9, p. 284-301, 2020.

MARCOLINO, Beatriz Aparecida; DA SILVEIRA, Daniel Barile. A Lei Geral de Proteção de Dados e as relações de trabalho: o Compliance como alternativa. **Revista Juris UniToledo**, v. 5, n. 04, 2020.

PINHEIRO, Patricia Peck. **Direito digital**. 6. ed. rev., atual. e ampl. São Paulo: Saraiva, 2016.

RAMOS, Lara Castro Padilha; GOMES, Ana Virgínia Moreira. Lei geral de proteção de dados pessoais e seus reflexos nas relações de trabalho. **Scientia Iuris**, v. 23, n. 2.

RUARO, Regina Linden; HAINZENREDER JÚNIOR, Eugênio. Proteção da privacidade no contrato de trabalho: da normatização legal a situações de conflitos. **Espaço Jurídico Journal of Law [EJLL]**, [S. l.], v. 16, n. 2, p. 601–636, 2015. DOI: 10.18593/ejll.v16i2.5051. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/5051>. Acesso em: 3 jul. 2021.

SANKIEVICZ, Alexandre; PINHEIRO, Guilherme Pereira. Aspectos da Proteção de dados nas relações de trabalho. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (Orgs.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

20. LGPD E SUA RELAÇÃO COM A PROTEÇÃO DE DADOS DO EMPREGADO NO TELETRABALHO⁵³

LGPD AND ITS RELATIONSHIP TO EMPLOYEE DATA PROTECTION IN TELEWORK

PALOMA MEDRADO⁵⁴

E THOMIRES ELIZABETH PAULIV BADARÓ DE LIMA⁵⁵

Resumo

A rápida evolução tecnológica, a globalização e a pandemia do covid-19 resultaram na maior implementação de novas formas de trabalho e comunicação, em especial do teletrabalho e das tecnologias de informação e comunicação a distância. Ocorre que o uso de tais tecnologias necessárias ao teletrabalho, somadas à nova legislação sobre proteção de dados, conhecida como LGPD (Lei Geral de Proteção de Dados), trouxeram novos desafios a serem vencidos pelos empregadores nas relações de teletrabalho. Com base nisso, o tema proteção de dados ainda ganha mais relevo, ressaltando os riscos de exposição de dados pessoais e sensíveis na rede. O presente artigo tem como objetivos adentrar ao conceito de teletrabalho no Brasil, analisar os conceitos mais importantes trazidos pela LGPD e traçar os primeiros olhares de seus impactos no contrato de trabalho do teletrabalhador. O método lógico de organização do trabalho é o teórico-dedutivo, partindo-se dos aspectos gerais para os particulares, utilizando-se de estudos jurídicos da doutrina, da legislação especial e de artigo científico sobre o tema. Dessa forma, faz-se necessária a reflexão sobre a repercussão da LGPD ao contrato de trabalho, principalmente ao que tange às formas que podem ser utilizadas pelo empregador, frente ao teletrabalho, razão pela qual reveste-se de vital importância o estudo da LGPD e sua relação com a proteção de dados do teletrabalhador. Como resultados obtidos até o presente momento, constata-se que os dados pessoais de um trabalhador não consistem apenas em aspirações profissionais, mas também em suas características culturais, sociais e privadas, e a LGPD revela-se como uma importante ferramenta para garantir maior segurança aos trabalhadores em regime de teletrabalho, uma vez que obriga o

53 O presente artigo foi originalmente publicado no livro *Direito, novas tecnologias e proteção de dados*. Direção: Angel Urquizu Cavalle e Luiz Eduardo Gunther. Curitiba: Instituto Memória. Centro de Estudos da Contemporaneidade, 2020, com parte dos trabalhos pesquisados no Grupo de Pesquisa do líder Luiz Eduardo Gunther.

54 Mestranda em Direito Empresarial e Cidadania pelo Programa do Centro Universitário Curitiba - PPGD - UNICURITIBA. Membro do grupo de pesquisa REFORMA TRABALHISTA - Proteção de dados e os Direitos da Personalidade - UNICURITIBA - PR. palomamedrado@hotmail.com.

55 Doutoranda e Mestre em Direito Empresarial e Cidadania pelo Programa do Centro Universitário Curitiba - PPGD UNICURITIBA. Membro do grupo de pesquisa REFORMA TRABALHISTA - Proteção de dados e os Direitos da Personalidade - UNICURITIBA - PR. thomiresbadaro@hotmail.com.

responsável pelo tratamento dos dados a avaliar o impacto de suas operações, finalidade e metodologias a serem utilizadas.

Palavras-Chave: Teletrabalho. LGPD. Proteção de Dados do Empregado.

Abstract

The rapid technological evolution, globalization and the covid-19 pandemic resulted in the greater implementation of new forms of work and communication, especially teleworking and information and distance communication technologies. It so happens that the use of such needs for telework, added to the new legislation on data protection, known as the LGPD (General Data Protection Law), brought new challenges to be overcome by employers in telework relations. Based on this, the topic of data protection gains even more importance, highlighting the risks of exposure of personal and sensitive data on the network. This article aims to get into the concept of telework in Brazil, analyze the most important concepts brought by the LGPD and trace the first glances of its impacts on the teleworker's employment contract. The logical method of work organization is the theoretical-deductive one, starting from the general aspects to the particular ones, using legal studies of the doctrine, special legislation and scientific article on the subject. Thus, it is necessary to reflect on the repercussion of the LGPD on the employment contract, especially with regard to the forms that can be used by the employer, in relation to telework, which is why the study of the LGPD and its relation to teleworker data protection. As results obtained so far, it appears that the personal data of a worker does not consist only of professional aspirations, but also of their cultural, social and private characteristics, and the LGPD reveals itself as an important tool to ensure greater safety for workers in a telework regime, as it requires the person responsible for data processing to assess the impact of its operations, appropriate and methodologies to be used.

Keywords: Telework. LGPD. Employee Data Protection.

1 . Introdução

A rápida evolução tecnológica, a globalização e a atual pandemia da covid-19 resultaram na implementação de novas formas de trabalho e comunicação, em especial do teletrabalho e das tecnologias de informação e comunicação a distância.

Em um contexto no qual o ambiente de trabalho e de casa (*home office*) se sobrepõem, trata-se de um desafio manter um padrão mínimo de segurança e preservação de informações confidenciais, principalmente de cunho privado e íntimo.

Ocorre que o uso de tais tecnologias necessárias ao teletrabalho, somadas à nova legislação sobre proteção de dados (Lei Geral de Proteção de Dados), trouxeram novos desafios a serem vencidos pelos empregadores nas relações de teletrabalho.

Notório que houve um aumento exponencial do consumo e tráfego de dados de comunicação eletrônica no mundo, principalmente em decorrência da pandemia, o que levou diversos colaboradores a usarem de seus meios eletrônicos pessoais ou fornecidos pela empresa para desempenhar o labor de forma remota.

Com base nisso, o tema proteção de dados ainda ganha mais relevo, ressaltando os riscos de exposição de dados pessoais e sensíveis na rede.

Diante disso, o presente artigo tem como objetivos adentrar o conceito de teletrabalho no Brasil, analisar os conceitos mais importantes trazidos pela Lei Geral de Proteção de Dados (LGPD) e traçar os primeiros olhares de seus impactos no contrato de trabalho do teletrabalhador.

O trabalho buscará ainda responder a seguinte problemática: em que medida, com a promulgação da Lei Geral de Proteção de Dados, o empregador deverá realizar adequações ao contrato de teletrabalho.

O método lógico de organização do trabalho é o teórico-dedutivo, partindo-se dos aspectos gerais para os particulares, utilizando-se de estudos jurídicos da doutrina, da legislação especial e de artigo científico sobre o tema.

O tema transcende o ambiente acadêmico, já que atinge diversos ramos da sociedade. Dessa forma, faz-se necessária a reflexão sobre a repercussão da LGPD no contrato de trabalho, principalmente no que tange às formas que podem ser utilizadas pelo empregador frente ao teletrabalho.

2. Teletrabalho na lei 13.467/2017

É cada vez mais comum no mundo empresarial a exigência de que o trabalhador possa realizar suas atividades em locais distintos das dependências da empresa, o que vem sendo conhecido como teletrabalho.

O teletrabalho é mais amplo do que o trabalho em domicílio, trata-se de um trabalhador que se encontra ausente da sede do empregador, mas virtualmente presente, por meios telemáticos, sendo capaz de desenvolver sua atividade laboral de forma externa (MARTINEZ, 2019, p. 252). O professor Luiz de Pinho Pedreira apresenta algumas características desta modalidade de trabalho:

- [...] a) trabalho executado a distância, fora do lugar onde o resultado do labor é esperado;
- b) o empregador não pode fisicamente fiscalizar a execução da prestação de serviços;
- c) a fiscalização do trabalho se faz por meio do aparelho informático e/ou dos aparelhos de telecomunicações. (PEDREIRA, 2000, p. 583-597).

Sandro Nahmias Melo afirma que o teletrabalho é:

[...] a forma de organização, execução do trabalho realizado prevalentemente a distancia e mediante o uso intensivo das tecnologias de informação e comunicação, podendo ser desenvolvido em diferentes modalidades, conforme o local onde é executado; home office é o desenvolvido na residência do trabalhador; telecentros são locais escolhidos pelas empresas fora de sua sedes; móvel ou nômade é o realizado por tra-

balhadores que não têm local fixo para a realização das tarefas. (MELO, 2001, p. 56)

Pertinente esclarecer o que é telemática. A referida expressão diz respeito ao método tecnológico de transmissão e comunicação a distância através do uso de uma linguagem computadorizada, capaz de armazenar informações automatizadas. É uma combinação de informática e telecomunicações (RODRIGUES, 2011, p. 32).

No Brasil, a prestação de serviços em regime de teletrabalho foi incorporada no ordenamento jurídico brasileiro por meio da reforma trabalhista, trazida pela Lei 13.467/2017, que introduziu os artigos 75-A a 75-E na CLT (BRASIL, 2017), os quais foram responsáveis pela regulamentação da atividade. Também houve a modificação do art. 62 do mesmo diploma legal, em que foi inserindo o inciso III, que afirma que o teletrabalho é incompatível com a fixação de horários de trabalho.

Com efeito, a Consolidação das Leis do Trabalho apresenta requisitos para caracterização do teletrabalho, conforme se nota no art. 75-B, *verbis*:

Art. 75-B. Considera-se teletrabalho a prestação de serviços preponderantemente fora das dependências do empregador, com a utilização de tecnologias de informação e de comunicação que, por sua natureza, não se constituam como trabalho externo. Parágrafo único. O comparecimento às dependências do empregador para a realização de atividades específicas que exijam a presença do empregado no estabelecimento não descaracteriza o regime de teletrabalho. (BRASIL, 1943).

Observa-se que o legislador brasileiro se ateu aos requisitos centrais universalmente aceitos para configuração do teletrabalho, os quais são análogos às características indicadas pelo professor Luiz de Pinho Pedreira, citado anteriormente.

No parágrafo único do art. 75-B da CLT, o legislador brasileiro ratifica que o aspecto fundamental é que a intensidade do labor em teletrabalho seja preponderante fora das dependências do empregador, porém esclarece que a presença eventual do trabalhador no estabelecimento empresarial, por si só, não desconfiguraria tal regime de trabalho. Logo, a *contrario sensu*, se a presença se tornar habitual, será inevitável a descaracterização deste regime (TOLEDO FILHO, 2019, p. 21).

Ao que pertine sobre os equipamentos necessários para realização do teletrabalho e despesas decorrentes, o legislador apresenta uma norma imprecisa, uma vez que prevê a possibilidade de negociação por meio de contrato escrito. Não obstante, a própria CLT, em outra oportunidade legal, prevê que os custos e encargos relativos à relação de emprego devem ser custeados pelo empregador, devendo ficar o alerta da interpretação sistemática e não simplesmente literal e gramatical do artigo ora em comento. Portanto, embora tal previsão do art. 75-D, *caput*, da CLT, a melhor doutrina entende que o ônus dos custos inerentes ao teletrabalho deve ser do empregador (DELGADO, 2017, p. 139).

De qualquer forma, cabe ressaltar o que afirma Delgado: “não determinou a fixação imperativa de qualquer custo ao empregador”, acenando-se “apenas à previsão em contrato escrito”, sendo passível de debate a interpretação (DELGADO, 2019, p. 1.070). Acredita-se que será necessária uma interpretação sistemática.

Ao que embarca o meio ambiente de trabalho do teletrabalhador, o art. 75-E da CLT prevê que o empregador terá a responsabilidade de instruir os empregados, de maneira expressa e ostensiva, quanto à precaução de acidentes e doenças do trabalho. Sendo, ainda, previsto que o empregado deverá assinar termo de responsabilidade se comprometendo em seguir as determinações indicadas pelo empregador (DELGADO, 2017, p. 139).

A partir desta análise, o autor Rocha Santos esclarece que:

a) o teletrabalho não é sinônimo de trabalho externo e se caracteriza pelo trabalho desenvolvido a distância, fora da empresa, com a utilização de meios de comunicação. Desnecessário reforçar que se trata de trabalho subordinado e que os artigos em comento acompanham o disposto no art. 6º da CLT;

b) o comparecimento às dependências da empresa não descaracteriza o regime de teletrabalho. Razoável, tendo em vista que é possível que haja a necessidade de comparecimentos na sede patronal em datas e momentos preestabelecidos pelo empregador (reuniões, treinamentos etc.);

c) necessidade de anotação da modalidade do teletrabalho na CTPS do empregado, com a indicação das atividades. Muito interessante e necessário, dá segurança a ambos os contratantes;

d) permitidas as alterações contratuais para tornar o regime presencial em regime de teletrabalho e também o inverso. [...];

e) o contrato de trabalho deve prever os critérios de fornecimento dos equipamentos, utilização de tecnologia, infraestrutura do local de trabalho [...]. (ROCHA SANTOS, 2020, p. 182-183).

Ocorre que há um receio de que o teletrabalho possa alimentar a desestabilização de algumas bases jurídicas consagradas ao longo da história (MAÑAS, 2003, p. 136). Portanto, a implantação do teletrabalho requer uma reestruturação empresarial, principalmente nas áreas de recursos humanos e tecnologia da informação, sempre com intuito de proteger o bem-estar dos colaboradores, independentemente do local que vem a desenvolver a prestação de serviço, eis que todo indivíduo tem direito a um meio ambiente de trabalho saudável em todos os seus níveis (LIMA, 2016, P. 150), possuindo o direito fundamental intrínseco à sua personalidade.

Dessa forma, observa-se que para o teletrabalho não há barreiras de tempo e espaço para o desenvolvimento da atividade laborativa.

3. A LGPD e o tratamento dos dados pessoais

No contexto das mudanças dos fatos sociais em que a sociedade é dinâmica, conectada e com intensa rapidez de relações e trocas de informações, observa-se necessário a proteção dos direitos fundamentais da pessoa, os quais são abstratamente previstos na Constituição da República Federativa do Brasil. Diante disso, vislumbram-se inovações legislativas infraconstitucionais necessárias que buscam tratar de forma mais concreta os direitos e garantias considerados fundamentais.

A doutrina, no Brasil, já vinha se manifestando sobre a relevante proteção dos dados pessoais. Nas palavras de Drummond:

[...] a devida atenção a um ponto especificamente delicado, qual seja: a denominada proteção dos dados pessoais. Com efeito a tecnologia permite o cruzamento, rápido e eficiente, de dados pessoais geradores de informações de diversas modalidades. Assim, pode rapidamente traçar o perfil (ou meramente – “um perfil”) de uma pessoa, ainda que não seja o seu perfil correto. Os dados coletados, o que pode vir a ser aprioristicamente desimportantes, herdamos, em decorrência da tecnologia, uma importância antes imaginada (e inimaginável!). A tecnologia deixa o cidadão comum à mercê das corporações e dos governos no que diz respeito à manutenção, ou ainda, à manipulação dos dados e informações a si referentes. (DRUMMOND, 2003, p. 05)

Diante da importância da proteção dos dados pessoais do cidadão, o Brasil promulgou a Lei Geral de Proteção de Dados, Lei 13.709/2018, conhecida como LGPD, que primordialmente se preocupa com os direitos fundamentais da personalidade dos indivíduos, especialmente relativos aos dados personalíssimos. A Lei propõe a proteção de dados em três características centrais: dado pessoal; tratamentos de dados precisa de base legal; e, legitimidade do interesse como hipótese para autorizar a realização de um teste de balanceamento (REGIS, 2020, p. 9).

A norma apresenta conceitos importantes sobre dado pessoal, sensível e de titular. Sendo o dado pessoal a informação pertinente a pessoa natural identificada ou identificável; o dado sensível aquele que como dado pessoal inerente à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter político, filosófico ou religioso, questões de cunho da saúde e vida sexual, dados genéticos ou biométricos, quando ligado a uma pessoa natural; o titular dos dados, trata-se da pessoa natural a quem se aludem os dados pessoais que são objeto de tratamento (BRASIL, 2018).

Ainda, a referida norma estabelece que as atividades de tratamento de dados pessoais deverão atentar ao princípio da boa-fé e aos princípios da finalidade, adequação, livre acesso, necessidade, transparência, qualidade, prevenção, segurança, responsabilidade, não discriminação e prestação de contas, inteligência do artigo 6º, I a X da Lei (BRASIL, 2018).

Simploriamente se observa que a lei busca proteger a privacidade e os demais direitos da personalidade da pessoa.

Importante ainda acrescentar que o trabalhador possui direitos da personalidade, sendo que seus dados pessoais devem igualmente ser objeto de proteção e ser respeitados. Dentro desse contexto, o autor Luiz Eduardo Gunther, no seu livro *Direito da personalidade nas relações de trabalho contemporâneas*, esclarece que:

O trabalhador, como se pode avaliar, só mais recentemente, durante os finais do século 20, início do século 21, passa a ter uma respeitabilidade que vai muito além da garantia do recebimento de um salário digno para sua sobrevivência e dos seus familiares. Busca-se, agora, respeitá-lo em todos os aspectos relacionados aos seus direitos da personalidade. (GUNTHER, 2014, p. 26).

A nova lei trouxe uma tutela jurídica protetiva e promocional da personalidade, além de garantir a proteção à privacidade dos titulares dos dados pessoais, bem como ratificar a responsabilidade civil para quem desrespeitar tais previsões (REGIS, 2020, p. 13).

Em linhas gerais, Santos afirma que:

A Lei Geral de Proteção de Dados tem por fundamentos a consolidação do respeito à privacidade, autodeterminação informativa, liberdade, privacidade, desenvolvimentos econômico e tecnológico, e inovação, bem como a livre-iniciativa, a livre concorrência e a defesa do consumidor, além dos direitos humanos, livre desenvolvimento da personalidade e dignidade. Para garantir a consumação do seu rol de fundamentos, é especialmente voltada para operações de tratamento de dados, inclusive nos meios digitais, ou seja, para operações realizadas com os dados pessoais, desde a sua coleta, até a sua eliminação, passando pela possibilidade de distribuição e transferência. A partir dessa ideia, toda e qualquer operação que reflita em algum tipo de manuseio de dados pessoais, passará pelo crivo da Lei Geral de Proteção de Dados. (SANTOS, 2020, p. 105).

Com isso, trata-se de um texto principiológico de modo que todas as operações e procedimentos precisam atender a um rol de princípios.

Convém acrescentar que a LGPD prevê aplicação de penas em caso de infração à norma. Diante desse contexto, observa-se a seguinte previsão legal no artigo 52 da Lei Geral de Proteção de Dados:

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta

Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

[...]

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. [...] (BRASIL, 2018).

Nota-se que foi observado, na medida do possível, o atendimento do requisito da proporcionalidade no artigo 52 acima transcrito, com o que se acredita que o intuito do legislador é de que sejam coletadas as menores quantidades de dados possíveis dos cidadãos, uma vez que dados pessoais são considerados bens valiosos para o desenvolvimento globalizado.

Conforme já exposto, a garantia da proteção dos direitos dos titulares dos dados pessoais é uma das prioridades da LGPD.

A previsão legal aponta os princípios norteadores do tratamento dos dados pessoais, destacando a observância da boa-fé, assim como a finalidade, limites, garantia de segurança por meio de medidas de segurança, prestação de contas, transparência e possibilidade de consultas pelos titulares (PINHEIRO, 2018, p. 64).

A proteção de dados, bem como seu processo de coleta e tratamento, deve ser aplicada tanto para o setor público quanto para o privado. Na sua metodologia existe o titular (que é o detentor do direito); o controlador (a quem cabe tomar as decisões sobre o tratamento); e o operador (quem realiza, em nome do controlador, o tratamento dos dados). (CRAVO, 2020, p. 55).

O ponto central, no que se refere à proteção, se constitui no consentimento do titular, sendo previsto no artigo 8º da lei *supra* citada. O consentimento deve ser realizado na forma escrita ou de outro modo que comprove a manifestação de von-

tade do detentor do direito. Outrossim, o parágrafo 4º do artigo em tela não permite autorizações genéricas, em que não seja possível comprovar a expressão do consentimento. Destarte, demonstra-se necessário garantir e comprovar o expresse consentimento em relação ao uso dos dados pessoais, bem como esclarecer o fim para o qual tais informações serão utilizadas (LUGATI; ALMEIDA, 2020, p. 20).

Ressalta-se que caberá à instituição detentora dos dados a responsabilidade de demonstrar que houve consentimento do titular do direito. Além de que se faz imperiosa a transparência das informações do tratamento de dados, indicando as características relativas ao livre acesso à informação. Dessa forma, terá que ser clara a exposição e fácil o acesso, sendo importante a gratuidade de tais consultas (PINHEIRO, 2018, p. 65-66).

Assim o controlador terá que apontar a finalidade dos dados, assim como a autoridade nacional deverá garantir a emissão de documentos relativos ao tratamento e seus impactos (PINHEIRO, 2018, p. 69).

Os dados sensíveis deverão ser altamente protegidos, em respeito à sua natureza e características, pois em caso de violação os direitos e as liberdades fundamentais do indivíduo não estarão garantidos e sua má utilização poderá gerar problemas e graves danos (DONEDA, 2011, p. 98).

Ainda a LGPD dispõe que um dos requisitos de validade do tratamento de dados será o alcance de atuação do procedimento, ou seja, o tratamento não deve ser realizado por prazo indeterminado. Dessa forma, os prazos devem ser apurados em consonância com a finalidade do tratamento. Descrevendo ainda Pinheiro, que chegando ao fim, os dados devem ser apagados (PINHEIRO, 2018, p. 76-77).

Portanto, a garantia do acesso e de comunicação entre o titular e os agentes dos dados precisam ser claros, uma vez que se faz primordial o respeito aos princípios da transparência e da boa-fé.

4. A proteção de dados do empregado no teletrabalho

O aumento da adoção do regime de teletrabalho e a possibilidade de o empregado utilizar os meios informáticos para fins pessoais suscitam preocupações naturais com a segurança da informação, tanto sobre a confidencialidade para a empresa quanto em relação a privacidade e intimidade do empregado.

Nas relações de emprego, a coleta e o tratamento de dados pessoais são usuais, de tal maneira que ocorrem nas fases pré-contratuais, durante o contrato e pós-contratuais. Não obstante, o foco do trabalho diz respeito aos dados pessoais obtidos pelo empregador durante a relação de emprego, especificamente, no teletrabalho.

Nota-se que o desafio do empregador é claro, pois terá de compatibilizar a relação de trabalho, de uso de meios telemáticos, com a proteção legal de dados pessoais e da privacidade de seus empregados.

O empregador usualmente utiliza sistemas que permitem controlar e rastrear as atividades desempenhadas pelos tele empregados, tratam-se de *softwares* que permitem o armazenamento e o controle dos dados produzidos pelo trabalhador (MOCELIN; BRIANCINI, 2020), sendo possível, inclusive, controlar a quantidade

de toques, produção, horários, telefonemas, gravações, reuniões por videoconferência, imagem, enfim, todos os atos praticados pelo trabalhador (REIS, 2007).

Não é novidade o direito do empregador de monitorar o ambiente de trabalho com o intuito de modular a produtividade. Trata-se de uma das formas de o empregador exercer seu poder diretivo (BIONI, 2019, p. 239).

Ocorre que há casos em que há absoluta assimetria entre empregado e empregador e que não se vislumbra o consentimento do titular dos dados a fornecê-los (BIONI, 2019, p. 240).

Ressalta-se que o empregador tem acesso a questões de cunho privado do trabalhador em diversas oportunidades, já que os meios tecnológicos e a informática tornam a transmissão de dados mais rápida e fluída. Por meio da Internet é possível auferir com precisão o tempo de conexão, bem como quando foi o último acesso a dados e registros (ATTADAMO; LEITE, 2019, p. 13).

Diante da promulgação da LGPD, constata-se a necessidade da adaptação do empregador, principalmente ao que tange o teletrabalhador, uma vez que seu poder fiscalizatório poderá ser mitigado.

Otávio Pinto e Silva assevera que o empregador, além de ter dificuldade no controle das atividades do teletrabalhador, enfrenta a vulnerabilidade das dificuldades inerentes à tecnologia, já que a relação está exposta a panes, vírus, quedas de energia e divulgação de dados (SILVA, 2004, p. 128).

Nesse contexto, denota-se trazer à tona questões pertinentes ao monitoramento do trabalhador, principalmente quanto ao consentimento dele para tanto. Inclusive afirma Bioni:

[...] Por isso, no contexto europeu, a base legal do legítimo interesse tem sido a mais utilizada diante do alto risco de o consentimento obtido ser inválido. As maiores controvérsias dizem respeito ao quão intrusivas e necessárias são tais técnicas de monitoramento do ambiente de trabalho. Por exemplo: ii.a) monitoramento do tráfego da rede corporativa: em vez de analisar todo o tráfego de navegação dos empregados, uma medida tão ou mais efetiva não seria a adoção de filtros de determinados websites que prejudicariam a produtividade do trabalhador?; ii.b) key-logger e screenshots: a adoção de softwares que registram tudo o que é digitado pelo empregado, bem como fotografam, em um certo intervalo de tempo, as páginas visitadas não seria uma medida desnecessária para garantir a produtividade dos empregados? (BIONI, 2019, p. 240).

Nota-se que tais práticas podem ser aplicáveis ao teletrabalho, inclusive, com somatória de justificativas, uma vez que o empregado estará fora do ambiente físico do empregador, o que poderia reforçar a necessidade de controle por meio de *softwares*.

Não obstante, caso o empregador exerça alguma forma de controle ou monitoramento do teletrabalho, precisará se adequar à LGPD.

Assim fica a reflexão: é possível o empregador se utilizar de métodos legítimos para zelar pela produtividade do tele empregado sem que adentre a questões de dados pessoais, principalmente de cunho sensível?

Há doutrinadores que acreditam que sim, inclusive Bioni aponta algumas possibilidades:

[...] uma das questões centrais é informar ao empregado a que tipo de monitoramento está sujeito. Esse informe deve ocorrer antes do início da coleta dos dados, de modo a possibilitar eventuais questionamentos que podem ser feitos perante o próprio empregador ou por meio das entidades sindicais. Outra questão é verificar quais são as possíveis providências para minimizar os riscos ao titular dos dados. Por exemplo, se o empregador está em dúvidas se irá ou não filtrar determinados websites, decidindo, por isso, verificar com que frequência seus funcionários acessam redes sociais e outras aplicações para fins pessoais. Essa análise precisaria ser individualizada com relação a cada um dos empregados, ou se poderia fazer uma análise geral do tráfego de rede? (BIONI, 2019, p. 240).

Nesse contexto, nota-se que existem novas formas de controle passíveis de serem aplicados sem violar o sigilo dos dados pessoais e direitos fundamentais dos teletrabalhadores. Ademais, tal dilema não é de exclusividade brasileira, diversas nações já debateram o assunto, diante da globalização das informações.

A Europa já está mais familiarizada com a contenda e possui regulamentação mais sólida em torno da segurança da informação, apresentando limites em torno da proteção de dados pessoais do trabalhador. No Brasil, a LGPD não cita em seu texto relações trabalhistas, de forma específica, mas é patente que muitos dados dos trabalhadores são sensíveis, na forma da proposta legal.

Considerando o direito comparado, nota-se que doutrinadores portugueses já debatem o assunto há mais tempo, sugerindo, muitos deles, que as empresas empregadoras avaliem o impacto da proteção de dados pessoais, de modo a constatarem os riscos à privacidade que seus métodos de labor podem ocasionar. Ainda, que devem pensar em novas configurações de suas plataformas a garantir um maior controle de acessos e participações, bem como uma revisão da Política de Privacidade e Termos e Condições da empresa. Além de asseverar a impossibilidade de divulgações de cunho confidencial. Pontuam, por fim, que todas as deliberações devem ser divulgadas aos colaboradores, individualmente, por meio de circulares (HENRIQUES, 2020).

Ademais, em Portugal já existem orientações jurídicas nas quais os *softwares* empregados no teletrabalho para controle de desempenho não devem ser usados, uma vez que se corre o risco de adentrar dados de cunho pessoal e sensível do colaborador. Assim, grande parte das companhias portuguesas estão se adaptando por meio das culturas de *compliance* em matérias de privacidade e de segurança

(HENRIQUES, 2020).

Susana Isabel Pinto Ferreira dos Santos Gil afirma em sua tese de doutorado que os empregadores:

[...] deverão informar os trabalhadores sobre a legislação aplicável nesta matéria, assim como sobre as regras que vigoram na empresa referentes à proteção de dados, em concreto se há ou não qualquer restrição na utilização das tecnologias e quais as sanções para o incumprimento destas imposições. Um dos pontos mais importantes do acordo é sobre a privacidade, uma vez que se declara que a entidade empregadora deverá respeitar a privacidade do teletrabalhador. (GIL, 2015, p. 17).

O que se observa é que a Europa de forma geral pugna pelo respeito ao princípio da proporcionalidade, no que diz respeito ao controle de informações dos teletrabalhadores pelas empresas, inclusive, no que tange ao acesso a dados pessoais e sensíveis (GIL, 2015, p. 200).

Em respeito à relevância do tema, a OIT (Organização Internacional do Trabalho), em 1997, já havia aprovado o repertório de recomendações práticas em matéria de proteção de dados pessoais dos trabalhadores:

Os empregadores, os trabalhadores e seus representantes devem cooperar na proteção de dados pessoais e na elaboração de uma política de empresa que respeite a vida privada dos trabalhadores, de acordo com os princípios estabelecidos neste repertório.⁵⁶ (OIT, 1997).

Note-se que desde esta época a OIT já recomendava a implementação dos programas de *compliance*, com o intuito de garantir a proteção de dados. Ressalta-se o significado do termo *compliance*:

[...] à adesão da companhia a normas ou procedimentos de determinado setor. Seu objetivo primordial é o combate à corrupção. Diferentemente da ética, que é assumida com espontaneidade, o *compliance* está relacionado à responsabilidade legal [...]. Ser ético é agir voluntariamente com princípios morais para com a sociedade. Já *compliance* é cumprir com regras e regulamentos; é trabalhar ou agir dentro da lei. [...] Formado por leis, decretos, resoluções, normas, atos e

56 Tradução livre. Texto original da OIT: “Los empleadores, los trabajadores y sus representantes deberían cooperar en la protección de los datos personales y en la elaboración de una política de empresa que respete la vida privada de los trabajadores, con arreglo a los principios enunciados en el presente repertorio”.

portarias, o *compliance* é todo arcabouço regulatório aplicado pelas agências que controlam e regulam o setor no qual a empresa está inserida. As maiores e mais organizadas corporações também criam suas próprias normativas internas para direcionar o comportamento de seus diretores e executivos e, assim, coibir comportamentos negativos, desvios de conduta e inconformidades. (ANTONIK, 2016, p. 976-987).

Dentro desse contexto, observa-se que o Brasil está encaminhando para um viés de proteção de dados nas telecomunicações, sendo de grande importância a adoção de mecanismos de *compliance* que:

[...] consubstancia valioso instrumento desse viés operacional e preventivo, auxiliando na promoção de condutas compatíveis com a regulamentação legal. No âmbito da proteção de dados pessoais, [...] seja por seu inerente dinamismo, seja por haver diversas lacunas para se viabilizar o cumprimento dos preceitos legais, o papel das ações dos agentes econômicos robustece-se ainda mais. A implementação de boas práticas no tratamento de dados pessoais possui estrondoso potencial para auxiliar no atendimento aos comandos gerais da lei de acordo com as particularidades de determinados agentes econômicos, bem como prevenir a ocorrência de violações aos direitos dos titulares, na medida em que permite orientar os agentes de tratamento, traduzindo para suas atividades cotidianas as premissas principiológicas da LGPD e concretizando vários dos seus standards e conceitos abertos. (FRAZÃO; TEPEDINO; OLIVA, 2019, p. 682).

Nota-se que o empregador brasileiro possui meios concretos de se precaver e de se adequar às determinações legais de proteção dos dados dos seus empregados, inclusive, no caso de teletrabalho. Constata-se que o empregador, em respeito à Consolidação das Leis do Trabalho, Lei Geral de Proteção de Dados e Constituição de 1988, deve se orientar por princípios da prevenção e da segurança do trabalhador, assim como ao direito constitucional fundamental da privacidade, direito da personalidade e sobretudo a dignidade do seu trabalhador.

5. Considerações finais

O teletrabalho é uma realidade neste momento mundial e vem ganhando proporções cada vez maiores, tendo em vista a evolução tecnológica e social.

O avanço tecnológico é uma mola propulsora do desenvolvimento econômico e os dados pessoais das pessoas passam a ter grande relevância social e econômica,

sendo necessário o legislador normatizar limite em seu uso.

No contexto do direito do trabalho é usual o acesso do empregador aos dados pessoais do empregado, inclusive por meios tecnológicos, como no caso de uso de *softwares* de monitoramento no teletrabalho.

Considerando que os dados pessoais de um trabalhador não consistem apenas em aspirações profissionais, mas também em suas características culturais, sociais e privativas, a LGPD revela-se como uma importante ferramenta para garantir maior segurança aos trabalhadores em regime de teletrabalho, uma vez que obriga o responsável pelo tratamento dos dados a avaliar o impacto de suas operações, finalidade e metodologias a serem utilizadas.

Dessa forma, o empregador é o responsável por tomar as medidas necessárias para garantir a proteção dos dados utilizados pelo teletrabalhador. Nesse sentido, denota-se que o teletrabalhador deverá receber as informações necessárias sobre métodos de privacidade e segurança da informação.

Espera-se que com o respeito à LGPD pelo empregador, no que toca ao teletrabalho, ocorra a obtenção de maior grau de segurança jurídica, pois o dever do Direito do Trabalho é a valorização do trabalho, como propulsor da economia e do crescimento social do país.

REFERÊNCIAS

ANTONIK, Luís Roberto. **Compliance, ética, responsabilidade social e empresarial: uma visão prática**. Rio de Janeiro: ALTA Books, 2016.

ATTADEMO, Patrícia; LEITE, Kallen Souza. Teletrabalho: um olhar sobre o direito ao desenvolvimento econômico e ao meio ambiente equilibrado. **Revista de Constitucionalização do Direito Brasileiro**, v. 02, n. 1, p. 1-17, jan/jun. 2019.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: A Função e os Limites do Consentimento**. Rio de Janeiro: Forense, 2. ed., 2019.

BRASIL. **Decreto-Lei nº 5.452, de 1º de maio de 1943**. Aprova a consolidação das leis do trabalho. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 8 set. 2020.

BRASIL. **Lei 13.467, de 13 de julho de 2017**. Altera a Consolidação das Leis do Trabalho (CLT), aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, e as Leis nº 6.019, de 3 de janeiro de 1974, nº 8.036, de 11 de maio de 1990, e nº 8.212, de 24 de julho de 1991, a fim de adequar a legislação às novas relações de trabalho. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13467.htm. Acesso em: 8 set. 2020.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 8 set. 2020.

CRAVO, Daniela Copetti. Direito do titular dos dados no poder público: análise da portabilidade de dados. **Revista da ESDM**, v. 6, n.11, p. 51-61, 2020.

DELGADO, Maurício Godinho. **Curso de Direito do Trabalho**. 18. ed. São Paulo: Ltr, 2019.

DELGADO, Mauricio Godinho; DELGADO, Gabriela Neves. **A reforma tra-**

balhista no Brasil: com os comentários à Lei n. 13.467/2017. São Paulo: LTr, 2017.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 02, p. 91-108, 2011.

DRUMMOND, Victor. **Internet, privacidade e dados pessoais**. Rio de Janeiro: Editora Lumen Juris, 2003.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. Barra Funda: Revista dos Tribunais, 2019.

GIL, Susana Isabel Pinto Ferreira dos Santos. **As perspectivas civis do contrato de trabalho - o teletrabalho subordinado: seu estudo nos Ordenamentos jurídicos português e espanhol**. Tese de doutorado, Universidade da Coruña, 2015.

GUNTHER, Luiz Eduardo. **Direito da personalidade nas relações de trabalho contemporâneas**. Curitiba: Instituto Memória – Centro de Estudos da Contemporaneidade, 2014.

HENRIQUES, Ricardo. Novo paradigma de teletrabalho, acrescidos desafios à proteção de dados. **Advocatus**. 2020. Disponível em: < <https://eco.sapo.pt/opiniaao/novo-paradigma-de-teletrabalho-acrescidos-desafios-a-protecao-de-dados/> > Acesso em: 5 mai. 2020.

LIMA, Thomires Elizabeth Pauliv Badaró de; MACIEL-LIMA, Sandra. *Assédio moral e a dignidade da pessoa humana: os limites do poder do empregador*. In: ANDRADE, Everaldo Gaspar Lopes de; SILVA, Luciana Aboim Machado Gonçalves da; MISAILIDIS, Mirta Gladys Lerená Manzo de (coords.) **Direito do trabalho e meio ambiente do trabalho I**. Florianópolis: CONPEDI/UnB/UCB/ IDP/UDF, 2016, p. 143-159.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. *Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa*. **Revista de Direito**, v. 12, n. 02, p. 01-33, 2020.

MAÑAS, Christian Marcello. A externalização da atividade produtiva: o impacto do teletrabalho na nova ordem socioeconômica. **Revista da Faculdade de Direito da Universidade Federal do Paraná**, v. 39, p. 121-139, 2003.

MARTINEZ, Luciano. **Curso de direito do trabalho: relações individuais, sindicais e coletivas do trabalho**. São Paulo: Saraiva Educação, 2019.

MELO, Sandro Nahmias. **Meio Ambiente do Trabalho: Direito Fundamental**. São Paulo: LTr, 2001.

MOCELIN, Juliana Boscarin; BRIANCINI, Valkiria. *Teletrabalho: Implicações nos direitos fundamentais à intimidade e vida privada do empregado*. **IMED**. Disponível em: [https://www.imed.edu.br/Uploads/valkiriabriancini2\(%-C3%A1rea3\).pdf](https://www.imed.edu.br/Uploads/valkiriabriancini2(%-C3%A1rea3).pdf). Acesso em: 8 set. 2020.

ORGANIZAÇÃO INTERNACIONAL DO TRABALHO (OIT). *Protection of workers' personal data: an ILO code of practice*, 1997. Commentary on the Code of Practice. Disponível Em: <https://www.ilo.org/wcmsp5/groups/pu->

blic/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf. Acesso em: 8 set. 2020.

PEDREIRA, Pinho Luiz de. **O teletrabalho**. São Paulo: LTr, v. 64, n. 5, 2000, p. 583-597.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

REGIS, Erick da Silva. Linhas gerais sobre a Lei 13.709/2018 (LGPD): Objetivos, fundamentos e axiologia da Lei Geral de Proteção de Dados Brasileira e a Tutela de Personalidade/Privacidade. **Revista de Direito Privado**, v. 103, p. 63-100, fev. 2020.

REIS, Jair Teixeira dos. **Subordinação Jurídica e o Trabalho à Distância**. São Paulo: LTr, 2007.

ROCHA SANTOS, Michel Carlos. O teletrabalho nos tempos da COVID 19 (CORONAVÍRUS): ensaio sobre a importância e necessidade de proteção aos trabalhadores. **Revista do TST**, São Paulo, v. 86, n. 2, p. 175-194, abr/jun. 2020.

RODRIGUES, Ana Cristina Barcellos. **Teletrabalho**: A tecnologia transformando as relações de trabalho. Dissertação de Mestrado em Direito, Universidade de São Paulo, São Paulo, 2011.

SANTOS, Ana Luiza Liz dos. Lei Geral de Proteção de Dados: um estudo comparativo em relação à efetividade dos direitos fundamentais. **Revista dos Tribunais**, v. 1013, p. 105-106, mar. 2020.

SILVA, Otavio Pinto e. **Subordinação, autonomia e parassubordinação nas relações de trabalho**. São Paulo: LTr, 2004.

OLEDO FILHO, Manoel Carlos. O teletrabalho na perspectiva da reforma trabalhista brasileira e do direito comparado. **Teletrabalho e a Reforma Trabalhista**, Curitiba, v. 8, n. 75, p. 21, fev. 2019.

21. A PROTEÇÃO AOS DADOS PESSOAIS E SENSÍVEIS DO TRABALHADOR COMO DIREITO FUNDAMENTAL

THE PROTECTION OF WORKERS' PERSONAL AND SENSITIVE DATA AS A FUNDAMENTAL RIGHT

BEATRIZ DE FELIPPE REIS⁵⁷

Resumo

Os dados pessoais e sensíveis, como um direito fundamental do trabalhador brasileiro, merecem especial atenção no ambiente laboral, principalmente em razão do uso intensivo de novas tecnologias por parte do empregador no exercício do poder de controle e de fiscalização. Diante desse cenário, por meio da análise da doutrina e da legislação relativas ao tema, a primeira parte do artigo abordou os principais princípios que norteiam o tratamento dos dados e a forma como eles podem ser aplicados nas relações laborais a fim de assegurar aos trabalhadores uma proteção adequada e, na sequência, foi examinada a teoria dos direitos fundamentais como fonte de proteção.

Palavras-chave: Direitos fundamentais. Proteção de dados. Trabalhador.

Abstract

Personal and sensitive data, as a fundamental right of Brazilian workers, deserve special attention in the labor environment, especially due to the intensive use of new technologies by the employer in the exercise of the power of control and supervision. In this scenario, by analyzing the doctrine and legislation on the subject, the first part of the article addressed the main principles that guide the treatment of data and how they can be applied in labor relations in order to assure workers adequate protection, and then the theory of fundamental rights as a source of protection was examined.

Key words: Fundamental rights. Data Protection. Worker.

1 INTRODUÇÃO

A concepção da proteção dos dados pessoais e sensíveis como um direito humano fundamental vem ganhando projeção no cenário jurídico. A preocupação em torno dos dados tem aumentado consideravelmente em decorrência do avanço tecnológico observado nas últimas décadas. A disponibilização, o tratamento e a combinação de informações tornam-se cada vez mais intensos, a ponto de resultar em uma sociedade gradativamente orientada por dados.

Na atualidade, as questões envolvendo violação da privacidade, da intimidade

⁵⁷ Mestra em Direito pelo Programa de Pós Graduação em Direito pela UNESC. Especialista em Direito do Trabalho pela UNISINOS. Graduada em Ciências Jurídicas e Sociais pela UFRGS. Analista Judiciário do TRT4ª Região. Membro do CIELO LABORAL. bialippe@hotmail.com.

e dos dados são progressivamente presentes. Paralelo a isso, no âmbito das relações laborais, os riscos aos direitos e liberdades fundamentais dos trabalhadores são crescentes.

Nesse contexto, ganha relevo o tema da proteção aos dados pessoais e sensíveis, essencial para a proteção humana da pessoa-trabalhadora, como um novo direito fundamental que garante aos seus titulares a capacidade de dispor de seus dados e controlar o uso que deles é feito.

Diante disso, neste artigo, serão abordados os principais princípios que norteiam o tratamento dos dados e de que forma eles podem ser aplicados nas relações laborais a fim de assegurar aos trabalhadores uma proteção adequada e, por fim, será desenvolvido o tema da proteção aos dados como um direito fundamental da pessoa-trabalhadora, na medida em que seus dados configuram expressão direta da própria personalidade.

2. Os princípios fundamentais do tratamento de dados e sua aplicação na relação do trabalho

A realidade aponta para a existência de uma desproporção entre os efeitos das novas tecnologias e a mudança de paradigma marcada pelo emergir da informação como recurso fundamental para a organização do futuro. As transformações são imensas, a ponto de os ordenamentos jurídicos não acompanharem tal velocidade. As técnicas tradicionais parecem insuficientes.

Em matéria de proteção de dados, há alguns documentos representativos do que já se encontra consolidado e do que está emergindo. “A atenção deve ser dirigida, por um lado, para os princípios que são afirmados; e, por outro, aos instrumentos necessários para assegurar a sua efetividade.” (RODOTÀ, 2008, p. 59).

Assim, como forma de acompanhar a transformação vivenciada, em termos de proteção de dados utilizam-se dois textos de relevância internacional: a Convenção do Conselho da Europa (de 28 de janeiro de 1981, para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal), e a Recomendação da OCDE (de 23 de setembro de 1980, que traça as diretrizes relativas à proteção da privacidade e dos fluxos transfronteiriços de dados pessoais), a partir das quais são deduzidos diversos princípios, como os que seguem:

1. *princípio da correção* na coleta e no tratamento das informações;
2. *princípio da exatidão* dos dados coletados, acompanhado pela obrigação de sua atualização;
3. *princípio da finalidade* da coleta dos dados, que deve poder ser conhecida antes que ocorra a coleta, e que se especifica na relação entre os dados colhidos e a finalidade perseguida (*princípio da pertinência*); na relação entre a finalidade da coleta e a utilização dos dados (*princípio da utilização não-abusiva*); na eliminação, ou na transformação em dados anônimos das informações

que não são mais necessárias (*princípio do direito ao esquecimento*);

4. *princípio da publicidade* dos bancos de dados que tratam as informações pessoais, sobre os quais deve existir um registro público;

5. *princípio do acesso individual*, com a finalidade de conhecer quais são as informações coletadas sobre si próprio, obter a sua cópia, obter a correção daquelas erradas, a integração daquelas incompletas, a eliminação daquelas coletadas ilegitimamente;

6. *princípio da segurança* física e lógica da coletânea dos dados. (RODOTÀ, 2008, p. 59).

Muitos desses princípios, já presentes no ambiente europeu, foram incorporados na Diretiva da Comunidade Europeia nº 95/46 de 1995 e na Carta de Direitos Fundamentais da Comunidade Europeia de 2000, servindo, posteriormente, de base para a criação do RGPD, o qual corresponde a uma normativa pautada por princípios e regras no âmbito da União Europeia.

A escolha brasileira, por seu turno, aproximou-se do modelo europeu, privilegiando uma legislação por princípios, o que se identifica a partir da redação do artigo 6º da Lei nº 13.709/2018, segundo o qual as atividades de tratamento de dados pessoais, além de observar a boa-fé, devem se pautar pelos princípios da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção, da não discriminação e da responsabilização e prestação de contas.

Portanto, em matéria de proteção de dados pessoais e sensíveis, as soluções devem passar, como propõe Rodotà (2008, p. 10):

[...] por uma legislação de princípios e códigos de deontologia – contando estes com a participação direta das categorias profissionais interessadas, que assim melhor podem assegurar a correspondência à realidade do setor – reunida com a finalidade de realizar uma disciplina equilibrada relativamente às mudanças sociais.

Diante disso, cabe analisar, à luz do artigo 6º da Lei nº 13.709/2018 e da doutrina especializada, os princípios gerais de proteção que deverão ser observados quando da realização do tratamento de dados pessoais e de que forma eles podem ser aplicados na relação de trabalho, a fim de assegurar uma proteção adequada aos dados dos trabalhadores.

O primeiro relaciona-se ao *princípio da boa-fé*. Trata-se de um princípio geral de Direito que orienta a conduta das partes, tendo como funções interpretar os negócios jurídicos (artigo 113 do Código Civil) e limitar o exercício de um direito (artigos 187 e 422 do Código Civil). Tal princípio, além de ser um dos vetores

da relação de trabalho⁵⁸, aplica-se aos dados pessoais, na medida em que quem recolhe dados de outrem, trata ou mantém sob sua custódia tem o dever ético de agir com correção, honestidade, confiança e lealdade, não podendo, em seus atos, ultrapassar os limites impostos por este valor. (CHEHAB, 2015). Assim, por força deste princípio:

[...] a entidade empregadora deve – antes de iniciar o tratamento – informar o trabalhador sobre as condições de utilização dos meios da empresa para fins privados e a realização do seu controlo (formas e metodologias adotadas), sobre a existência do tratamento de dados que lhe está associado, suas finalidades, os dados tratados e o seu tempo de conservação, bem como sobre o grau de tolerância admitido e as consequências da má utilização ou utilização indevida dos meios de comunicação colocados à sua disposição. (CNPD, 2013, p. 11).

O *princípio da finalidade* determina que o tratamento de dados deve ser feito “para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.” (BRASIL, Lei nº 13.709, de 14 de agosto de 2018). A propósito, Doneda (2006, p. 216) dispõe que:

[...] toda utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da sua coleta. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que é possível a estipulação de um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade).

No campo laboral, o Repertório de Recomendações da OIT (OIT, 1997) dispõe que os dados pessoais devem ser utilizados apenas para a finalidade para os quais foram coletados e, havendo exploração para outros fins, o empregador deve garantir que eles não sejam usados de forma incompatível com o objetivo inicial e adotar medidas necessárias para evitar qualquer má interpretação devido a sua aplicação em outro contexto.⁵⁹

58 Importante notar que “todas as conclusões do direito civil sobre boa-fé nos contratos são aplicáveis ao direito do trabalho. É uma decorrência do princípio da eticidade nos contratos, o que não é reserva do direito civil, mas uma ideia básica comum aos contratos em qualquer setor do direito. O comportamento dos sujeitos dos contratos de trabalho deve respeitar um conjunto de deveres previstos pelo direito positivo, tanto o empregado como o empregador, e boa-fé tanto no período pré-negocial como na constância de contratos e na fase da extinção dos contratos, e o comportamento que contrariar o princípio estará em desacordo com o direito.” (NASCIMENTO, 2011, p. 578).

59 Na visão de Moreira (2016, p. 45-46), o princípio da finalidade “constitui o princípio verdadeira-

O *princípio da adequação* estabelece que deve haver “compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.” (BRASIL, [Lei nº 13.709, de 14 de agosto de 2018](#)).

Com relação ao *princípio da necessidade*, a Lei nº 13.709/2018 dispõe tratar-se de “limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.” (BRASIL, [Lei nº 13.709, de 14 de agosto de 2018](#)).

Já o *princípio do livre acesso* garante aos titulares “consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.” Junto deste, há o *princípio da qualidade dos dados* que estabelece a “garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.” E, em igual sentido, há o *princípio da transparência*, que garante, aos titulares, “informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.”⁶⁰ (BRASIL, [Lei nº 13.709, de 14 de agosto de 2018](#)).

No ambiente laboral, o Repertório de Recomendações Práticas da OIT (OIT, 1997) assegura aos trabalhadores o direito a serem informados regularmente sobre os dados pessoais que lhes dizem respeito e sobre seu tratamento, independentemente destes dados estarem sujeitos a processamento automático ou mantidos em um arquivo manual ou em qualquer outro arquivo que inclua seus dados pessoais.

Há, ainda, o *princípio da segurança*, o qual determina que sejam utilizadas “medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.” Reforçando tal diretriz, o *princípio da prevenção* estabelece a “adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.” (BRASIL, [Lei nº 13.709, de 14 de agosto de 2018](#)).

Refere-se, ainda, o *princípio da não discriminação* que firma a “impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.” (BRASIL, [Lei nº 13.709, de 14 de agosto de 2018](#)). Trata-se de um princípio de extrema importância para a seara laboral, uma vez que o tratamento dos dados não deve conduzir a uma discriminação ilícita em matéria de emprego ou ocupação. No tocante, o próprio Repertório (OIT, 1997) reforça este princípio geral de não discriminação em emprego, substancial para evitar que o uso de dados pessoais e sensíveis comporte, direta ou indiretamente, a discriminação contra pessoas ou grupos de trabalhadores.

mente cardinal da proteção de dados, sendo os demais princípios função deste na medida em que os dados devem ser adequados, pertinentes e não excessivos em relação à finalidade pretendida; devem ser exatos, completos e atualizados em função da finalidade; e só devem ser conservados pelo tempo que a finalidade exige.”

⁶⁰ Um exemplo de aplicação prática do princípio da transparência consiste em levar ao conhecimento do trabalhador ou de seus representantes a existência de um sistema de vigilância e de controle pelo empregador, sendo isso essencial para o tratamento de dados pessoais. Além disso, o controle oculto ou secreto sobre os trabalhadores através de meios audiovisuais viola o princípio da boa-fé empresarial, como destaca Moreira (2016).

Além disso, dada a relevância do tema, a Declaração da OIT sobre os Princípios e Direitos Fundamentais no Trabalho (OIT, 1998) prevê como um de seus princípios *a eliminação da discriminação em matéria de emprego e ocupação*. Menciona-se, também, a existência da Convenção nº 111 e a Recomendação nº 111, ambas da OIT, as quais proíbem tal discriminação, assim como, em âmbito nacional, o artigo 3º, inciso IV, e o artigo 7º, incisos XXX, XXXI e XXXII, ambos da Constituição Federal.

E, por último, o *princípio da responsabilização e da prestação de contas*, o qual consiste na “demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.” (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Assim, tal arcabouço principiológico, além de orientar as atividades que envolvem o tratamento de dados pessoais, servem como guia para o processamento na área trabalhista, observadas as particularidades que tal relação envolve.

Nesse sentido, haverá casos em que mesmo dados pessoais sensíveis deverão ser de conhecimento do empregador. Em tais situações, havendo dúvidas quanto à existência de legítimo interesse por parte de quem os trata, o balanceamento de direitos, amparado em princípios, permitirá verificar se as legítimas expectativas e os direitos e liberdades fundamentais do trabalhador estão sendo respeitados.

Não obstante, vale mencionar que o Repertório de Recomendações Práticas da OIT ilustra alguns casos em que, apesar da sensibilidade de alguns dados, nem sempre é possível descartar pura e simplesmente a sua coleta. Nesse ponto, o Repertório (OIT, 1997) exemplifica a situação envolvendo a contratação de um jornalista para trabalhar em jornal afiliado a um determinado partido político, caso em que é preciso levar em consideração as ideias políticas do profissional. Na hipótese, o fato de os dados serem sensíveis não é suficiente para excluí-los da tarefa de coleta, porém é preciso respeitar certos princípios, a fim de compensar a posição mais vulnerável dos trabalhadores.

Dessa forma, o Repertório apresenta uma série de situações nas quais o recolhimento de dados só deve ser autorizado em caráter excepcional e apenas quando tenham relação direta com uma decisão em matéria de emprego. Trata-se de hipóteses em que a coleta deve ser feita em conformidade com a legislação nacional, com as leis contra a discriminação ou com os regulamentos sobre o tratamento de dados sensíveis, compreendidos nas leis nacionais.

Feitas tais considerações, analisa-se as hipóteses previstas no Repertório. A primeira delas diz respeito aos dados referentes à vida sexual dos trabalhadores.⁶¹ Segundo o Repertório, estes dados podem ser obtidos quando houver uma acusação de assédio sexual, devendo ser utilizados apenas para este fim.

Quanto aos antecedentes criminais, por se tratar de um dado potencializador

61 No que tange ao aspecto sexual, é preciso lembrar que a orientação sexual configura um dado pessoal sensível do trabalhador, o qual, se objeto de questionamento ou de revelação, pode conduzir a situações de assédio e de discriminação no ambiente de trabalho. Além disso, vale lembrar que o novel artigo 223-C da CLT inclui a sexualidade como um dos bens jurídicos tuteláveis, inerente à pessoa física. (BRASIL. Decreto-Lei nº 5.452, de 1º de maio de 1943).

de discriminação do empregado, a coleta deve limitar-se a alguns circunstâncias, como, por exemplo, quando envolve cuidado de filhos, pois o candidato pode ter sido condenado por molestar uma criança, ou, no caso de motorista profissional, este deve divulgar as penalidades criminais a que submetido por dirigir em estado de embriaguez. Segundo o Repertório da OIT, este tipo de dado deve ser obtido diretamente do interessado, para ter certeza de que a coleta não vá além do necessário.

Em relação à filiação sindical, as empresas podem coletar dados apenas para cumprir as disposições relativas à dedução da contribuição sindical ou para facilitar o funcionamento das comissões de empresa, por exemplo. A legalidade desta coleta decorre da própria norma trabalhista, na medida que cabe aos empregadores informarem aos representantes dos trabalhadores tais questões. Da mesma forma, os representantes devem manter todo o tipo de precaução para impedir que as informações caiam nas mãos de terceiros não autorizados a conhecê-las. Parte superior do formulário

E quanto à coleta de dados médicos, deve se restringir ao necessário para determinar se o trabalhador é apto para um trabalho específico, para cumprir as regras de segurança e saúde no trabalho e para ter direito a benefícios sociais, sob pena de haver uma utilização prejudicial da informação, a ponto de a empresa criar uma situação de desigualdade, como no exemplo trazido por Limberger (2009, p. 43-44):

No que se refere à saúde, um portador do vírus HIV pode não ser contratado em virtude da doença ou ser despedido. A possibilidade de a empresa escolher um trabalhador sadio, no momento da contratação, é muito grande, o que caracterizaria uma discriminação.

Por isso, salvo em um número restrito de atividades profissionais pode ser pedido o exame de HIV, ou seja, aqueles em que o empregado realiza uma atividade que, se for portador da enfermidade, pode causar um contágio. Há de se ponderar a proteção individual do trabalhador com o perigo de expor a saúde da coletividade.

Com relação ao tema, para evitar que os dados pessoais do trabalhador, em especial, os dados sensíveis sejam utilizados para fins discriminatórios, o Repertório de Recomendações da OIT propõe nas cláusulas 10.8 e 10.9 que o empregador não tenha acesso direto aos resultados dos exames, mas tão somente à indicação da aptidão ou não do trabalhador para realizar a atividade proposta, ou ainda, a indicação dos tipos de trabalhos que, temporária ou definitivamente, lhe estão contraindicadas.

Atenta-se, também, para o fato de que as informações inerentes a cada trabalhador são manipuladas pelo empregador ou por prepostos, havendo a necessidade da instituição de marcos regulatórios específicos e adequados, bem como de políticas e procedimentos que garantam a segurança dos dados, por meio da implementação de mecanismos de mitigação dos riscos adotados, sob pena de

responsabilização das empresas.

Assim, além da criação de mecanismos para salvaguardar os dados pessoais no ambiente de trabalho, especialmente na perspectiva preventiva, é preciso enfrentar a proteção aos dados como um novo direito fundamental do trabalhador, o qual deve ter conhecimento e controle sobre seus próprios dados, visto que representam expressão direta de sua própria personalidade, questão esta a ser abordada no tópico seguinte.

3. A proteção dos dados pessoais e sensíveis como direito fundamental do trabalhador

Com a expansão da realidade digital, os direitos fundamentais, especialmente a privacidade, a intimidade e os dados pessoais e sensíveis do trabalhador encontram-se ainda mais expostos. Em decorrência disso, a própria noção de privacidade passou por uma releitura: o notório conceito do “direito a ficar só” ou “direito a ser deixado em paz” já não atende aos atuais anseios sociais, estando superado, nascendo, assim, a privacidade como “direito à autodeterminação informativa”, que concebe a cada pessoa um real poder de controle sobre suas próprias informações, seus próprios dados.

Assim, com as transformações advindas, houve a evolução do conceito de privacidade como “o direito a ser deixado em paz” para a perspectiva de “controle sobre as próprias informações”. O sentido de isolamento inicialmente existente já não atendia aos novos desafios, a noção de privacidade passava a exigir uma concepção mais ampla:

[...] no direito ao respeito à vida privada e familiar manifesta-se, sobretudo, o momento individualista e o poder exaure-se substancialmente na exclusão da interferência de outrem; a tutela, portanto, é estática e negativa. Já a proteção dos dados pessoais, ao contrário, fixa regras sobre a modalidade de tratamento dos dados e concretiza-se em poderes de intervenção; a tutela é dinâmica, segue os dados em sua circulação. (RODOTÀ, 2008, p. 8).

Nesse sentido, a ampliação do conceito de privacidade decorre:

[...] em grande medida, por conta da evolução das formas de divulgação e apreensão de dados pessoais. Com o advento de novas tecnologias, notadamente o desenvolvimento da biotecnologia e da Internet, o acesso a dados sensíveis e, conseqüentemente, a sua divulgação, foram facilitados de forma extrema. Como resultado, existe uma expansão das formas potenciais de violação da esfera privada, na medida em que se mostra a facilidade por meio da qual é possível o acesso não autorizado de terceiros a

esses dados. Com isso, a tutela da privacidade passa a ser vista não só como o direito de não ser molestado, mas também como o direito de ter controle sobre os dados pessoais e, com isso, impedir a sua circulação indesejada. (BODIN DE MORAES, 2018, p. 42).

Tomando como base essa nova perspectiva, Bodin de Moraes (2018, p. 52-57) ainda elenca a existência de três diferentes concepções sobre o direito à privacidade:

(i) O direito a ser deixado só, em acepção originária, tradicional, e referenciada a um período de liberalismo político e econômico, que direcionava a proteção da privacidade a um ideal burguês de tutela patrimonial; (ii) O direito de ter controle sobre a circulação dos dados pessoais, determinado por meio da construção teórica e jurisprudencial da denominada autodeterminação informativa, estabelecendo a prerrogativa da pessoa de acessar, corrigir, controlar e disponibilizar dados pessoais, somente por sua livre escolha; e (iii) O direito à liberdade das escolhas pessoais de caráter existencial, representando a ligação entre a autonomia existencial da pessoa e a construção de sua identidade pessoal por meio da proteção de seus dados sensíveis – i.e. posição política, expressão partidária, afiliação sindical, opção sexual, condições de saúde etc (dignidade).

Além disso, tal evolução confere uma supervisão e poderes não somente às pessoas interessadas (os sujeitos dos dados), mas também a uma autoridade independente. “A proteção não é mais deixada somente aos sujeitos dos dados, uma vez que existe um órgão público permanente responsável por isso. Logo, há uma redistribuição de poderes sociais e legais se formando.” (RODOTÀ, 2008, p. 17).

Por outro lado, os usuários podem limitar o fluxo de dados que liberam ou compartilham no âmbito das múltiplas relações sociais das quais participam. Contudo, tal medida, por si só, não é suficiente para protegê-los de eventuais danos aos seus direitos fundamentais de personalidade.

Em um mundo digitalizado, a expansão do volume de conteúdo multimídia, juntamente com *smartphones* e mídias sociais, desempenha expressivo papel na coleta de dados pessoais. Logo, é preciso entender como estes afetam a vida dos usuários. A dignidade das pessoas está em risco. Daí a importância de a proteção aos dados pessoais e sensíveis serem compreendidos como um novo direito fundamental tutelado pelo Estado.

Nesse sentido, Bioni (2019, p. 92) defende a proteção dos dados como uma categoria autônoma dos direitos da personalidade:

[...] o direito à proteção dos dados pessoais reclama uma normatização própria que não pode ser reduzida a uma mera “evolução” do direito à privacidade, mas encarada como um novo direito da personalidade que percorre, dentre outras liberdades e garantias fundamentais, a liberdade de expressão, de acesso à informação e de não discriminação. Em última análise, trata-se da nossa própria capacidade de autodeterminação.

Reconhecer que as pessoas vivem em um mundo globalizado e interconectado, no qual os dados circulam pelo mundo virtual sem se submeterem aos tradicionais controles e limites democrático-territoriais é o primeiro passo. A partir daí, necessário se faz repensar o papel do Estado-nação no controle dos fluxos globais de dados, pois, como alerta Ruaro e Rodriguez (2010, p. 165), “a solução para este problema global não poderá ser encontrada isoladamente, senão em conjunto com todas as culturas e sociedades”, caso contrário haverá uma vulneração ainda maior na proteção aos direitos fundamentais, isso porque:

[...] os modelos de direito e de Estado vigentes demonstram pouca – ou nenhuma – capacidade para lidar com conflitos que envolvem as novas tecnologias, intrinsecamente desespacializadas. Não se trata, aqui, de propor o fim do Estado, mas, pelo contrário, de reconhecer que a coleta e o processamento de dados pessoais são questões de relevância pública que escapam, em grande parte, ao controle estatal. Em vez da clássica *quis custodiet ipsos custodes?*, deve-se perguntar qual a legitimidade democrática das categorias em que os indivíduos são classificados. Somente mediante a democratização e a transparência desses critérios será possível proteger os direitos fundamentais, ou seja, tornar-se-á as relações de (in)visibilidade mais visíveis. (BOLZAN DE MORAIS; JACOB NETO, 2018, p. 88).

Partilhando de semelhante sentimento, Bodin de Moraes (2018, p. 77) aduz que:

[...] dói reconhecer o descompasso entre a rapidez do progresso tecnológico e a lentidão da capacidade de elaboração de instrumentos jurídicos que moldurem essa nova realidade. Com base nesta constatação, é preciso pensar remédios institucionais mais adequados (políticas regulatórias, por exemplo), na medida em que os remédios jurídicos existentes (normas jurídicas proibitivas) encontram-se engessados, obsoletos ou fadados à obsolescência, na medida em que a tecnologia vai se aprimorando e evoluindo.

Para enfrentar o fenômeno informático que atua com extrema velocidade, desafiando o ritmo mais lento com o qual atuam os operadores do direito, Limberger (2009) propõe uma reaproximação da normatividade dos princípios. Segundo a autora (2009, p. 34), “de longo tempo os princípios estão no direito, a novidade é sua estatuição constitucional.” Apoiando-se nisso, propugna:

[...] uma construção ou uma leitura dos direitos fundamentais com base nos valores superiores do ordenamento jurídico: a liberdade, a justiça, a igualdade e o pluralismo político, bem como na dignidade da pessoa, na perspectiva do fenômeno informático. A informática atuando a serviço do homem, e não como restritiva dos direitos fundamentais. (LIMBERGER, 2009, p. 34).

Assim, a necessidade de proteção aos dados pessoais e sensíveis provocou o surgimento de um novo eixo no que tange à tutela da privacidade, uma vez que o seu titular deseja manter um controle exclusivo sobre o conjunto de ações privadas que lhe dizem respeito (comportamentos, preferências e opiniões). Tal tutela há de basear-se em um novo “direito à autodeterminação informativa”, atualmente presente em diversos ordenamentos⁶², que estabelece condições para um efetivo controle das informações pessoais em circulação.⁶³ (DONEDA, 2000).

Essa mudança de enfoque, que culminou na concretização da proteção de dados pessoais como direito fundamental da pessoa humana, é resultado das mudanças sociais ocorridas durante os séculos 20 e 21. Com o fortalecimento e ampliação da sociedade industrial e, conseqüentemente, da de consumo, que se deu, especialmente, a partir de meados do século 20, os dados pessoais passaram a ter importância ímpar e valor econômico, em razão, principalmente, do surgimento das relações massificadas, seja de consumo ou de trabalho. Surgiram, a partir de então, empresas especializadas em recolhimento e tratamento de dados pessoais para posterior venda a interessados, o que veio a causar inúmeros prejuízos às pessoas diretamente envolvidas e também à coletividade. A decisão do Tribunal Constitucional Alemão, datada de 1983, foi, de certa forma, uma imposição de limites a tais

62 Mencionam-se as Constituições de Portugal e Espanha.

63 Murcia e Cardo (2019) destacam que, embora o surgimento de um novo direito possa levar ao surgimento de novas frentes regulatórias, estas não precisam ser exclusivamente protetivas. Segundo os autores, regular o “tráfego” de dados pessoais por meio de canais capazes de garantir, ao mesmo tempo, a proteção adequada das pessoas afetadas e o legítimo exercício das atividades de nossa vida é fundamental, pois sem acesso a dados pessoais seria muito difícil o desenvolvimento não apenas das relações econômicas e comerciais, mas também de outras facetas da realidade social, muitas delas ligadas a direitos básicos ou fundamentais para o nosso modo de vida.

práticas invasivas e danosas a direito fundamental. (STIVAL, 2015, p. 131).

No sistema europeu vige o entendimento de que o direito à proteção de dados pessoais é direito fundamental autônomo, digno, por si só, de todos os atributos e prerrogativas concernentes aos direitos fundamentais.

No Brasil, em 2018, houve a aprovação da lei geral em matéria de proteção de dados. A propósito do tema, recentemente o Plenário do Senado Federal aprovou a Proposta de Emenda à Constituição (PEC) nº 17, de 2019, que inclui expressamente no texto constitucional o direito à proteção de dados pessoais.

Assim, entre nós, até então a proteção dos dados pessoais ainda não constituía categoria de direito independente e autônomo do direito à privacidade ou ao segredo das comunicações, o que demonstrava certo atraso legislativo na maneira de conduzir a proteção à pessoa.

Segundo Bioni (2019, p. 98), “o direito à proteção de dados pessoais angaria autonomia própria. É um novo direito da personalidade que não pode ser amarrado a uma categoria específica, em particular ao direito à privacidade”, ou seja:

O direito à proteção dos dados pessoais deve ser alocado como uma nova espécie do rol aberto dos direitos da personalidade, dando elasticidade à cláusula geral da tutela da pessoa humana. Caso contrário, corre-se o risco de ele não se desprender das amarras conceituais e da dinâmica do direito à privacidade e, em última análise, inviabilizar uma normatização própria para regular o fluxo informacional como fator promocional da pessoa humana. (BIONI, 2019, p. 100).

Contundo, cabe salientar que muito mais importante do que haver a inclusão expressa no texto constitucional da proteção de dados pessoais como um direito fundamental autônomo, é que esta proteção seja observada e garantida, mediante a adoção de medidas adequadas e específicas para salvaguardar tal direito.

Avançando para o campo das relações laborais, estas constituem campo propício para a coleta de dados e informações pessoais do trabalhador. Logo, mesmo neste ambiente, a necessidade de proteção aos dados do titular permanece, não se limitando à esfera doméstica, sendo imprescindível compreender a noção de proteção de dados como direito fundamental do trabalhador.

Até porque não se pode esquecer que o empregado, quando ingressa na relação laboral, traz consigo a condição de pessoa humana titular de direitos fundamentais. Nessa perspectiva:

[...] a pessoa do trabalhador conjuga os predicados da pessoa que trabalha, que produz trabalho, de modo indissociável e inseparável, portanto, da qualidade ser pessoa humana – esta, inerente a ele. A relação jurídica que

envolve os direitos da personalidade alicerça-se a partir da concepção do Direito tendo em primeiro plano a proteção da própria pessoa, do homem. [...] É o elemento humano, como se vê, que justifica a progressividade dos bens tutelados pelos direitos da personalidade, assim considerando todos aqueles que tenham fundamento de existência na preservação da pessoa humana, tal como acontece com a proteção da privacidade da pessoa, ainda que inserida em contexto de relação de emprego. (WEINSCHENKER, 2013, p. 23 e 27).

Portanto, as ações do empregador devem estar pautadas pelo equilíbrio e respeito aos direitos fundamentais da personalidade dos trabalhadores, dentre eles, o da proteção aos dados pessoais e sensíveis destes. Ressalta-se que o próprio direito à intimidade e à vida privada do trabalhador é um direito inespecífico que, apesar de não estar previsto expressamente no artigo 6º da Constituição Federal como um direito social, tem como destinatário o trabalhador-cidadão. O mesmo raciocínio aplica-se à proteção dos seus dados.

Por fim, evidentemente tal direito não é absoluto, podendo em determinadas situações haver a ponderação, mas desde que observados o devido processo legal, os princípios gerais de proteção e os direitos do titular, garantias estas que ajudam a definir limites ao exercício do tratamento dos dados pelo empregador.

4. Considerações finais

O grande fluxo de dados possibilitados pelas novas tecnologias vêm transformando o cenário atual, especialmente as relações de trabalho. As empresas adentram cada vez mais nos dados pessoais e sensíveis dos trabalhadores, obtendo informações que vão muito além do aspecto profissional. Ocorre que tais dados pessoais e sensíveis refletem uma das múltiplas expressões da personalidade do trabalhador.

Assim, como destacado, o direito à proteção dos dados pessoais e sensíveis não é absoluto, contudo, é fundamental se trabalhar com uma perspectiva preventiva, pois é muito mais difícil recuperar um dado violado do que defendê-lo de uma primeira violação.

Diante disso, a teoria dos direitos fundamentais, somada à aplicação dos princípios da boa-fé objetiva e da proporcionalidade, servem como importante instrumento operacional e preventivo da ocorrência de violações aos direitos dos titulares, na medida em que orientam os agentes de tratamento, traduzindo para suas atividades cotidianas as premissas principiológicas da LGPD e concretizando vários dos seus conceitos abertos.

Por fim, vale lembrar que, quando se fala em dados pessoais e sensíveis, a sua tutela é essencial para a proteção da pessoa humana, ainda que no exercício de atividade laboral, pois enquanto pessoa-trabalhadora a condição humana não desaparece. Daí a importância de se melhorar as disposições de proteção espe-

cificamente dirigidas à utilização de dados pessoais dos trabalhadores, de modo a salvaguardar a sua dignidade, proteger a sua privacidade e garantir seu direito fundamental de determinar dados, bem como os propósitos e condições de uso.

REFERÊNCIAS

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BODIN DE MORAES, Maria Celina; MULHOLLAND Caitlin (org.). **Privacidade hoje**: Anais do I Seminário de Direito Civil da PUC-RIO. Rio de Janeiro: PUC-RIO, 2018. *E-book*. Disponível em: <https://ler.amazon.com.br/?asin=B07F-CQBCDB>. Acesso em: 07 set. 2019.

BOLZAN DE MORAIS, Jose Luis; JACOB NETO, Elias. O que é isto, a surveillance? Direito e fluxos de dados globais no século XXI. *In*: BAEZ, Narciso Leandro Xavier; MOZETIC, Vinicius Almada; MARTIN, Nuria Beloso; SÁNCHEZ, Helena Nadal. (org.). **O impacto das novas tecnologias nos direitos fundamentais**. Joaçaba: Unoesc, 2018. p. 85-104.

BRASIL. **Decreto-lei nº 5.452, de 1º de maio de 1943**. Aprova a Consolidação das Leis do Trabalho. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del5452compilado.htm. Acesso em: 21 jul. 2019.

BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm. Acesso em: 27 ago. 2021.

CHEHAB, Gustavo Carvalho. **A privacidade ameaçada de morte**: desafios à proteção dos dados pessoais na relação de emprego pelo uso da informática. São Paulo: LTr, 2015.

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS (CNPD). **Deliberação nº 1638/2013**: aplicável aos tratamentos de dados pessoais decorrentes do controlo da utilização para fins privados das tecnologias de informação e comunicação no contexto laboral. Lisboa, Portugal: 2013. Disponível em: https://www.cnpd.pt/bin/orientacoes/Delib_controlo_comunic.pdf. Acesso em: 25 out. 2019.

DONEDA, Danilo Cesar Maganhoto. **Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade**. 2000. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/8196-8195-1-PB.htm>. Acesso em: 24 jul. 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

LIMBERGER, Têmis. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. **Novos Estudos Jurídicos**, Itajaí, v. 14, n. 2, p. 27-53, 2º Quadrimestre. 2009. Disponível em: <https://siaiap32.univali.br/seer/index.php/nej/article/view/1767/1407>. Acesso em: 10 set. 2019.

MOREIRA, Teresa Alexandra Coelho. **Estudos de direito do trabalho**. Coimbra, Portugal: Almedina, 2016. v. 2.

MURCIA, Joaquín García; CARDO, Iván Antonio Rodríguez. La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo

marco normativo. **Revista Española de Derecho del Trabajo**. Cizur Menor, n. 216, p. 1-28, 2019.

NASCIMENTO, Amauri Mascaro. **Curso de direito do trabalho: história e teoria geral do direito do trabalho, relações individuais e coletivas do trabalho**. 26. ed. São Paulo: Saraiva, 2011.

ORGANIZAÇÃO INTERNACIONAL DO TRABALHO (OIT). **Declaração da OIT sobre os Princípios e Direitos Fundamentais no Trabalho**. 1998. Disponível em: https://www.ilo.org/public/english/standards/declaration/declaration_portuguese.pdf. Acesso em: 01 nov. 2019.

ORGANIZACIÓN INTERNACIONAL DEL TRABAJO (OIT). **Repertorio de recomendaciones prácticas de la OIT**. Ginebra: Oficina Internacional del Trabajo, 1997. Disponível em: http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_112625.pdf. Acesso em: 23 ago. 2021.

RODOTÁ, Stefano. **A vida na sociedade da vigilância**. Rio de Janeiro: Renovar, 2008.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção dos dados pessoais: uma leitura do sistema europeu e a necessária tutela dos dados sensíveis como paradigma para um sistema jurídico brasileiro. **Revista Brasileira de Direitos Fundamentais & Justiça**. Programa de Pós-Graduação Mestrado e Doutorado em Direito da PUCRS. Porto Alegre, ano 4, n. 11, p. 162-180, abr./jun. 2010.

STIVAL, Juliane. O anteprojeto brasileiro de lei de proteção dos dados pessoais e os dados dos Trabalhadores na relação laboral. *In*: FINCATO, Denise Pires (org.). **Novas tecnologias, processo e relações de trabalho**. Porto Alegre: Sapiens, 2015. p. 129-145.

WEINSCHENKER, Marina Santoro Franco. **A vida laboral e extralaboral do empregado: a privacidade no contexto das novas tecnologias e dos direitos fundamentais**. São Paulo: LTr, 2013.

22. REFLEXÕES ACERCA DA APLICAÇÃO DA LGPD NAS RELAÇÕES DE TELETRABALHO

REFLECTIONS ON THE APPLICATION OF THE LGPD IN TELEWORK RELATIONS

RAQUEL HOCHMANN DE FREITAS⁶⁴

Resumo

As alterações trazidas tanto pela Lei nº 13.467/17 quanto pela Lei nº 13.709/2018 impactaram o Direito do Trabalho, especialmente no que diz respeito ao teletrabalho. Com a necessidade de enfrentamento da crise gerada pelo coronavírus, as empresas precisaram remodelar sua forma de atuação, assim como os empregados precisaram aprender a gerir seu tempo a fim de cumprir corretamente o seu mister. Com vantagens e desvantagens que merecem a atenção do operador do direito, o teletrabalhador precisa receber a devida proteção atinente aos seus direitos de privacidade e intimidade, ante a redução da fronteira entre a vida pública e privada e a vida laboral e familiar. Nesse cenário, a proteção de dados deve permitir a adequada utilização das informações decorrentes do contrato de trabalho a fim de que este cumpra sua relevância constitucional enquanto meio de efetivação dos direitos fundamentais sociais. Para tanto, no primeiro capítulo, será examinada a questão atinente à privacidade e intimidade do empregado que desenvolve o teletrabalho. No segundo capítulo, serão examinadas as situações envolvendo a LGPD, diante das novas exigências legais, e o papel dos atores sociais envolvidos. Por fim, conclui-se no sentido de que todos os atores sociais devem voltar sua atenção à proteção do teletrabalhador, evitando que estejamos um passo atrás da evolução da sociedade e do próprio conceito de trabalho.

Palavras-Chave: Teletrabalhador. Privacidade. Proteção de dados.

Abstract

The changes brought about both by Law 13,467/17 and by Law 13,709/2018 impacted the Labor Law, especially concerning telework. With the need to face the crisis generated by the coronavirus, companies needed to remodel their way of operating, just as employees needed to learn how to manage their time to correctly fulfill their mission. With advantages and disadvantages that deserve the attention of the operator of the right, teleworkers need to receive due protection regarding their rights to privacy and intimacy, given the reduction of the boundary between public and private life and work and family life. In this scenario, data protection must allow the proper use of information arising from the employment contract so that it fulfills its constitutional relevance as a means

64 Doutoranda em Direito na PUCRS. Mestre em Direito pela PUCRS. Juíza do Trabalho no TRT da 4ª Região.

of enforcing fundamental social rights. Therefore, in the first chapter, the issue regarding the privacy and intimacy of the employee who develops telework will be examined. In the second chapter, situations involving the LGPD will be examined, given the new legal requirements, and the role of the social actors involved. Finally, it is concluded that all social actors should turn their attention to the protection of teleworkers, preventing us from being one step behind the evolution of society and the very concept of work.

Keywords: Teleworker. Privacy. Data protection.

1. Introdução

A Lei nº 13.467/2017, conhecida como Reforma Trabalhista, trouxe ao direito material do trabalho, especialmente, diversas alterações em relação às quais o operador do direito permanece em constante estudo a fim de adequar-se a realidade com a qual se depara e a novel legislação, sempre de modo a observar os ditames constitucionais vigentes.

Uma das alterações trazidas pela nova legislação vincula-se à regulamentação do teletrabalho⁶⁵, já que antes somente contávamos com o disposto no art. 6º da CLT, a partir da alteração havida com a Lei nº 12.551/11, no sentido de igualar o trabalho presencial ao trabalho a distância, prevendo, em seu parágrafo único, a mesma eficácia entre os controles telemáticos e presenciais para o fim de identificar a subordinação como elemento da relação de emprego⁶⁶.

A partir de março de 2020, com o início da pandemia no Brasil, todas as atenções voltaram-se para o teletrabalho, já que se constituiu em alternativa fundamental para a manutenção não apenas dos empregos e da renda, mas também da própria atividade empresarial (FINCATO; STURMER, 2020, p. 341). A transposição do local de trabalho da empresa para a residência do trabalhador não trouxe a este apenas comodidade, mas também uma série de questões envolvendo sua saúde laboral, uma vez que a preservação do meio ambiente laboral “residencial” é mais complexa, exigindo cautela para que não se violem direitos da personalidade fundamentais, a exemplo da privacidade e intimidade desse trabalhador.

Embora se possa admitir o controle remoto das atividades executadas, ainda assim o controle do meio ambiente laboral permanece ao encargo do empregador, detentor dos riscos da atividade econômica. Para tanto, cada vez mais deverá fazer uso do princípio da precaução (FREITAS, 2014, p. 119), instruindo seus empregados sobre os riscos do trabalho, salientando a relevância de um ambiente seguro, educando-os e inspecionando o local em que são realizadas as atividades (FINCATO; ANDRADE, 2018, p. 281-300).

65 Na forma do art. 75-B da CLT, com redação dada pela Lei nº 13.467/17, “considera-se teletrabalho a prestação de serviços preponderantemente fora das dependências do empregador, com a utilização de tecnologias de informação e de comunicação que, por sua natureza, não se constituam como trabalho externo”.

66 Art. 6º da CLT: “Não se distingue entre o trabalho realizado no estabelecimento do empregador, o executado no domicílio do empregado e o realizado a distância, desde que estejam caracterizados os pressupostos da relação de emprego. Parágrafo único. Os meios telemáticos e informatizados de comando, controle e supervisão se equiparam, para fins de subordinação jurídica, aos meios pessoais e diretos de comando, controle e supervisão do trabalho alheio”.

Mas a utilização dos meios tecnológicos exigirá o redobrado cuidado com o tratamento dos dados deste trabalhador. O acesso às informações do empregado antecede a própria contratação, exigindo a legislação pátria o dever de documentação, pelo empregador, desde a fase pré-contratual, postergando-se à fase pós-contratual.

Diferentemente de Portugal, país que estabelece no código de trabalho a proteção da privacidade e intimidade do trabalhador (MELO, 2018), ou mesmo da Argentina, que prevê em sua legislação relativa ao teletrabalho a salvaguarda do direito à privacidade (KROST, 2020), no Brasil temos que nos socorrer do disposto na Constituição Federal⁶⁷ e na Lei Geral de Proteção de Dados⁶⁸, construindo, assim, a concepção da importância da proteção de dados do trabalhador, cuja autonomia de vontade não se dá de forma absoluta na contratação, mormente considerando a condição vulnerável que detém e que decorre da própria necessidade de conseguir ou manter o liame de emprego⁶⁹.

Nesse cenário, o presente artigo tem como objetivo examinar os meios pelos quais o empregador reorganiza sua forma de atuação a fim de atender os deveres de proteção que lhe competem, especialmente no que atine às disposições do art. 5º, X, da CF/88.

Para tanto, no primeiro capítulo, será examinada a questão atinente à privacidade e intimidade do empregado que desenvolve o teletrabalho. No segundo capítulo, serão examinadas as situações envolvendo a LGPD, diante das novas exigências legais, e o papel dos atores sociais envolvidos.

Por fim, o presente artigo conclui no sentido de que, para a correta preservação dos direitos fundamentais envolvidos, todos os atores sociais devem voltar sua atenção à proteção do teletrabalhador, evitando que estejamos um passo atrás da evolução da sociedade e do próprio conceito de trabalho.

Quanto à abordagem, a presente pesquisa segue o método dedutivo, utilizando, quanto ao procedimento, a pesquisa bibliográfica.

2. Privacidade e intimidade do teletrabalhador

Quando falamos em teletrabalhador nos vem logo à mente a questão do meio ambiente em que está inserido este, ou seja, distante fisicamente do seu empregador e fazendo uso das tecnologias da informação e comunicação (FINCATO, 2016). Também nos remete à ideia de redução de custos, maior comodidade, pro-

67 Nos termos do art. 5º, inciso X, da Constituição Federal de 1988: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”.

68 Na forma do art. 1º da Lei nº 13.709/18, “esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”.

69 O Plenário do Senado Federal aprovou, na data de 20.10.2021, a PEC 17/2019, que trata da inclusão da proteção de dados pessoais como direito fundamental. O texto segue para promulgação, em sessão a ser designada pelo Congresso Nacional. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/10/20/senado-inclui-protacao-de-dados-pessoais-como-direito-fundamental-na-constituicao>. Acesso em: 25 out. 2021.

atividade, o desejo da maioria dos trabalhadores no sentido de dispor melhor do próprio tempo sem descuidar da vida pessoal, especialmente quando somos hábeis em dividir nosso tempo de trabalho e lazer, ampliando a qualidade de vida. A realidade, contudo, nos indica não apenas a existência de vantagens pela adoção de tal modalidade contratual, mas também a presença de riscos que vão desde o adoecimento desse trabalhador até a violação da sua privacidade.

Nos termos do art. 5º, X, da CF/88, a privacidade e a intimidade devem ser respeitadas, tendo a Lei Geral de Proteção de Dados previsto, em seu artigo 5º, incisos I e II, a definição de dado pessoal e dado pessoal sensível⁷⁰.

Vale lembrar que foi com a Constituição Federal de 1988 que o constitucionalismo brasileiro presenciou, pela primeira vez, a inserção de um capítulo próprio para os direitos e garantias fundamentais, consagrando, igualmente, um capítulo destinado aos direitos sociais, com previsão de um grande rol de direitos para os trabalhadores (SARLET; MARINONI; MITIDIERO, 2012, p. 541).

Os direitos fundamentais sociais, como refere Ingo Sarlet,

[...] não são sociais pelo fato de serem, em primeira linha, ou mesmo exclusivamente, direitos coletivos, no sentido de sua titularidade ser eminentemente coletiva. Os direitos sociais assim foram e têm sido designados por outra razão, mesmo no âmbito da superada distinção entre direitos individuais e direitos sociais, visto que tal distinção não repousa na titularidade coletiva dos direitos sociais, mas na natureza e objeto dos direitos [...]

Os direitos sociais, ou foram como tal designados por serem direitos a prestações do Estado na consecução da justiça social, mediante a compensação de desigualdades fáticas e garantia do acesso a determinados bens e serviços por parte de parcelas da população socialmente vulneráveis, ou mesmo, como é o caso dos trabalhadores (que incluem uma série de direitos típicos de liberdade e de igualdade, no sentido de proibições de discriminação), a qualificação de tais direitos como sendo também direitos sociais está diretamente vinculada à garantia de tutela de uma determinada classe social (os trabalhadores) no âmbito de relações no mais das vezes marcadas por níveis de manifesta assimetria – e desequilíbrio – de poder econômico e social (2018, p. 225).

Como é sabido, no âmbito de uma relação laboral, a responsabilidade do empregador pela guarda e segurança dos dados de seu empregado antecede a fase

70 “Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (...).”

contratual. Inicia na fase pré-contratual e posterga-se para além do término da relação laboral, inclusive considerando as diversas determinações legais atinentes ao dever de documentação que lhe compete.

Certamente, o poder diretivo atribuído ao empregador não lhe gera direito absoluto de disponibilização dos dados cuja guarda detém em razão do liame jurídico estabelecido. Tampouco poderá, fazendo uso de tais informações, criar situações que atentem aos direitos fundamentais elementares do trabalhador.

O avanço da tecnologia e da inteligência artificial (FREITAS; BELLINI FREITAS, 2020) baseia-se nos dados com os quais são alimentados tais sistemas e muitas vezes podem ser utilizados para o fim de criar perfis altamente discriminatórios, como seria o caso de perfil racial, religioso ou até mesmo a gestão de informações atinentes à saúde do trabalhador e empresas contra as quais demandou ao longo dos anos.

Ademais disso, a autonomia privada do empregado é relativa, em razão de sua condição de vulnerabilidade (WYZYKOWSKI, 2019) natural, não lhe permitindo total liberdade para dispor sobre as cláusulas que comporão ou não o contrato de trabalho, o que exige do operador do direito a cautela necessária para o fim de preservação de seus direitos, especialmente os relativos à personalidade.

Privacidade, intimidade e proteção de dados, ainda que considerados sob uma mesma perspectiva, não se confundem em essência. Enquanto a intimidade pode ser considerada uma espécie mais reservada da privacidade, a proteção de dados diz respeito a toda e qualquer informação que detenha relevância para o indivíduo, independentemente de estar ou não inserida no conceito de privacidade (DONEDA, 2021). Tal temática envolve uma questão fundamental, centrada no fato de que todos os aspectos da vida moldados pela tecnologia não encontram mais fronteiras definidas, não havendo mais como precisar os limites entre a vida pública e a vida privada, tampouco entre a vida familiar e a vida profissional, especialmente em tempos em que o teletrabalho se tornou realidade como forma efetiva de enfrentamento da crise do coronavírus.

Enquanto a legislação argentina sobre o teletrabalho expressamente prevê a proteção da intimidade do teletrabalhador, como o faz o código de trabalho português, a legislação trabalhista brasileira é omissa, precisando se socorrer, portanto, da Lei Geral de Proteção de Dados, em complemento ao direito fundamental insculpido no art. 5º, X, da CF/88⁷¹.

E, enquanto atividade cuja tendência é de ampliação em diversas áreas possíveis, mais e mais é preciso que voltemos nossas atenções ao teletrabalhador para que não se torne um trabalhador invisível e dissociado do sistema organizacional empresarial. É de extrema relevância que pensemos em como os impactos gerados pelas novas tecnologias atuam concretamente na deterioração da saúde psíquica e emocional do trabalhador, gerando efeitos que ultrapassam o mundo do trabalho.

3.Lei Geral de Proteção de Dados e o papel dos atores sociais

Sobre a importância da proteção de dados no âmbito das relações laborais, Verissa Coelho Cabral Pieroni refere que:

71 Ver PEC 17/2019, referida na nota de rodapé nº 10 do presente artigo.

[...] o tratamento dos dados, quando utilizado para traçar perfis comportamentais, pode ensejar situações tendenciosas ou discriminatórias que venham a mitigar oportunidades de emprego às pessoas, apenas pautadas em suas escolhas, opiniões ou informações lançadas em redes informáticas, o que talvez não reflita, ao certo, o que de fato ela pensa ou quem ela é, produzindo filtros de seleção pautados na discricionariedade do empregador/recrutador, esbarrando, assim, no princípio da não discriminação, por exemplo.

[...]

Quando se pensa na proteção de dados pessoais, não há como não se preocupar com a quantidade de informações de empregados que estão presentes em arquivos, muitas vezes, de acesso disponível a qualquer um que adentra no recinto. Ali estão informações de empregados como nome, telefone, RG, CPF, dados eleitorais e de residência, comprovante de escolaridade, dados bancários, certificado de alistamento militar ou reservista, bem como algumas informações de saúde, tipo sanguíneo, Atestado de Saúde Ocupacional (ASO); também são coletados dados de cônjuges ou companheiros, de filhos e dados de imagem, biométricos, entre tantos outros tratados ao curso do contrato laboral, que merecem especial proteção contra vazamentos (2020, p. 34).

Vicente Vasconcelos Coni Junior e Rodolfo Pamplona Filho defendem a cautela adicional no que tange à obtenção do consentimento esclarecido do empregado, na forma do previsto no art. 5º, inciso XII, da LGPD, o que exigirá relevante adaptação não apenas dos contratos de trabalho mas também de toda a documentação firmada pelo empregado, a fim de tutelar efetivamente os interesses da parte mais vulnerável da relação, especialmente no que tange a dados pessoais sensíveis e potencialmente prejudiciais ao empregado (2020, p. 108-109).

Referidos autores apontam, igualmente, para a importância das normas coletivas, relativamente à obtenção de consentimento válido no que tange à promoção e regulamentação de dados (2020, p. 111). Como leciona Gilberto Stürmer,

O interesse coletivo não é a soma dos interesses individuais, mas a sua combinação, sendo, portanto, indivisível, no sentido de que satisfaz não diversos bens destinados às necessidades individuais, mas um único bem apto a satisfazer as necessidades de uma coletividade. O objeto do sindicalismo é regular as condições de trabalho de uma categoria (de interessados, independentemente de local de trabalho ou de atividade) através das normas coletivas e exercer a atividade sindical plena, no sentido

de regular os interesses gerais da classe e dos trabalhadores como um todo, aspecto não encontrado nas relações individuais (2015, p. 124).

Os avanços tecnológicos e a mudança na forma como prestado o trabalho, com ênfase ao teletrabalho, na atualidade, exigem uma atuação sindical diferenciada, especialmente diante da relevância da entidade sindical na atuação voltada para a proteção de um número considerável de trabalhadores “invisíveis”, distantes da sede física de seu empregador e, portanto, muitas vezes afastados da participação sindical.

É possível que o teletrabalhador se encontre em posição ainda mais vulnerável no que diz respeito à proteção de seus dados pessoais, já que o uso da tecnologia da informação e comunicação ocorre de forma menos propensa a um maior controle quanto ao aumento da transmissão da informação. Tal condição se torna ainda mais relevante se considerarmos que a nova realidade social não mais apresenta fronteiras claras quanto ao que é de domínio público e privado e, especificamente no que diz respeito ao teletrabalhador, já não separa mais a vida profissional da familiar.

Nesse cenário, a fim de obter resultados que se coadunem com a finalidade protetiva da nova legislação, se faz necessária a participação consciente de todos os envolvidos, especialmente empregadores e sindicatos. Na lição de Juan Luis Moreno Fontela,

[...] para argumentar que las cooperativas son positivas para la sociedad, es preciso considerar que los valores cooperativos son valores éticos. Cuando los valores em relación com los cuales se formulan juicios sobre una cooperativa se entienden como valores éticos, es posible usa esos valores para juicios sobre la sociedad que exceden el ámbito cooperativo (por ejemplo, que es deseable que un valor este presente em la sociedad). Por el contrario, si dichos valores son juicios técnicos solo relativos a la práctica cooperativa, no se pueden emplear para juicios sobre la sociedad. Así, las cooperativas serían adecuadas para introducir valores éticos deseables en la sociedad, valores que actúan como criterios normativos de la actividad y desarrollo humanos y no al cumplimiento de los criterios de una práctica (2017, p. 118).

Enquanto dos empregadores se exigirá maior zelo e cuidado no trato das informações e dados pessoais de seus trabalhadores, bem como, especialmente no que diz respeito ao teletrabalhador, da manutenção de um canal de comunicação ativo capaz de ultrapassar a barreira da distância física, observando a natureza sensível das informações cujo acesso se dá em decorrência da natureza da relação jurídica mantida, nessa mesma linha deve a gestão sindical estar voltada ao cumprimento de suas atribuições fundamentais, atendendo ao interesse maior daquele que precisa do sindicato como instrumento realizador dos direitos fundamentais

previstos pela Constituição Federal de 1988.

O sindicato é, em última análise, o garantidor constitucional dos direitos humanos do trabalhador e todo o seu enfoque deve estar voltado para essa responsabilidade, especialmente quando se encontra diante de um trabalhador cuja vulnerabilidade apresenta-se exacerbada pelo fato de estar distante da realidade física laboral e do contato presencial com sua entidade de classe.

4. Considerações finais

No dizer de Jorge Miranda (2005, p. 90), a Constituição, sendo o fundamento do poder político, é igualmente responsável por fundamentar a validade, tanto formal quanto substancial, de todos os órgãos e de cada um deles, em relação aos quais se projeta, determinando sua subsistência, direta ou indiretamente. Assim, o ordenamento jurídico deve guiar-se de modo a observar a natureza central da Constituição e dos direitos fundamentais nela insculpidos.

Interpretar conforme a Constituição e visando sempre a dar a maior efetividade possível aos direitos fundamentais implica, de certa forma, repensar se os meios até então utilizados se mostram capazes de atender as demandas impostas por lei. A revisão da estrutura laboral implica questionar se o modo como enxergamos as relações trabalhistas se mostra adequado para fazer frente às inúmeras novas situações e demandas advindas com a revolução tecnológica.

Nesse contexto, faz-se necessário rediscutir, no âmbito trabalhista, a manutenção do conceito de fiscalização e poder diretivo nos moldes em que o conhecemos, especialmente diante dos ditames constitucionais e legais que envolvem a preservação das informações relevantes e constituem elementos integrantes da privacidade e intimidade do trabalhador.

Questionar se o teletrabalhador atua de forma saudável, na concepção física, psicológica e emocional é o desafio do operador do direito na atualidade, devendo ter o empregador ciência da essencialidade que detém no tocante ao papel que desempenha – ou deveria desempenhar, na salvaguarda dos direitos fundamentais dos trabalhadores e sua efetivação concreta. Significa, ainda, readaptar os conceitos estruturais das relações laborais à nova dimensão trazida pelas alterações – sejam legislativas, tecnológicas ou sociais – que moldam o novo contexto produtivo.

Ora, como em todos os aspectos, o avanço tecnológico exige que tenhamos “lucidez para não ser vítima de falácias e armadilhas argumentativas” (FREITAS, 2019, p. 147), estando mais do que na hora de nos desapegarmos da armadilha do *status quo* (FREITAS, 2019, p. 167), do verdadeiro apego ao estado de coisas como vem se conduzindo ao longo dos anos.

Essa nova mentalidade exigirá a transposição de antigos paradigmas, das muitas falácias e armadilhas argumentativas e da própria forma como se apresenta nossa postura política no trato dos direitos essenciais dos trabalhadores.

Inexiste razão para a não implementação de uma postura operacional diferenciada frente à realidade, uma postura que não implique diminuição da relevância constitucional atribuída aos direitos fundamentais dos trabalhadores e sim a efetivação plena destes, sem restrições, limitações ou requisitos outros que não o cumprimento

ético dos deveres legais, tanto de empregadores quanto dos empregados cômicos de seu papel na construção de uma nova realidade laboral que se impõe, quanto das entidades sindicais representativas dos empregados, alcançando a todos que dela efetivamente necessitem, de forma substancial, e não meramente formal.

A inteligência artificial modifica não apenas a forma da prestação do trabalho, como igualmente altera a maneira pela qual percebemos esse mesmo trabalho e, certamente, os meios pelos quais devemos garantir proteção ao trabalho prestado e ao valor humano que se esconde cada vez mais por trás dele.

Alerta Rogério Luís Marques de Mello que “[...] os algoritmos não são imparciais. Eles são enviesados pelas visões de mundo de seus programadores e, de forma geral, reforçam preconceitos e promovem desigualdades” (2019, p. 78), acrescentando, com propriedade, que “a tecnologia é realidade relativamente recente no mundo e impõe, ao direito, as mudanças necessárias para o equilíbrio entre a preservação dos direitos humanos e a possibilidade de evolução da espécie humana” (2019, p. 79).

Que o novo norte se dê no caminho da verdadeira reflexão e ponderação dos interesses envolvidos, e não apenas pela inércia na tomada de decisões essenciais para a proteção da realidade laboral.

REFERÊNCIAS

BRASIL. **Senado Federal**. Proposta de Emenda à Constituição nº 17, de 2019. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/10/20/senado-inclui-protecao-de-dados-pessoais-como-direito-fundamental-na-constituicao>. Acesso em: 25 out. 2021.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados**. 3. ed. Revista dos Tribunais, 2021, 368p.

FINCATO, Denise Pires. A regulamentação do teletrabalho no Brasil: indicações para uma contratação minimamente segura. **Revista Jurídica Luso Brasileira**, Ano 2, número 2, 2016, p. 365-396. Disponível em: https://repositorio.pucrs.br/dspace/bitstream/10923/11404/2/A_regulamentacao_do_teletrabalho_no_Brasil_indicacoes_para_uma_contratacao_minimamente_segura.pdf. Acesso em: 17 set. 2021.

FINCATO, Denise Pires; DE ANDRADE, Amanda Scotá. Home office: direitos fundamentais, meio ambiente laboral e reforma trabalhista. **Revista de Direito Econômico e Socioambiental**, Curitiba, v. 9, n. 2, p. 281-300, dez. 2018. ISSN 2179-8214. Disponível em: <https://periodicos.pucpr.br/index.php/direito-economico/article/view/22123>. Acesso em: 17 set. 2021.

FINCATO, Denise Pires; STURMER, Gilberto. Teletrabalho em Tempos de Calamidade por Covid19: Impacto das Medidas Trabalhistas de Urgência. In: **O Direito do Trabalho na crise da COVID-19**. BELMONTE, Alexandre Agra; MARTINEZ, Luciano; MARANHÃO, Ney. (coord.) Salvador: Editora JusPodivm, 2020.

FREITAS, Juarez. **A Interpretação Sistemática do Direito**. 5. ed. São Paulo: Malheiros Editores, 2010.

FREITAS, Juarez. **Direito Fundamental à Boa Administração Pública**. 3. ed. São Paulo: Malheiros Editores, 2014.

FREITAS, Juarez. **Sustentabilidade: direito ao futuro**. 4. ed. Belo Horizonte: Fórum, 2019.

JUNIOR, Vicente Vasconcelos Coni; FILHO, Rodolfo Pamplona. A Lei Geral de Proteção de Dados e seus Reflexos nas Relações Jurídicas Trabalhistas. **Reflexos da LGPD no Direito e no Processo do Trabalho**. MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (coord.). São Paulo: Thompson Reuters Brasil, 2020.

KROST, Oscar. Teletrabalho no Direito Argentino: comentários sobre a Lei nº 27.555/20. **Revista Direito UNIFACS**, n. 243, set. 2020. Disponível em: <https://revistas.unifacs.br/index.php/redu/article/view/6923>. Acesso em: 17 set. 2021.

MELLO, Rogério Luís Marques de. Inteligência artificial e os direitos fundamentais da pessoa humana. **Revista Direito, Democracia e Cidadania**, [S.l.], v. 1, n. 1, abr. 2019. ISSN 2596-2930. Disponível em: <<http://ojs.funepe.edu.br/index.php/Direito/article/view/46>>. Acesso em: 22 jul. 2021.

MÉLO, Marcela Alves. **Teletrabalho: um estudo comparado entre Portugal e Brasil sobre a transformação das relações de trabalho**. 2018. Dissertação de Mestrado em Direito na área de especialização Ciências Jurídico-Civilísticas. Faculdade de Direito. Universidade do Porto, Porto, 2018, 60p.

MIRANDA, Jorge. **Manual de Direito Constitucional**. Tomo VI. 2. ed. Coimbra: Coimbra Editora, 2005.

MORENO FONTELA, Juan Luis. Las relaciones entre los valores y principios cooperativos y los principios de la normativa cooperativa. **REVESCO. Revista de Estudios Cooperativos**, n. 124, mayo/agosto de 2017, p. 114-127. Universidad Complutense de Madrid, Madrid, España.

PIERONI, Verissa Coelho Cabral. Noções Gerais sobre Proteção de Dados nas Relações de Emprego. In: MIZIARA, Raphael; PESSOA, André Pessoa, MOLLICONE, Bianca (coord.). **Reflexos da LGPD no Direito e Processo do Trabalho**. São Paulo: Revista dos Tribunais, 2020.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. 13. ed. Porto Alegre: Livraria do Advogado, 2018.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional**. São Paulo: Revista dos Tribunais, 2012.

STURMER, Gilberto. A liberdade sindical no Brasil e as concepções do direito de Ronald Dworkin. **Arquivo Jurídico**, Teresina – PI, v. 2, nº 1, 2015, p. 120-129.

WYZYKOWSKI, Adriana Brasil Vieira. **Autonomia privada e vulnerabilidade do emprego: critérios e limites para o exercício da liberdade negocial individual no direito do trabalho**. 2019. Tese (Doutorado em Direito) – Programa de Pós-Graduação em Direito, Universidade Federal da Bahia, Salvador, 2019. Disponível em: <http://repositorio.ufba.br/ri/handle/ri/30090>. Acesso em: 19 out. 2021.

23. CONTORNOS JURÍDICOS NO TRATAMENTO DE DADOS DE COLABORADORES E A LGPD

MÁRCIA SANTANA FERNANDES⁷²
E SÍLVIA WEIGERT MENNA BARRETO⁷³

Resumo

O objetivo é tratar das bases legais de tratamento, conforme a Lei Geral de Proteção de Dados – LGPD, Lei 13.709, de 14 de agosto de 2018⁷⁴, de dados e informações pessoais na área das relações de trabalho, na perspectiva dos responsáveis (controladores - empregadores) pela coleta, registro, armazenamento, organização, interpretação e descarte dos dados e informações pessoais de seus empregados. O texto está organizado em dois capítulos: 1- as exigências e bases legais de tratamento de dados pessoais e 2- exigências legais e regulatórias para o compartilhamento de dados pessoais de colaboradores.

Abstract

The objective is to address the legal bases of treatment, according to the General Data Protection Act - LGPD, Law 13.709, of August 14th 2018, of personal data and information in the area of employment relations, from the perspective of those responsible (controllers - employers) for collecting, recording, storing, organizing, interpreting and disposing of their employees' personal data and information. The text is organized in two chapters: 1- the legal requirements and bases for processing personal data and 2- legal and regulatory requirements for sharing personal data of employees.

1. Introdução

Os espaços digitais na sociedade da informação abalaram a noção e a garantia da privacidade, pois as fronteiras espaciais e temporais pré-estabelecidas e reconhecidas entre o público e o privado podem ser facilmente rompidas. A denominada Quarta Revolução, por Luciano Floridi, instaura um contexto diverso, denominado pelo autor como a “infosfera” (*infosphere*), e exige que façamos reflexões reontológicas (*re-ontology*), estudos e pesquisas para compreender, em sentido amplo, os impactos e desafios na vida dos seres humanos, individual ou coletivamente.^{75,76}

72 Doutora em Direito pela UFRGS. Pós-Doutora em Medicina pela UFRGS. Professora do Mestrado Profissional em Pesquisa Clínica e Pesquisadora do Laboratório em Pesquisa em Bioética e Ética na Ciência (LAPEBEC) do Hospital de Clínicas de Porto Alegre – HCPA. Professora Colaboradora do PPG/Direito da PUCRS. Advogada Sócia do escritório Santana Fernandes Advocacia e Consultoria. msfernandes@hcpa.edu.br

73 Mestre em Pesquisa Clínica pelo Hospital de Clínicas de Porto Alegre. Advogada trabalhista do Hospital de Clínicas de Porto Alegre. swmbarreto@hcpa.edu.br

74 A Lei Geral de Proteção de Dados (LGPD) - Lei 13.709, de 14 de agosto de 2018.

75 FLORIDI, Luciano. *The Fourth Revolution: How the infosphere is reshaping human reality*. Oxford: Oxford University, 2014

76 FERNANDES, Márcia S. Privacidade, sociedade da informação e Big Data. In: *Direito, Cultura e Método* - Leituras da obra de Judith Martins-Costa. (org.) BENETTI, G.; CORREA, A. R.; FERNAN-

As modificações provocadas pela Sociedade da Informação, devido à associação entre as tecnologias de informática e de comunicação, a popularização da Internet, a criação do ambiente de *Big Data*, além de outras conjugações, alteram as dinâmicas sociais e comportamentos até então reconhecidos, inerentes à *sociedade e ao mundo em risco*, como propôs Beck.^{77,78}

Em particular, é importante estudarmos e predizermos os riscos e os desafios no que concerne ao tratamento de dados pessoais dos colaboradores e trabalhadores, na perspectiva da Proteção de Dados Pessoais no ambiente de trabalho - os impactos nas relações jurídicas de subordinação do empregado (titulares de direitos à proteção de dados pessoais) pelo empregador (controlador), este detentor do poder potestativo de organizar, administrar, gerenciar, demandar, fiscalizar e dispensar as atividades laborais.

Na atualidade, o significado da palavra “trabalho” é abrangente. A Constituição Federal estabelece o trabalho como um dos fundamentos do Estado Democrático de Direito (artigo 1º, IV), um direito fundamental a prestações (art. 6º), um fundamento da ordem econômica (art. 170, *caput*) e base da ordem social (art. 193).⁷⁹

O sistema jurídico, representado pelo Direito do Trabalho (Direito Individual do Trabalho e Direito Coletivo do Trabalho, com conotação coletiva, social, regras internacionais, nacionais e setoriais), tem por objetivo a melhoria da condição social dos trabalhadores, a proteção das minorias e dos hipossuficientes e a proteção da classe trabalhadora em respeito à sua dignidade e personalidade.⁸⁰

Neste sentido, o objetivo deste trabalho é tratar das bases legais de tratamento, conforme a Lei Geral de Proteção de Dados – LGPD, Lei 13.709, de 14 de agosto de 2018⁸¹, de dados e informações pessoais na área das relações de trabalho, na perspectiva dos responsáveis (controladores - empregadores) pela coleta, registro, armazenamento, organização, interpretação e descarte dos dados e informações pessoais de seus empregados. O texto está organizado em dois capítulos: 1- as exigências e bases legais de tratamento de dados pessoais e 2- exigências legais e regulatórias para o compartilhamento de dados pessoais de colaboradores.

2 . A LGPD e as exigências e bases legais de tratamento de dados pessoais

A sociedade da informação e os sistemas de informação e comunicação ampliaram as possibilidades de interconectar, armazenar e tratar um grande e complexo volume de dados e informações, em um contexto de *Big Data*, *text Analytics*, *Data mining*, *Blockchain* (tratados por meio de algoritmos), Inteligência Artificial

DES, M.S.; NITSCHKE, G. C. M.; PARGENDLER, M.; VARELA, L. B. 1ª ed., Rio de Janeiro: GZ Editora, 2019, v.1, p. 182-210.

77 BECK, Ulrich. *Sociedade de risco – rumo a uma modernidade*. 2ª edição em tradução em português, por Sebastião Nascimento. São Paulo: Editora 34, 2011. A expressão “sociedade em risco” foi cunhada na primeira edição da obra, de 1986, *Risikogesellschaft: auf dem Weg in eine andere Moderne*.
78 BECK, Ulrich. *World at Risk*. Translated by Ciaran Cronin. Cambridge: Policy Press, 2009. A primeira edição da obra é de 2007.

79 MENNA BARRETO, Sílvia W.; FERNANDES, Márcia S. *Pesquisa Clínica e os vínculos de trabalho*. São Paulo: Editora Mizuno, 2021. *E-book*.

80 *Op. cit.*

81 A Lei Geral de Proteção de Dados (LGPD) - Lei 13.709, de 14 de agosto de 2018.

(AI), além da estatística, o que amplifica a preocupação, em âmbito nacional e internacional, em normatizar este fenômeno imposto pela *Quarta Revolução*.⁸² A Lei Geral de Proteção de Dados e o Regulamento Geral de Proteção de Dados (RGPD)⁸³, publicado em 2016, são exemplos.⁸⁴

A Lei Geral de Proteção de Dados (LGPD), em seu artigo 5º e incisos, estabelece a sua finalidade e os conceitos centrais. Destacamos cinco aspectos que devem ser obrigatoriamente considerados, sem prejuízo de outros, para enfrentar a questão da proteção de dados e informações. Os conceitos de dado pessoal, de dado sensível; da anonimização de dados; do consentimento e o uso compartilhado de dados. Os dados e informações pessoais têm natureza individual e parte deles têm natureza sensível, (artigo 5º, incisos I e II e 11 da LGPD); os fundamentos (artigo 2º), os princípios (artigo 6º), requisitos aplicáveis (artigo 7º); a forma para o consentimento informado (artigo 8º); a finalidade, a necessidade e o limite para organização e elaboração do PEP (artigo 9º); a demonstração do legítimo interesse para o tratamento dos dados (10º) e, primordialmente, as exigências para o tratamento de dados pessoais sensíveis (artigo 11º).^{85, 86}

A Lei 13.709/2018 pauta sua estrutura normativa no fundamento *dos direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais* (artigo 2º), balizados pela Constituição Federal. E como não poderia ser diferente também, estes são os fundamentos das normas relacionadas às relações de trabalho para garantir a adequada forma de tratamento de dados pessoais de colaboradores e de trabalhadores. Assim, todas as instituições, públicas ou privadas ou profissionais responsáveis (controladores) pelo tratamento de dados pessoais, deverão ter suas atividades estruturadas e ajustadas conforme as regras e princípios da LGPD e por diretrizes e regramentos ditados pela Autoridade Nacional de Proteção de Dados (ANPD), criada pelo Decreto 10.474/2020.⁸⁷

82 FLORIDI, Luciano. *The Fourth Revolution – How the infosphere is reshaping human reality*. Oxford: Oxford University, 2014

83 O Regulamento (UE) 2016/679/79 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, revoga a Diretiva 95/46/CE.

84 FERNANDES, Márcia; GOLDIM, J.R. A Sistematização de Dados e Informações em Saúde em um Contexto de Big Data e Blockchain; p. 333-357, In: *Direito & Internet: Sistema de Proteção de Dados Pessoais*. vol. 4. (org). De Lucca, Newton; Simão Filho, Adalberto; Lima, Cíntia Rosa Pereira de; Maciel, Renata Mota. São Paulo: Quartier Latin, 2019.

85 GOLDIM, J.R. Consentimento, Alteridade e Capacidade. In: Giovana Benetti; André Rodrigues Corrêa; Márcia Santana Fernandes; Guilherme Monteiro Nitschke; Mariana Pargendler; Laura Beck Varela. (org.). *Direito, Cultura e Método - Leituras da obra de Judith Martins-Costa*. 1ª ed. Rio de Janeiro: GZ Editora, 2019, v. 1, p.168-181.

86 FERNANDES, M. S. *Prontuário eletrônico e a Lei Geral de Proteção de Dados*. Disponível em <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/340202/prontuario-eletronico-e-a-lei-geral-de-protecao-de-dados>. Acesso em: 30 jul. 2021.

87 SARLET, Gabrielle B. S.; FERNANDES, Márcia S.; RUARO, Regina L. A proteção de dados no setor da saúde em face do sistema normativo brasileiro atual. In: *Tratado de Proteção de Dados Pessoais*. Mendes, Laura; Doneda, Danilo; Sarlet, Ingo W.; Rodrigues Jr., Otávio; (coord). Rio de Janeiro: Editora Forense, 2021.

Portanto, empregadores (controladores) têm o dever de observar e respeitar os direitos fundamentais de liberdade, de intimidade e de privacidade dos titulares, expressamente previstos nos artigos 17 ao 22 da LGPD, reforçando a previsão expressa da Constituição Federal, artigo 5º, e 20 e 21 do Código Civil Brasileiro. Em particular, devem ser previstas formas e estruturas institucionais para, em segurança, guarnecer os dados de funcionários, colaboradores ou terceiros, conforme deveres previstos no artigo 18 da LGPD.

É importante, neste cenário, destacar o papel das figuras do controlador, operador e encarregado (artigo 5º, incisos VI, VII e VIII) para o ajuste de políticas e culturas em prol da proteção de dados pessoais de colaboradores e empregados. Em particular, o controlador, a *quem compete as decisões referentes ao tratamento de dados pessoais*, e que deve exigir do operador a implementação de todas as medidas técnicas, de segurança e de certificação dos sistemas utilizados, e exigir do encarregado a composição e elaboração de políticas institucionais, educacionais e de assessoria, por meio de comissões específicas ou grupos de trabalho.⁸⁸

A LGPD estabelece as possibilidades do tratamento de dados pessoais, além e independentemente do consentimento informado do titular (art. 8º), em situações específicas conforme previsto no Capítulo II, art.7.º e art. 11. É importante destacar, no caso das relações de trabalho, as seguintes hipóteses: para o cumprimento de obrigação legal ou regulatória pelo controlador (art.7º, inciso II e art. 11, inciso II, letra a); quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados (art.7º, inciso V e art. 11, inciso II, letra d); VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral (art.7º, inciso VI e art. 11, inciso II, letra d), entre outros.

Por sua vez, o consentimento informado, base de tratamento prevista na LGPD, artigos 7º, inciso I; 8º; 11, inciso I, para o tratamento de dados pessoais ou dados pessoais sensíveis do titular (empregado ou colaborador), poderá ser necessário para aquelas situações em que a finalidade do tratamento não esteja no escopo das atividades laborais ou funcionais do funcionário (titular) ou que não estejam em nenhuma das outras formas de tratamento exigidas pela Lei. Como, por exemplo, realizar campanhas promocionais para a empresa, interna e externamente à sede da empresa.⁸⁹

Neste contexto, além das cláusulas contratuais e dos acordos coletivos, as Políticas de Privacidade e Proteção de Dados, as Diretrizes, Procedimentos Operacionais Padrão (POPs) são fundamentais para balizar e estabelecer boas práticas no ambiente de trabalho e pautar as relações trabalhistas. Estes documentos podem ser vinculados ao contrato de trabalho para o fortalecimento da cultura de privacidade e proteção de dados em sentido amplo – tanto para proteger o empregado

88 FERNANDES, Marcia S. *Prontuário eletrônico e a Lei Geral de Proteção de Dados*. Disponível em <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/340202/prontuario-eletronico-e-a-lei-geral-de-protecao-de-dados>. Acesso em: 30 jul. 2021.

89 FERNANDES, Marcia S.; GOLDIM, José Roberto. *Os diferentes processos de consentimento na pesquisa envolvendo seres humanos e na LGPD – Parte I*. Acessível em <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/352528/processos-de-consentimento-na-pesquisa-envolvendo-seres-humanos>. Acesso em: 30 jul. 2021.

ou colaborador (titular) como para proteger direitos de terceiros, por exemplo: clientes, prestadores de serviços e terceirizados etc.

3. Exigências legais e regulatórias para o compartilhamento de dados pessoais de colaboradores

O tratamento de dados deve ter finalidades específicas e legítimas, como vimos. Nesse momento, verifica-se que a LGPD se comunica com o Direito do Trabalho porque o empregador (controlador), ao cadastrar o contrato de trabalho nos órgãos governamentais específicos, deve fazê-lo no estrito limite do estabelecido em leis trabalhistas e particularmente pela LGPD, respeitando, por conseguinte, a finalidade do registro.

Os princípios, previstos no artigo 6º, pautados pelo princípio core da boa-fé objetiva⁹⁰, compõem o alinhamento que a LGPD deverá encaminhar às situações concretas. No ambiente do Direito do Trabalho, os princípios da finalidade (inciso I), adequação (inciso II), necessidade (inciso III), não discriminação (inciso IX) e segurança (inciso VII) representam os cinco pilares para a proteção da dignidade do titular, dos direitos fundamentais, de personalidade e sociais, assim como estabelecem aspectos relacionados às condições seguras de trabalho.

No que concerne ao registro do contrato de trabalho, previsto como base específica de tratamento (art. 7º, inciso V, e art. 11, inciso II, letra d), é necessário, por diversos motivos, quais sejam: o empregador deve anotar a carteira de trabalho do empregado (CTPS) e, para tanto, poderá obter dados sensíveis do empregado para a sua inscrição no Cadastro Geral de Empregados e Desempregados – CAGED⁹¹, e também a inscrição na Relação Anual de Informações Sociais – RAIS.^{92,93}

Com o contrato de trabalho ativo, o empregador deverá recolher o Fundo de Garantia por Tempo de Serviço (FGTS), deverá recolher contribuição previdenciária, sendo que todas essas coletas de informação deverão ser repassadas à administração pública pelo empregador (ou controlador), no estrito cumprimento das finalidades legais regulatórias. Ressalta-se que como a administração pública também está submetida às normas da LGPD, ela como controladora dos dados recebidos e compartilhados terá as mesmas responsabilidades quando à observância da Lei. Cabe destacar que o preenchimento dos dados inerentes ao contrato de trabalho, além de servir ao próprio trabalhador (titular), é responsável por estudos que viabilizam políticas públicas governamentais, isto é, auxiliam a administração pública.

90 Para estudos aprofundados sobre o princípio da boa-fé objetiva, ver: MARTINS-COSTA, Judith. *A Boa-Fé no Direito Privado* – critérios para sua aplicação. Paulo: Marcial Pons, 2015.

91 CAGED é a sigla para Cadastro Geral de Empregados e Desempregados e é o dispositivo legal utilizado pelo Ministério do Trabalho e Emprego para acompanhar a situação da mão de obra formal no Brasil, a fim de levantar dados de geração de emprego e desemprego.

92 RAIS é importante fonte de direito do trabalhador para comprovação de tempo de serviço para aposentadoria ou experiência de trabalho, para concessão do pagamento do abono salarial, cálculo de FGTS, dentre outras finalidades.

93 MIZIARA, RAPHAEL. Reflexos da LGPD no direito e no processo do trabalho. São Paulo: Thomson Reuters, 2020. *E-book*.

O governo federal criou o E-SOCIAL⁹⁴, programa eletrônico, sigiloso, no qual o empregador deve preencher os dados do empregado, que será utilizado para cálculo do recolhimento da contribuição previdenciária – patronal e do empregado, bem como será calculado o valor de recolhimento do FGTS; deverá informar eventual acidente do trabalho, doença do trabalhador, período de férias, salário, remuneração, vale-transporte, horas extras, faltas, número da carteira de trabalho, CPF, endereço, horário de trabalho, dependentes etc. Ou seja, o e-Social é um sistema informatizado da administração pública que contém dados sensíveis do trabalhador, preenchido pelo empregador, em observância à sua finalidade estrita, ainda que sem anuência, porque não há liberalidade no cadastramento.

Além das situações elencadas acima, de fornecimento compulsório de informação de empregados ao poder público, dentro da empresa, muitas vezes, também se faz necessária a transmissão de informações de empregados entre departamentos. Por exemplo, ao receber a notificação do ajuizamento de uma reclamatória trabalhista, o departamento jurídico deve, invariavelmente, requisitar informações ao departamento de recursos humanos; empresas terceirizadas para oferecimento de benefícios aos empregados (como vale transporte e alimentação); agentes financeiros; seguradoras etc.

O compartilhamento com o Poder Judiciário tem tratamento previsto na LGPD (art. 7º, inciso VI, e art. 11, inciso II, letra d), pois há necessidade no fornecimento de informações que devem instrumentalizar a ação processual, assim como para a demonstração dos fatos. Portanto, o compartilhamento deve ser realizado e o titular das informações não pode se opor a que o departamento jurídico obtenha os dados necessários para contestar o processo, já que o próprio titular dos dados deu causa à necessidade de transmissão de informações sensíveis ao ajuizar a ação. No entanto, todas as pessoas (físicas ou jurídicas) de direito privado ou público têm o compromisso de respeito e observância aos princípios da LGPD.

Situação diferente, contudo, ocorre quando o empregado faz consulta médica no próprio estabelecimento no qual trabalha e o seu consequente registro em prontuário médico. Conforme Código de Ética Médica⁹⁵, Capítulo I, Princípios Fundamentais, XI, o médico guardará sigilo a respeito das informações de que detenha conhecimento no desempenho de suas funções, com exceção dos casos previstos em lei.⁹⁶ E quando o empregado trabalha em empresa que faz pesquisa em saúde, o consentimento informado deve atender às exigências regulatórias envolvendo pesquisa com seres humanos. A participação do empregado na pesquisa clínica, entretanto, somente ocorrerá com a sua anuência, devendo ser preenchido termo de consentimento livre e esclarecido⁹⁷, consoante estabelece a Resolução nº

94 O e-Social é uma plataforma online do governo que unificou a entrega de 15 obrigações da área trabalhista para empresas, outras pessoas jurídicas e também para pessoas físicas.

95 O Código de Ética Médica foi publicado pelo Conselho Federal de Medicina em 27 de setembro de 2018 pela Portaria 2.217.

96 A Portaria 1.271, de 6 de junho de 2014, define a Lista Nacional de Notificação Compulsória de doenças, agravos e eventos de saúde pública nos serviços de saúde públicos e privados em todo o território nacional, nos termos do anexo.

97 Termo de Consentimento Livre e Esclarecido (TCLE) é documento no qual é explicitado o consentimento livre e esclarecido do participante e/ou de seu responsável legal, de forma escrita, devendo

466, de 12 de dezembro de 2012.⁹⁸

O consentimento da LGPD é uma das bases legais de tratamento (art.7º, inciso I; art. 8º e art. 11, inciso I), que não deve e não pode ser confundido com o processo de consentimento na pesquisa em saúde. No entanto, ambos podem ser necessários, conjuntamente ou não, de acordo com o caso concreto. Conforme esclarecido por Fernandes e Goldim, no texto “Os diferentes processos de consentimento na pesquisa envolvendo seres humanos”⁹⁹, que passamos a transcrever:

1) o tratamento de dados pessoais poderá ser realizado em situações de pesquisas, desde que realizadas por órgão de pesquisa, artigo 5º, inciso XVIII;

2) a LGPD dispensa o consentimento, art. 8º, quando outras bases legais legitimarem o tratamento de dados, previstos no artigo 7º e 11.

3) a LGPD autoriza no seu artigo 13 e parágrafos, o tratamento de dados pessoais para a realização de “estudos em saúde pública”, diz o artigo que os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro.

4) O processo de consentimento para realização de pesquisa envolvendo seres humanos “é exigido pelo sistema CEP/CONEP e também pela ANVISA nas situações de pesquisa clínica”. Entendemos que este processo tem momentos essenciais: o primeiro concerne ao dever de informar à pessoa convidada para ser um participante de pesquisa. (...) A segunda é diretamente conectada ao acompanhamento do participante, durante e após a realização da pesquisa, para suporte e esclarecimento de quaisquer situações ou aspectos decorrentes da pesquisa. O terceiro relaciona-se ao estabelecimento de canais de comunicação adequados e seguros para fortalecer e ampliar os graus de entendimento do participante durante todo tempo em que este estiver envolvido com a pesquisa, e até mesmo após o seu término formal.

5) O consentimento previsto na LGPD, a princípio, não será exigido nos casos de pesquisas clínicas ou pes-

conter todas as informações necessárias, em linguagem clara e objetiva, de fácil entendimento, para o mais completo esclarecimento sobre a pesquisa a qual se propõe participar. RESOLUÇÃO N° 466, DE 12 DE DEZEMBRO DE 2012.

98 A Resolução 466 contém diretrizes e normas regulamentadoras de pesquisas envolvendo seres humanos.

99 FERNANDES, Marcia S.; GOLDIM, José Roberto. Os diferentes processos de consentimento na pesquisa envolvendo seres humanos e na LGPD – Parte I. Disponível em <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/352528/processos-de-consentimento-na-pesquisa-envolvendo-seres-humanos>. Acesso em: 30 jul. 2021

quisas em saúde pública, pois estas situações têm base legal própria, previstas na LGPD, para tratamento de dados pessoais.

6) Da mesma forma, medidas de segurança devem ser tomadas pelos controladores dos dados de pesquisa, que são os responsáveis pela pesquisa, para garantir os níveis de proteção, prevenção, segurança, controle, gestão e verificação de dados e informações dos participantes, exigidas pela LGPD.¹⁰⁰

Contudo, é fundamental destacar que a regra para o tratamento de dados e informações pessoais adequadas, em particular a transmissão ou compartilhamento, deve respeitar o binômio: o dever de informar do controlador e o direito de ser informado do titular, sob o fundamento no princípio da confiança, são elementos essencialmente relevantes em qualquer atividade humana.

4. Considerações finais

O Direito do Trabalho tem papel regulatório preponderante na organização das atividades produtivas e nas demais searas da vida social. Por meio dele o poder público, através da legislação, assegura direitos trabalhistas a serem seguidos pelos empregadores, com o objetivo de garantir o mínimo de garantias aos indivíduos. Também é por meio do Direito do Trabalho que o trabalhador, com anotação da carteira de trabalho, filia-se, automaticamente, ao Regime Geral de Previdência Social e à rede de proteção aos seus direitos sociais e fundamentais.

Por sua vez, a LGPD fortalece os princípios em respeito à pessoa, à sua dignidade, aos direitos fundamentais e da personalidade e particularmente fortalece a necessidade do desenvolvimento da cultura da proteção, prevenção e segurança da proteção de dados e informações pessoais nas diversas atividades e momentos da vida em sociedade, entre elas as relações de trabalho. Portanto, nas relações de trabalho, há a necessidade de tratar dados e informações pessoais, no entanto, o tratamento deve respeitar as regras e princípios estabelecidos pela LGPD.

REFERÊNCIAS

BECK, Ulrich. *Sociedade de risco – rumo a uma modernidade*. 2ª ed. São Paulo: Editora 34, 2011.

BECK, Ulrich. *World at Risk*. Cambridge: Policy Press, 2009.

BRASIL. **Lei 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD)**. Disponível em <http://www.planalto.gov.br>

_____. Conselho Federal de Medicina. Portaria 1.271. Disponível em: <http://www.in.gov.br/>

_____. Ministério da Economia. CAGED. Disponível em: <https://portalfat.mte.gov.br/>

_____. Ministério da Economia. Relação Anual de Informações Sociais.

100 Ibid.

Disponível em: <http://www.rais.gov.br/sitio/index.jsf>.

_____. Ministério da Economia. Disponível em <https://www.gov.br/esocial>

BRASIL. Ministério da Saúde. **Resolução 466**. Disponível em <http://conselho.saude.gov.br/>

FERNANDES, M. S. Prontuário eletrônico e a Lei Geral de Proteção de Dados. Disponível em <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/340202/prontuario-eletronico-e-a-lei-geral-de-protecao-de-dados>. Acesso em: 30 jul. 2021.

FERNANDES, Márcia S. Privacidade, sociedade da informação e Big Data *In: Direito, Cultura e Método - Leituras da obra de Judith Martins-Costa*. BENETTI, G.; CORREA, A. R.; FERNANDES, M.S.; NITSCHKE, G. C. M.; PARGENDLER, M.; VARELA, L. B. (org.) 1ª ed., Rio de Janeiro: GZ Editora, 2019, v.1, p. 182-210.

FERNANDES, Marcia S.; GOLDIM, José Roberto. Os diferentes processos de consentimento na pesquisa envolvendo seres humanos e na LGPD – Parte I. Acessível em <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/352528/processos-de-consentimento-na-pesquisa-envolvendo-seres-humanos>

FERNANDES, Márcia; GOLDIM, José Roberto. *A Sistematização de Dados e Informações em Saúde em um Contexto de Big Data e Blockchain*; p. 333-357. *In: Direito & Internet 4*. Sistema de Proteção de Dados Pessoais. De Lucca, Newton; Simão Filho, Adalberto; Lima, Cíntia Rosa Pereira de; Maciel, Renata Mota (org). São Paulo: Quartier Latin, 2019.

FLORIDI, Luciano. **The Fourth Revolution** – How the infosphere is reshaping human reality. Oxford: Oxford University, 2014.

GOLDIM, J.R. Consentimento, Alteridade e Capacidade. *In: Direito, Cultura e Método - Leituras da obra de Judith Martins-Costa*. Giovana Benetti; André Rodrigues Corrêa; Márcia Santana Fernandes; Guilherme Monteiro Nitschke; Mariana Pargendler; Laura Beck Varela. (org.). 1ed. Rio de Janeiro: GZ Editora, 2019, v. 1, p.168-181.

MARTINS-COSTA, Judith. **A Boa-Fé no Direito Privado** – critérios para sua aplicação. São Paulo: Marcial Pons, 2015.

MENNA BARRETO, Sílvia W.; FERNANDES, Márcia S. **Pesquisa Clínica e os vínculos de trabalho**. São Paulo: Editora Mizuno, 2021. *E-book*.

MIZIARA, RAPHAEL. **Reflexos da LGPD no direito e no processo do trabalho**. São Paulo: Thomson Reuters, 1 ed. 2020. p. 19. *E-book*.

SARLET, Gabrielle B. S.; FERNANDES, Márcia S.; RUARO, Regina L. A proteção de dados no setor da saúde em face do sistema normativo brasileiro atual. *In: Tratado de Proteção de Dados Pessoais*. Mendes, Laura; Doneda, Danilo; Sarlet, Ingo W. e Rodrigues Jr.; Otávio (coord). Rio de Janeiro: Editora Forense, 2021.

24. LEI GERAL DE PROTEÇÃO DE DADOS E PRINCÍPIO DA PROTEÇÃO NA RELAÇÃO LABORAL

RENATA DUVAL MARTINS¹

Resumo

O presente artigo tem por escopo realizar análise da aplicação da Lei Geral de Proteção de Dados na esfera laboral, tendo por base a vulnerabilidade do trabalhador e o Princípio da Proteção. Aborda-se a real liberdade do empregado para consentir ou não sobre o tratamento de seus dados pelo empregador, bem como a necessidade de expansão dos Direitos Humanos Laborais no Brasil cabendo à sociedade científica realizar estudos aprofundados sobre a proteção de dados nas relações de trabalho.

Palavras-chave: Lei Geral de Proteção de Dados; Direito Laboral; Vulnerabilidade do Trabalhador; Princípio da Proteção.

Abstract

This article aims to analyze the application of the General Data Protection Law in the labor sphere, based on the vulnerability of the worker and the Principle of Protection. It addresses the real freedom of the employee to consent or not to consent to the processing of his data by the employer, as well as the need to expand Human Labor Rights in Brazil with the scientific society being responsible for carrying out in-depth studies on data protection in labor relations.

Keywords: General Data Protection Law; Labor Law; Worker Vulnerability; Protection Principle.

1. Introdução

O presente artigo aborda a aplicação da Lei Geral de Proteção de Dados (LGPD) à prática trabalhista no Brasil, considerando a vulnerabilidade do trabalhador e o Princípio da Proteção como bases norteadoras da análise. Assim, verifica-se que a proteção do titular dos dados proposta na LGPD é insuficiente diante da realidade de subordinação jurídica e econômica dos empregados.

Na primeira parte do trabalho, discorre-se sobre a hipossuficiência do trabalhador e sua vulnerabilidade perante o empregador, tendo em vista a subordinação jurídica e a subordinação econômica, típicas da relação laboral. Assim, indica-se o Princípio da Proteção, direcionador da atuação do legislador na formulação das normas e dos magistrados na aplicação e interpretação da lei, como necessário na análise do caso concreto a fim de aferir a real liberdade do empregado para consentir ou não sobre o tratamento de seus dados pelo empregador.

Na segunda parte, abordam-se as normas da LGPD essenciais na análise dos exemplos expostos na terceira parte do estudo, são estas: princípios da proteção de

¹ Doutoranda em Direito pela Universidade Federal do Rio Grande do Sul. Mestra em Direito pela Universidade Federal do Rio Grande do Sul. Assistente em Administração na Universidade Federal do Rio Grande. Advogada.

dados (artigo 6º); conceitos de dado pessoal, de dado pessoal sensível e de tratamento de dados (artigo 5º); determinações relativas ao consentimento para o tratamento dos dados não sensíveis e dos dados sensíveis (artigos 7º e 11); direitos do titular dos dados (artigo 9º); legítimo interesse do controlador e o tratamento de dados pessoais estritamente necessários para a finalidade pretendida (artigo 10); e hipóteses de término do tratamento dos dados pessoais (artigo 15). Já na terceira parte são analisados oito exemplos de conflitos entre empregador e empregado, aplicando a estes a LGPD e o Princípio da Proteção do Direito Laboral.

Desta forma, verifica-se que a aplicação da proteção de dados à relação empregatícia é essencial a fim de preservar a intimidade, a privacidade e a dignidade do trabalhador vulnerável. No entanto, tal deve ter por base o Princípio da Proteção, bem como a ampliação dos Direitos Humanos Laborais no âmbito nacional.

2. Aspectos teóricos do Direito do Trabalho

Os hipossuficientes são os “não proprietários, que só possuem sua força de trabalho” a fim de alcançar os meios necessários para a sua sobrevivência, ou seja, o trabalhador empregado que vende a sua força de trabalho para o empregador. A doutrina também diferencia autossuficientes e hipersuficientes, os primeiros são os “proprietários de capitais, imóveis, mercadorias, maquinaria, terras”, enquanto os segundos “são auto-suficientes em posição econômica superior”, grandes capitalistas ou industriais (CESARINO JÚNIOR, 1980, pp. 44-45). Apenas o grupo dos hipossuficientes é objeto de proteção para o Direito do Trabalho, tendo em vista sua situação de hipossuficiência absoluta relativamente aos dois outros grupos.

A proteção do trabalhador vulnerável, hipossuficiente absoluto, também decorre da sua subordinação ao empregador, fator que configura a disparidade de forças entre as partes da relação contratual. A desigualdade econômica, a hierarquia e a prevalência dos interesses do empregador também corroboram para a vulnerabilidade do empregado. A subordinação é jurídica quando se relaciona aos poderes do empregador (dirigir as atividades, fiscalizá-las, cessar o contrato de trabalho) e é econômica quando relativa à necessidade que o trabalhador tem do salário para garantir a sua subsistência (dependência econômica da remuneração).

Em razão desta vulnerabilidade do empregado perante o empregador, o Direito do Trabalho tem como base o Princípio da Proteção, indicando aquele como a parte mais frágil na relação empregatícia, direcionando a atuação do legislador na formulação das normas e dos magistrados na aplicação e interpretação da lei. Também, justifica garantias aos trabalhadores previstas na Constituição Federal (CF) e na Consolidação das Leis do Trabalho (CLT) – como a irredutibilidade de remuneração (artigo 7º, inciso VI, da CF); a justa causa reversa (artigo 483 da CLT); a proteção à maternidade e à paternidade (artigo 7º, incisos XVIII e XIX, da CF) –, não sendo menor a sua força sobre as normas da LGPD. Assim, cabe ao operador desta aplicá-la e interpretá-la para as relações laborais sempre tendo em vista o Princípio da Proteção.

Por todo o exposto, a questão do livre consentimento (artigo 5º da LGPD) é relativizada pelo Direito do Trabalho, não sendo suficiente para eximir o empregador de suas responsabilidades decorrentes do mau tratamento dos dados

de seus empregados. Logo, é necessária a análise do caso concreto a fim de aferir a real liberdade para consentir ou não, tendo em vista que, em razão de sua vulnerabilidade: o indivíduo em busca de trabalho que recusar consentimento para o tratamento de seus dados, provavelmente não será contratado; e o indivíduo já empregado que recusar consentimento para o tratamento de seus dados, possivelmente será demitido.

3. Aspectos teóricos da LGPD

Algumas normas da LGPD serão essenciais na análise realizada no próximo subtítulo, no qual serão abordados exemplos de conflitos entre empregador e empregado, por isso cabe explicá-las detalhadamente antes de aplicá-las à realidade laboral, são elas: princípios da proteção de dados (artigo 6º); conceitos de dado pessoal, de dado pessoal sensível e de tratamento de dados (artigo 5º); determinações relativas ao consentimento para o tratamento dos dados não sensíveis e dos dados sensíveis (artigos 7º e 11); direitos do titular dos dados (artigo 9º); legítimo interesse do controlador e o tratamento de dados pessoais estritamente necessários para a finalidade pretendida (artigo 10); e hipóteses de término do tratamento dos dados pessoais (artigo 15).

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tra-

tamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Sobre o Princípio da Boa Fé, trata-se de uma cláusula geral que contém um princípio, razão para a sua inserção em destaque no caput do artigo, logo, garante a coesão na interpretação e na aplicação da lei. A “[...] Boa fé é um pensar refletido, é o pensar no outro, no mais fraco, no parceiro contratual, nas suas expectativas legítimas, é lealdade, é transparência, é informação, é cooperação, é cuidado, é visualização e respeito pelo outro [...]” (MARQUES, 2002, p. 48). Ademais, implica nos deveres de informar, de transparência e de cooperar (MARQUES, 2002, p. 50-51), evitando a violação de dados pessoais e de dados sensíveis no curso de seu tratamento. No artigo 5º, incisos I, II e X, da LGPD constam as definições de dado pessoal, de dado pessoal sensível e de tratamento de dados:

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Os dados de caráter pessoal contêm informação das

pessoas físicas que permitem sua identificação no momento ou posteriormente. Na sociedade tecnológica, os cadastros armazenam alguns dados que possuem um conteúdo especial, e por isso são denominados dados sensíveis. Tais dados podem referir-se a questões como ideologia, religião ou crença, origem racial, saúde ou vida sexual. Exige-se que os cadastros que os armazenam contenham uma segurança especial, como forma de evitar que sejam mal utilizados. Com as cautelas especiais relativas aos dados sensíveis, seja quando são recolhidos, seja quanto à segurança em seu armazenamento, tenta-se garantir que os mesmos não sejam utilizados para outra finalidade ou de maneira equivocada. O dado pessoal é uma informação que permite identificar uma pessoa de maneira direta. A proteção do dado sensível tenta prevenir ou eliminar discriminações. Pode-se dizer que é uma nova leitura do princípio da igualdade, e sua intenção é a de que os dados armazenados não sirvam para prejudicar as pessoas.²

O Princípio da Finalidade impõe que “qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados” (DONEDA, 2011, p. 100). Além disso, o princípio fundamenta a restrição da “transferência de dados pessoais a terceiros”, bem como estrutura “um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade)” (DONEDA, 2011, p. 100). Enquanto, o Princípio da Adequação determina que as informações obtidas sejam “adequadas, pertinentes e não excessivas em relação a seus fins” (MAIA, 2006, p. 463), bem como limita o modo de coleta dos dados, pois “todos os dados devem ser obtidos por meios legais e justos, onde seja adequado, com o conhecimento ou consentimento do sujeito dos dados” (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [on line]). Já o Princípio da Necessidade determina a “limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados”, ou seja, não se devem tratar mais dados do que o necessário para os fins almejados. Ademais, o princípio se encontra projetado ao longo de outros dispositivos da LGPD, como o artigo 10:

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

- I - apoio e promoção de atividades do controlador; e
- II - proteção, em relação ao titular, do exercício re-

² LIMBERGER, Têmis. **Da evolução do direito a ser deixado em paz à proteção dos dados pessoais.** [on line] p. 149-150.

gular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

O Princípio do Livre Acesso determina que o indivíduo tenha acesso ao banco de dados a seu respeito, podendo solicitar a correção das informações incorretas, obsoletas ou impertinentes (DONEDA, 2011, pp. 100-101). Ademais, impõe que “os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade que sua coleta e seu tratamento sejam feitos com cuidado e correção, e que sejam realizadas atualizações periódicas destes dados conforme a necessidade” (MAIA, 2006, p. 463). O supracitado princípio se encontra projetado ao longo da LGPD, especialmente no artigo 9:

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

- I - finalidade específica do tratamento;
- II - forma e duração do tratamento, observados os segredos comercial e industrial;
- III - identificação do controlador;
- IV - informações de contato do controlador;
- V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
- VI - responsabilidades dos agentes que realizarão o tratamento; e
- VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência,

de forma clara e inequívoca.

§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

O Princípio da Qualidade dos Dados trata da “exatidão dos dados pessoais alvo de tratamento” (KAMEDA; PAZELLO, 2015, p. 8), impondo que “os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade” (DONEDA, 2011, p. 100), bem como que “os dados pessoais devem ser relevantes para os fins para os quais devem ser utilizados e, na medida do necessário para esses fins, devem ser precisos, completos e atualizados” (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [on line]). Já o Princípio da Transparência determina que “a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja através da exigência de autorização prévia para seu funcionamento, pela notificação de sua criação a uma autoridade; ou pela divulgação de relatórios periódicos” (MAIA, 2006, p. 463), bem como “toda pessoa tem direito à informação por parte do responsável pelo tratamento de dados que lhe digam respeito, inclusive no que tange ao modo, à finalidade, período de conservação etc” (CORRÊA; GEDIEL, 2008, p. 147). O supracitado princípio se projeta em vários dispositivos da LGPD, especialmente nos artigos 9º e 10, abordados anteriormente.

O Princípio da Segurança protege a privacidade da pessoa titular dos dados (MAIA, 2006, p. 464). Logo, referido princípio é violado quando não são os dados do titular protegidos, física e logicamente, contra riscos de extravio, destruição, modificação, perda, transmissão, acesso não autorizado ou divulgação não permitida (DONEDA, 2011, p. 101), podendo causar prejuízos com “impacto sobremaneira elevado” (LIMA; MONTEIRO, 2013, pp. 68-69). Enquanto, o Princípio da Prevenção se refere à “utilização das medidas técnicas e administrativas proporcionais ao atual estado da tecnologia, à natureza dos dados pessoais e às características específicas do tratamento”, prevenindo “destruição, perda, alteração e difusão, tanto acidentais quanto ilícitas, bem como o acesso não autorizado” (KAMEDA; PAZELLO, 2015, p. 8) dos dados.

Sobre o Princípio da Não Discriminação, este protege os dados sensíveis – conceito no artigo 5º, inciso II, da LGPD –, as liberdades individuais e a dignidade humana perante a livre-iniciativa. Além disso, o princípio preserva a autodetermi-

nação informativa, pois garante a liberdade do titular fornecer ou não seus dados, corrigir ou cancelar cadastros próprios, sem ser prejudicado por tal motivo. Logo, verifica-se que o princípio se projeta em outros dispositivos da LGPD, como os artigos 7º e 11, que tratam do consentimento para o tratamento de dados pessoais e de dados sensíveis, e o artigo 15, que traz as hipóteses de término do tratamento dos dados pessoais por comunicação do titular revogando o consentimento.

Com respeito aos artigos 7º³ e 11 da LGPD, impõem que o consentimento para a coleta de dados não sensíveis deve ser livre, informado e inequívoco, nos casos em que a lei exigir, enquanto o consentimento para a coleta de dados sensíveis deve ser livre, informado, inequívoco, específico e destacado, excepcionalmente tratados sem o consentimento do titular nas hipóteses em que forem indispensáveis, conforme os casos definidos em lei:

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir,

3 Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei.

de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Enquanto, o artigo 15 da LGPD aborda as hipóteses de término do tratamento dos dados pessoais, como: a “verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada” (inciso I); o “fim do período de tratamento” (inciso II); a “comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento [...], resguardado o interesse público” (inciso III); a “determinação da autoridade nacional” (inciso IV).

Por fim, o Princípio da Responsabilização e Prestação de Contas determina a “demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas”. Caso não seja comprovada a adoção e eficácia, tal gera o dever de reparar quaisquer danos patrimoniais e morais causados aos titulares dos dados pessoais expostos.

4. LGPD e relação empregatícia

No presente subtítulo, a fim de facilitar o entendimento dos efeitos da vulnerabilidade do empregado e do Princípio da Proteção, elementos basilares do Direito

do Trabalho brasileiro, na interpretação e aplicação da LGPD ao caso concreto, a análise será realizada por meio de exemplos, indicando ao empregador como realizar o tratamento dos dados coletados tanto de indivíduos à procura de emprego, quanto daqueles efetivamente contratados. Sobre o tratamento de dados nas diferentes fases da relação empregatícia:

No âmbito trabalhista, portanto, os impactos dos direitos dos titulares dos dados pessoais serão bastantes relevantes, eis que englobam os mais diversos momentos da relação empregatícia:

I. Fase pré-contratual: Durante todo o processo seletivo e suas fases anteriores à celebração do contrato de emprego, a empresa recebe diversas informações sobre o candidato, currículo, histórico funcional, dados pessoais, incluindo endereço, estado civil etc., o que, inclusive deve gerar a “revisão por parte dos recursos humanos quanto aos processos seletivos, para contratação laboral, especialmente quanto ao tipo de informações/dados requisitados aos candidatos, especialmente aqueles considerados sensíveis”, devendo ainda ter a cautela de requerer o consentimento deles para eventual armazenamento dos currículos em bancos de dados para futuros processos seletivos, para aqueles candidatos que não tenham sido selecionados;

II. Fase de formalização do contrato: Na celebração do contrato de trabalho, são coletados dados cadastrais como CPF, RG, CNH, título de eleitor, carteira de reservista, CTPS, PIS, filiação a sindicato, endereço, nomes dos genitores, escolaridade, situação familiar, nomes dos filhos, idade, tipo sanguíneo, propriedade de veículo, marca, cor, modelo, placa policial, para permitir acesso ao estabelecimento empresarial etc.;

III. Fase contratual: No decorrer da execução do contrato de trabalho é gerada outra enormidade de dados pessoais, tais como os referentes à jornada de trabalho, inclusive aqueles mais sensíveis como os biométricos usualmente coletados pelos empregadores que se valem de registro eletrônico de ponto, o valor do salário/remuneração, descontos, faltas e seus respectivos motivos (justificáveis ou não), doenças, incluindo todo prontuário de saúde, com exames admissionais e periódicos (atestados de saúde ocupacionais – ASO’s), acidentes de trabalho, utilização de informações para geolocalização dos funcionários, dados eventualmente solicitados pelo sindicato da categoria, situações conjugais que podem ter reflexos em providências da empresa, como o pagamento de

pensão alimentícia, inclusão de um dependente no plano de saúde, escolha dos beneficiários de um seguro de vida ou de benefícios previdenciários, dados decorrentes da monitorização do trabalhador, por meio de sistemas que permitem aos empregadores controlar quem pode entrar nas suas instalações e/ou certas áreas e departamentos, rastreando as atividades dos funcionários etc.;

IV. Fase pós-contratual: Dados relevantes também surgem ao término do contrato de trabalho, tais como informações sobre o motivo do desligamento, valor das verbas rescisórias, dados pessoais de empregado falecido, questões ligadas a possíveis pedidos de referência sobre o ex-empregado a pedido de futuros empregadores, dados necessários à elaboração do Perfil Profissiográfico Previdenciário-PPP, que acaba sendo por si só um documento que deve ser objeto de tratamento, justamente por conter todo histórico-laboral do trabalhador reunindo dados das mais diversas matizes durante todo o período em que este exerceu suas atividades na respectiva empresa etc.;

V. Relações interempresariais: Há ainda necessidade de tratamento de dados em relação a eventuais empregados das empresas terceirizadas que forem eventualmente compartilhados com a contratante, tais como prestadores de serviço de limpeza e segurança, por exemplo.⁴

Inicia-se a análise com três exemplos hipotéticos no período de seleção para emprego: 1º) um indivíduo em busca de emprego entrega seu currículo em vários possíveis locais de trabalho, porém, em um destes estabelecimentos, uma loja de venda de calçados, o currículo entregue é descartado e usado para a confecção de etiquetas dos produtos comercializados e dispostos em prateleiras ao alcance dos clientes. Logo, qualquer pessoa na loja, ao virar as etiquetas dos produtos, encontra em seu verso os dados fornecidos no currículo descartado; 2º) um indivíduo em busca de emprego entrega seu currículo em vários possíveis locais de trabalho, porém, em um destes estabelecimentos, os dados fornecidos são cadastrados para fim diverso – envio de promoções ao titular dos dados. Este, além de não conseguir a vaga de emprego, passa a receber mensagens no celular e/ou e-mails promocionais do referido estabelecimento comercial; 3º) a empresa X está contratando funcionários e obtém acesso a um banco de dados da empresa Y, neste verifica que um dos concorrentes à vaga sofre de uma doença grave, porém que não o incapacita para o trabalho. Logo, tendo em vista o conhecimento deste dado sensível por parte da empresa, esta decide não contratar o trabalhador.

Observa-se que em todos os exemplos há violação das diretrizes expostas na LGPD, com alguns pontos de convergência. No primeiro caso, ocorreu o vazamento

4 CONI JUNIOR, Vicente Vasconcelos; PAMPLONA FILHO, Rodolfo. **A Lei Geral de Proteção de Dados e seus reflexos nas relações jurídicas trabalhistas**. 2020, pp. 74-124.

para terceiros dos dados fornecidos pelo titular, tendo em vista que qualquer pessoa teve acesso aos dados quando o currículo não foi descartado corretamente, sendo reutilizado na confecção das etiquetas dos produtos. Assim, verifica-se neste caso violação dos Princípios da Boa-Fé, da Segurança e da Responsabilização (artigo 6º, caput, incisos VII e X, da LGPD), bem como do artigo 15 da LGPD.

Afinal, o empregador foi descuidado com os dados do indivíduo à procura de trabalho, favorecendo a transmissão destes a terceiros não autorizados, bem como não adotando medidas eficazes capazes de proteger os dados que lhe foram fornecidos. Ressalta-se que para proteger física e logicamente os dados, deveria o empregador reforçar a segurança no tratamento destes, adotando medidas a fim de evitar falhas, como, por exemplo, criar bancos de dados no meio digital criptografados⁵ ou um arquivo físico protegido, nos quais fossem armazenados os currículos recebidos.

Ademais, conforme estipula o artigo 15, inciso I, da LGPD, termina o tratamento dos dados pessoais quando verificado “que a finalidade foi alcançada ou [...] que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada”, portanto, encerrada a seleção de emprego, cabia ao empregador desfazer-se dos dados de forma segura. Por fim, demonstrado que não houve a adoção de medidas eficazes e capazes de proteger os dados pessoais do titular, gera-se no caso ora analisado o dever de reparar quaisquer danos patrimoniais e morais causados ao titular dos dados pessoais expostos.

No segundo exemplo, ocorreu a utilização dos dados para fins diversos daqueles para os quais o titular consentiu, tendo em vista que estes foram fornecidos especificamente para concorrer à vaga de trabalho, não para integrar a clientela da empresa. Logo, verifica-se neste caso violação dos Princípios da Boa-Fé, Finalidade e Responsabilização (artigo 6º, caput, incisos I e X, da LGPD), bem como dos artigos 7º e 15 da LGPD. Isto porque o empregador foi desleal ao coletar dados e utilizá-los para fins distintos ao que justificou sua coleta, logo, os dados obtidos em currículo para fins de seleção de emprego não poderiam ter sido utilizados pelo empregador para qualquer outro fim, nem mesmo para comunicações futuras cujo objetivo não fosse a oferta de vaga de emprego⁶.

5 A autora Tatiana Roxo, ao abordar o tema da implementação prática de um programa empresarial de proteção de dados, expõe: “A implementação do programa será feita de acordo com o porte e a capacidade econômica das companhias, sob pena de inviabilização da observância da lei. De toda sorte, a despeito das diferenças na forma como os programas serão adotados, inclusive em relação ao uso de recursos tecnológicos, é possível seguir um conjunto de procedimentos básicos, dentro da realidade de cada empresa, de forma a explorar a atividade econômica respeitando as normas de proteção aos dados pessoais.” (ROXO, Tatiana Bhering. **Como implementar na prática um programa de proteção de dados**. 2020, pp. 296-326)

Compreende-se que o programa de proteção de dados deve ser adequado a capacidade econômica das empresas, no entanto, é importante ressaltar que a criação de pastas criptografadas (a fim de guardar documentos que necessitam de maior proteção/sigilo) em dispositivos eletrônicos, atualmente, pode ser realizada de forma fácil e gratuita por indivíduos sem grandes conhecimentos de informática. Nos computadores, por exemplo, pode-se fazer download do Software VeraCrypt e nos celulares do Encrypted Data Store - EDS lite. Ambos os programas contam com criptografia avançada, são gratuitos e seguros. Logo, são meios acessíveis aos pequenos empregadores a fim de garantir a proteção de informações relevantes. Obviamente, médias e grandes empresas precisarão desenvolver programas mais complexos para a proteção de dados.

6 “qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados” (DONEDA, 2011, p. 100)

Ademais, foi violado o artigo 7º da LGPD, pois o titular não consentiu o tratamento dos seus dados não sensíveis para fins diversos, bem como foi violado o artigo 15, inciso I, da LGPD, pois termina o tratamento dos dados pessoais quando verificado “que a finalidade foi alcançada ou [...] que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada”, portanto, encerrada a seleção de emprego, cabia ao empregador desfazer-se dos dados de forma segura. Por fim, demonstrado que não houve a adoção de medidas eficazes e capazes de proteger os dados pessoais do titular, gera-se no caso ora analisado o dever de reparar quaisquer danos patrimoniais e morais causados ao titular dos dados pessoais expostos.

No terceiro exemplo, a empresa Y e a empresa X violaram diretrizes da LGPD. Esta relativamente aos Princípios da Boa-Fé e Não Discriminação. Aquela relativamente aos Princípios da Boa-Fé, Finalidade, Segurança, Prevenção e Responsabilidade, bem como ao artigo 11 (consentimento para o tratamento dos dados sensíveis) e artigo 9º, inciso V (direitos do titular dos dados sobre informações acerca do uso compartilhado de dados pelo controlador e a finalidade). Observa-se que ambas as empresas foram desleais em relação ao titular dos dados: a empresa Y ao transmitir dado sensível, potencialmente prejudicial, não adotando as medidas necessárias para manter seu sigilo e evitar o acesso de terceiros; e a empresa X ao acessar tais dados que não lhe foram fornecidos pelo próprio titular, usando a informação sobre a saúde deste desfavoravelmente na seleção para vaga de emprego.

Prosseguindo na análise, têm-se quatro exemplos relativos ao período de contrato, ou seja, de efetivo exercício da atividade laboral: 1º) o empregador decide monitorar os empregados a fim de aumentar a produtividade e lucratividade de seu negócio, assim, instala secretamente nos computadores da empresa software de espionagem, com este consegue ter acesso às telas de computador dos empregados em tempo real, lê mensagens do e-mail pessoal, vê fotos e vídeos do instagram, whatsapp, etc. (monitoramento online), recebe cópia de tudo que é por estes digitado, inclusive senhas de sites, número de cartão de crédito, etc. (*keylogger*); 2º) o empregador decide monitorar os empregados a fim de garantir que estes não estão concorrendo de forma desleal com ele no horário fora de expediente, assim, instala secretamente nos celulares da empresa software de espionagem, com este consegue rastrear o empregado por meio do GPS aparelho, bem como gravar as chamadas recebidas/realizadas e os sons dos arredores do telefone; 3º) o empregador decide instalar câmeras no local de trabalho a fim de por meio de reconhecimento facial realizar o registro do horário de trabalho de seus funcionários, bem como garantir maior segurança em seu estabelecimento, sendo as alterações realizadas sem a ciência dos empregados; 4º) o empregador opta por realizar as reuniões da empresa por meio virtual, registrando por meio de gravação e de *prints* esse momento com a equipe de funcionários. A gravação é guardada nos arquivos criptografados da empresa, no entanto, os *prints* feitos são disponibilizados nas redes sociais para fins comerciais sem o consentimento e ciência dos funcionários.

Observam-se nos exemplos 1º e 2º vários pontos de convergência, pois ambos os casos apresentam a violação do direito à privacidade dos trabalhadores e abuso

do poder de direção⁷ por parte do empregador. No primeiro caso, o empregador extrapola seu direito de fiscalizar o trabalho executado nas dependências da empresa, enquanto no segundo caso, o empregador intrumete-se na vida privada do funcionário até mesmo fora do horário de expediente. Ademais, em nenhuma das situações os empregados foram informados sobre a vigilância, tampouco consentiram com a coleta de seus dados pelo empregador.

Verifica-se em ambos os casos violação dos Princípios da Boa-Fé, da Finalidade, da Adequação, da Necessidade e da Transparência, afinal os empregados foram tratados com deslealdade, seus dados coletados para propósitos não legítimos e não explícitos, não foram informados a respeito da vigilância, sendo esta imperitante, desproporcional, excessiva e realizada de forma inadequada ao contexto laboral. Também, ocorreu a violação dos artigos 7º e 9º da LGPD, tendo em vista que não houve consentimento para a coleta de dados, logo, os empregados sequer tiveram a oportunidade de receber informações sobre o tratamento de suas informações pessoais.

Importante ressaltar que não existem justificativas legais para que o empregador monitore a vida do empregado de forma descomedida, conforme os exemplos citados, ainda que o objetivo seja evitar a procrastinação ou a concorrência desleal do funcionário. Os empregados têm o direito de saber: que estão sendo monitorados; as razões para serem monitorados; a base legal do monitoramento; as informações coletadas pelo empregador; o período que estas informações ficarão retidas; seus direitos quanto às informações coletadas; e o direito de revogar o consentimento dado para a coleta.

Isto não significa que o empregador está impedido de exercer qualquer monitoramento, mas que deve realizá-lo com respeito à privacidade, intimidade e dignidade do empregado. Logo, o consentimento deste e a transparência sobre o procedimento adotado pela empresa são essenciais, podendo o empregador, por exemplo, adotar o bloqueio de sites não relacionados ao trabalho (facebook, instagram, youtube, etc.) nos computadores da empresa, não sendo esta considerada uma medida invasiva de vigilância. Ainda é possível ao empregador exercer o seu poder de direção, porém este deve ser exercido com razoabilidade e proporcionalidade; o empregador pode coletar os dados do empregado, mas apenas para finalidades legítimas, bem como necessários para fins previamente informados.

Nos exemplos 3º e 4º a violação é de dados considerados sensíveis, pois ocorre a coleta das imagens dos empregados, logo, o ataque é à norma do artigo 11 da LGPD. Em ambas as situações, os empregadores falham por não dar ciência aos empregados, tampouco solicitar o consentimento destes para as ações de coleta

7 “O empregador é dotado do poder de direção por comandar, escolher e controlar os fatores de produção da empresa. O poder de direção se desdobra em poder diretivo, em poder disciplinar e em poder hierárquico ou de organização.

Poder diretivo - Constitui a capacidade de o empregador de dirigir a empresa, escolher seus rumos e estratégias, dar conteúdo concreto à atividade do trabalhador, visando aos objetivos da empresa.

Poder disciplinar - Traduz-se no poder que tem o patrão de impor punições aos empregados.

Poder hierárquico ou de organização - Capacidade do empregador de determinar e organizar a estrutura econômica e técnica da empresa, aí compreendida a hierarquia dos cargos e funções.” (CASSAR, Vólia Bomfim. **Resumo de Direito do Trabalho**. 2018, pp. 49-50)

de dados realizadas pela empresa. Logo, observa-se que não é proibido ao empregador instalar câmeras de segurança, realizar reconhecimento facial para registro do horário de trabalho, gravar as reuniões da empresa realizadas por meio virtual ou fazer *prints* desta atividade. No entanto, o empregado deve ser previamente informado, bem como concordar com a coleta e disponibilização de sua imagem para fins comerciais.

Verifica-se violação aos Princípios da Boa-Fé, da Transparência e da Segurança. Afinal, o empregador omitiu informações dos empregados, bem como não solicitou a concordância destes para a coleta de dados. Também, não protegeu os dados coletados contra os riscos de sua transmissão, inclusive, no último exemplo, divulgou-os sem a anuência dos titulares. Além disso, as violações aos artigos 9º, incisos I e II, e 11, inciso II, alínea g, da LGPD, decorrem da coleta e transmissão da imagem do trabalhador (dado sensível) sem o consentimento deste, sem informá-lo da finalidade específica do tratamento, tampouco sua forma e duração. Ademais, o artigo 10 da LGPD foi violado, tendo em vista que, apesar de haver legítimo interesse do controlador na coleta dos dados e o tratamento destes ser estritamente necessário para a finalidade pretendida (segurança do local, controle de jornada, propaganda empresarial), não houve transparência por parte do empregador quanto à realização da coleta.

Salienta-se que no quarto exemplo se enfrenta a questão do consentimento livre do empregado no curso da relação de emprego. Conforme exposto no início do presente artigo, o trabalhador – “não proprietários, que só possuem sua força de trabalho” (CESARINO JÚNIOR, 1980, pp. 44-45) – é um hipossuficiente, sendo objeto de proteção para o Direito do Trabalho. A vulnerabilidade decorre de sua subordinação – jurídica e econômica – ao empregador, tendo em vista a desigualdade hierárquica e econômica da relação. Logo, precisa vender a sua força de trabalho para sobreviver, dependendo da remuneração recebida para tanto, provavelmente, o empregado se sujeitará aos desígnios do empregador, cedendo sempre às determinações deste. Inclusive, consentindo com a coleta de dados pessoais e/ou sensíveis a fim de evitar a perda do emprego. Dificilmente o empregado poderá manifestar seu desconforto ou discordância com a coleta das informações sem que seja repreendido pelo empregador.

Em razão do exposto, o Princípio da Proteção será muito necessário no curso de processos judiciais trabalhistas sobre a coleta de dados pessoais e/ou sensíveis de empregados, pois, em razão de sua vulnerabilidade perante o empregador, a possibilidade de o empregado fornecer o seu consentimento livre para o tratamento de dados é discutível. Logo, caso o empregado afirme que se sentia coagido a ceder seus dados ao empregador, bem como o empregador não comprove nos autos que a coleta respeitava os limites impostos pelos princípios de proteção de dados do artigo 6º da LGPD (inversão do ônus da prova⁸), cabe ao magistrado

8 Assim como já ocorre em relação à comprovação da jornada de trabalho: Súmula nº 338 do TST

JORNADA DE TRABALHO. REGISTRO. ÔNUS DA PROVA (incorporadas as Orientações Jurisprudenciais nºs 234 e 306 da SBDI-1) - Res. 129/2005, DJ 20, 22 e 25.04.2005

I - É ônus do empregador que conta com mais de 10 (dez) empregados o registro da jornada de trabalho na forma do art. 74, § 2º, da CLT. A não-apresentação injustificada dos controles de frequência

reconhecer a maior fragilidade do empregado na relação empregatícia, reparando o mal sofrido.

Por último na análise, tem-se um exemplo relativo ao período de encerramento do contrato de trabalho: um empregado, ciente do monitoramento dos computadores da empresa, utiliza sua conta pessoal de troca de mensagens (whats app web, facebook messenger, etc.) no referido dispositivo eletrônico e em mensagem para terceiro admite conduta passível de justa causa. O empregador tem acesso à comunicação e demite o funcionário.

Observa-se que o empregador informou o empregado a respeito da coleta de dados nos computadores da empresa, bem como este consentiu com a prática. No entanto, apesar de ciente do monitoramento, o funcionário utilizou conta pessoal de troca de mensagens no dispositivo eletrônico. Ainda que se possa afirmar que cabia ao empregado ter o devido cuidado com suas contas pessoais, não as utilizando nas máquinas da empresa⁹, é importante ressaltar que os dados só podem

gera presunção relativa de veracidade da jornada de trabalho, a qual pode ser elidida por prova em contrário. (ex-Súmula nº 338 – alterada pela Res. 121/2003, DJ 21.11.2003)

II - A presunção de veracidade da jornada de trabalho, ainda que prevista em instrumento normativo, pode ser elidida por prova em contrário. (ex-OJ nº 234 da SBDI-1 - inserida em 20.06.2001)

III - Os cartões de ponto que demonstram horários de entrada e saída uniformes são inválidos como meio de prova, invertendo-se o ônus da prova, relativo às horas extras, que passa a ser do empregador, prevalecendo a jornada da inicial se dele não se desincumbir. (ex-OJ nº 306 da SBDI-1- DJ 11.08.2003)

9 Na decisão de 1º Grau do Processo nº 0000505-73.2017.5.10.0007 (tramitando no TRT10), um dos pontos tratados foi a dispensa por justa causa de trabalhadora que, apropriando-se de agenda esquecida por colega no local de trabalho, na qual constavam as senhas das redes sócias desta, acessou as contas particulares da mesma e fez inúmeros comentários e postagens desabonadoras. Os atos da trabalhadora contra a colega foram descobertos, pois a primeira esqueceu o whats app web aberto em computador da escola, vindo três outros funcionários a ter acesso aos diálogos nos quais a trabalhadora confessava para outras pessoas ser a responsável pelos atos difamatórios. Assim, o Tribunal Regional do Trabalho da 10ª Região confirmou a justa causa, discorrendo que cabe ao próprio empregado ter o devido cuidado com as suas contas particulares, desconectando-as após o uso, a fim de que suas correspondências pessoais não permaneçam abertas nas máquinas da empresa, podendo seu empregador lê-las.

Discorda-se do exposto na decisão, por dois motivos:

1º) ressalta-se que afirmar que um empregador curioso tem o direito de ler uma conversa de cunho privado, realizada em conta particular, pois aberta e acessível no computador da empresa, violando o artigo 5º, inciso XII, da Constituição Federal – “é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal” – não difere de afirmar: se o empregado esquecer a chave de sua casa no local de trabalho, isto dá direito ao empregador adentrar sua residência sem autorização, ou seja, dá-se o direito de violar o artigo 5º, inciso XI, da Constituição Federal – “a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial” –, afinal tem a posse da chave e esta foi negligenciada em sua propriedade.

2º) Ainda que na decisão supracitada a trabalhadora tenha cometido falta punível com justa causa, o empregador não confirmaria o fato sem o acesso às conversas privadas na rede social da empregada, ou seja, sem a grave violação do artigo 5º, inciso XII, da Constituição Federal. Apesar da conduta terrível da trabalhadora, tal não justifica que o Poder Judiciário apoie violação de garantia fundamental da Carta Maior, afinal a única exceção à inviolabilidade do sigilo das comunicações pessoais é a ordem judicial, não existindo menção na lei às exceções: curiosidade do empregador; ou cometimento de

ser coletados para finalidades específicas (Princípio da Finalidade), só devem ser coletados os dados realmente necessários (Princípio da Necessidade) e as informações obtidas devem ser pertinentes e não excessivas (Princípio da Adequação). Tendo por escopo o presente artigo uma análise condizente com os direitos humanos, considera-se que obter dados de contas pessoais dos trabalhadores deveria ser considerado desnecessário, desleal e inadequado em quaisquer hipóteses.

Logo, em uma análise ideal da relação trabalhista, na qual prevalecessem os direitos humanos laborais, tendo relevância a vulnerabilidade do trabalhador e o Princípio da Proteção, poderia se estabelecer dois limites: 1º) a coleta de dados nos dispositivos da empresa deve ser usada para fins punitivos apenas se previamente cientificado o empregado de tal possibilidade; 2º) jamais deve ser realizada a coleta de dados em contas particulares dos trabalhadores, mesmo se acessadas nos dispositivos da empresa, podendo o empregador bloquear os aplicativos nos dispositivos de trabalho ou proibir seu uso no local.

Ademais, ainda imaginando um cenário laboral condizente com a igualdade em dignidade das partes contratantes, o empregador que cometer a falta grave de violar as comunicações privadas em contas particulares de funcionário, vindo a descobrir falta grave deste passível de demissão por justa causa, teria duas opções: 1º) poderia demitir o empregado sem justa causa, efetuando o pagamento de todas as verbas rescisórias, assim, não confessaria a invasão de privacidade; 2º) ou poderia discutir a questão em juízo, levando à consideração do magistrado a possibilidade de compensação da rescisão indireta e da justa causa (justa causa do empregador com fulcro no artigo 483, alínea e, da CLT – tendo em vista a falta grave cometida por este ao violar as comunicações privadas do trabalhador – e a justa causa do empregado com fulcro no artigo 482 da CLT).

Por fim, frisa-se que o artigo 5º, inciso XII, da Constituição Federal garante o sigilo das correspondências e comunicações: “é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal”. Logo, nem mesmo o descuido do titular das correspondências ou comunicações justifica a violação de seu direito ao sigilo, apresentando a lei apenas uma exceção mitigadora da garantia: a ordem judicial.

Considerações finais

No presente artigo se analisou a aplicação de normas da Lei Geral de Proteção de Dados na resolução de conflitos da seara laboral, tendo em vista a vulnerabilidade do empregado e o Princípio da Proteção, preceitos basilares do Direito do Trabalho brasileiro. Além disso, por meio de exemplos, demonstrou-se que o livre consentimento do empregado para a coleta de seus dados é relativa, não sendo

falta grave pelo empregado. Logo, a demissão por justa causa deveria ser convertida em demissão sem justa causa, pagando o empregador todas as verbas rescisórias ou deveria ocorrer a compensação da rescisão indireta e da justa causa (justa causa do empregador com fulcro no artigo 483, alínea e, da CLT – tendo em vista a falta grave cometida por este ao violar as comunicações privadas da trabalhadora – e a justa causa do empregado com fulcro no artigo 482 da CLT).

suficiente para eximir o empregador de suas responsabilidades. Também, ressaltou-se que o poder de direção do empregador não pode servir como justificativa para a invasão da intimidade do empregado, tampouco pode mitigar garantias expostas na Constituição Federal.

No decorrer do estudo foram abordadas as seguintes normas: princípios da proteção de dados (artigo 6º); conceitos de dado pessoal, de dado pessoal sensível e de tratamento de dados (artigo 5º); determinações relativas ao consentimento para o tratamento dos dados não sensíveis e dos dados sensíveis (artigos 7º e 11); direitos do titular dos dados (artigo 9º); legítimo interesse do controlador e o tratamento de dados pessoais estritamente necessários para a finalidade pretendida (artigo 10); e hipóteses de término do tratamento dos dados pessoais (artigo 15). Todas estas normas foram relacionadas aos casos apresentados no último subtítulo, observando-se, em análise ainda superficial, que há um longo caminho a ser percorrido no desenvolvimento da ciência de proteção de dados para a esfera laboral, a fim de tornar o tratamento de dados mais seguro, justo e igualitário, bem como preservar a intimidade dos dados pessoais e dos dados sensíveis do obreiro.

Desta forma, ainda que o sistema de proteção de dados seja bastante desenvolvido no Brasil, na seara laboral a sua utilização está em fase inicial, existindo muitas questões pendentes de análise por parte do legislador e da doutrina. Logo, cabe à sociedade científica iniciar os debates e os questionamentos necessários ao desenvolvimento nacional dos Direitos Humanos Laborais, com fulcro na proteção de dados.

REFERÊNCIAS

BRASIL. Consolidação das leis do trabalho. Decreto-lei nº 5.452, de 1º de maio de 1943. Aprova a consolidação das leis do trabalho. Disponível na URL: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em 13 de abril de 2021.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Disponível na URL: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 13 de abril de 2021.

BRASIL. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível na URL: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em 10 de abril de 2021.

BRASIL. Tribunal Regional do Trabalho (10ª Região). Processo nº 0000505-73.2017.5.10.0007. Disponível na URL: <https://pje.trt10.jus.br/consultaprocessual/detalhe-processo/0000505-73.2017.5.10.0007/1#f13fb75>. Acesso em 13 de abril 2021.

BRASIL. Tribunal Superior do Trabalho. Súmula nº 338. Jornada de trabalho. Registro. Ônus da prova (incorporadas as Orientações Jurisprudenciais nºs 234 e 306 da SBDI-1) - Res. 129/2005, DJ 20, 22 e 25.04.2005. Disponível na URL: https://www3.tst.jus.br/jurisprudencia/Sumulas_com_indice/Sumulas_Ind_301_350.html#SUM-338. Acesso em 13 de abril 2021.

CASSAR, Vólia Bomfim. **Resumo de Direito do Trabalho**. 6. ed. Rio de Janeiro: Forense; São Paulo: Método, 2018.

CONI JUNIOR, Vicente Vasconcelos; PAMPLONA FILHO, Rodolfo. A Lei Geral de Proteção de Dados e seus reflexos nas relações jurídicas trabalhistas. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (org.). **Reflexos da LGPD do Direito e no Processo do Trabalho**. São Paulo: Revista dos Tribunais, 2020. pp. 74-124.

CORRÊA, Adriana Espíndola; GEDIEL, José Antônio Peres. **Proteção jurídica de dados pessoais: a intimidade sitiada entre o Estado e o Mercado**. Disponível na URL: <https://revistas.ufpr.br/direito/article/view/15738>. Acesso em 02 de abril de 2021.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Disponível na URL: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658>. Acesso em 02 de abril de 2021.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

KAMEDA, Koichi; PAZELLO, Magaly. **E-Saúde e desafios à proteção da privacidade no Brasil**. Disponível na URL: https://nupef.org.br/sites/default/files/downloads/artigo%20poli%20tics_esaude%20e%20privacidade.pdf. Acesso em 02 de abril de 2021.

LIMA, Caio Cesar Carvalho; MONTEIRO, Renato Leite. **Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada**. Disponível na URL: <https://revistas.ufpr.br/atoz/article/view/41320>. Acesso em 02 de abril de 2021.

LIMBERGER, Têmis. **Da evolução do direito a ser deixado em paz à proteção dos dados pessoais**. Disponível na URL: <https://online.unisc.br/seer/index.php/direito/article/view/580/472>. Acesso em 02 de abril de 2021.

MAIA, Luciano Soares. **A privacidade e os princípios de proteção do indivíduo perante os bancos de dados pessoais**. Disponível na URL: http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/bh/luciano_soares_maia.pdf. Acesso em 02 de abril de 2021.

MARQUES, Claudia Lima. Boa-fé nos serviços bancários, financeiros de crédito e securitários e o Código de Defesa do Consumidor: informação, cooperação e renegociação?. **Revista da Faculdade de Direito**, v. 1, n. 22, p. 47-83, 2002.

MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, v. 20, n. 79, p. 45-81, 2011.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. **Revista de Direito do Consumidor**, São Paulo, v. 120, p. 469-483, nov.-dez, 2018.

MENKE, Fabiano. A interpretação das cláusulas gerais: a subsunção e a concreção dos conceitos. **Revista de Direito do Consumidor**. vol. 50. p. 9. Abr, 2004. Doutrinas Essenciais de Direito do Consumidor. vol. 4. p. 107. Abr, 2011. DTR\2004\878.

OECD. **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. Disponível na URL: <https://www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonal->

data.htm. Acesso em 02 de abril de 2021.

ROXO, Tatiana Bhering. Como implementar na prática um programa de proteção de dados. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (org.). **Reflexos da LGPD do Direito e no Processo do Trabalho**. São Paulo: Revista dos Tribunais, 2020. pp. 296-326.

SANDEN, Ana Francisca Moreira de Souza. **A proteção de dados pessoais do empregado no direito brasileiro: um estudo sobre os limites na obtenção e no uso pelo empregador da informação relativa ao empregado**. Disponível na URL: <http://www.teses.usp.br/teses/disponiveis/2/2138/tde-05082013-165006/en.php>. Acesso em 02 de abril de 2021.

25. A LEI GERAL DE PROTEÇÃO DE DADOS E A (AUSÊNCIA DE) PROTEÇÃO AOS TRABALHADORES, OU O DITO PELO NÃO DITO

ALMIRO EDUARDO DE ALMEIDA¹ E OSCAR KROST²

“Muitos teriam protestado, se tivessem encontrado os argumentos corretos.”
(George Orwell, **A revolução dos bichos**)

Resumo

A Lei Geral de Proteção de Dados (LGPD - Lei n. 13.709/18) objetivou estabelecer diretrizes para a proteção às pessoas naturais titulares de dados. Como diploma de aplicabilidade universal, somente em situações específicas deveria recair sobre minúcias, hipóteses em que situar-se-ia o empregado, polo hipossuficiente da relação laboral, o que não veio, contudo, a ocorrer. Ditas omissões ou escolhas do legislador formam o objeto do estudo proposto.

Palavras-chave: Lei Geral de Proteção de Dados. Direito do Trabalho. Interpretação.

1. Introdução

A Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709) foi editada em 14 de agosto de 2018 e, antes mesmo de entrar em vigor, teve vários de seus dispositivos alterados pela Lei n. 13.853, de 8 de julho de 2019. Em sua integralidade, a lei somente entra em vigor em agosto de 2021. Vários textos doutrinários já foram escritos sobre a implicação da LGPD no Direito do Trabalho.

O presente artigo tem uma finalidade um tanto distinta: queremos destacar aqui a ausência de uma proteção adequada à pessoa do trabalhador. Tal *déficit* fica ainda mais evidente quando se verifica, já no artigo 2º da Lei, a defesa do consumidor como um de seus fundamentos. Ou seja, o ser humano é protegido expressamente enquanto consumidor de bens e serviços, mas não se lhe dedica a mesma proteção quando se trata de sua dimensão de produtor. Soma-se a tal discrepância a tutela especialmente dedicada à livre iniciativa e à livre concorrência, sem qualquer menção aos valores sociais que devem balizar tais liberdades, conforme pre-

1 Juiz do Trabalho vinculado ao TRT da 4ª Região, professor em cursos de pós-graduação, especialista em Direito do Trabalho pela Universidad de la República Oriental del Uruguay, especialista em Relações de Trabalho pela Faculdade de Ciências Econômicas da Universidade Federal do Rio Grande do Sul, mestre em Direitos Sociais e Políticas Públicas pela Universidade de Santa Cruz do Sul – UNISC, doutor em Direito do Trabalho pela Universidade de São Paulo – USP.

2 Juiz do Trabalho vinculado ao TRT da 12ª Região, professor em Cursos de Especialização em Direito e Processo do Trabalho, mestre em Desenvolvimento Regional (PPGDR/FURB), pós-Graduando em Relaciones del Trabajo y Sindicalismo pela Facultad Latinoamericana de Ciencias Sociales (FLACSO/Argentina), membro do Instituto de Pesquisas e Estudos Avançados da Magistratura e do Ministério Público do Trabalho (IPEATRA), autor do blog www.direitodotrabalhocritico.com.

conizado pelo artigo 1º da Constituição Federal. Até mesmo o desenvolvimento tecnológico e a inovação são elencados como fundamentos da proteção de dados, mas, em toda a lei, nenhuma vez é mencionado o ser humano que trabalha. Não se poderia identificar melhor exemplo de fetichismo das coisas, que acarreta a correspondente coisificação do ser humano.

Utilizando-nos de diferentes esforços interpretativos, examinaremos, na próxima seção, as diferentes formas de proteção que, mesmo não estabelecidas de forma expressa, podem ser depreendidas da LGPD. Para isso, partiremos do que a doutrina chama de “falsas lacunas”.

A seguir, investigaremos a questão da responsabilidade civil do empregador no que diz respeito ao tratamento e utilização dos dados de seus empregados. Nesse ponto, discutiremos o que efetivamente a lei traz de inovação, o que não passa de repetição de legislação já existente, bem como a possibilidade da extensão de sua aplicação para o âmbito trabalhista, inobstante a sua destinação específica diversa.

Por fim, passando pelo que se convencionou chamar de lacunas axiológicas, ou sociológicas, trataremos das diversas formas de proteção ao trabalhador que deixaram de ser positivadas, ainda que de forma implícita. Buscamos, dessa forma, formular uma análise crítica, não só especificamente do texto legal, mas das possíveis repercussões da omissão do seu processo legiferante.

2. Das proteções que se podem estender aos trabalhadores: o dito pelo não dito

O Direito, enquanto sistema normativo, é composto por regras e princípios, almejando a completude. Aspiração desejável, mas a cada dia mais distante, por conta da velocidade exponencial com que as sociedades, em um mundo globalizado, se modificam.

A lei, principal instrumento na disciplina de condutas em nosso sistema jurídico, alcança um número limitado de hipóteses, deixando as demais situações em um campo de ausência de regulamentação, dando margem às chamadas lacunas jurídicas. Recorde-se a centralidade da atuação legiferante do Estado para o Direito brasileiro, vinculado à família romano-germânica, por conta do Princípio da Legalidade, expresso no artigo 5º, inciso II, da Constituição, segundo o qual “*ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei*”.

Para Alexandre de Moraes, “*tal princípio visa combater o poder arbitrário do Estado*”, de modo que apenas “*conforme as regras do processo legislativo constitucional, podem-se criar obrigações para o indivíduo, pois são expressão da vontade geral*”. Além da referência expressa à vontade geral, de Rousseau, o ministro lembra ainda de Aristóteles, para quem a lei poderia ser definida como a inteligência sem paixão.³

Não obstante tal vinculação à lei, a inexistência de regra específica não pode ser invocada pelo Estado-Juiz como justificativa a eximi-lo do dever de decidir casos

3 MORAES, Alexandre de. *Direito constitucional*. 13a ed. São Paulo: Atlas, 2003, p. 69. Esse viés interpretativo do Princípio da Legalidade se molda ao agir dos particulares em relação a si e perante o Estado, havendo uma particularidade em sede de Direito Administrativo. Ao gestor público, a legalidade significa não poder agir senão naquilo que a lei autoriza, em uma espécie de parâmetro a ser seguido. O cidadão não pode ser obrigado, senão pela lei; o administrador não está autorizado, senão pela lei.

concretos a ele submetidos,⁴ demonstrando o reconhecimento do próprio sistema a respeito de lacunas das leis, mas não do ordenamento. O artigo 8º da CLT, por exemplo, um de seus mais complexos dispositivos, estabelece critérios exemplificativos para a colmatação e preenchimento das omissões do legislador, com destaque aos princípios gerais de direito, analogia, equidade, usos e costumes.⁵

Se de um lado a dinâmica em questão evita a paralisia do tráfego jurídico e o engessamento das regras diante das mudanças sociais, de outro, enfraquece o ideal de segurança jurídica. Acaba-se convivendo com a escolha do mal menor.

Quanto à natureza das lacunas, Norberto Bobbio classifica-as como próprias ou impróprias. Aquelas estariam dentro de um determinado sistema, enquanto estas decorreriam da comparação entre um sistema real e outro ideal. Haveria, ainda, lacunas subjetivas, atribuídas ao legislador, e objetivas, fruto do avanço das relações sociais. Por fim, existiriam as lacunas *praeter legem*, decorrentes do excesso de especificidade das regras, e *intra legem*, quando as regras são abertas em excesso.⁶

Importante à análise aqui desenvolvida reconhecer o quanto a LGPD, intencionalmente ou não, deixou de atentar em suas disposições abertas às relações de trabalho naquilo que as caracteriza e as diferencia dos demais vínculos jurídicos. Ao assim se posicionar, não impediu o legislador a aplicação da regra aos liames laborais, o que seria inviável por flagrante inconstitucionalidade. Ainda que tenha caráter eminentemente comercial, ou consumerista, tratando-se de uma lei geral, não apenas pode, como deve ser aplicada, com as adequações necessárias, aos di-

4 Lei de Introdução às Normas do Direito Brasileiro, arts. 4º e 5º.

Art. 4º: Quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais de direito.

Art. 5º: Na aplicação da lei, o juiz atenderá aos fins sociais a que ela se dirige e às exigências do bem comum.

Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm. Acesso em: 06 abr. 2021.

5 Neste sentido, o magistério de Homero Batista, ao comentar o art. 8º:

“Eis um dos mais complexos dispositivos da CLT. Ele pode ser lido de duas maneiras. A forma mais simples é encará-lo como uma regra de supressão de lacunas, de modo que, diante de alguma omissão da CLT, entram em ação sete mecanismos integrativos: julgados, analogia, equidade, princípios, normas, costumes e direito estrangeiro.

(...)

Há, todavia, outras análises mais aprofundadas desse art. 8º, com enorme dificuldade de angariar algum consenso: a) dicuste-se se a jurisprudência pode ser considerada uma forma de supressão de lacuna (...) b) discute-se qual o limite do uso da analogia (...)c) controverte-se sobre o uso da equidade (...) d) pouco se compreende o que o legislador quis dizer sobre o uso subsidiário de outras normas gerais do direito (...) e) da mesma forma como o juiz do trabalho poderia avançar mais no uso da equidade, também o conhecimento e o respeito aos usos e costumes de determinada prática trabalhista poderiam avançar para além dos exemplos clássicos (...) f) o direito estrangeiro quase nunca é ventilado em peças processuais ou em julgados trabalhistas (...)”(SILVA, Homerto Batista Mateus da. *CLT comentada*. 3a ed. São Paulo: Thomson Reuters Brasil, 2021, p. 50-1)

6 BOBBIO, Norberto. *Teoria do Ordenamento Jurídico*. Trad. Maria Celeste J. C. Santos. Brasília: Editora Universidade de Brasília, 10a ed., 1999, p.143-5.

ferentes ramos do Direito, inclusive o trabalhista. Pamplona Filho e Coni Junior chegam a afirmar que “os principais destinatários da proteção do banco de dados serão os empregados”.⁷

Não obstante isso, a adequada tutela do sujeito subordinado ficou à mercê de consideráveis esforços hermenêuticos de parte dos operadores, gerando insegurança e indefinição, sujeitando trabalhadores a riscos e à necessidade de contar não apenas com a boa-fé, mas a boa vontade do intérprete.

Na verdade, mais do que boa vontade – que se trata de um conceito moral-filosófico ou religioso⁸ –, do que se precisa é aquilo que Konrad Hesse chamou de vontade de constituição:

Embora a Constituição não possa, por si só, realizar nada, ela pode impor tarefas. A Constituição transforma-se em força ativa se essas tarefas forem efetivamente realizadas, se existir a disposição de orientar a própria conduta segundo a ordem nela estabelecida, se, a despeito de todos os questionamentos e reservas provenientes dos juízos de conveniência, se puder identificar a vontade de concretizar essa ordem. Concluindo, pode-se afirmar que a Constituição converter-se-á em força ativa se fizerem-se presentes na consciência geral — particularmente, na consciência dos principais responsáveis pela ordem constitucional —, não só a vontade de poder (Wille zur Macht), mas também a vontade de Constituição (Wille zur Verfassung).⁹

É preciso, pois, da parte de todos os sujeitos envolvidos nas relações jurídico-laborais, uma vontade genuína de respeitar e fazer implementar o texto constitucional. Essa vontade, repita-se, não decorre de nenhum comando moral ou religioso, mas de uma imposição jurídica, fruto da própria Constituição que, independentemente de vieses ideológicos, posições filosóficas ou confissões de fé, todos têm o dever de cumprir.

Não obstante a ausência de tratamento específico à figura do trabalhador, por parte da lei, é possível depreender de seus dispositivos uma série de proteções, caso se faça uma leitura em conformidade com o texto constitucional.

Sabe-se que o empregador tem o dever legal de documentar a relação de emprego, criando registros e armazenando dados referentes aos seus empregados nos diferentes momentos contratuais. Daí falar-se em dados pré-contratuais, dados contratuais e dados pós-contratuais.

De acordo com a LGPD, os dados podem ser pessoais, pessoais sensíveis ou anonimizados. Os primeiros constituem-se de informações relacionadas à pessoa natural identificada ou identificável (artigo 5º, inciso I). Nessa categoria entrariam

7 PAMPLONA FILHO, Rodolfo; CONI JUNIOR, Vicente Vasconcelos. A Lei Geral de Proteção de Dados Pessoais e seus impactos no Direito do Trabalho. In: *Revista Direito Unifacs*. Salvador, 2020, p. 25. Disponível em <https://revistas.unifacs.br/index.php/redu/article/view/7108/4278>. Acesso em: 19 abr. 2021.

8 No sentido moral-filosófico da expressão, Kant sustenta que nada é mais puramente bom do que uma boa vontade (KANT, Immanuel. *Fundamentação da metafísica dos costumes*. In: KANT. Coleção Os pensadores. Seleção de Marilena de Souza Chauí Berlinck. Tradução de Paulo Quintela. São Paulo: Nova Cultural, 1974, p. 2003). Já no seu sentido religioso, Lucas clama a Deus por “paz na Terra aos homens de boa vontade” (Lucas 2:14).

9 HESSE, Konrad. *A força normativa da Constituição*. Tradução Gilmar Ferreira Mendes. Porto Alegre: Sergio Antonio Fabris Editor, 1991, p. 19.

a grande maioria dos dados que o empregador detém, com os números da Carteira de Trabalho, do Registro Geral, do Cadastro de Pessoa Física e da inscrição no INSS. Já os dados pessoais sensíveis caracterizam-se por se referirem a “dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (artigo 5º, inciso I). Alguns desses dados também são comumente armazenados pelo empregador, em especial a origem racial ou étnica, dado biométrico e filiação sindical. Esses merecem especial atenção.

Sabe-se que, via de regra, é proibido ao empregador coletar ou armazenar informações que possam gerar qualquer tipo de discriminação em relação à pessoa do empregado. Entretanto, essa regra comporta algumas exceções, como, por exemplo, a exigência de exame toxicológico para o motorista profissional, restanho assegurada, entretanto, a confidencialidade do seu resultado em caso positivo;¹⁰ e o atestado de antecedentes criminais para vigilante¹¹.

Por fim, dados anonimizados são aqueles relativos “a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento” (artigo 5º, inciso III). Embora não costumem fazer parte dos dados relativos a contratos de trabalho, serão objeto de análise na próxima seção.

Na relação de emprego, o tratamento dos dados pessoais, sejam sensíveis ou não, normalmente ocorrerá quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados, conforme previsto no inciso V do artigo 7º da Lei. Ocorre que o inciso I do mesmo artigo prevê hipótese de uso mediante o simples consentimento do titular. Essa possibilidade mostra-se perigosíssima em âmbito laboral.

Todos sabemos que a relação de emprego é conceitualmente um negócio entre desiguais. A sua desigualdade possui caráter subjetivo e objetivo. Subjetivamente, o empregado é subordinado ao empregador, devendo, portanto, cumprir as suas ordens. Além disso, a fragilíssima proteção contra a despedida arbitrária ou sem justa causa deixa o trabalhador à mercê da vontade exclusiva do patrão, que pode a qualquer momento, livremente e sem qualquer razão justificável, escolher extinguir a fonte de subsistência não só daquele que lhe presta serviços, mas de toda a sua família. Sob outro aspecto, o objeto da relação é desigual: troca-se dinheiro por força de trabalho. Considerando essa última como as potencialidades humanas de trabalhar e que, justamente por isso, nunca se separam do próprio ser humano, o empregador paga pela própria pessoa do empregado. Este entrega a si mesmo, embora não de uma forma absoluta, como ocorreria na escravidão,

10 Art. 168 (...)

§ 6º, da CLT: Serão exigidos exames toxicológicos, previamente à admissão e por ocasião do desligamento, quando se tratar de motorista profissional, assegurados o direito à contraprova em caso de resultado positivo e a confidencialidade dos resultados dos respectivos exames.

11 Lei nº 7.102/83:

Art. 16 - Para o exercício da profissão, o vigilante preencherá os seguintes requisitos: (...)

VI - não ter antecedentes criminais registrados.

mas de forma relativa, limitando o tempo de vida oferecido ao empregador pelos limites impostos pela lei à jornada de trabalho. É justamente em virtude das desigualdades subjetiva e objetiva, que existem em toda a relação de emprego, que se justifica a proteção especial à figura do trabalhador.

Essa dupla fragilidade a que o sujeito subordinado está exposto fundamenta também a necessidade da aplicação do princípio da irrenunciabilidade no Direito do Trabalho, que, conforme lição de Américo Plá Rodriguez, significa “a impossibilidade jurídica de privar-se voluntariamente de uma ou mais vantagens concedidas pelo direito trabalhista em benefício próprio”.¹²

Nesse cenário, falar-se em consentimento do trabalhador para coleta, armazenamento e manipulação dos seus dados pessoais é no mínimo temerário. Não bastasse toda a história das relações de trabalho e do Direito do Trabalho a demonstrar isso, no Brasil, pelo menos desde 1966,¹³ não é mais aceitável a ingenuidade, quando não perversidade, de se deixar quaisquer aspectos da relação de emprego condicionados à vontade do trabalhador.

Ainda que os artigos 8º e 9º estabeleçam alguns requisitos para a validade do consentimento, não se mostram suficientes para impedir eventual mácula da manifestação de vontade por parte do empregado em face do poder exercido pelo empregador, não só no momento da execução do contrato, mas também e especialmente no momento da contratação. Assim, indispensável aplicarmos, aqui, o quanto previsto no artigo 9º da CLT, com uma interpretação extensiva do dispositivo, para considerar nulo de pleno direito todo consentimento do trabalhador que possa expô-lo a qualquer forma de discriminação, ou lhe causar, direta ou indiretamente, prejuízo.

A propósito da possibilidade de lesão aos direitos patrimoniais e extrapatrimoniais dos trabalhadores, impõe-se analisar a questão da responsabilidade do empregador no que diz respeito aos danos decorrentes dos tratamentos de dados.

3. Da responsabilidade patronal: quando não se pode deixar o dito pelo não dito

Quanto à responsabilidade por eventuais danos decorrentes do tratamento dos dados, a lei praticamente não inova a teoria geral de responsabilidade civil já prevista nos artigos 927 e seguintes do Código Civil.¹⁴ A responsabilidade civil e a obrigação de reparação solidária alcançam operadores, controladores e todos os que sejam causadores do dano.

A lei prevê hipóteses de inversão do ônus da prova quando se verificar: 1) verossimilhança da alegação; 2) hipossuficiência para fins de produção de prova; e

12 RODRIGUEZ, Plá. *Princípios do Direito do Trabalho*. 3a edição. São Paulo: LTr, 2000, p. 144.

13 O ano faz referência à edição da Lei nº 5.107, que instituiu o FGTS de forma facultativa ao trabalhador. Como se observou, a partir de então, somente passaram a ser contratados trabalhadores que optassem pelo sistema fundiário, abrindo mão, assim, da possibilidade de garantia de emprego prevista na CLT.

14 Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.

Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

3) que a produção de prova pelo titular resultar-lhe excessivamente onerosa. Esta última possibilidade de inversão já está contemplada tanto pelo CPC (artigo 373, §1º), quanto pela CLT (artigo 818, §1º). A primeira e a segunda hipóteses, entretanto, não encontram tratamento semelhante nem no diploma processual geral, nem no processo do trabalho. Aquela pode se entender como uma decorrência do brocardo atribuído a Malatesta de que o ordinário se presume e o extraordinário se prova. Especial atenção merece a segunda previsão – hipossuficiência do titular do direito para a produção da prova. Esta, em nosso sentir, estará (quase) sempre presente nas relações de trabalho, não só pela hipossuficiência do empregado e pelos poderes atribuídos ao empregador, mas pelo próprio dever de produção e guarda dos documentos que lhe compete. Sendo assim, nos processos que versem sobre reparação de danos decorrentes do tratamento de dados, o ônus da prova deverá, via de regra, recair sobre o empreendedor da atividade econômica.

As hipóteses de exclusão de reponsabilidade civil previstas no artigo 43 da Lei são taxativas e devem ser aplicadas também, como *numerus clausus*, ao empregador. Não obstante, a especificidade do Direito do Trabalho faz com que tais hipóteses tenham de ser analisadas *cum grano salis*.

Quanto à primeira hipótese – não ter realizado o tratamento de dados pessoais que lhe é atribuído –, nada a ressaltar. O empregador não terá nenhum dever de reparação caso comprove (observe-se que o ônus da prova lhe incumbe) que não realizou o tratamento de dados que lhe é atribuído.

Quanto à segunda possibilidade de exclusão de responsabilidade – ausência de violação à legislação de proteção de dados –, ressalva-se que não basta a prova da inoocorrência de violação apenas à LGPD; deve ser demonstrada a ausência de violação de qualquer preceito jurídico, em especial a Consolidação das Leis do Trabalho e legislação esparsa de proteção ao trabalhador.

No que concerne à última hipótese de exclusão de responsabilidade civil – o dano decorrer de culpa exclusiva do titular dos dados ou de terceiro –, há de se atentar a tudo o que já se avançou acerca da teoria da responsabilidade civil em acidentes de trabalho.¹⁵ Como o dever de documentação (produção, guarda e destinação final dos documentos) compete ao empregador, apenas de forma excepcional este poderá ser isento de qualquer responsabilidade, mesmo que outros sujeitos tenham contribuído em alguma medida para a produção do resultado. Nestas situações, poderia se cogitar em culpa concorrente da vítima ou de terceiro, reduzindo, jamais isentando totalmente a responsabilidade do empregador.

O artigo 45 da Lei, que dispõe que “as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente” deve, por justiça, equidade e a fim evitar qualquer forma de discriminação, ser aplicável, com os devidos ajustes, às relações de emprego. Atente-se que a não discriminação é princípio que informa expressamente a Lei Geral de Proteção de Dados (artigo 6º, inciso IX), além de ser finalidade precípua da referida lei.

Verificadas algumas possibilidades de aplicação da lei, por extensão, às relações

¹⁵ Sobre o tema, ver OLIVEIRA, Sebastião Geraldo de. *Indenizações por acidente do trabalho ou doença ocupacional*. São Paulo: LTr, 2005.

de emprego, passaremos a tratar, agora, daquelas proteções que a LGPD poderia ter dispensado ao trabalhador, mas não o fez.

4. Das lacunas da LGPD: o não dito que efetivamente nada diz

Ao lado das lacunas normativas, também chamadas de falsas lacunas, existem as lacunas axiológica e ontológica. Conforme ensina Maria Helena Diniz, lacuna normativa é a própria ausência de norma sobre determinado caso. Já a lacuna ontológica caracteriza-se pela falta de correspondência de uma norma em relação aos fatos sociais, decorrente do avanço social e da inércia do legislador. Por fim, lacuna axiológica seria a ausência de norma justa para o caso concreto; ou seja, até existe o preceito normativo, mas a sua aplicação implicaria uma solução injusta, ou pelo menos insatisfatória.¹⁶

Como exemplo de lacuna axiológica, podemos citar a omissão legislativa em atualizar e buscar maior efetividade à execução no processo do trabalho, especialmente se comparado às inovações legislativas que tem sofrido o processo civil nos últimos anos. Nesse último, que parte do pressuposto da igualdade das partes, a execução se mostra, atualmente, muito mais efetiva do que no processo do trabalho, em que as partes (empregado e empregador) encontram-se em posições desiguais como decorrência intrínseca da própria relação de emprego. Além disso, se considerarmos que, via de regra, o trabalhador somente ingressará na Justiça do Trabalho, pleiteando seus direitos desrespeitados após a extinção do contrato de trabalho (decorrência da ausência de uma efetiva proteção contra a despedida arbitrária), o trabalhador, na grande maioria das vezes, ingressa no processo trabalhista em situação de extrema necessidade. É evidente, pois, a lacuna ontológica da ausência de atualização legislativa para buscar a efetividade da execução trabalhista.

Se a lacuna ontológica se percebe no Direito do Trabalho pela inércia do legislador, a lacuna axiológica pode ser percebida pela sua ação. As últimas alterações legislativas, com especial destaque para a Reforma Trabalhista de 2017, têm evidenciado uma tendência de alteração das normas para aumentar ainda mais as diferenças já existentes entre empregado e empregador. Estudo realizado pelo juiz do Trabalho Alessandro da Silva (TRT12) demonstrou que, das mais de cem alterações realizadas pela Reforma, apenas 3,77% favoreceram os trabalhadores, enquanto que 65,09% foram benéficas aos patrões.¹⁷ Trata-se de típico exemplo em que existe a norma, e até mesmo norma atualizada, mas o preceito normativo se mostra, mais do que insatisfatório, claramente injusto!

As principais obrigações de empregado e empregadores são, respectivamente, prestar trabalho e pagar salários, formando, ao lado dos demais deveres contratuais, um verdadeiro “feixe obrigacional”. Seja na fase contratual ou nas etapas prévia e posterior ao liame, uma postura ética de ambos os sujeitos se mostra não apenas recomendável, mas essencial a fim de não gerar expectativas indevidas ou potenciais danos.

16 DINIZ, Maria Helena. *Compêndio de Introdução à Ciência do Direito*. 14 ed., São Paulo: Saraiva, 2001, p. 437.

17 MUNHOZ, José Lúcio. Comentário ao art. 1º. In: LISBÔA, Daniel. MUNHOZ, José Lucio. *Reforma Trabalhista comentada por Juizes do Trabalho*: artigo por artigo. 2a ed. Revista, aumentada e atualizada. São Paulo: LTr, 2019, p. 30.

Na etapa de seleção de candidatas a vagas de emprego, os interessados devem evitar a produção de expectativas infundadas, assim como cingir a busca de dados a temas essenciais ao preenchimento do perfil profissional. Neste particular, a LGPD apresentou uma espécie de grave “silêncio eloquente”.

O artigo 4º da lei afasta do campo de incidência o tratamento de dados pessoais realizados por pessoa natural para fins exclusivamente particulares e não econômicos (inciso I). Sendo inerentes à relação de emprego a busca por lucro e a onerosidade (artigos 2º e 3º da CLT), não há dúvida de que as informações referentes ao contrato laboral merecem tutela.

Contudo, a sequência do artigo abre margem a dúvidas e à insegurança quanto ao vínculo celetista ao também excepcionar o trato de dados realizado para fins “exclusivamente” (inciso II) jornalístico e artístico (alínea a), acadêmico (alínea b) ou proveniente de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei (inciso IV).

No que diz respeito a este último preceito, há de se observar que a proteção de dados pessoais do trabalhador pode não estar prevista na LGPD, mas em outras normas, de cunho especificamente trabalhista. Assim, sendo a norma brasileira mais benéfica ao trabalhador, não deveria ser aplicada a lei estrangeira, ao menos não antes de examinado o conjunto legislativo nacional.

O que marca o capitalismo e a relação laboral subordinada é a geração de riqueza em proveito do detentor dos meios de produção, pela extração do mais valor.¹⁸ O lucro do capital decorre do trabalho excedente do sujeito empregado, assim entendido o que supera o mínimo necessário à sobrevivência do trabalhador e de sua família.

A razão de ser do Direito do Trabalho e da tutela do empregado está em limitar essa forma de exploração. Irrelevante a destinação dada pelo empregador ao resultado do serviço: artística, jornalística ou acadêmica. Se, sob o ponto de vista do capital, o que importa é o lucro obtido a partir da realização do trabalho, sob o ponto de vista da proteção ao trabalhador, o que deve importar é a própria atividade laboral desempenhada, independentemente do resultado material obtido.

Na mesma linha, a proteção dos cidadãos brasileiros ou estrangeiros vinculados ao Brasil que laborem nos moldes previstos na CLT decorre do status de sujeito de direito subordinado, sobre os quais, em suas relações, incidem a Constituição, a Consolidação e a normatividade trabalhista geral.

Afastar a incidência da LGPD em detrimento de normatividade estrangeira, supostamente mais favorável na matéria, desconsidera que dentre os destinatários da aplicação da norma geral existem sujeitos cujas relações específicas demandem atenção singular. Sem isso, pode o intérprete ser levado ao “esquecimento” dos princípios e das particularidades do Direito do Trabalho brasileiro, em prejuízo manifesto aos hipossuficientes.

18 MARX, Karl. *O Capital*: crítica da economia política: Livro I: O processo de produção do capital. Tradução de Rubens Enderle. São Paulo: Boitempo, 2013.

Deveria o Legislador especificar se as exceções também incidem em hipóteses atinentes a vínculos de emprego ou de trabalho *lato sensu*, justificadamente. Nada impede que determinada atividade não lucrativa, em 2021, pouco tempo depois venha a gerar ganhos financeiros, transmutando a intenção original e de exceção. Como ficaria, neste caso, a tutela dos dados dos empregados? Além disso, a proteção destinada ao trabalhador não deve estar condicionada à efetiva, ou mesmo pretensa, obtenção de lucro por parte do empregador, como se depreende do § 1º do artigo 2º da CLT.

Ademais, como regra, a LGPD limita o tratamento de dados pessoais a hipóteses taxativas (art. 7º), exigindo, na captação, o consentimento do titular (inciso I) ou a necessidade de execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados (item V), bem como a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (inciso X).

A exigência do consentimento do titular do dado antes ou durante a relação de emprego parece situação chancelada pela norma, embora não de modo expresso, dando margem, ainda que mínima, a dúvidas. Mesmo que o fosse, esse consentimento teria que ser analisado com o máximo cuidado, como já se argumentou na seção anterior.

Contudo, se a proteção da dignidade da pessoa humana que trabalha não foi mencionada, por que motivo a proteção do crédito teria sido? Qual a mensagem enviada ao intérprete-aplicador? Para além de preciosismo ou questão de técnica, atos falhos de tal gravidade não apenas demonstram os valores e intenções por trás da regra, como também permitem compreender a potencial racionalidade que permeará sua aplicação prática, causando justificada preocupação.

O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva (art. 9º). Quando o consentimento é exigido, considerar-se-á nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca (§1º).

Mais uma vez, sabendo-se da hipossuficiência dos empregados diante dos empregadores, poderia a lei especificar a quem cabe a prova da prestação suficiente de explicações e de sua compreensão, não apenas determinando que ocorram.

Outro aspecto gerador de dilemas é a possibilidade de mudanças dos fins para o tratamento de dados pessoais não compatíveis com o consentimento original. Quando verificada, acarreta o dever ao controlador de informar o titular, podendo este revogar o consentimento se discordar das alterações (§2º). Tal hipótese é aplicável à relação laboral? Dados fornecidos no procedimento seletivo poderão ser usados quando concluída a etapa em questão? Caso aprovado, tem o empregado condições de negar o reaproveitamento dos dados fornecidos ao empregador sem pôr em risco a manutenção do contrato, sem que haja vício do negócio, semelhante ao estado de perigo e à lesão?¹⁹

19 Código Civil:

Art. 156. Configura-se o estado de perigo quando alguém, premido da necessidade de salvar-se, ou

Uma vez atendida a finalidade da informação pelo preenchimento da vaga, a lei deveria, a fim de preservar a tutela do titular do dado, determinar a destruição das informações obtidas, conforme previsto mais adiante (art. 15, inciso I), bem como por ser corolário direto do princípio protetivo e da finalidade da proposta original de tratamento.

A eliminação obrigatória dos dados pessoais após o término de seu tratamento é medida louvável, pelo equacionamento entre meios e fins (art. 16), causando, contudo, dúvida sobre a aplicação das exceções aos sujeitos laborais. A cogência da destruição é relativizada quando verificados o cumprimento de obrigação legal ou regulatória pelo controlador (inciso I), estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais (inciso II), a transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na LGPD (inciso III) ou uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados (inciso IV).

Apenas a primeira situação se mostra suficientemente compreensível. O que representa a expressão “sempre que possível”, de elevadas cargas de subjetividade e vagueza? A quem cabe a prova da possibilidade? E o repasse a terceiros de dados que deveriam por imposição legal ser eliminados, de modo que o agente deve se livrar, mas pode repassar a outro, desde que observados os termos da lei? O que dizer, ainda, da guarda de dados, bastando que sejam anonimizados, processo posterior à identificação dos sujeitos? Isso sem considerar a possibilidade de pseudoanonimização, hipótese em que, mesmo após a anonimização, a identificação do indivíduo continua possível pelo uso de informação adicional mantida separadamente pelo controlador dos dados.²⁰

A ausência de menção ao contrato de trabalho e aos sujeitos dele participantes causa estranheza em situações envolvendo a comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica (artigo 11, §3º). Mais, ainda, quando a LGPD aventa a possibilidade de regulamentação pela autoridade nacional, bastando a oitiva de órgãos setoriais do poder público, no âmbito de suas competências.

Parece evidente que dados sensíveis dizem respeito à exceção máxima, por definirem o “lugar no mundo” de cada sujeito, individualmente em sua dignidade. Contudo, justamente por tal relevância e pela inspiração humanista e cidadã da Constituição, cuidado nunca será demais, no particular.

Além disso, o conceito normativo padece de abertura desmedida, sendo vago e impreciso. “Vantagem econômica” é mais ou menos ampla que “vantagem concorrencial”? Pode-se alcançar uma fatia maior de mercado sem obter lucro, se praticados preços menores do que os habituais apenas para vencer o concorrente em um lapso de tempo? Institutos de pesquisa podem se valer de dados sensíveis e fazer disto seu nicho de mercado, se autorizados para tanto? Isso não fere os princípios

a pessoa de sua família, de grave dano conhecido pela outra parte, assume obrigação excessivamente onerosa.

Art. 157. Ocorre a lesão quando uma pessoa, sob premente necessidade, ou por inexperiência, se obriga a prestação manifestamente desproporcional ao valor da prestação oposta.

20 A hipótese encontra-se expressamente prevista no parágrafo 4º da artigo 13 da lei.

e objetivos da LGPD, de tutelar os sujeitos de direito e sua intimidade?

Enfim, muitas são as dúvidas geradas pela LGPD no campo das relações laborais, contrariamente a outros ramos do Direito, dando conta de não se tratar de lapso ou esquecimento, mas de uma racionalidade que prestigia determinados titulares de dados e sua posição jurídica. Cabe aos operadores do Direito do Trabalho ficarem atentos a tantas particularidades, de modo que a Lei Geral de Proteção não venha a se tornar uma Lei Específica de Proteção ou de Exclusão tutelar.

Conclusão: afinal, fica o dito pelo não dito?

As relações sociais, em um tempo marcado por incessantes avanços tecnológicos e em espaços cada vez menos territoriais, acabam sendo regidas por regras não cogentes. Raras vezes o Direito nacional de determinado país encontra modos próprios para disciplinar condutas.

Diante de tal realidade, louvável a elaboração pelo Brasil de uma Lei Geral de Proteção de Dados (LGPD, Lei n. 13.709/18) aplicável, não em razão da qualificação dos vínculos jurídicos, mas da pessoa humana titular de direitos de personalidade codificados sob a forma de dados. Contudo, o elevado grau de abertura das regras de proteção acaba acarretando mais dúvidas e controvérsias do que tutela, se analisadas dentro do contexto juslaboral.

Transcorrido o prazo de dois anos de vacância da Lei, não houve o amadurecimento em seu texto sobre as relações trabalhistas em suas particularidades, o que se mostra essencial e premente. Sem uma postura ativa e crítica, a despeito da existência de todo o arcabouço constitucional e legal de proteção do sujeito subordinado, ficará a tutela em sede de tratamento de dados na dependência de esforços hermenêuticos e de boa vontade dos intérpretes. Ao cabo – parafraseando a obra que serve de inspiração para a epígrafe do presente artigo –, a Lei Geral de Proteção de Dados será apenas mais uma forma jurídica para a manutenção da desigualdade social, de forma que todos os dados sejam igualmente protegidos, mas uns mais protegidos do que outros.²¹

REFERÊNCIAS

BOBBIO, Norberto. **Teoria do Ordenamento Jurídico**. Trad. Maria Celeste J. C. Santos. 10ª ed. Brasília: Editora Universidade de Brasília, 1999.

DINIZ, Maria Helena. **Compêndio de Introdução à Ciência do Direito**. 14 ed. São Paulo: Saraiva, 2001.

HESSE, Konrad. **A força normativa da Constituição**. Tradução Gilmar Ferreira Mendes. Porto Alegre: Sergio Antonio Fabris Editor, 1991.

KANT, Immanuel. **Fundamentação da metafísica dos costumes**. In: KANT. Coleção Os Pensadores. Seleção de Marilena de Souza Chauí Berlinck. Tradução de Paulo Quintela. São Paulo: Nova Cultural, 1974.

MARX, Karl. **O Capital**: crítica da economia política: Livro I: O processo de

21 O trecho exato em que verificada a máxima em questão está no capítulo X, nos seguintes termos: “Pela primeira vez Benjamin consentiu em quebrar sua norma, e leu para ela o que estava escrito na parede. Nada havia, agora, senão um único Mandamento dizendo: TODOS OS ANIMAIS SÃO IGUAIS MAS ALGUNS SÃO MAIS IGUAIS DO QUE OUTROS.” ORWELL, George. **A revolução dos bichos**. Tradução de Heitor Ferreira. 24a edição. Porto Alegre/Rio de Janeiro: Globo, 1986, p. 128.

produção do capital. Tradução de Rubens Enderle. São Paulo: Boitempo, 2013.

MORAES, Alexandre de. **Direito constitucional**. 13ª ed. São Paulo: Atlas, 2003.

MUNHOZ, José Lúcio. Comentário ao art. 1º *In*: LISBÔA, Daniel. MUNHOZ, José Lucio. **Reforma Trabalhista comentada por Juízes do Trabalho**: artigo por artigo. 2ª ed. Revista, aumentada e atualizada. São Paulo: LTr, 2019.

OLIVEIRA, Sebastião Geraldo de. **Indenizações por acidente do trabalho ou doença ocupacional**. São Paulo: Ltr, 2005.

ORWELL, George. **A revolução dos bichos**. Tradução de Heitor Ferreira. 24ª edição. Porto Alegre/Rio de Janeiro: Globo, 1986.

PAMPLONA FILHO, Rodolfo; CONI JUNIOR, Vicente Vasconcelos. A Lei Geral de Proteção de Dados Pessoais e seus impactos no Direito do Trabalho. *In*: **Revista Direito Unifacs**. Salvador, 2020.

RODRIGUEZ, Plá. **Princípios do Direito do Trabalho**. 3ª edição. São Paulo: LTr, 2000.

SILVA, Homerto Batista Mateus da. **CLT comentada**. 3ª ed. São Paulo: Thomson Reuters Brasil, 2021.

26. PROMETEU ACORRENTADO, LGPD E O DIREITO DO TRABALHO

OSCAR KROST¹

“A arte dos limites é, para o Direito, o que o sentido das portas e janelas é para a arquitetura: eles devem, ao mesmo tempo, proteger e se abrir para o exterior.”

*Alain Supiot*²

1. Introdução

A história da humanidade traz a marca da luta pela sobrevivência, sendo permeada por criações e descobertas não apenas úteis, mas essenciais à perpetuação da espécie. Da pedra lascada à roda, da agricultura à criação animal, cada ciclo superado permite ao *homo sapiens* almejar novos horizontes.

Nas últimas décadas, especialmente pelo advento da microinformática e da telecomunicação, a “velocidade” do tempo com que os inventos se disseminam e são superados passou de milênios e séculos, para anos e meses. Todas as esferas da vida se viram expostas a tais mudanças, acarretando uma redefinição sem precedentes dos conceitos de intimidade e de privacidade. Informações e dados viajam por todo o globo instantaneamente, sendo utilizados para os mais diversos fins, o que veio a atrair a preocupação da política nacional e internacional.³

No Brasil, a Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709/18) representa um novo marco normativo, abrangendo diversos campos sociais, inclusive o trabalho. Propõe-se neste estudo, a partir do mito do “Prometeu acorrentado”, compreender, em linhas gerais, a relevância do acesso e da guarda de informações, desde a Antiguidade clássica, e apresentar alguns critérios hermenêuticos e exemplificativos importantes na interpretação da regra tutelar, com ênfase à relação de emprego. Utilizar-se-ão textos doutrinários e arquivos de informação geral disponíveis na *web*.

2. Prometeu acorrentado e a centralidade da informação

“Prometeu acorrentado” é um clássico da dramaturgia universal, escrito por Êsquilo, por volta de 462 a. C., na Grécia. Trata da história do titã Prometeu, “pro-

1 Juiz do Trabalho vinculado ao TRT da 12ª Região, professor, mestre em Desenvolvimento Regional (PPGDR/FURB), membro do Instituto de Pesquisas e Estudos Avançados da Magistratura e do Ministério Público do Trabalho (IPEATRA), autor do blog <https://direitodotrabalhocritico.wordpress.com/>, além de colaborador de sites, revistas e obras jurídicas.

2 SUPLOT, Alain. *O espírito de Filadélfia: a Justiça Social diante do Mercado total*. Porto Alegre: Sulina, 2014, p. 98.

3 Sobre a influência das grandes corporações de tecnologia no comportamento social de hoje, bem como os riscos e as possibilidades, ver o documentário *Dilema das redes* (Original Netflix), dirigido por Jeff Orlowski (2019), 89min.

to-deus”,⁴ filho de Jápeto, que decide roubar o fogo divino do monte Olimpo e levá-lo aos homens, habitantes da terra. Prometeu é descoberto e preso por Zeus, sendo acorrentado a uma rocha, onde dia após dia seu fígado é devorado por uma grande ave. À noite, o órgão se regenera, à espera do ataque seguinte.

Como qualquer texto, “Prometeu acorrentado” dá ensejo a diversas interpretações. Dentre as mais conhecidas, destaque-se a que considera o fogo uma fonte de luz e de conhecimento e a punição a consequência pela busca do saber. Não haveria aprendizado livre de dor, apresentando-se as trevas e a ignorância como estados de conforto e de segurança.⁵ Quem se dispuser a superá-los, acaba sujeito à sorte advinda da tentativa de acessar níveis superiores.⁶

Em que medida reler uma peça teatral escrita há quase 2.500 anos pode contribuir para a aplicação de uma lei de proteção de dados em um tempo de características voláteis e imateriais?

Muito mais do que podemos imaginar. No afã de conhecer o **texto**, somos levados a desprezar o **contexto**. No primeiro, as coisas são descritas, enquanto que tão somente no segundo, efetivamente, ocorre a interação entre elas, como coisas, ações ou seres, de modo dinâmico e vivo.

Judith Martins-Costa lembra que “não apenas a História permite apanhar os traços incertos, mas sempre significativos, das mentalidades”. Para ela, “a literatura é testemunha, e não reflexo”,⁷ permitindo confrontar perspectivas, bem como conduzir a outros universos.

Na mesma linha, José Roberto de Castro Neves questiona: “para a formação de um advogado, basta conhecer as leis? Para um juiz cumprir sua função é suficiente dominar o ordenamento jurídico? Os bons juristas são formados apenas com o estudo de Direito?”⁸ A resposta a cada pergunta é mais do que evidente, principalmente se considerarmos a relação inversamente proporcional experimentada hoje em dia entre **facilidade de acesso a informações x dificuldade de estabelecer filtros sobre o conteúdo**.

4 Sobre mais informações sobre os titãs, ver [https://pt.wikipedia.org/wiki/Tit%C3%A3#:~:text=Os%20tit%C3%A3s%20\(masculino\)%20e%20as,os%20gigantes%2C%20Tif%C3%A3o%20e%20%C3%93rion](https://pt.wikipedia.org/wiki/Tit%C3%A3#:~:text=Os%20tit%C3%A3s%20(masculino)%20e%20as,os%20gigantes%2C%20Tif%C3%A3o%20e%20%C3%93rion). Acesso em: 15 set. 2020.

5 Na Internet podem ser encontrados diversos trabalhos sobre outros enfoques a respeito da peça de Ésquilo, a exemplo da leitura sobre a relação entre o fogo e a sociologia da produtividade acadêmica ou a ação discursiva nas relações de poder, disponíveis em https://www.researchgate.net/publication/228635897_Prometeu_acorrentado_analise_sociologica_da_categoria_produtividade_e_as_condicoes_atuais_da_vida_academica e https://www.researchgate.net/publication/318835255_PROMETEU_ACORRENTADO_UMA_LEITURA_DISCURSIVA_DE_RELACOES_DE_PODER_E_RESISTENCIA, respectivamente. Acesso em: 15 set. 2020.

6 Há diversas traduções do texto *Prometeu acorrentado* em meio físico ou eletrônico. Neste texto, foi utilizada a seguinte edição: ÉSQUILO. *Prometeu acorrentado*. Tradução J. B. de Mello e Souza. Clássicos Jackson, vol. XXII, 2005, versão para e-book disponível em <http://www.ebooksbrasil.org/adobeebook/prometeu.pdf>. Acesso em: 18 set. 2020. Disponibilizado pela Oficina de Teatro em <https://oficinadeteatro.com/component/jdownloads/viewdownload/4-pecas-gregas-classicas/68-prometeu-acorrentado>. Acesso em: 15 set. 2020.

7 MARTINS-COSTA, Judith. Nota da coordenadora: entre prestação de contas e introdução. In: MARTINS-COSTA, Judith (coord.). *Narração e normatividade: ensaios de Direito e Literatura*. Rio de Janeiro: GZ Ed. 2013, p. IX.

8 NEVES, José Roberto de Castro. Introdução. In: NEVES, José Roberto de Castro (org). *Ele, Shakespeare, visto por nós, os Advogados*. Rio de Janeiro: Edições de Janeiro, 2019, p. 08.

Em apertada síntese, tanto um quanto outro defendem aquilo que Boaventura de Sousa Santos chama de “crítica à razão indolente”, ou seja, algo contrário ao “desperdício da experiência” acumulada. Para Boaventura, em momentos de rupturas paradigmáticas, se mostra essencial a construção de uma epistemologia da visão, de modo a elevar a solidariedade a uma forma de conhecimento.⁹

Objetivamente, podemos enxergar o “fogo dos deuses” como um “dado” e Prometeu como alguém que empreende (emprega) ou é “empreendido” (empregado), tendo por pano de fundo o mercado e suas “leis”. A tragédia alcança maior atualidade, diante dos dilemas enfrentados na sociedade contemporânea, em que raras são as pessoas livres do peso de lidar com o manejo de dados próprios ou de terceiros.

Não por outro motivo, Milton Santos chamou a 3ª fase da Revolução Industrial, iniciada na década de 1970 e marcada pelo avanço da microinformática e da transmissão de dados, de Revolução Técnico-Científica Informacional.¹⁰ Para além de novas máquinas, matérias-primas e combustíveis, como nas etapas anteriores, o mundo se viu diante da produção e da circulação de riquezas em uma fração de segundos.

Na trama grega, a relação entre saber e força é tamanha a ponto de três das personagens principais, de um total de oito, se chamarem “o Poder”, “a Violência” e “Vulcano”. O Poder abre a peça dirigindo as seguintes palavras a Vulcano, deus do fogo objeto da tentativa de furto de Prometeu:

“Eis-no chegados aos confins da terra, à longínqua região da Cítia, solitária e inacessível! Cumpre-te agora, ó Vulcano, pensar nas ordens que recebeste de teu pai, e acorrentar este malfeitor, com indestrutíveis cadeias de aço, a estas rochas escarpadas. Ele roubou o fogo, - teu atributo precioso fator das criações do gênio, para transmiti-lo aos mortais! Terá, pois, que expiar este crime perante os deuses, para que aprenda a respeitar a potestade de Júpiter e a renunciar a seu amor pela Humanidade.”¹¹

Em resposta, Vulcano faz um breve discurso, concluindo, em relação a Prometeu:

“(…) como castigo por esta temeridade, ficarás sobre esta rocha terrífica, em pé, sem sono e sem repouso; de balde farás ouvir suspiros e clamores dolorosos; o coração de Júpiter é inexorável...Um novo senhor é sempre severo!”¹²

A personagem Violência, por sua vez, nada diz ao longo de toda a história, pois, ironicamente, é a única persona muda da obra. Nota-se com clareza o quanto o conhecimento, o poder e a violência representam em termos de força e possibi-

9 Para Boaventura de Sousa Santos, “a solidariedade como forma de conhecimento é o reconhecimento do outro como igual, sempre que a diferença lhe acarrete inferioridade, e como diferente, sempre que a igualdade lhe ponha em risco a identidade”. (SANTOS, Boaventura de Sousa. *A crítica da razão indolente: contra o desperdício da experiência*. 3a ed. - São Paulo: Cortez, 2001, vol. 1, p. 246.

10 SANTOS, Milton. *Por uma outra globalização: do pensamento único à consciência universal*. 22a ed. Rio de Janeiro/São Paulo: Editora Record, 2012.

11 ÊSQUILO. Prometeu acorrentado. Tradução J. B. de Mello e Souza. Clássicos Jackson, vol. XXII, 2005, versão para e-book disponível em <http://www.ebooksbrasil.org/adobeebook/prometeu.pdf>. Acesso em: 18 set. 2020.

12 *Ibid.*

lidades na Grécia Antiga, no Brasil atual e em qualquer tempo ou lugar. **Como tal, os direitos de acesso, de uso e de guarda de dados também devem vir acompanhados de deveres e responsabilidades**, conteúdo específico da LGPD.

No século 21, mais do que em outras épocas, a informação se revela um elemento central no tráfico de riquezas e pessoas. Serve para antever mudanças climáticas ou geológicas, planejar ações públicas ou privadas ou, ainda, mensurar riscos possíveis e prováveis no tocante a práticas das mais diversas ordens. Aquele que a acessar estará em franca vantagem comparado a seus pares, o que em termos econômicos, políticos, jurídicos e sociais não pode ficar à margem de regulação.

3. Lei Geral de Proteção de Dados, Direitos de Personalidade e Direito do Trabalho

Antes do advento da LGPD, a proteção da intimidade e da privacidade se encontrava prevista em âmbitos internacional, a exemplo da Declaração Universal dos Direitos Humanos,¹³ e nacional, conforme o disposto na Constituição brasileira.¹⁴ A novidade trazida pela norma diz respeito à disciplina em minúcias de situações concretas, embora não taxativas.

Neste cenário, essencial lembrar que **informações não representam meros acessórios a direitos de personalidade; integram os próprios titulares destes direitos como partes indissociáveis**. Sob qualquer perspectiva que se analise a questão, não há justificativa plausível para manter uma visão na qual pessoas sejam tratadas como números, recursos humanos ou variáveis. Lembremos que o ser humano é o fim maior do ordenamento jurídico, jamais seu meio.

Recorda Rodrigo Goldschmidt que o intérprete “deve sempre estar sintonizado com a realidade do seu tempo, atento para novas ou renovadas formas de possíveis violações de direito da personalidade, sopesando as possibilidades e os limites da disposição contratual por parte de seu titular”.¹⁵ Jamais existirá, portanto, uma proteção pronta e acabada em se tratando da esfera da personalidade, exigindo-se uma atenção constante a qualquer prática voltada a violá-la ou ameaçá-la.

Tão inegável quanto o interesse econômico jacente à edição da norma, devem

13 Art 12. Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques a sua honra e reputação. Todo o homem tem direito à proteção da lei contra tais interferências ou ataques. Inteiro teor da Declaração Universal dos Direitos Humanos disponível em <http://www.dhnet.org.br/direitos/deconu/textos/integra.htm>. Acesso em: 15 set. 2020.

14 Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no país a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

(...)

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

Constituição brasileira disponível em http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 15 set. 2020.

15 GOLDSCHMIDT, Rodrigo. *Direitos da personalidade do trabalhador: aproximações conceituais e tentativa de conformação de um microsistema trabalhista*. In: GOLDSCHMIDT, Rodrigo (org.). *Direitos da Personalidade do Trabalhador*. Rio de Janeiro: Editora Lumen Juris, 2019, p. 09.

ser os olhares humanizado e humanizante em sua concretização. Lembremos da lição de Henri Dominique Lacordaire (1802-1861), para quem “*entre os fortes e fracos, entre ricos e pobres, entre senhor e servo é a liberdade que oprime e a lei que liberta*”.

Não se deve devotar à LGPD o dogma da completude, sendo ponto de partida à disposição dos sujeitos. Por mais cauteloso que tenha procurado ser o legislador, lacunas e ambiguidades sempre existirão em qualquer enunciado jurídico, não por falha técnica, mas pela dinâmica da vida, fruto da dialética e da constante evolução das coisas.

Se no mundo globalizado em que empresas possuem lucros superiores ao Produto Interno Bruto (PIB) de algumas das principais economias nacionais¹⁶ as pessoas físicas devem ter seus dados protegidos, maior tutela ainda demandam quando se encontram em situação de “oferecimento à venda” de sua força de trabalho a quem detém os meios de produção, incluindo-se aí o acesso a meios de informação.

Poucas vezes a desigualdade material entre os ocupantes dos polos da relação de emprego se fez tão manifesta. Neste panorama, para além de expor os sentidos possíveis de cada um dos artigos da LGPD, prática útil, porém arriscada diante da experiência acumulada atualmente no Brasil, propõe-se apresentar três critérios hermenêuticos úteis a guiar o intérprete em situações dúbias em termos de leitura e incidência legal.

3.1 Compatibilidade com os Princípios do Direito do Trabalho

Entre duas ou mais possibilidades de compreensão dos dispositivos da nova lei, deve-se buscar a adoção daquela que se alinhe de forma ótima aos Princípios da Proteção e suas projeções (*in dubio pro operario, aplicação da regra mais favorável e da condição mais benéfica*), da Irrenunciabilidade, da Continuidade e da Primazia da Realidade, rol meramente exemplificativo. Princípios, como a própria semântica indica, são pontos fundantes, de partida, de qualquer sistema jurídico, devendo ser revisitados a todo o tempo, jamais relativizados ou esquecidos, quando muito, ponderados entre si.

Respeitados entendimentos em contrário, forçoso reafirmar sem trégua a centralidade da dignidade da pessoa humana e dos valores sociais do trabalho e da livre iniciativa para o Estado Democrático de Direito instituído no país (art. 1º, incisos III e IV, da Constituição). O trabalho e a livre iniciativa devem ser entendidos em sentido dinâmico e em prol do coletivo, não só em benefício dos envolvidos na geração e circulação de riquezas.

3.2 Horizontalidade dos Direitos Fundamentais

Embora os Direitos Fundamentais tenham sido gestados para prevenir excessos do Estado em relação aos cidadãos (eficácia vertical), a evolução histórica e as mudanças sociais, políticas, culturais e econômicas também os levaram a proteger

¹⁶ Apenas a título de exemplo, o Brasil ocupa o 9º lugar no ranking dos países com maior Produto Interno Bruto (PIB), sendo superado, em 2020, pelos lucros da empresa Apple, conforme veiculado em <https://www.dgabc.com.br/Noticia/3418831/descubra-quais-sao-as-10-maiores-economias-do-mundo-eua-lideram> e <https://www.poder360.com.br/economia/valor-de-mercado-da-apple-supe-ra-pib-brasileiro-de-2019/#:~:text=A%20Apple%20alcan%C3%A7ou%20nesta%20semana,segundo%20dados%20do%20Banco%20Mundial>. Acesso em: 15 set. 2020.

os cidadãos entre si, em suas relações privadas (eficácia horizontal). O Direito do Trabalho não ficou à margem desta nova abrangência, sendo um campo de relevante aplicação.

De acordo com Christiana D´Arc Damasceno Oliveira, “o papel da horizontalização é mais pujante nas relações trabalhistas, seara abundante em ofensas de diversas modalidades a direitos básicos, considerando o correlato caráter social e o desequilíbrio de forças entre os integrantes da relação de labuta.”¹⁷ A fundamentação dos Direitos Fundamentais, com o perdão do pleonasma, deve se tornar um verdadeiro mantra em matéria de proteção de dados do sujeito trabalhador, pois de nada adianta preservar a parte material da pessoa em estado de subordinação, deixando a descoberto seus aspectos imateriais.

3.3 Princípio da Proporcionalidade

“Nada em excesso” é uma máxima grega contemporânea de Ésquilo, inscrita no templo de Apolo, na cidade de Delfos.¹⁸ Representa a importância de cuidar da relação das medidas entre si em termos avaliativos.

A proporcionalidade sob a forma de princípio jurídico é entendida, segundo a doutrina, sob três vertentes: Princípio da Conformidade ou da adequação de meios (*relação adequada entre meios e fins*), Princípio da Necessidade (*fim deve ser atingido com a menor gravosidade a terceiros*) e Princípio da Proporcionalidade em sentido estrito (*avaliação se os efeitos produzidos justificam a carga de coerção aplicada*).¹⁹

Sua origem remonta ao século 18, marcado por revoluções burguesas consagradoras da primeira dimensão dos Direitos Fundamentais, de liberdades, sendo também conhecido por Princípio da Proibição do Excesso.²⁰ Assim, diante de dúvidas, observe-se a via de menor potencial ofensivo e de maior pertinência à finalidade pretendida, algo semelhante à legítima defesa para o Direito Penal.

Retornando a Prometeu, cabe lembrar que os deuses do Olimpo, durante o cumprimento da pena, tentam convencê-lo, de várias formas, a pedir perdão a Zeus. De modo peremptório, ele se nega, afirmando saber que um dia o maior dos deuses precisará dele, nada mais revelando a respeito.

O motivo para tamanha segurança não poderia ser outro além do acesso a dado privilegiado sobre alguém que viria destronar o Senhor do Olimpo. E mais: Prometeu sabia como impedir tal acontecimento, justificando o significado de seu nome, que em grego quer dizer “aquele que sabe antecipadamente”.²¹

Considerações finais

O atual estágio tecnológico representa um avanço sem igual nas comunicações

17 OLIVEIRA, Christiana D´Arc Damasceno. *(O) Direito do Trabalho Contemporâneo: Efetividade dos Direitos Fundamentais e Dignidade da Pessoa Humana no Mundo do Trabalho*. São Paulo: LTr, 2010, p. 308-309.

18 Sobre Delfos, ver <https://pt.wikipedia.org/wiki/Delfos>. Acesso em: 15 set. 2020.

19 STUMM, Raquel Denize. *Princípio da Proporcionalidade no Direito Constitucional brasileiro*. Porto Alegre: Livraria do Advogado, 1995, p. 77 e ss.

20 *Ibid.*, p. 78.

21 Informações obtidas em <https://oficinadeteatro.com/component/jdownloads/viewdownload/4-pecas-gregas-classicas/68-prometeu-acorrentado>. Acesso em: 15 set. 2020.

e nas trocas em todo o planeta. Juntamente com tais facilidades, imensuráveis riscos são gerados, quanto à violação a Direitos da Personalidade, em especial, intimidade e privacidade, pelo uso sem parâmetros de dados e informações.

A esfera trabalhista não se encontra alheia a tais possibilidades, tornando aplicáveis as disposições da LGPD, regra de caráter geral, cuja leitura será permeada pelos Princípios juslaborais. Conforme o art. 64 da LGPD, em redação bastante familiar,²² “os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.” Ou seja, mesmo implantado um verdadeiro microsistema normativo, este apresenta um caráter aberto, apresentando hipóteses não taxativas de tutela.

Sob qualquer prisma que se enfrente a questão, é de suma importância manter o foco na centralidade da dignidade da pessoa humana e na construção histórica do arcabouço protetivo trabalhista, a fim de alcançar um sentido ótimo das regras. A obra está longe de se encontrar acabada, encontrando-se apenas no começo. Ou seria no Princípio?

REFERÊNCIAS

ÉSQUILO. **Prometeu acorrentado**. Tradução J. B. de Mello e Souza. Clássicos Jackson, vol. XXII, 2005, versão para *e-book* disponível em <<http://www.ebooksbrasil.org/adobeebook/prometeu.pdf>>. Acesso em: 18 set. 2020.

GOLDSCHMIDT, Rodrigo. Direitos da personalidade do trabalhador: aproximações conceituais e tentativa de conformação de um microsistema trabalhista. In: GOLDSCHMIDT, Rodrigo (org.). **Direitos da Personalidade do Trabalhador**. Rio de Janeiro: Editora Lumen Juris, 2019, p. 01-36.

MARTINS-COSTA, Judith. Nota da coordenadora: entre prestação de contas e introdução. In: MARTINS-COSTA, Judith (coord.). **Narração e normatividade**: ensaios de Direito e Literatura. Rio de Janeiro: GZ Ed. 2013

NEVES, José Roberto de Castro. Introdução. In: NEVES, José Roberto de Castro (org.). **Ele, Shakespeare, visto por nós, os Advogados**. Rio de Janeiro: Edições de Janeiro, 2019.

OLIVEIRA, Christiana D’Arc Damasceno. **(O) Direito do Trabalho Contemporâneo**: Efetividade dos Direitos Fundamentais e Dignidade da Pessoa Hu-

22 O art. 5º, §2º, da Constituição parece ter inspirado o art. 64 da LGPD, como se constata de sua leitura:

“Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no país a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

(...)

§2º Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte.

Constituição brasileira disponível em http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 15 set. 2020.

mana no Mundo do Trabalho. São Paulo: LTr, 2010.

SANTOS, Milton. **Por uma outra globalização**: do pensamento único à consciência universal. 22ª Ed. Rio de Janeiro/São Paulo: Editora Record, 2012.

SUPIOT, Alain. **O espírito de Filadélfia**: a Justiça Social diante do Mercado total. Porto Alegre: Sulina, 2014.

STUMM, Raquel Denize. **Princípio da Proporcionalidade no Direito Constitucional brasileiro**. Porto Alegre: Livraria do Advogado, 1995.

27. A LEI GERAL DE PROTEÇÃO DE DADOS E O COMPLIANCE COMO MEIOS DE SUPERAÇÃO DOS DESAFIOS IMPOSTOS PELO ATUAL CENÁRIO ECONÔMICO

THE GENERAL DATA PROTECTION LAW AND COMPLIANCE AS MEANS OF OVERCOMING THE CHALLENGES IMPOSED BY THE CURRENT ECONOMIC SCENARIO

LINCOLN ZUB DUTRA¹

Resumo

O presente artigo busca explorar as razões por trás da formulação da Lei Geral de Proteção de Dados (LGPD) elaborada em 2018 tanto quanto de que forma a utilização concomitante com o instituto do compliance podem contribuir para a superação dos desafios impostos pelo atual cenário econômico. Para tanto, será necessário analisar os direitos fundamentais que baseiam a LGPD, as peculiaridades do tratamento de dados e o poder do controlador, os impactos que a lei apresenta sobre o direito do trabalho, bem como de que forma há correlação entre a LGPD e o compliance. Assim, poderá se chegar ao objetivo proposto e vislumbrar a comprovação da hipótese suscitada. Isto se dará através de metodologias dedutiva e, também, indutiva, com base em estudos legislativos, doutrinários, tanto quanto por meio de análises bibliográficas.

Palavras-chave: Lei Geral de Proteção de Dados. Direito do trabalho. Compliance. Ordem Econômica.

Abstract

This article seeks to explore the reasons behind the formulation of the General Data Protection Law (LGPD) drafted in 2018 as well as how the concomitant use with the compliance institute can contribute to overcoming the challenges imposed by the current economic scenario. Therefore, it will be necessary to analyze the fundamental rights that underlie the LGPD, the peculiarities of data processing and the power of the controller, the impacts that the law has on labor law, as well as how there is a correlation between the LGPD and the compliance. Thus, it will be possible to reach the proposed objective and glimpse the proof

1 Pós Doutorando em Direitos Humanos, Difusos e Sociais pela Universidade de Salamanca/ESPA-NHA. Doutor em Direito pela Pontifícia Universidade Católica do Paraná (PUC/PR). Mestre em Direitos Fundamentais e Democracia pelo Centro Universitário Autônomo do Brasil- UNIBRASIL. Pós-graduado em Direito do Trabalho e Processo do Trabalho pela Pontifícia Universidade Católica do Paraná (PUC/PR). Graduado em Direito pela Universidade Católica do Paraná (PUC/PR). Professor universitário na Universidade Católica de Santa Catarina. Coordenador da pós-graduação em Direito do Trabalho da Universidade Católica de Santa Catarina. Professor convidado em programas de pós-graduação. Sócio fundador do escritório Lincoln Zub Sociedade de Advogados. Escritor e coordenador de obras jurídicas. lincoln.zub@gmail.com

of the raised hypothesis. This will be done through deductive and also inductive methodologies, based on legislative and doctrinal studies, as well as through bibliographic analysis.

Keywords: General Data Protection Law. Labor law. Compliance. Economic Order.

1. Introdução

A Lei Geral de Proteção de Dados (Lei n.º 13.709), aprovada no ano de 2018 e com a vigência iniciada em agosto de 2020, tem como objetivo a proteção de dados pessoais de todo cidadão que esteja no território brasileiro, seja ele cidadão ou estrangeiro, de forma a criar um cenário de segurança jurídica no modo como estes dados serão colhidos e processados. Dentro dos dados pessoais, existe uma subcategoria sobre os dados considerados mais sensíveis e os que tratam de crianças e adolescentes, os quais deverão ter um cuidado maior.

A lei inteira possui uma base muito específica para que os dados possam ser tratados: é necessário o consentimento do dono do dado para que isto ocorra. Entretanto, nas hipóteses do art. 7º da lei, é possível a utilização sem o consentimento adequado, como nos casos de obrigação legal, defender direitos em processos, preservar a vida e a integridade física, entre outros.

Com a nova legislação, os principais afetados serão as empresas, que deverão ter uma tríade de pensamento: transparecer ao titular o porquê de aquele dado estar sendo coletado; qual o objetivo que aquele dado tem com a finalidade da questão discutida; e se as informações solicitadas são realmente necessárias ou podem ser dispensadas.

Ademais, o titular terá mais poder sobre o controle dos dados, de forma que poderá solicitar a exclusão destes, a migração, revogar consentimento e outras garantias de direitos autônomos.

O objetivo da lei não é impedir o tratamento desses dados pessoais informados, mas sim a forma como serão tratados e uma maior informação ao proprietário a respeito das destinações e protocolos de segurança aplicados.

Desse modo, a presente pesquisa buscou evidenciar a importância do compliance como instrumento viabilizador de conformidade à LGPD e, portanto, de superação da atual ordem econômica globalizada à medida que tal conformidade passou a ser algo primordial, necessária e inderrogável, especialmente no âmbito das relações trabalhistas.

O presente artigo busca explorar as razões por trás da formulação da Lei Geral de Proteção de Dados (LGPD), elaborada em 2018, tanto quanto de que forma a utilização concomitante com o instituto do compliance podem contribuir para a superação dos desafios impostos pelo atual cenário econômico. Para tanto, serão utilizadas as metodologias dedutiva e, também, indutiva, com base em estudos legislativos, doutrinários, tanto quanto por meio de análises bibliográficas.

2. Contextualização histórica da LGPD

A liderança do debate sobre esse tema surgiu na União Europeia (UE) e se con-

solidou com a promulgação do Regulamento Geral de Proteção de Dados Europeu nº 679, aprovado em 27 de abril de 2016 (GPDR), com o objetivo de abordar a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação de dados, conhecido pela expressão “free data flow”.²

Em relação às normas internas, a proteção de dados pessoais das pessoas físicas relativamente ao tratamento dos seus dados pessoais é um direito fundamental, garantido por diversas legislações no Brasil e em muitos países³. No Brasil, já tinha previsão no Marco Civil da Internet (artigos, 7º, I, III, VIII, IX, X, XI e 11, parágrafos 1º e 2º), no Código de Defesa do Consumidor (artigo 43) e na Lei do Cadastro Positivo, Decreto nº 7.962/2013 (artigo 4º, VII), pautados em nossa Constituição⁴, onde pode-se citar o artigo 3º, I e II; artigo 4º; II; artigo 5º, X e XII; artigo 7º, XX-VIII; e art. 219.

A Lei Geral de Proteção de Dados⁵ (LGPD) aprovada em agosto de 2018 dispõe sobre o tratamento do uso de dados pessoais, seja por pessoa física como por pessoa jurídica, visando o direito de proteção a todos, na condição de pessoa natural. E é a partir deste marco que o Brasil realmente entra na era da Internet, voltado aos aspectos das garantias aos indivíduos no direito de privacidade e liberdade, como os demais países do mundo.⁶

Isso seria a consolidação de um debate global que vem se desenvolvendo desde os anos 1990, quando os avanços tecnológicos, em especial o desenvolvimento da Internet, acabou por criar um fluxo de dados e informações, de modo que se tornou necessário o marco normativo que fizesse frente a essa nova realidade.⁷

Um dos principais objetivos desta Lei é acabar com as divulgações de dados pessoais sem o consentimento. Frequentemente, surgem notícias na mídia de que ocorreram vazamentos de CPFs de “n” pessoas sem qualquer aprovação, dados bancários expostos a todos na Internet, podendo rapidamente surgirem ataques virtuais de criminosos a pessoas inocentes e que acabam sendo prejudicadas por estes incidentes.

O mundo digital trouxe muitas facilidades, mas, paralelamente, muitas dificuldades, dilemas que fizeram necessária a criação de leis para tentar frear esse avanço no mundo da Internet, onde muitas vezes, o ser humano é vítima. Isto posto,

2 PINHEIRO, Patricia Peck. *Proteção de Dados Pessoais*: Comentários à Lei n.º 13.709/2018-LGPD. São Paulo: Saraiva Educação SA, 2020, p. 32.

3 PRADO, Fabiany Estavas; LIPPMANN, Rafael Knorr; TORRES, Rafael Lima. *Lei Geral de Proteção de Dados: origens, vigência e principais aspectos*. In: **Revista Direito UTP**, Curitiba, v. 1, n. 1, p. 141-156, jul./ dez. 2020, p. 5.

4 BRASIL. **Constituição da República Federativa do Brasil**. Brasília: Senado, 1988.

5 BRASIL. **Lei Geral de Proteção de Dados (LGPD). Decreto Lei nº 13709 de 14 de agosto de 2018**. Brasília, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/113709.htm. Acesso em: 21 out. 2021.

6 ALMEIDA, Leonardo Goês de; GOMES, Andréa Salcedo Monteiro dos Santos. **Direito ao esquecimento, LGPD e liberdade de expressão**: como ponderá-los?. Disponível em: <https://www.conjur.com.br/2021-fev-28/opiniao-direito-esquecimento-lgpd-liberdade-expressao>. Acesso em: 16 abr. 2021, p. 8.

7 LOURENÇO, Ana Lucia; TAQUES, João Daniel Vilas Boas. O papel das Ouvidorias Públicas na implementação da Lei Geral de Proteção de Dados (LGPD). In: **Revista do MPC/PR**, Curitiba, v. 7, n. 13, p.12-28, nov. 2020/maio 2021.

o Brasil avançou neste tema e criou a LGPD, prevenindo que os dados pessoais sejam tratados de formas irresponsáveis ou sem a concordância dos indivíduos.

A Lei possui duas vertentes principais: dados pessoais e dados pessoais sensíveis. A distinção entre os dois ocorre na característica de cada um. Os dados sensíveis são as informações que podem causar algum preconceito ao ser humano, tais como etnia, cor, raça, religião. Enquanto o dado pessoal remete ao ser humano identificado ou identificável, como data de nascimento, Cadastro de Pessoa Física – CPF e qualificação profissional. Além desses dois dados, ainda há o dado anonimizado, que é aquele onde não pode ser identificado e que sofreu algum tratamento.

Com a vigência da LGPD, será necessário que as empresas, bem como os órgãos públicos, se adequem às normas estabelecidas na Lei quanto à proteção dos dados pessoais⁸. Qualquer informação referente a pessoas deverá ser tratada com zelo e cautela, porém ela não tem efeito imediato.

Desta forma, o tratamento de dados pessoais por pessoas jurídicas de direito privado só será permitido observando os limites impostos por pessoa jurídica de direito público responsável para tal, e, em relação aos bancos de dados que contêm o tipo de informação resguardada pela referida lei, estes devem ser controlados pelo poder público.⁹

Todavia, olvidar não se deve que apenas constituir um ambiente seguro sob a ótica de proteção de dados não é suficiente¹⁰. A empresa precisa demonstrar tais ações à sociedade (accountability).

3. Responsabilidades e obrigações na LGPD

O legislador buscou estabelecer regras de coleta, uso, armazenamento e compartilhamento de dados de um cidadão por outra pessoa natural ou jurídica, bem como criar um cenário de segurança jurídica, com a padronização de normas e práticas para promover a proteção, de forma igualitária e dentro do país e no mundo, aos dados pessoais de todo cidadão que esteja no Brasil.

A lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (art. 1º).

A norma ainda contempla conceitos importantes em seu art. 5º, tais como: dado pessoal, que é definido como toda informação relacionada a pessoa natural identificada ou identificável, e dado pessoal sensível, que são dados relacionados à

8 GNAF, Ana Paula: Os limites da publicidade no processo judicial e os direitos da personalidade face aos dados sensíveis. Aplicação subsidiária da Lei Geral de Proteção de Dados nº 13.709/2018. Percurso - Anais do IX do CONBRADEC, Curitiba, v. 1, n. 32, p. 283-287, 2020.

9 GUÉRIOS, Ana Carolina Ferreira Jacomet; VIEIRA, Guilherme Vidal. Lei Geral de Proteção de Dados: desafios e expectativas. Percurso - Anais do IX do CONBRADEC, Curitiba, v. 1, n. 32, p. 40-56, 2020.

10 SANTOS, Alexandre da Silva. A importância da atuação da auditoria interna na implementação da Lei Geral de Proteção de Dados nas empresas públicas. São Paulo, 2019. Digitado. Projeto de Mestrado Profissional em Gestão e Políticas Públicas - MPGPP da Escola de Administração de Empresas de São Paulo, Fundação Getúlio Vargas. Orientação: Marco Antonio Carvalho Teixeira. Não publicado.

origem racial ou etnia, à saúde, à vida sexual, às convicções políticas, filosóficas e religiosas e que, portanto, merecem cuidados ainda mais específicos.

Havendo o conteúdo de pessoas brasileiras ou não, mas que estejam em território nacional, a LGPD deve ser cumprida, independentemente se a sede da organização ou o centro de dados estejam localizados no Brasil ou no exterior. No entanto, é permitido o compartilhamento de dados com organismos internacionais e com outros países, desde que sejam feitos a partir de protocolos seguros e/ou para cumprir exigências legais, nos termos elencados no art. 33, sempre visando a segurança e proteção do indivíduo. Para a efetivação da transferência, o nível de proteção de dados no país estrangeiro ou no organismo internacional deverá ser compatível com o previsto na LGPD¹¹. Assim, antes de qualquer transferência de dados, deverá ser feita uma avaliação prévia do nível de proteção de dados do destinatário pela autoridade nacional, que levará em consideração o previsto nos incisos I a VI do art.34, in verbis:

- “I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;
- II - a natureza dos dados;
- III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;
- IV - a adoção de medidas de segurança previstas em regulamento;
- V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e
- VI - outras circunstâncias específicas relativas à transferência (...).”¹²

Outro elemento essencial da LGPD é o consentimento. O consentimento do indivíduo é o requisito para que dados pessoais possam ser tratados. Mas o que significa “tratar dados” ou “tratamento de dados” na LGPD? O sentido vai muito além de cuidar, proteger, zelar dados. O tratamento de dados pessoais na LGPD refere-se a todas as operações/manipulações realizadas com informações de pessoas naturais, inclusive nos meios digitais, por outras pessoas naturais ou pessoas jurídicas, tanto de direito privado quanto de direito público¹³. Assim, infere-se que:

11 KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. **Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais:** mecanismos de tutela para o livre desenvolvimento da personalidade. 2020. Dissertação (mestrado em Direito) .Faculdade de Direito da Universidade Federal de Juiz de Fora. Juiz de Fora, 2019. Disponível em:<https://repositorio.ufjf.br/jspui/bitstream/ufjf/11438/1/mariareginade-tonicavalcantirigolonkorkmaz.pdf>. Acesso em: 20 out. 2021.

12 BRASIL. **Lei Geral de Proteção de Dados (LGPD). Decreto Lei nº 13.709 de 14 de agosto de 2018.** Brasília, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 out. 2021.

13 VILELA, Camila Maria de Moura; LEMOS, Christine Mattos Albiani. A responsabilização decorrente do tratamento de dados pessoais e o sistema sancionatório da lei geral de proteção de dados

Não é permitido mais no Brasil fazer tratamento de dados sem uma fundamentação jurídica, que pode ser o consentimento, o cumprimento de um contrato, a realização de uma política pública, mas ela precisa existir. Para o consumidor cria-se um novo hall de direitos que permite acessar os dados dele. O consumidor pode pedir para retificar e a qualquer momento revogar o consentimento que deu.¹⁴

O fornecimento de consentimento pelo titular corresponde a apenas um item do rol apresentado no art. 7º, da LGPD, que disciplina as hipóteses e as especificidades em que é permitido o tratamento de dados pessoais, tais como: para o cumprimento de obrigação legal ou regulatória pelo controlador; para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; para a proteção da vida ou da incolumidade física do titular ou de terceiro, entre outros.

Assim, para o tratamento de dados deverão ser observados os requisitos do art. 7º e seguintes, bem como os princípios elencados no art. 6º da LGPD, que incluem os princípios: da finalidade, da segurança, da prevenção, da não discriminação, da responsabilização e prestação de contas, entre outros.

A Lei nº 13.853, de 14 de agosto de 2019, define a Autoridade Nacional de Proteção de Dados – ANPD como órgão da Administração Pública Direta Federal que tem como missão institucional assegurar a mais ampla e correta observância da LGPD no Brasil e, nessa medida, garantir a devida proteção aos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade dos indivíduos.

Importante ressaltar que, a partir de 1º de agosto de 2021 (art. 20, da Lei nº 14.010/2020), encontram-se em vigor os artigos referentes às sanções administrativas para quem descumprir a Lei Geral de Proteção de Dados.

A LGPD prevê, em seu artigo 52¹⁵, a imposição de multa, limitada em até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado, baseado no seu último exercício, excluídos os tributos, estando o valor máximo restrito a R\$ 50 milhões por infração, além das seguintes sanções que, além de penalizar a empresa economicamente, afeta a sua reputação e imagem. Vejamos:

pessoais (“LGPD”). *Revista Ilustração*, v. 1, n. 2, p. 57-67, 2020.

14 KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. **Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade**. 2020. Dissertação (mestrado em Direito). Faculdade de Direito da Universidade Federal de Juiz de Fora, Juiz de Fora, 2019. Disponível em: <https://repositorio.ufjf.br/jspui/bitstream/ufjf/11438/1/mariareginadetonicalcantirigolonkorkmaz.pdf>. Acesso em: 20 out. 2021.

15 BRASIL. **Lei Geral de Proteção de Dados (LGPD). Decreto Lei nº 13.709 de 14 de agosto de 2018**. Brasília, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 out. 2021.

- advertência, com indicação de prazo para adoção de medidas corretivas;
- multa diária;
- publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- eliminação dos dados pessoais a que se refere a infração;
- suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
- suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
- proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

As sanções previstas na LGPD são aplicáveis a fatos ocorridos após 1º de agosto de 2021 ou para delitos de natureza continuada iniciados antes de tal data. Cabe observar que há critérios para se aplicar tais sanções, de acordo com o parágrafo 1º do artigo 52: a gravidade da natureza das infrações e direitos afetados; a boa-fé do infrator; vantagem econômica do infrator; adoção reiterada e demonstrada de medidas de segurança e de procedimentos internos capazes de mitigar os riscos; adoção de política de boas práticas e um plano de governança; pronta adoção de medidas corretivas e proporcionalidade entre a gravidade da infração e a intensidade da sanção.

A publicação da infração pode impactar de forma muito negativa a organização por ser considerada uma propaganda negativa e afetar a confiabilidade da empresa perante seus consumidores e fornecedores¹⁶. A sanção de bloqueio dos dados pessoais a que se refere a infração, ou até mesmo a eliminação dos dados pessoais, representa medida que pode inviabilizar diversos modelos de negócios que dependem desse tratamento de dados pessoais.¹⁷

Vale destacar que se encontra em fase de conclusão a elaboração do Regulamento de Fiscalização e Aplicação de Sanções Administrativas, que passou por Consulta Pública entre 28 de maio e 28 de junho de 2021 e que ainda será submetida à consulta pública sobre norma específica para tratar das sanções e dosimetria.

16 VILELA, Camila Maria de Moura; LEMOS, Christine Mattos Albiani. A responsabilização decorrente do tratamento de dados pessoais e o sistema sancionatório da lei geral de proteção de dados pessoais (“LGPD”). **Revista Ilustração**, v. 1, n. 2, p. 57-67, 2020.

17 PRADO, Fabiany Estavas; LIPPMANN, Rafael Knorr; TORRES, Rafael Lima. Lei Geral de Proteção de Dados: origens, vigência e principais aspectos. *In: Revista Direito UTP*, Curitiba, v. 1, n. 1, p. 141-156, jul./ dez. 2020, p. 5.

Assim, de modo a conferir segurança jurídica aos administrados, a ANPD iniciará sua atuação sancionadora somente após a aprovação das referidas legislações; no entanto, a atuação da autoridade pode se dar com relação a fatos ocorridos a partir de 1º de agosto de 2021 ou para delitos de natureza continuada iniciados antes de tal data.

É importante destacar que as penalidades provenientes de infração à LGPD não substituem as sanções ou multas cíveis ou penais previstas em legislação específica.

4. O *compliance* e sua aplicação no âmbito do Direito do Trabalho

O termo *compliance* tem sua origem na língua inglesa, no verbo “to comply”, que significa tanto concordar, consentir, condescender quanto cumprir, corresponder, estar de acordo. Atualmente, *compliance* é compreendido como estar em conformidade com as leis, regulamentações, normas, princípios éticos e códigos de conduta.¹⁸

O *compliance* opera em pequenas e/ou grandes instituições, a partir de ferramentas e regras, no sentido de prevenir riscos legais provenientes de comportamentos e/ou atitudes inadequadas de sócios e colaboradores. O *compliance* vai além do cumprimento de disciplinas ou normas de uma empresa, pois busca evitar, identificar e tratar as não conformidades ou desvios existentes. Assim, a ação e implantação do *compliance* interfere diretamente na cultura organizacional na medida em que evita ações antiéticas, corrige desvios, bem como possíveis perdas de receita provenientes de ações que comprometam a relação com o cliente e a imagem da organização.¹⁹

Antes do surgimento do *compliance*, as empresas utilizavam-se de diferentes mecanismos como formas preventivas de verificações internas, tais como a auditoria interna, a governança corporativa, a advocacia preventiva, o código de ética empresarial, entre outros. Assim, o *compliance* pode ser concebido como sendo uma cultura de adequação às leis e regulamentos que deve iniciar na alta administração, com um propósito empresarial²⁰. A auditoria, por sua vez, complementa o *compliance* com o propósito de encontrar irregularidades na empresa para maior eficiência do programa. Essa mesma autora ressalta que no *compliance* trabalhista é necessário também a adequação aos princípios fundamentais da Constituição Federal.

Ao deliberar acerca do *compliance*, tem-se como referência os sistemas de controles internos que têm como intuito permitir maior segurança à empresa²¹. Desse modo, os estudos econômico-financeiros devem permitir uma atuação apropriada

18 MARTINS, Sérgio Pinto. *Compliance no direito trabalhista*. In: _____. (org.). *Compliance no direito*. São Paulo: **Revista dos Tribunais**, 2020, v. 6, p. 24-29.

19 CUEVA, Ricardo Villas Bôas. *Funções e Finalidades dos Programas de Compliance*. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). **Compliance: perspectivas e desafios dos programas de conformidade**. Belo Horizonte: Fórum, 2018.

20 CARLOTO, Selma. **Compliance trabalhista**. 2. ed. São Paulo: LTR, 2020, p. 25.

21 COLARES, Wilde Cunha. *Ética e compliance nas empresas de outsourcing*. 2014. Monografia (LLM – Legal Law Master) - Programa de Pós-graduação em Direito - Insper - Instituto de Ensino e Pesquisa, São Paulo, 2014. Disponível em: <http://dspace.insper.edu.br/xmlui/handle/11224/1238>. Acesso em: 20 out. 2021.

que preserve a empresa de riscos, fraudes e corrupção em programas que envolvam processos licitatórios, por exemplo.

O compliance também vem organizar normas internas para que estejam em conformidade com os valores e princípios da companhia, garantindo que seja cumprida por todos e de conhecimento dos colaboradores.²²

O surgimento do compliance teve origem nos Estados Unidos no início do século 20, marcado pelo início da normatização de conduta nas empresas²³. A necessidade de um programa de compliance surgiu, inicialmente, no mercado financeiro, em decorrência da globalização²⁴. Inúmeros eventos afetaram o mercado de capitais e fizeram com que o compliance não só se desenvolvesse, mas também se apresentasse como fundamental para as empresas.

Um marco na história do compliance foi a promulgação pelo Congresso americano da Foreign Corrupt Practices Act - FCPA, em 19 de novembro de 1977. Essa foi a primeira lei sobre anticorrupção no país e tinha como objetivo prevenir e combater práticas de pagamentos aos funcionários públicos estrangeiros para obter vantagens indevidas.²⁵

Outros marcos foram a crise financeira de 2008 nos Estados Unidos, que provocou o fechamento de empresas e bancos. A falência do banco Lehman Brothers Holding Inc. provocou um clima de desconfiança, em razão de empréstimos efetuados de origem imobiliária que tiveram devedores insolventes. Como consequência criou-se em 2010 o compliance e o Dodd-Frank Wall Street Reform and Consumer Protection Act visando a proteção do consumidor.²⁶

Em 2010, no Reino Unido, o UK Bribery Act - UKBA tornou crime o pagamento e/ou recebimento de propina por agentes públicos e para agentes públicos. Do mesmo modo, outros países da Europa, tais como Espanha, Portugal e Alemanha, também criaram mecanismos legais determinando regras de compliance²⁷. O Bribery Act foi consequência de um grande empenho do Reino Unido para atualizar a legislação anticorrupção dos países que o compõem, mas repercutiu mundialmente, pelas suas inovações legais no tocante à corrupção.²⁸

22 SEIN, José Luis Goñi. Programas de cumplimiento empresarial (compliance programs): aspectos laborales. In: PUIG, Santiago Mir et al. **Responsabilidad de la empresa y compliance**: programas de prevención, detección y reacción penal. Madrid: Edisofers, 2014, p 176.

23 MARTINS, Sérgio Pinto. Compliance no direito trabalhista. In: _____. (org.). Compliance no direito. São Paulo: **Revista dos Tribunais**, 2020, v. 6, p. 24-29.

24 SWISTALSKI, Andressa; LOBATO, Carla Cristina Cavalheiro. Compliance no setor financeiro e mercado de capitais. In: CARVALHO, André Castro et al. **Manual de compliance**. 2. ed. Rio de Janeiro: Forense, 2020. p. 659.

25 CUEVA, Ricardo Villas Bôas. Funções e Finalidades dos Programas de Compliance In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). Compliance: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018.

26 SWISTALSKI, Andressa; LOBATO, Carla Cristina Cavalheiro. Compliance no setor financeiro e mercado de capitais. In: CARVALHO, André Castro et al. **Manual de compliance**. 2. ed. Rio de Janeiro: Forense, 2020. p. 668.

27 CUEVA, Ricardo Villas Bôas. Funções e Finalidades dos Programas de Compliance. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. (coord.). Compliance: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018, p. 36.

28 BERTOCCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Castro et al. **Manual de compliance**. 2. ed. Rio de Janeiro: Forense, 2020, p. 39.

No que diz respeito ao regulamento interno, ele é obrigatório em alguns países²⁹. O regulamento interno disciplinar ou regimento interno são ferramentas do compliance trabalhista, apresentam normas internas que facilitam o cumprimento da norma externa. Na França, por exemplo, é obrigatório o regimento interno para empresas que possuem mais de 20 funcionários. Em Portugal, no artigo 99 do Código de Trabalho, está prevista a obrigatoriedade e representatividade dos funcionários e sindicatos em sua elaboração.

Inicialmente o Brasil assumiu compromissos em relação ao combate à corrupção nas convenções internacionais da Organização das Nações Unidas (ONU), da Organização dos Estados Americanos (OEA) e, principalmente, da Organização para a Cooperação e Desenvolvimento Econômico (OCDE). Somente mais tarde implementa legislação própria e específica sobre a corrupção.³⁰

Historicamente, o Brasil passa por uma crise ética, por inúmeros escândalos envolvendo a corrupção e outras atividades ilegais, mas somente a Lei nº 12.683/2012 dispõe sobre os crimes de lavagem de dinheiro, ocultação de bens e valores. Trovão e Carmo (2018) abordam o compliance como sendo a ferramenta para desenvolvimento social e para a diminuição do déficit ético das empresas, entendendo-se déficit ético enquanto todos os atos de corrupção. Segundo seus estudos, a preservação da ética nas empresas determina a trajetória das atividades empresariais bem como suas transações econômicas. A corrupção – déficit ético - acaba por contagiar não somente as pessoas diretamente envolvidas, mas também a sociedade em geral através dos consumidores e dos contribuintes.

O compliance vem crescendo progressivamente no ordenamento jurídico brasileiro, através da criação da Lei n.º 12.846/2013, Lei Anticorrupção, que foi regulamentada pelo Decreto n.º 8.420/2015. Essa legislação impulsiona os programas de compliance nas empresas brasileiras de modo que estão cada vez mais presentes nos variados segmentos empresariais.

A Lei Anticorrupção veio suprir uma lacuna existente quanto à responsabilização das pessoas jurídicas pela prática de atos contra a administração pública, principalmente relativos à corrupção, fraudes em contratos administrativos e em licitações.³¹

O Decreto n.º 8.420/2015, que regulamenta a Lei n.º 12.846/2013, em seu artigo 41, caput, estabelece sobre o programa de integridade como um conjunto de procedimentos, visando a aplicação de códigos de conduta, instruções de identificação de práticas delituosas, como fraudes, desvios, irregularidades, praticados contra a administração pública, nacional ou estrangeira.

Considerando a pessoa jurídica, a Lei n.º 12.846/2013, no artigo 7º, prevê que a aplicação de sanções deve considerar a existência de mecanismos e incentivo à denúncia de irregularidades, procedimentos internos de integridade, auditoria interna, códigos de ética e de conduta. Desse modo, tem-se que o Decreto n.º

29 CARLOTO, Selma. **Compliance trabalhista**. 2. ed. São Paulo: LTR, 2020, p. 29.

30 BERTOCCELLI, Rodrigo de Pinho. Compliance. *In*: CARVALHO, André Castro et al. **Manual de compliance**. 2. ed. Rio de Janeiro: Forense, 2020, p. 45.

31 DUTRA, Lincoln Zub. (org.) **Compliance no ordenamento jurídico brasileiro**. Curitiba: Juruá, 2018, p. 60.

8.420/2015 também estabelece os parâmetros para a redução de multas, previstas na Lei Anticorrupção, para empresas que adotam programas de integridade.

A Lei Anticorrupção, também conhecida como Lei da Empresa Limpa, concedeu ao Estado meios administrativos para ensinar, delegar e conseguir reparar o erário de atos fraudulentos e corruptos realizados por pessoas jurídicas, com foco nas licitações públicas e execução dos contratos administrativos.³²

Além da Lei Anticorrupção, os programas de compliance no Brasil também se amparam na Lei n.º 9.613/98, aprovada em 1998, sobre lavagem de capitais, na Lei n.º 8.249/92, que versa sobre a improbidade administrativa, na Lei n. 8.666/93 sobre licitações, bem como com o Código Penal brasileiro.³³

Outra importante contribuição ocorreu em meados de 2015, quando o Conselho Administrativo de Defesa Econômica (CADE) publicou o Guia de Programas de Compliance, visando orientar sobre a estruturação e os benefícios da adoção do programa de compliance.³⁴

Em relação às principais funções do compliance, tem-se a proteção, orientação, qualidade, inovação e monitoramento³⁵. A função de proteção ocorre na medida em que o compliance resguarda a empresa, seus dirigentes, bem como os colaboradores através de ações preventivas que evitem transgressões e penalidades, bem como prejuízos financeiros à atividade e à imagem da empresa. A função orientativa é decorrente de medidas de promoção de informações e conscientização de todos os envolvidos na empresa, principalmente através de setor de compliance, que deverá acolher e responder a todas as dúvidas e suspeitas, bem como orientar e promover treinamentos com intuito de que todos internalizem a cultura organizacional de conformidade. As funções de qualidade e inovação estão atreladas aos processos internos, mas também à interação com os clientes que fornecem informações quanto aos produtos e/ou serviços ofertados. A função de monitoramento faz alusão ao dinamismo do compliance através de treinamento e supervisão contínuos. O monitoramento é peça fundamental para que todo o programa funcione e para que promova as adequações e atualizações necessárias.

Nesse sentido, além do compliance geral, que se volta à administração pública e governabilidade corporativa, destaca-se atualmente o compliance trabalhista, que vem conquistando maior espaço no contexto empresarial.

O programa de compliance trabalhista propõe uma mudança de paradigma organizacional, no sentido de combater a corrupção e sonegação de direitos trabalhistas. Além disso, os programas de compliance levam em consideração as

32 SWISTALSKI, Andressa; LOBATO, Carla Cristina Cavalheiro. Compliance no setor financeiro e mercado de capitais. *In*: CARVALHO, André Castro et al. **Manual de compliance**. 2. ed. Rio de Janeiro: Forense, 2020. p. 670.

33 MARTINS, Juliane Caravieri; MONTAL, Zélia Maria Cardoso. Compliance trabalhista e o direito à educação para o trabalho: desafios em face da responsabilidade social da empresa. **Revista Eletrônica do TRT da 9ª Região**, Curitiba, PR, v. 9, n. 91, p. 38-55, ago. 2020. Disponível em: <https://hdl.handle.net/20.500.12178/154352>. Acesso em: 20 out. 2021.

34 SILVA, Fabrício Lima; PINHEIRO, Iuri; BOMFIM, Vólia. **Manual do compliance trabalhista: teoria e prática**. 2. ed. Salvador: JusPodivm, 2021, p. 26.

35 CUEVA, Ricardo Villas Bôas. Funções e Finalidades dos Programas de Compliance. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. (coord.). **Compliance: perspectivas e desafios dos programas de conformidade**. Belo Horizonte: Fórum, 2018, p. 49.

peculiaridades de cada empresa, realizam antecipadamente um mapeamento dos processos e rotinas internas para poder indicar as correções necessárias.

O programa de compliance trabalhista, através da implantação de mecanismos de controle e padronização de condutas, busca criar um ambiente de trabalho congruente com as leis trabalhistas, mas também em conformidade com os princípios do Direito como um todo.

5. A LGPD e o *compliance* como meios de superação do atual cenário econômico

O compliance teve origem nas relações empresariais, mas vem crescendo em diversas áreas, especialmente na trabalhista, em decorrência de inúmeros casos envolvendo situações ilícitas no âmbito do trabalho³⁶. Entretanto, ainda não há regulamentação específica para o compliance trabalhista, o Decreto n.º 8.420/2015, que regulamenta a Lei Anticorrupção, traz importantes elementos para a sua aplicação³⁷. Os programas de compliance trabalhista são desenvolvidos embasados na legislação, com o propósito de retificar práticas contrárias às leis existentes.

A aplicabilidade do compliance trabalhista é baseada em outras normas legais, como, por exemplo, a Lei Geral de Proteção de Dados (LGPD), demonstrando assim evidente conexão entre ambas, tendo como principal foco os direitos humanos e fundamentais, além da dignidade da pessoa humana e proteção de dados pessoais. Desse modo, evita-se a punição das empresas em multas administrativas, como também em altas condenações no judiciário ou em ações coletivas por falta de ajustamento.³⁸

A Lei Geral de Proteção de Dados - LGPD, a Lei n.º 13.709/2018, a Lei n.º 9.029/95, bem como o artigo 373-A da Lei n.º 13.467/2017 – Consolidação das Leis do Trabalho - CLT e a Constituição Federal de 1988 têm como finalidade a proteção dos trabalhadores de práticas discriminatórias. Ademais, a Lei n.º 9.029/95 responsabiliza criminalmente a prática de exigência de testes, exames, perícias, laudos, atestados ou declarações que versem sobre o estado gravídico da mulher, com pena de detenção de um a dois anos, aplicação de multa e proibição de empréstimo e financiamento junto às instituições financeiras, motivado por preconceito de etnia, raça, cor ou deficiência.

Com o surgimento da LGPD, tem-se como instrumento de compliance os relatórios de impacto à Proteção de Dados Pessoais, além de ferramentas exclusivas no compliance trabalhista como o regulamento empresarial e a política de advertências³⁹. Desta forma, resta indubitável a necessidade de adequação às leis trabalhistas a fim de evitar multas como aquelas decorrentes do eSocial. Isto justifica, inclusive, a necessidade da adoção de um

36 DUTRA, Lincoln Zub. (org.) **Compliance no ordenamento jurídico brasileiro**. Curitiba: Juruá, 2018, p. 52.

37 CARLOTO, Selma. **Compliance trabalhista**. 2. ed. São Paulo: LTR, 2020, p. 75.

38 CUEVA, Ricardo Villas Bôas. Funções e Finalidades dos Programas de Compliance. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). **Compliance: perspectivas e desafios dos programas de conformidade**. Belo Horizonte: Fórum, 2018, p. 52.

39 CARLOTO, Selma. **Compliance trabalhista**. 2. ed. São Paulo: LTR, 2020, p. 64.

programa de compliance trabalhista.⁴⁰

O programa de compliance trabalhista deve ter apoio na responsabilidade social e na ética organizacional, com suporte jurídico na Constituição Federal e nas demais leis brasileiras⁴¹. Para sua implementação é necessária uma equipe composta por diversos profissionais, com o intuito de solucionar as demandas. Na equipe, é essencial a presença de advogados, técnicos de segurança do trabalho, contadores, profissional de recursos humanos e outros profissionais.

No tocante aos colaboradores, o compliance trabalhista se demonstra como uma ferramenta de regulação e responsabilização na observância das normas trabalhistas na contratação, na vigência de um contrato de trabalho e no término deste⁴². Sua aplicabilidade ocorre na observância do código de ética e de conduta, incluindo os pagamentos trabalhistas e tratamento dado aos colaboradores pelos empregadores. Da mesma forma, no término do contrato de trabalho, tomando medidas preventivas que mitiguem a litigiosidade entre empregados e empresa, especialmente cumprindo com todas as obrigações previstas na legislação trabalhista.

Sendo assim, o objetivo do compliance trabalhista é tanto evitar o ajuizamento de ações trabalhistas quanto promover um ambiente saudável em termos relacionais e operacionais⁴³. A aplicação do compliance na seara trabalhista visa afastar a aplicação de multas, conservar a ética, a integridade, a idoneidade, a transparência e o cumprimento das leis relativas aos direitos humanos do trabalhador⁴⁴. Desse modo, a empresa conserva a sua reputação, um importante ativo empresarial, bem como viabiliza a redução dos custos relativos aos passivos trabalhistas, assim a empresa consegue investir mais e beneficiar o ambiente laboral.

Não há um modelo pronto de programa a ser seguido, pois o mesmo deve ser desenvolvido de acordo com as características de cada empresa, tais como seu ramo de atividade, seu tamanho, quantidade de funcionários, entre outros fatores.⁴⁵ Porém, entre os diversos procedimentos necessários, as autoras destacam a importância do engajamento da alta gestão, imprescindível para que a cultura da integridade possa se tornar, de fato, parte do negócio da empresa.

Desse modo, o suporte da alta administração da empresa é um fator fundamental para que os diversos processos de programa de compliance sejam implantados e efetivos, visto que é através do suporte dos membros da diretoria e do conselho de administração, da responsabilidade de condutas exemplares para os demais co-

40 DUTRA, Lincoln Zub (org.). **Compliance no ordenamento jurídico brasileiro**. Curitiba: Juruá, 2018, p. 77.

41 MARTINS, Juliane Caravieri; MONTAL, Zélia Maria Cardoso. Compliance trabalhista e o direito à educação para o trabalho: desafios em face da responsabilidade social da empresa. *Revista Eletrônica do TRT da 9ª Região*, Curitiba, PR, v. 9, n. 91, p. 38-55, ago. 2020. Disponível em: <https://hdl.handle.net/20.500.12178/154352>. Acesso em: 20 out. 2021.

42 CORREIA, Henrique. Compliance e sua aplicação no direito do trabalho. *Revista Eletrônica do TRT da 9ª Região*, Curitiba, PR, v. 9, n. 91, p. 16-30, ago. 2020. Disponível em: <https://hdl.handle.net/20.500.12178/151250>. Acesso em: 20 out. 2021.

43 MARTINS, Sérgio Pinto. Compliance no direito trabalhista. In: _____. (org.). *Compliance no direito*. São Paulo: **Revista dos Tribunais**, 2020, v. 6, p. 24-29.

44 CARLOTO, Selma. **Compliance trabalhista**. 2. ed. São Paulo: LTR, 2020, p. 48.

45 DUTRA, Lincoln Zub (org.). **Compliance no ordenamento jurídico brasileiro**. Curitiba: Juruá, 2018, p. 89.

laboradores, que atuam como canalizadores de força para todo o sistema.

Nas relações de trabalho, a fase pré-contratual é importante no sentido de evitar processos trabalhistas e prejuízos dessa ordem. Inúmeros litígios com origem nessa fase são relativos às divulgações de vagas de emprego, conservação de dados pessoais, promessa de admissão, certidão de antecedentes, exigências de experiências profissionais, posse da carteira de trabalho, entre outros.⁴⁶

Constantemente as empresas anunciam vagas de trabalho com especificações discriminatórias, relacionadas ao gênero, idade, etnia, origem, condição familiar, boa aparência, entre outros. Diante disso, pode-se destacar que as instituições, em sua fase pré-contratual, devem ter cuidados para afastar atos discriminatórios.

A discriminação pode ser evitada através de treinamentos e conscientização dos recrutadores acerca da responsabilidade nas tratativas iniciais. Pode-se afirmar assim que é necessário ter atenção e responsabilidade em todas as fases do contrato de trabalho, no intuito de reduzir os riscos contratuais.⁴⁷

É importante ressaltar que as instituições devem estabelecer, na fase pré-contratual, o modelo de contrato de trabalho que planejam aderir para que esse esteja de acordo com os requisitos e qualificações para as atividades, sua vigência, a atividade a ser desempenhada, os recursos disponíveis, entre outros.⁴⁸

O programa de compliance trabalhista pode ser instituído desde a admissão do empregado⁴⁹, levando-se em conta a dignidade da pessoa humana, o panorama regulatório – legislação, valores e código de ética da empresa – abrangendo assim os direitos e deveres dos empregados.

No processo seletivo, com intuito de conhecer melhor o perfil dos candidatos, a empresa pode apresentar sua política interna, seu regulamento ou código de conduta, bem como realizar dinâmicas de grupo, treinamentos e verificação dos antecedentes criminais dos participantes do processo.

Ademais, para a fase pré-contratual, tratando-se da exigência de experiência, com base na Lei n.º 11.644/2008, art. 442-A, o empregador não poderá exigir do seu futuro funcionário experiência prévia maior de seis meses no mesmo tipo de atividade. Caso a contratação seja direcionada para outra atividade, nesse caso poderá ser exigida a experiência na função pretendida.

Quanto à idade do candidato, a partir da Lei n.º 10.741/2003, Estatuto do Idoso, em seu artigo 27 consta que não deve haver discriminação na contratação de uma pessoa idosa. A exceção se dá unicamente quando a natureza do cargo o exigir, sendo de potencial perigo à saúde do trabalhador. Já em seu artigo 100, inciso II, cita ainda que não se deve negar, seja cargo ou emprego, em razão da idade, sendo passível de punição caso ocorra tal discriminação.

Em relação à cor, raça, sexo, crença religiosa, política, etnia, origem ou nacionalidade do candidato não pode haver restrição, nem ser usado como fator de

46 SILVA, Fabrício Lima; PINHEIRO, Iuri; BOMFIM, Vólia. **Manual do compliance trabalhista: teoria e prática**. 2. ed. Salvador: JusPodivm, 2021, p. 40.

47 DUTRA, Lincoln Zub (org.). **Compliance no ordenamento jurídico brasileiro**. Curitiba: Juruá, 2018, p. 84.

48 SILVA, Fabrício Lima; PINHEIRO, Iuri; BOMFIM, Vólia. **Manual do compliance trabalhista: teoria e prática**. 2. ed. Salvador: JusPodivm, 2021, p. 45.

49 CARLOTO, Selma. **Compliance trabalhista**. 2. ed. São Paulo: LTR, 2020, p. 51.

discriminação. A Lei n.º 13.467/2017, em seu artigo 223-C, deixa evidente que a discriminação fere a honra, autoestima, imagem, sexualidade e integridade física da pessoa. Além do mais, a Constituição Federal, artigo 5º, inciso VIII, assegura que ninguém será privado por crença religiosa, filosófica e política.

Dessa forma, infere-se que no processo de contratação não pode haver violação da privacidade e/ou da intimidade do trabalhador, ou seja, o direito da empresa em contratar alguma pessoa de acordo com seus princípios e políticas internas não pode ferir o direito do trabalhador no que tange à sua imagem e dignidade⁵⁰. Caso a empresa ou o empregador não ajam em conformidade, poderá incorrer em responder e responsabilizar-se por danos morais.

Uma vez na empresa, os colaboradores são instados a assimilar e internalizar o significado de ética e integridade de modo a reproduzirem-no em suas atividades e atitudes. Essa conscientização dará sustentação a um programa de compliance, tornando-o bem sucedido. Desse modo, o programa de compliance trabalhista busca o constante aperfeiçoamento do clima organizacional na empresa, bem como evitar processos judiciais, punições administrativas ou suspensão das atividades empresariais.⁵¹

No caso de colaboradores terceirizados, na tentativa de escapar da responsabilização da empresa tomadora dos serviços terceirizados, o sistema de compliance prevê ferramentas para a fiscalização de todas as prestadoras de serviços, impondo-lhes a obrigação de apresentar documentos que comprovem o cumprimento do pagamento das verbas trabalhistas, assim como também a divulgação de dados financeiros, certificando que terá condições de respeitar as incumbências trabalhistas durante o cumprimento do contrato de serviços.⁵²

Da mesma forma, o compliance trabalhista, por meio do incentivo à boa governança, de treinamentos de empregados e gestores de todos os níveis, promove ações em concordância com os princípios constitucionais, tais como da dignidade da pessoa humana, da igualdade primando por valores sociais do trabalho e da não discriminação⁵³. Desse modo, a empresa adequa-se às normas e cobra uma conduta ética por parte de seus colaboradores e gestores.

Desta forma a utilização do compliance trabalhista adaptado à Lei Geral de Proteção de Dados demonstra ser como meios eficazes de superação das peculiaridades da atual ordem econômica global, haja vista a percepção da importância que as informações passaram a ter, especialmente aquelas de cunho personalíssimo e sensível, tais como aquelas decorrentes das relações de trabalho.

Os tribunais brasileiros já vêm aplicando a LGPD em casos de violações, seja de comprometimento dos dados tratados, vazamentos etc. Vejamos:

50 SILVA, Fabrício Lima; PINHEIRO, Iuri; BOMFIM, Vólia. **Manual do compliance trabalhista: teoria e prática**. 2. ed. Salvador: JusPodivm, 2021, p. 51.

51 CORREIA, Henrique. Compliance e sua aplicação no direito do trabalho. **Revista Eletrônica do TRT da 9ª Região**, Curitiba, PR, v. 9, n. 91, p. 16-30, ago. 2020. Disponível em: <https://hdl.handle.net/20.500.12178/151250>. Acesso em: 20 out. 2021.

52 KRUPPA, Roberta Potzik Soccio; GONÇALVES, Anselmo. Compliance trabalhista. **Revista FAE de Direito**, Curitiba, v. 2, n. 1, p. 123-145, jun. 2020. Disponível em: <https://revistadedireito.fae.edu/direito/issue/view/7>. Acesso em: 20 out. 2021.

53 CARLOTO, Selma. **Compliance trabalhista**. 2. ed. São Paulo: LTR, 2020, p. 66.

AGRAVO DE INSTRUMENTO. MANDADO DE SEGURANÇA COLETIVO. DIVULGAÇÃO DE LISTA DE VACINADOS CONTRA A COVID-19. Pretensão do impetrante de que, em sede de liminar, seja ordenada a divulgação da lista de vacinados contra a COVID-19, nos termos da Lei Municipal nº 9.011/2021. Juízo de primeira instância que deferiu parcialmente o pedido, indeferindo o pleito relacionado às pessoas que já tomaram a vacina. Decisão que deve ser suspensa. Requisitos para a concessão de liminar não preenchidos. Necessidade de suspensão da divulgação de lista de pessoas imunizadas com a vacina contra a COVID-19. Lei Municipal nº 9.011/2021 que, com o objetivo de coibir irregularidades daqueles que desrespeitam a ordem de vacinação, pretende a divulgação de dados pessoais dos munícipes de Franca. Norma municipal que colide com a Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais. LGPD). Privacidade da pessoa natural que deve ser respeitada, sobretudo quando existentes métodos alternativos eficazes para satisfazer a finalidade pretendida pela norma municipal sem afrontar a Lei Geral de Proteção de Dados Pessoais. Recurso não provido. (TJSP; AI 2122916-70.2021.8.26.0000; Ac. 14906428; Franca; Primeira Câmara de Direito Público; Rel. Des. Rubens Rihl; Julg. 10/08/2021; DJESP 22/09/2021; Pág. 2745)

No caso acima, a Lei Municipal que instituiu a divulgação da lista de todos os cidadãos que tomaram a vacina contra a covid-19, com base em Lei Municipal, foi suspensa com fundamento em violação à Lei Geral de Proteção de Dados.

APELAÇÃO. AÇÃO CONDENATÓRIA. PRESTAÇÃO DE SERVIÇOS EDUCACIONAIS. VAZAMENTO DE DADOS PESSOAIS POR PREPOSTO. CELULAR DA AUTORA PASSADO A UM TERCEIRO. RECEBIMENTO DE MENSAGENS DE ASSÉDIO SEXUAL. RECURSO DE AMBAS AS PARTES. LEGITIMIDADE PASSIVA DA RÉ. RESPONSABILIDADE PELOS DANOS DECORRENTES DA VIOLAÇÃO AO TRATAMENTO DE DADOS PESSOAIS. LEI GERAL DE PROTEÇÃO DE DADOS. DANOS MORAIS EVIDENTES. MAJORAÇÃO. GRAVE VIOLAÇÃO À INTIMIDADE E À PRIVACIDADE 1. A empresa controladora de dados pessoais é figura legítima para figurar no polo passivo de demanda que objetive a indenização pelo vazamento de dados da autora

orquestrados por preposto da ré, que repassou o celular da autora para um colega para fins de assédio sexual (LGPD, art. 42). 2. A ré, ao dar causa ao vazamento de dados, responde pelos danos morais sofridos (LGPD, art. 5º, VI e 42, caput). 3. É cabível a indenização por danos morais, considerando a violação grave ao direito à intimidade e à privacidade causado pela quebra do dever de proteção de dados pessoais, o que propiciou assédio sexual agressivo. 4. Indenização majorada, pois a gravidade da situação, a séria negligência da empresa, a postura recalcitrante em reconhecer o erro, e a incipiente jurisprudência estadual autorizam resposta mais enérgica. Valor de dez mil reais que se mostra mais condizente com o cenário narrado. RECURSO DA RÉ NÃO PROVIDO. RECURSO DA AUTORA PROVIDO. (TJSP; AC 1006311-89.2020.8.26.0001; Ac. 14982708; São Paulo; Trigésima Câmara de Direito Privado; Relª Desª Maria Lúcia Pizzotti; Julg. 01/09/2021; DJESP 10/09/2021; Pág. 2749)

O réu foi condenado a pagar indenização para a vítima pois repassou o número de celular dessa para colega de trabalho, o qual veio a praticar assédio sexual através de mensagens.

Em 20/10/2021, foi descoberto que a empresa Hariexpress, que atende empresas como a Amazon, Americanas, Mercado Livre, Magalu, Shopee, Correios, entre outra, por falha no sistema de segurança aplicado aos sites, vazou em torno de 1,75 bilhões de dados dos clientes cadastrados nestas plataformas. Como ainda não se trata de um processo propriamente dito, após as devidas investigações, a empresa poderá ser multada em valor exorbitante, parecido com o caso NetShoes.

O mesmo ocorreu recentemente no Banco do Estado de Sergipe, em que houve vazamento de dados de 395 mil chaves Pix.

Estes casos são apenas alguns exemplos práticos que ocorrem na sociedade. Mas pequenos casos de vazamentos também podem ocorrer internamente das mais diversas empresas.

O fato de um funcionário não autorizado possuir acesso a dados sensíveis já caracteriza falha no tratamento e conservação dos dados, podendo a empresa ser responsabilizada por isso.

No âmbito da Justiça do Trabalho, também se demonstra latente a proteção aos dados, que poderia ser dirimida por uma política de compliance efetiva, senão vejamos:

Liminar de procedência à quebra de sigilo da reclamante, determinando que a reclamada forneça os dados de geolocalização do aplicativo do Banco em que trabalhava, para comprovação de jornada de trabalho. Arts. 7º e 22 da Lei 12.965/2014; e arts. 7º, VII e 11, II, “d” da

LGPD. Processo nº 0020997-19.2020.5.04.0405.

Ação pleiteava reversão de justa causa por não ter cometido ato irregular, apesar de ter divulgado exame de paciente para familiares, sem autorização do hospital. Foi deferido o pedido, uma vez que os dados do pacientes foram revelador para familiares, e não a terceiros. E que apesar de não seguir o protocolo padrão do hospital, a informação possibilitou a proteção à saúde de familiares, amigos e profissionais agentes funerários. Processo nº 0000938-24.2020.5.12.0005.

Comercialização ilícita e maciça de dados pessoais sem autorização do Titular de Dados pessoais - gera violação à privacidade, intimidade e imagem das pessoas. (art. 7, I, §5º). Ordem de suspensão da comercialização de dados pessoais como produto. Ação Civil Pública. Agravo de Instrumento nº 0749765-29.2020.8.07.0000.

Com efeito, demonstram-se inquestionáveis os efeitos que a Lei Geral de Proteção de Dados e o compliance têm para a sociedade, demonstram-se como meios efetivos de superação dos desafios do atual cenário econômico global e necessários para o próprio desenvolvimento econômico de maneira socialmente responsável.

Conclusão

Considerando todo o abordado, é possível inferir que o processo de adequação à LGPD é de extrema importância e complexo, pois envolve uma análise jurídica dos tratamentos realizados por cada setor da empresa, bem como análises realizadas por profissionais de tecnologia da informática, podendo levar à necessidade de mudanças e/ou aquisição de sistemas.

As empresas precisam estar preparadas e precavidas contra ataques de hackers ou uso indevido de dados, pois o titular de dados que se sentir prejudicado pelo uso indevido poderá buscar a proteção de seus direitos junto ao Poder Judiciário.

O principal risco que as empresas passam a ter com a lei em vigor é a possibilidade de serem alvos de fiscalização pela Autoridade Nacional de Proteção de Dados - ANPD, na medida em que as sanções administrativas já poderão ser aplicadas. As penalidades vão de simples advertências a multas de até 2% do faturamento bruto anual da empresa, limitada a R\$50 milhões por infração, multas diárias, publicização da infração, bloqueio ou eliminação de dados pessoais, suspensão e até proibição parcial ou total das atividades das empresas.

A implantação de um programa de compliance trabalhista vem não somente mitigar falhas e litígios por desconhecimento da legislação, como se supunha, mas também evitar atitudes preconceituosas e discriminatórias que firam a dignidade humana, entre outros benefícios. Nas leituras se confirma que, desde a fase pré-contratual, o compliance possibilita um processo ético, com respeito e segurança aos candidatos.

Observou-se, primeiramente, que no próprio conceito de compliance está intrínseca a ideia de conformidade à legislação, normas e regulamentos, de modo que sua implantação deverá, necessariamente, através de mecanismos próprios, promover uma mudança na cultura organizacional.

O surgimento do compliance nos Estados Unidos, motivado pela globalização e questões do mercado financeiro, remete a pensar que no Brasil, um país que historicamente tem enfrentado dificuldades sociais, políticas e econômicas, tem se atualizado somente algumas décadas depois em relação ao compliance.

Atualmente, principalmente a partir da Lei n.º 12.846/2013 - Lei Anticorrupção, observou-se que são inúmeros os intentos em estabelecer práticas de conformidade legal nas empresas brasileiras com intuito de evitar fraudes. O Conselho Administrativo de Defesa Econômica - CADE, ao publicar em 2015 o Guia de Programas de Compliance, vem incentivar, conscientizar, bem como listar possíveis benefícios de seguir um programa de compliance. Destaca-se daí que, ao perceber a possibilidade de evitar prejuízos e de melhorar a imagem da empresa, a adesão se torna maior por parte das instituições. Essas condutas vêm, segundo os estudos realizados, não somente fortalecer o compliance no Brasil, mas ampliar o leque de possibilidades em diversos campos do Direito, incluindo também a área trabalhista.

Por não haver uma legislação específica para o compliance trabalhista, o mesmo se ampara em diversas leis, uma vez que a relação trabalhista é complexa e precisa atentar-se a diversos aspectos do trabalho e da pessoa do trabalhador, como é o caso da Lei Geral de Proteção de Dados mencionada nesse estudo. Por esse motivo, pode-se concluir que o compliance trabalhista se torna ainda mais relevante na seara do ordenamento jurídico, como mecanismo de adequação à legislação.

Aponta-se outra particularidade, uma vez que a aplicação do compliance trabalhista se dá não somente na vigência do contrato de trabalho, mas também antes da contratação de um colaborador e depois do desligamento do colaborador, abrandando os riscos de ações trabalhistas. Os processos de recrutamento e seleção precisam, necessariamente, estar alinhados à política da empresa e à regulação trabalhista em todos os âmbitos, evitando assim incorrer em atitudes preconceituosas e discriminatórias.

É importante ressaltar que no tocante ao processo de implantação do compliance trabalhista, para além de todos os instrumentos e ferramentas utilizados já mencionados nesse estudo, está a conscientização da alta cúpula da organização, que dará real sustentação ao compliance em todas as esferas da empresa. Dessa forma, percebeu-se que a cultura de integridade precisa ser internalizada por todos, para não prejudicar os demais processos ou até mesmo comprometer a aplicabilidade do compliance.

Ressalta-se também a dinamicidade do compliance trabalhista, uma vez que o mesmo exige a necessidade de mecanismos de acompanhamento de sua eficácia, de revisões constantes, de correções de rumo, de código de conduta, de auditoria, de treinamentos periódicos, de princípios e valores bem definidos.

Da mesma forma, pode-se dizer ainda que o compliance trabalhista é mais um processo na engrenagem do trabalho de uma empresa, e, ao mesmo tempo, perpassa todos os demais processos, num sistema dialógico de desenvolvimento.

Os riscos observados foram, principalmente, relacionados ao falso compliance ou compliance de fachada e aos excessos que possam engessar o processo e/ou impedir a atividade da empresa. Mas observou-se também que a ausência de programas de treinamento, de comunicação clara, de processo de conscientização eficaz podem resultar em falhas no programa. Ressalva-se que a não participação de todos, inclusive da alta gestão, também pode comprometer a aplicabilidade do compliance.

Em relação aos principais benefícios observados, as práticas de integridade do compliance amplificam e solidificam a imagem da empresa, tornando-a atrativa para novos colaboradores, clientes e fornecedores. Além do mais, fortalece a credibilidade e a rede de negócios da empresa. Pode-se citar ainda a satisfação e motivação gerada nos colaboradores pela segurança e confiabilidade da empresa à qual se dedicam. Percebeu-se assim que os benefícios vão além da prevenção de riscos e redução de custos com multas e/ou litígios.

O programa de compliance pode ser percebido como um vetor estratégico nas empresas brasileiras, dando-lhes não somente um caráter de coerência ética, mas também de sustentabilidade, de modo a estar em conformidade com a legislação, evitar prejuízos e abusos e preservar os direitos trabalhistas, bem como a dignidade humana.

Assim, demonstram-se inquestionáveis os efeitos que a Lei Geral de Proteção de Dados e o compliance têm para a sociedade, demonstram-se como meios efetivos de superação dos desafios do atual cenário econômico global, sendo necessários para o próprio desenvolvimento econômico de maneira socialmente responsável.

REFERÊNCIAS

ALMEIDA, Leonardo Goés de; GOMES, Andréa Salcedo Monteiro dos Santos. Direito ao esquecimento, LGPD e liberdade de expressão: como ponderá-los? Disponível em: <<https://www.conjur.com.br/2021-fev-28/opinioao-direito-esquecimento-lgpd-liberdade-expressao>>. Acesso em: 16 abr. 2021.

BERTOCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Castro et al. Manual de compliance. 2. ed. Rio de Janeiro: Forense, 2020.

BRASIL. Lei nº 13.467 de 13 de julho de 2017. Consolidação das Leis do Trabalho (CLT). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13467.htm>.

_____. Constituição da República Federativa do Brasil. Brasília: Senado, 1988.

_____. Lei de Acesso à Informação. Decreto Lei nº 12.527, de 18 de novembro de 2011. Brasília, 18 nov. 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>.

_____. Conversão da MP nº 869 de 2018. Decreto Lei nº 13.853, de 14 de agosto de 2018. Brasília, 19 dez. 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1>.

_____. Medida Provisória nº 954 de 2020. Brasília, 17 abr. 2020. Disponível

em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm>.

_____. Lei Geral de Proteção de Dados (LGPD). Decreto Lei nº 13.709 de 14 de agosto de 2018. Brasília, 14 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>.

_____. Lei nº 13.810, de 8 de março de 2019. Brasília, 8 mar. 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13810.htm>.

_____. Lei nº 9.613, de 3 de março de 1998. Brasília, 3 mar. 1998. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9613.htm>.

_____. Instrução Normativa DREI Nº 76, de 9 de março de 2020. Brasília, 10 mar. 2020. Disponível em: <<https://www.gov.br/economia/pt-br/assuntos/drei/legislacao/arquivos/legislacoes-federais/indrei76.pdf>>.

_____. Portaria nº 300, de 13 de junho de 2019. Brasília, 14 jun. 2019. Disponível em: <https://www.gov.br/esocial/pt-br/centrais-de-conteudo/legislacao/empresas/portaria-300_textoconsolidado.pdf>.

CADE - CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA. Guia programas de compliance: orientações sobre estruturação e benefícios da adoção dos programas de compliance concorrencial. 2016. Disponível em: <<https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/guias-do-cade/guia-compliance-versao-oficial.pdf>>.

CARLOTO, Selma. Compliance trabalhista. 2. ed. São Paulo: LTR, 2020.

COLARES, Wilde Cunha. Ética e compliance nas empresas de outsourcing. 2014. Monografia (LLM – Legal Law Master) - Programa de Pós-graduação em Direito - Insper - Instituto de Ensino e Pesquisa, São Paulo, 2014. Disponível em: <<http://dspace.insper.edu.br/xmlui/handle/11224/1238>>. Acesso em: 20 out. 2021.

CORREIA, Henrique. Compliance e sua aplicação no direito do trabalho. Revista Eletrônica do Tribunal Regional do Trabalho da 9ª Região, Curitiba, PR, v. 9, n. 91, p. 16-30, ago. 2020. Disponível em: <<https://hdl.handle.net/20.500.12178/151250>>. Acesso em: 20 out. 2021.

CUEVA, Ricardo Villas Bôas. Funções e Finalidades dos Programas de Compliance. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). Compliance: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018.

DUTRA, Lincoln Zub (org.) Compliance no ordenamento jurídico brasileiro. Curitiba: Juruá, 2018.

GNAP, Ana Paula: Os limites da publicidade no processo judicial e os direitos da personalidade face aos dados sensíveis. Aplicação subsidiária da Lei Geral de Proteção de Dados nº 13.709/2018. Percurso - Anais do IX do CONBRADEC, Curitiba, v. 1, n. 32, p. 283-287, 2020.

GUÉRIOS, Ana Carolina Ferreira Jacomel; VIEIRA, Guilherme Vidal. Lei Geral de Proteção de Dados: desafios e expectativas. Percurso - Anais do IX do CONBRADEC, Curitiba, v. 1, n. 32, p. 40-56, 2020.

KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. Dados Sensíveis na

Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade. 2020. Dissertação (mestrado em Direito). Faculdade de Direito da Universidade Federal de Juiz de Fora. Juiz de Fora, 2019. Disponível em: <<https://repositorio.ufjf.br/jspui/bitstream/ufjf/11438/1/maria-reginadetonicavalcantirigolonkorkmaz.pdf>>. Acesso em: 20 out. 2021.

KRUPPA, Roberta Potzik Soccio; GONÇALVES, Anselmo. Compliance trabalhista. Revista FAE de Direito, Curitiba, v. 2, n. 1, p. 123-145, jun. 2020. Disponível em: <<https://revistadedireito.fae.edu/direito/issue/view/7>>. Acesso em: 20 out. 2021.

LOURENÇO, Ana Lucia; TAQUES, João Daniel Vilas Boas. O papel das Ouvidorias Públicas na implementação da Lei Geral de Proteção de Dados (LGPD). Revista do MPC/PR, Curitiba, v. 7, n. 13, p.12-28, nov. 2020/maio 2021.

MARTINS, Juliane Caravieri; MONTAL, Zélia Maria Cardoso. Compliance trabalhista e o direito à educação para o trabalho: desafios em face da responsabilidade social da empresa. Revista Eletrônica do Tribunal Regional do Trabalho da 9ª Região, Curitiba, PR, v. 9, n. 91, p. 38-55, ago. 2020. Disponível em: <<https://hdl.handle.net/20.500.12178/154352>>.

MARTINS, Sérgio Pinto. Compliance no direito trabalhista. In: _____. (org.). Compliance no direito. São Paulo: Revista dos Tribunais, 2020, v. 6, p. 24-29.

PINHEIRO, Patricia Peck. Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018-LGPD. Saraiva Educação SA, 2020.

PRADO, Fabiany Estavas; LIPPMANN, Rafael Knorr; TORRES, Rafael Lima. Lei Geral de Proteção de Dados: origens, vigência e principais aspectos. Revista Direito UTP, Curitiba, v. 1, n. 1, p. 141-156, jul./ dez. 2020.

SANTOS, Alexandre da Silva. A importância da atuação da auditoria interna na implementação da Lei Geral de Proteção de Dados nas empresas públicas. São Paulo, 2019. Digitado. Projeto de Mestrado Profissional em Gestão e Políticas Públicas - MPGPP da Escola de Administração de Empresas de São Paulo, Fundação Getúlio Vargas. Orientação: Marco Antonio Carvalho Teixeira. Não publicado.

SEIN, José Luis Goñi. Programas de cumplimiento empresarial (compliance programs): aspectos laborales. In: PUIG, Santiago Mir et al. Responsabilidad de la empresa y compliance: programas de prevención, detección y reacción penal. Madrid: Edisofers, 2014.

SILVA, Fabrício Lima; PINHEIRO, Iuri; BOMFIM, Vólia. Manual do compliance trabalhista: teoria e prática. 2. ed. Salvador: JusPodivm, 2021.

SWISTALSKI, Andressa; LOBATO, Carla Cristina Cavalheiro. Compliance no setor financeiro e mercado de capitais. In: CARVALHO, André Castro et al. Manual de compliance. 2. ed. Rio de Janeiro: Forense, 2020.

VILELA, Camila Maria de Moura; LEMOS, Christine Mattos Albiani. A responsabilização decorrente do tratamento de dados pessoais e o sistema sancionatório da lei geral de proteção de dados pessoais (“LGPD”). Revista Ilustração, v. 1, n. 2, p. 57-67, 2020.

28. NEGOCIAÇÃO COLETIVA E LGPD

LUCIANE CARDOSO BARZOTTO¹

1. Introdução

A Reforma Trabalhista trouxe novos contornos para a negociação coletiva, agora regulada quanto ao conteúdo no art. 611 da CLT. O art. 611-A estabelece hipóteses nas quais a convenção coletiva e o acordo coletivo de trabalho têm prevalência sobre a lei. Já o art. 611-B aduz os temas que não deverão ser tratados em convenção coletiva do trabalho ou acordo coletivo de trabalho. Estes dispositivos devem ser lidos à luz da Constituição Federal em seu artigo 7º (inciso XXVI), no qual se estabelece o reconhecimento das convenções e acordos coletivos de trabalho. Além disto, as Convenções de n.º 98 e de n.º 154 da OIT, ratificadas pelo Brasil, destacam a necessidade de os países fomentarem e valorizarem as negociações coletivas como meio eficaz para estabelecer melhores condições do trabalho.

Portanto, o que se perquire neste artigo é se a privacidade dos empregados, agora regulada pela Lei nº 13.709/2018 (BRASIL, 2020c), também conhecida como Lei Geral de Proteção de Dados (LGPD), é passível de ter seu conteúdo esmiuçado e descrito em cláusulas de negociação coletiva entre empregados e empregadores e seus respectivos entes de representação coletiva.

A *priori*, pela interpretação dada ao art. 611 da CLT em conformidade com a Constituição Federal, responde-se positivamente para que negociações coletivas possam contemplar de modo explícito diversos direitos trazidos pela LGPD a todo o cidadão, incluindo-se o trabalhador, na proteção de sua autodeterminação informativa, visto que as negociações coletivas servem para atuar no vazio da lei, criando direitos e obrigações laborais.

Entretanto, discute-se se a negociação coletiva seria o meio adequado para regular direitos individuais de trabalhadores com relação a dados pessoais. Salienta-se que os direitos do titular dos dados expressam direitos fundamentais, consagrados na Constituição Federal, no art. 5º, inciso X da Carta Magna, adicionados a novos direitos. Tramita no Congresso projeto de lei - PEC 17/2019- tendente a dar ao direito à proteção de dados um caráter de direito fundamental autônomo, ou seja, categoria especial de direitos da personalidade.

Por enquanto, verifica-se em que medida alguns aspectos da proteção de dados já estão contemplados em cláusulas negociais coletivas. Como ilustra o teletrabalho, ou trabalho remoto da pandemia, encontram-se cláusulas sobre utilização de imagem, que é um dado sensível, à luz do art. 5º da LGPD. Além da regulamentação do uso da imagem (biometria) mediante fontes negociais, no Brasil e no exterior, perquire-se sobre novas possibilidades de negociação com relação à vacina contra a covid-19, cujos contornos envolvem outro dado sensível, a saúde do trabalhador.

Por fim, elencam-se possibilidades de estipulações por meio de fontes norma-

¹ Desembargadora federal do Trabalho do TRT4. Professora da UFRGS (graduação/mestrado/ doutorado).

tivas autônomas diversos temas trazidos pela Lei Geral de Proteção de Dados. As novidades da Lei n.º 13.709/2018 tendem a dar novos contornos à negociação coletiva a ponto de constituírem verdadeira oportunidade para os sindicatos demonstrarem sua efetividade na defesa dos direitos individuais e coletivos da categoria, numa adequação aos novos tempos de autodeterminação informativa na sociedade em que os dados possuem valor.

2. Negociação coletiva para proteção de direitos dos titulares de dados: o papel do sindicato

A entidade sindical terá papel central na efetividade da LGPD diante da necessidade de proteção de dados nas relações trabalhistas? Recordar-se que a Lei n.º 13.709/2018 (BRASIL, 2020c) é aberta, geral, transversal, com flexibilidade de interpretação, válida para qualquer organização, autorizando regulamentações supletivas dos sindicatos, porquanto traz uma ideia unificada do tratamento dos dados. Diante das inúmeras situações envolvendo concretamente os dados pessoais dos trabalhadores no contexto laboral, a LGPD é um mandado de otimização legal, traçando metas para os empregadores se alinharem no tratamento dos dados gerados durante relação de trabalho.

Alguns entendem que cláusulas que disciplinam sobre proteção de dados não poderiam ser incluídas em negociação coletiva laboral por dizerem respeito a direitos individuais personalíssimos, para os quais o titular deve anuir (CORREIA e BOLDRIN, 2020), não sendo, em princípio, direitos de base coletiva.

Outros entendem que é possível a fixação por negociação coletiva de matéria que envolva proteção de dados (VÓLIA e IURI, 2020; PAMPLONA e CONI, 2020). Adota-se a segunda corrente por analogia ao GDPR, art. 88, o qual contempla matéria laboral, ou pela permissão do art. 8º da CLT. Entende-se, a partir da ideia de negociação coletiva, que os diversos direitos do titular, por possuírem matriz constitucional, não podem ser flexibilizados.

Nas questões sindicais, a primeira pontuação importante é a própria filiação sindical do empregado. Temos expressamente na lei que a filiação sindical é dado pessoal sensível, conforme o art. 5º. A filiação a sindicato deve ser informação fornecida para o empregador desde que a contribuição sindical passou a ser facultativa (art. 545 da CLT). Como o pagamento da contribuição é devido apenas pelos associados, o empregador deve saber a filiação, dispensando-se o consentimento do empregado visto que é exigência legal para o empregador o desconto da contribuição. No curso da relação de emprego e para a finalidade de recolhimento sindical questiona-se se a filiação seria viável, mas não se pode utilizar a ideia do legítimo interesse do controlador (art. 10 da LGPD), a qual não está elencada entre as bases de tratamento dos dados pessoais sensíveis, constantes no art. 11 da LGPD, que abaixo se transcreve:

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for

indispensável para:

- a) cumprimento de obrigação legal ou regulatória pelo controlador;
- b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
- c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
- d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- e) proteção da vida ou da incolumidade física do titular ou de terceiro;
- f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Entende-se que, no caso de requerimento do empregador ao empregado sobre o fato de ser ou não o empregado sindicalizado, ou mesmo a obrigação do sindicato fornecer o rol dos associados às empresas, com dever fixado em eventual cláusula decorrente de negociação coletiva, estaria embasado na forma de tratamento que é o cumprimento de obrigação legal ou regulatória do controlador, por exemplo (art. 11, inciso II, a).

Em um primeiro momento, pode-se dizer, em tese, que as entidades sindicais terão amplas possibilidades de regulamentar direitos inerentes à lei, conforme o melhor interesse de seus representados.

O titular de dados é detentor de diversos direitos em relação aos seus dados, a iniciar pela liberdade, privacidade e livre desenvolvimento da sua personalidade (art. 1º), além dos elencados no art. 18, direitos estes que poderiam ser explicitados por normas coletivas, a fim de que correspondam à principiologia legal do art. 6º da LGPD e respondam ao titular algumas perguntas: para que fim são guardados os dados, em que contexto etc.

Nestes termos, cumpre referir que os direitos do titular dos dados correspondem aos princípios fixados na lei, como didaticamente indica-se:

princípios	perguntas sobre dados	direitos do titular
I- finalidade	PARA QUE FIM	INFORMAÇÃO- ART 9º
II- adequação	EM QUE CONTEXTO	PORTABILIDADE- ART 18, V
III- necessidade	POR QUE É PRECISO	NEGATIVA- art. 18, VII
IV - livre acesso	ONDE	ACESSO - art. 9º
V - qualidade dos dados	COMO	CORREÇÃO - Art. 7, § 6º
VI - transparência	QUAL MODO	CONFIRMAÇÃO- ART 8º, 3º
VII - segurança	COM QUE MEDIDAS	ELIMINAÇÃO - Art. 16.
VIII - prevenção	EM VISTA DE QUE	ANONIMIZAÇÃO - Art. 11, II, c
IX - não-discriminação	PARA QUE NÃO	REVISÃO - Art. 20.
X -responsabilização e prestação	QUEM RESPONDE	REVOGAÇÃO Art. 8, § 5º

Todos estes aspectos acima elencados, de direitos de titulares de dados, com suas perguntas sobre o tratamento dos dados (art. 5º, X, e art. 7º da LGPD) e a designação do princípio a orientar o tratamento podem receber uma resposta coletiva, enquanto trabalhadores sindicalizados. Este feixe de direitos enseja proteção pela via de negociação sindical porquanto dizem respeito ao tratamento de dados constantes em documentos individuais mas que são tratados homogeneamente, ou seja, de modo coletivo e, diga-se, sem discriminação pelos empregadores. Documentos como fichas de registro de empregados, termos aditivos para adequação dos contratos de trabalho, necessidade de realização de exames de saúde periódicos, bem como a forma de armazenamento de diversos outros dados laborais, com expressa determinação de como se dará o tratamento pelo controlador de outras informações relevantes são aspectos os quais permitem tratamento coletivo. Estes itens são apenas uma síntese do que ao sindicato se faculta negociar sobre a política de tratamento e acesso de dados dos trabalhadores, a partir dos direitos elencados no art. 18 da LGPD.

Aqui o sindicato poderá indicar ao titular do dado (empregado) e ao controlador (empregador) de que modo os direitos podem ser exercidos concretamente, em conformidade aos princípios, constantes no art. 6º da LGPD, sob a égide do macro vetor da boa fé, baliza orientadora do sistema (MENKE, 2021).

Aos sindicatos é autorizada a atuação de modo a dar efetividade aos diversos fundamentos, aparentemente colidentes e indicados no art. 2º da lei, a saber:

- I - o respeito à privacidade;
- II - a autodeterminação informativa;
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV - a inviolabilidade da intimidade, da honra e da imagem;
- V - o desenvolvimento econômico e tecnológico e a inovação;
- VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Por outro lado, o sindicato, além de garantidor dos fundamentos do sistema de proteção, também é agente ao desempenhar a função de controlador dos dados, no contexto de sua atuação. É imperioso ao sindicato adequar-se à LGPD, uma vez que trata dados dos sindicalizados. Anteriormente à LGPD já se discutiu no âmbito judicial a responsabilização do sindicato por repasse indevido de dados de representados (compartilhamento de dados), o que poderá ser doravante ajustado também em negociações coletivas. Neste sentido a jurisprudência abaixo transcrita, anterior à vigência da Lei Geral de Proteção de Dados:

AGRAVO DE INSTRUMENTO EM RECURSO DE REVISTA. PROCEDIMENTO SUMARÍSSIMO. INDENIZAÇÃO POR DANO MORAL. NÃO CONFIGURAÇÃO. EMPREGADO NÃO SINDICALIZADO QUE TEVE DESCONTADA NO CONTRACHEQUE A CONTRIBUIÇÃO ASSISTENCIAL/CONFEDERATIVA. O Regional, instância soberana na análise de matéria fática, a teor da Súmula 126 do TST, concluiu que não houve dano moral, fundamentando que o acesso aos dados do reclamante não foi feito pessoalmente pelo Sindicato recorrido, e sim pelo Estado do Piauí, a quem o autor se encontra vinculado estatu-

tariamente, e, justamente por isso, possui suas informações pessoais e financeiras. Asseverou também que, embora o Sindicato, ao receber do Estado do Piauí valores descontados de seu contracheque, tenha conhecido seus dados funcionais, não se infere daí a existência de danos morais, pois não há informação de que houve divulgação desses dados sem permissão do autor. Em tal contexto, não há falar em violação dos arts. 5º, X, e 8º, V, da CF. Agravo de instrumento conhecido e não provido. (AIRR-1739-76.2011.5.22.0004, 8ª Turma, Relatora Ministra Dora Maria da Costa, DEJT 12/04/2013).

No caso acima, o sindicato não restou responsabilizado por repassar indevidamente dados de empregado não sindicalizado, eis que o ato de encaminhamento das informações foi do próprio estado do Piauí, no caso, empregador público. No entanto, com a entrada em vigor da LGPD, o sindicato enquanto guardião de direitos deve atuar de forma cada vez mais responsável no tocante à proteção de dados para não expor indevidamente os representados/associados em caso de eventual compartilhamento fora da base legal e das finalidades estritamente necessárias ao desempenho de sua missão.

Neste sentido, na jurisprudência espanhola (ASENCIO, 2013), encontrou-se uma relação difícil entre direitos de informação dos representantes dos trabalhadores e proteção de dados pessoais porque deveriam equilibrar-se direitos coletivos com o direito individual de privacidade ou mesmo intimidade. Vislumbra-se até eventual colisão entre direitos constitucionalmente protegidos: direitos coletivos e direitos individuais. Embora alguma jurisprudência tenha tentado subdividir dados pessoais em profissionais, econômicos e sociais, o Tribunal constitucional espanhol manteve o conceito unitário e amplo de dado pessoal, mantendo a possibilidade de oposição individual do trabalhador, embora tendendo a entender que a informação repassada ao sindicato deva ser suficiente para garantir a efetividade das funções de representação dos trabalhadores. A concorrência de direitos em sede coletiva faz com que o dado transmitido aos representantes dos trabalhadores, por força de dispositivos legais, tenha nos sindicatos um papel de garantidores e novos “responsáveis” pelos dados dos trabalhadores enquanto exercem o direito de representação. Estas questões são complexas e não estão resolvidas, embora tenham surgido diretrizes na Agência Espanhola de proteção de dados².

Em Portugal, a partir da Lei n.º 58/2019, de 8 de agosto, que é a Lei de Execução do Regulamento (UE) 2016/679, entende-se que as negociações vão aumentar.

Colacionam-se acordos coletivos que exemplificam a negociação sindical em busca de dados para exercício das próprias funções e em defesa dos representados. Conforme boletim de trabalho e emprego de Portugal de janeiro de 2021, aparecem algumas cláusulas de negociação coletiva sobre dados:

1. Acordo de empresa entre a Exide Technologie, Lda e o Sindicato das Indústrias Eléctricas do Sul e Ilhas - SIESI, a Cláusula 11.ª, que trata sobre o Relatório único (p.47), dispõe que a empresa obriga-se a enviar o conteúdo

2 Guía de “la protección de datos en las relaciones laborales” de la propia Agencia Española de Protección de Datos. Disponível em: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_RelacionesLaborales.pdf.

do relatório anual referente à informação sobre a sua actividade social (Relatório Único) à comissão de trabalhadores e aos sindicatos representativos de trabalhadores da empresa que o solicitem, nos termos da lei vigente e tendo em conta a Lei de Proteção de Dados. Na mesma página, consta na Cláusula 12.^a, que são deveres da empresa: i) Prestar aos sindicatos os esclarecimentos que por estes lhe sejam solicitados, relativos às relações de trabalho, nos termos do Código do Trabalho e da Lei da Proteção de Dados”, e “q) Ouvir os órgãos representativos dos trabalhadores sempre que tal se justifique, nos termos do Código do Trabalho e Lei da Proteção de Dados.

2. Acordo de empresa entre a AGERE – Empresa de Águas, Efluentes e Resíduos de Braga, EM e o Sindicato dos Trabalhadores da Administração Pública e de Entidades com Fins Públicos - SINTAP e outro, a cláusula 5.^a é sobre proteção de dados pessoais (p.74), com início de vigência em 01/07/2020:

1. A empresa não pode exigir ao candidato a emprego ou ao trabalhador que preste informações respeitantes à sua vida privada, salvo quando estas sejam estritamente necessárias e relevantes para avaliar a respetiva aptidão no que respeita à execução do contrato de trabalho e seja fornecida por escrito a respetiva fundamentação.

2. A empresa não pode exigir ao candidato a emprego ou ao trabalhador que preste informações respeitantes à sua saúde ou estado de gravidez, salvo quando particulares exigências inerentes à atividade profissional o justifiquem e seja fornecida por escrito a respetiva fundamentação.

3. As informações relativas à saúde ou ao estado de gravidez previstas no número anterior são prestadas a médico que só pode comunicar à empresa se o candidato a emprego ou o trabalhador está ou não apto a desempenhar a atividade.

A cláusula 9.^a trata sobre utilização de dados biométricos:

A empresa só pode proceder ao tratamento de dados biométricos se os dados a utilizar forem necessários, adequados e proporcionais aos objetivos a atingir e observando a regulamentação em cada momento em vigor no âmbito da proteção de dados pessoais e demais regulamentação aplicável.

3. Acordo de empresa entre a BRAVAL – Valorização e Tratamento de Resíduos Sólidos, SA e o Sindicato dos Trabalhadores da Administração Pública e de Entidades com Fins Públicos - SINTAP e outro, encontra-se com a mesma redação da cláusula 5.^a sobre proteção de dados, conforme acima transcrita.

Todos estes exemplos, acima transcritos, revelam que a mesma complexidade negocial quanto a dados deverá ser enfrentada pelos sindicatos brasileiros ao se adaptarem à LGPD.

O certo é que em âmbito europeu o acordo coletivo também tem um lugar importante na definição deste direito à privacidade e proteção de dados. O art. 88 do RGPD incorpora um regulamento específico em matéria laboral ao estabelecer que “os Estados membros podem, por meio de disposições legislativas ou acordos coletivos, estabelecer regras mais específicas para garantir a proteção de direitos e liberdades em relação ao tratamento de dados pessoais dos trabalhadores no local de trabalho (...)”. O Considerando (155) do RGPD recorda o “Direito dos Estados membros editarem os acordos coletivos, incluindo “acordos de empresa”, podem estabelecer regras específicas relativas ao tratamento de dados pessoais de trabalhadores no campo do trabalho, em particular em relação às condições em que os dados pessoais neste contexto podem estar sujeitos a tratamento com base no consentimento do trabalhador para fins de contratação, a execução do contrato de trabalho, incluindo o cumprimento das obrigações estabelecidas por lei ou por acordo coletivo, a gestão, planejamento e organização do trabalho, igualdade e segurança no trabalho, saúde e segurança no trabalho, bem como as finalidades de exercício e gozo, individual ou coletivo, de direitos e benefícios relacionados ao emprego e para efeitos de cessação da relação laboral”. A limitação na autonomia da vontade nas relações privadas, por conta da subordinação da relação de emprego, autoriza que outras instituições possam velar pela proteção de dados e, neste sentido, no art. 80 do GDPR há expressa autorização de que o sindicato seja autorizado a representar o titular de dados diante do empregado, perante a Agência Nacional de Proteção de Dados, ou mesmo em juízo (UGUINA, 2018).

A doutrina laboral defende o que poderia ser chamado de governança coletiva de proteção de dados, a partir dos sindicatos, os quais poderiam fiscalizar processos de seleção, avaliações e despedidas e a gestão dos dados nestes momentos contratuais (SIGNES, 2018). Isto acompanharia o tratamento e processos de coleta automatizados de dados, bem como uma espécie de vigilância para evitar discriminações algorítmicas e arbitrariedades no mundo do trabalho, atividades que demandariam a presença da atuação sindical.

A crítica que se faz é: há um caráter individualista da proteção de dados presente no âmbito europeu, sendo que o GDPR, por sua vez, influenciou a norma brasileira.

Cumprir lembrar que a LGPD alude explicitamente à tutela coletiva de dados pessoais (arts. 22 e 42, *caput* e § 3º), incidindo no caso de judicialização, a legislação específica: Lei n.º 7.347/1985 e os arts. 81 a 104 do CDC, a Lei n.º 4.717/1965, sobre a ação popular, e os arts. 21 e 22 da Lei n.º 12.016/2009, sobre o mandado de segurança coletivo. O sindicato é considerado associação civil para fins de legitimidade ativa para propositura de Ação Civil Pública, conforme pacífica jurisprudência do STF e consoante o art. 5º da Lei n.º 7.347/1985. Ou seja, tanto na negociação autônoma, quando o sindicato produz fonte de Direito do Trabalho, como na ação judicial para assegurar os direitos de proteção de dados, temos uma autorização legal para a atuação sindical em questão de proteção de dados, espe-

cialmente no interesse da categoria, em situações de evidentes violações a direitos individuais homogêneos, como seria o resguardo de dados de uma determinada coletividade laboral de eventual incidente de segurança ou violação do tratamento legal em desconformidade com a finalidade declarada pelo controlador. Por estes motivos, entendemos viável e legal a existência de cláusula convencional prevendo a autorização de envio de dados dos trabalhadores aos sindicatos, pela categoria econômica, cuja autorização foi feita em assembleia geral e em conformidade com a vontade dos associados.

3. Negociação coletiva: uso de imagem em teletrabalho

Neste momento, examinam-se cláusulas negociais específicas sobre dados de empregados. Em rápida busca no sistema MEDIADOR³ da Secretaria do Trabalho sobre negociações sindicais, é possível que se encontrem acordos e convenções coletivas as quais trazem regras atinentes ao uso da imagem do empregado, como se transcreve abaixo, num contexto de teletrabalho ou trabalho remoto em época de pandemia, com vigência ainda atual:

e) Fica ajustado que a visualização das imagens capturadas em eventual chamada por vídeo com o empregado equivalem a uma reunião pública, ocorrida no interior da empresa, podendo ser gravada e utilizada para fins lícitos de exercício do poder empregatício, sendo dever do empregado livrar o ambiente filmado de acontecimentos íntimos e de sua vida privada.

f) A aceitação de chamadas por vídeo dependerá de ato próprio do empregado, ficando proibida a ativação remota da câmera pelo empregador para qualquer finalidade⁴.

Observa-se *a priori* que a cláusula negocial não refere expressamente o consentimento do empregado, mas ainda que referisse não poderia o sindicato autorizar nada em nome do empregado em face do direito personalíssimo que está envolvido na imagem das reuniões.

O que se percebe, na prática, é uma limitação na esfera de direção patronal quanto à “ativação remota da câmera pelo empregador para qualquer finalidade”. No entanto, a cláusula representa mais uma garantia para a empresa para o exercício do poder diretivo patronal do que uma salvaguarda para o direito dos empregados, até porque atribui ao empregado o resguardo de acontecimentos íntimos da sua vida privada, no âmbito de sua residência.

No entanto, o caso ilustra o uso da imagem dos trabalhadores que, embora já protegido constitucionalmente (art. 5º, inciso X), ganha mais uma camada de proteção pela LGPD, ao ser considerado dado biométrico e, portanto, dado sensível.

Os dados biométricos podem ser definidos como “aqueles relacionados às características físicas, fisiológicas e comportamentais de uma pessoa natural que

3 Disponível em: <http://www3.mte.gov.br/sistemas/mediador/>

4 SINDICATO DOS EMPREGADOS EM ADMINISTRADORAS DE CONSORCIOS E EMPREGADOS EM CONCESSIONARIAS E DIST. DE VEIC. DO ESTADO DE PERNAMBUCO - SINDCON-PE. Disponível em: <https://sindconpe.com.br/uploads/clauses/mcDWnzO3PqqTjWUwFMkYcg8i4hPejaB6KCowm0B2.pdf>. E SIND DOS TRAB EM TRANSP ROD CARGA DO RECIFE E DA REGIAO METROP E M SUL E NORTE DE PE. Disponível em: <https://www.setcepe.com.br/noticias/TermoAditivodeConvenoColetivaHOMOLOGADOMTE.pdf>

permitem ou confirmam de maneira inequívoca a sua identidade, tais como imagens faciais ou impressões digitais” conforme definição da autoridade francesa de proteção de dados⁵. Aqui se verifica que a classificação de dados biométricos relacionados à imagem, como dados sensíveis, deveriam ter uma proteção especial, à luz do art. 5º da LGPD, abaixo transcrito:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

O conceito de dados sensíveis foi formulado de modo pragmático (DONEDA, 2020, p.143) porque algumas informações apresentariam um elevado potencial ofensivo dos titulares, em determinada situação. Dados sensíveis para o regulamento europeu são uma categoria especial de dados relacionados a determinadas características identitárias da pessoa natural.

De fato, conforme Bioni, “os dados sensíveis são uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade: discriminação”. (BIONI, 2020, p.85). Ou seja, a utilização incorreta ou abusiva destes dados sensíveis pode levar a violações de direitos fundamentais específicos, como por exemplo a exclusão injusta do direito fundamental ao trabalho, por meio de criação de perfis que identificam negativamente determinado trabalhador.

A discriminação por uso de dados sensíveis (MENDES, et alii, 2021) segundo a doutrina ocorre: a) por ilicitude, quando a lei determina a proteção de dados sensíveis e eles são tratados de forma a discriminar grupos vulneráveis ou determinada pessoa, em afronta à lei⁶; b) quando o uso de dados gera abusividade por conta de correlação estatística feita por algoritmos enviesados, o que traz grande prejuízo para o titular de dados, em razão da total aleatoriedade ou mesmo ausência completa de causalidade; c) discriminação por generalização injusta quando há a utilização de um dado relativo ao exercício de um direito para um fim discriminatório. Aqui vale lembrar que a máxima para interpretar a correta utilização de dados sensíveis está presente no art. 21 da LGPD, que refere: os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Os dados biométricos, para serem tratados, em princípio dependeriam de consentimento do titular ou responsável legal, isso de forma destacada, específica e para finalidades específicas, conforme define o art. 11 da LGPD. O consentimento, no entanto, para a relação de emprego, diante da assimetria de poder entre empregado e empregador, pela presença da subordinação, não seria a melhor base de tratamento, a partir de orientações e trabalhos do GDPR- grupo 29 e diversos

⁵ Disponível em: <https://www.cnil.fr/fr/le-controle-dacces-biometrique-sur-les-lieux-de-travail>

⁶ Aqui a discriminação é o mesmo conceito utilizado em seara laboral. Para a Convenção 111 da OIT, em seu art. 1º.1, “a”, o termo “discriminação” compreende toda distinção, exclusão ou preferência fundada na raça, cor, sexo, religião, opinião política, ascendência nacional ou origem social, que tenha por efeito destruir ou alterar a igualdade de oportunidade ou de tratamento em matéria de emprego ou profissão.

autores, restando, portanto, outras opções de tratamento, como cumprimento de obrigação legal ou exercício regular de direitos, bases contempladas no art. 11 da LGPD. O legítimo interesse, outra base de tratamento, prevista no art. 7º e art. 10, também não consta como base prevista para o tratamento de dados sensíveis.

Portanto, a gravação da imagem em reuniões como a identificada nas negociações mencionadas acima pode ser apenas um exemplo de definição de procedimentos biométricos pela via negocial. Deste exemplo podemos extrair várias constatações. Primeiro: que os dados dos trabalhadores já estão sendo objeto de negociação coletiva e está sendo informada a finalidade, ainda que possa ser questionada. Segundo, a LGPD veio para garantir direitos aos titulares de dados, e eventual política dos empregadores ajustadas em negociações coletivas não podem se sobrepor à vontade individual do titular do dado porque excedem à autonomia privada coletiva. De nenhuma maneira, portanto, o sindicato poderia consentir pelo titular. Terceiro, como se viu a partir do direito à imagem e das cláusulas acima ajustadas, outras tantas questões poderiam ser regulamentadas via negociação coletiva, tais como: permissão para aposição de câmeras de monitoramento, afixação de sistemas de Inteligência Artificial que coletam dados dos computadores de empregados, questões de reconhecimento facial, controles de acesso, geolocalizadores, uso de leitores de impressão digital etc.

Interessante é que estes temas começam a aparecer em diversas negociações coletivas a partir do exemplo acima, da regulação do uso da imagem, especialmente no direito europeu visto que estão mais adiantados no tema.

Encerra-se, pois, este capítulo com duas cláusulas recentes de acordos coletivos de trabalho em vigor, as quais expressamente invocam a LGPD, mostrando-se o já início de inclusão de temas de forma explícita.

Neste caso, abaixo, se negam direitos laborais via LGPD (o não fornecimento de cópia de motivo de rescisão), segundo exegese protetiva tanto da LGPD como da CLT:

SETOR: indústria ATIVIDADE: construção e mobiliário PARTES: SIND DOS TRAB NAS IND DA CONSTR E MOB DE S CRUZ DO SUL (95.439.774/0001-20);XALINGO SA INDUSTRIA E COMERCIO (95.425.534/0001-76) INSTRUMENTO COLETIVO: MR063015/2020 TIPO: ACT REGIÃO: S UF: RS ENDEREÇO: <http://www3.mte.gov.br/sistemas/mediador/Resumo/ResumoVisualizar?nrSolicitacao=MR063015/2020> CLÁUSULA DÉCIMA OITAVA - DEMISSÃO POR JUSTA CAUSA A empresa que demitir o empregado sob alegação de justa causa fica obrigada a fornecer ao mesmo, comunicação por escrito onde conste resumidamente a falta cometida, cujo documento deverá estar assinado por ambas as partes, funcionário e empresa. Parágrafo Primeiro - Em havendo a negativa da assinatura do respectivo documento, por qualquer razão, a empresa providenciará a assinatura do documento por duas testemunhas, porém, devido à legislação vigente (LGPD-LEI 13.709/2018) não será fornecida cópia assinada do respectivo documento, cujo arquivamento e tratamento dos dados ali constantes ficarão a cargo do departamento de Recursos Humanos da empresa.

No caso acima a cláusula nega dado ao empregado, o que significa que esta

renúncia de antemão, por cláusula negocial, significa mitigação de direitos e tem validade absolutamente questionável.

Já abaixo se explicitam aspectos da LGPD, via negociação coletiva, entendendo-se viável a validade da cláusula coletiva:

SETOR: serviços ATIVIDADE: turismo e hospitalidade PARTES: SINDICATO DOS EMPREGADOS NO COMERCIO HOTELEIRO E SIMILARES DE CANELA (90.615.378/0001-92);M A DELAROSA SCHROEDER PADARIA (31.366.717/0001-85) INSTRUMENTO COLETIVO: MR065672/2020 TIPO: ACT REGIÃO: S UF: RS ENDEREÇO: <http://www3.mte.gov.br/sistemas/mediador/Resumo/ResumoVisualizar?nrSolicitacao=MR065672/2020> CLÁUSULA OITAVA - CÂMERAS DE SEGURANÇA, AUTORIZAÇÃO DE IMAGEM E INFORMAÇÕES PESSOAIS Declaram os EMPREGADOS ter ciência que nas áreas comuns do estabelecimento comercial da empresa ora acordante, existem câmeras de segurança com sistema de vídeo e áudio por questões de segurança dos próprios empregados, colaboradores e clientes, razão pela qual concordam que as filmagens sejam armazenadas e utilizadas para eventuais expedientes administrativos e policiais. II. Fica desde já acordado entre as partes, que os empregados poderão estar sujeitos a ter as suas imagens divulgadas em publicidade, que envolva o seu setor de trabalho, sem que de tal decorram quanto aos adicionais remuneratórios em decorrência de sua participação, sendo que a reprodução da imagem fica expressamente autorizada pelos empregados, para fins de divulgação comercial do estabelecimento comercial da empresa. a) Declaram os empregados ter ciência que todas as informações fornecidas e coletadas na hora da contratação serão usadas unicamente para registro no programa da folha de pagamento e para atender a legislação e encaminhamento ao banco de dados do e-social. A empresa preserva todas as informações sigilosamente de acordo o que prevê a Lei 13.709 de 14/08/2018.

4. Negociação coletiva e a saúde dos trabalhadores: a vacinação e os dados

Outra frente importante sobre proteção da saúde dos trabalhadores pode ser uma atribuição sindical negocial especialmente no que tange à saúde e à proteção de dados de saúde em período de pandemia.

As ações Diretas de Inconstitucionalidade (ADIs) 6586 e 6587, que tratam unicamente de vacinação contra a covid-19, e do Recurso Extraordinário com Agravo (ARE) 1267879 foram julgadas pelo Plenário do Supremo Tribunal Federal (STF) em 17/12/2020. Na decisão, entendeu-se que o Estado pode determinar aos cidadãos que se submetam, compulsoriamente, à vacinação contra a covid-19, prevista na Lei 13.979/2020.

Aqui reflita-se sobre a obrigatoriedade de vacinação de profissionais da saúde a ser fixada por normas coletivas. Antes, um parêntesis. Na Itália, legislação de 31/03/2021, Decreto 44, autoriza que empregados da saúde que não quiserem se vacinar possam ser deslocados para outros trabalhos ou setores que não exijam contato com público. Este é um exemplo de exercício do poder patronal de gestão da crise sanitária, sendo que a lei em comento autoriza medidas de salários sus-

pensos⁷, tudo como forma de contenção da pandemia. No Brasil, a Lei n.º 14.128, de 26 de março de 2021, dispõe sobre compensação financeira a ser paga pela União aos profissionais e trabalhadores de saúde que ficaram incapacitados por contato com covid. Por certo, os empregadores é que deverão repassar estes dados ao órgão previdenciário por obrigação legal, dados que serão compartilhados, sendo urgente regulação do trânsito dos mesmos. Por outro lado, questiona-se sobre a possibilidade, no Brasil, de solicitação de registros de vacinação no âmbito da relação de emprego. Estes dados, pela LGPD, correspondem a um tipo específico de dado sensível, dados relacionados à saúde (art. 5º), e perquire-se se seu tratamento poderia ser regrado por normas coletivas. Entende-se possível o traçado coletivo de condutas gerais para empregados na saúde, por exemplo. Neste caso, é possível regrar tanto o comportamento (a vacinação) e como manter o dado resultante do comportamento exigido em âmbito da saúde: como armazenar os dados sobre os vacinados.

É viável que a negociação coletiva estabeleça, inclusive, qual seria a base legal do tratamento, se seria o art. 11, inciso II, letra “e”, o qual define o tratamento de dado até mesmo sem o consentimento do titular para fins de proteção da vida ou incolumidade física do titular ou de terceiro (no caso a proteção da vida da comunidade laboral que trabalha em determinado lugar), ou outra base legal, como por exemplo o cumprimento de obrigação legal, exercício regular de direito etc. Mas tudo isso deve ser estudado e visto com muita parcimônia, diante das peculiaridades dos dados relacionados à saúde e aos direitos fundamentais envolvidos na situação.

Convém lembrar que entre as decisões do TST encontra-se um acórdão mantendo a validade da negociação coletiva que preconizava que o empregador, hospital, fornecesse a vacina aos empregados de modo gratuito. Veja-se na SDC - Acórdão do processo nº RO - 441100-53.2008.5.04.0000, em 13 de dezembro de 2010, no qual o recurso ordinário não provido da Federação dos Hospitais do Rio Grande do Sul, obteve a seguinte decisão:

VACINAS. Mantém-se cláusula que determina o fornecimento de vacinas contra a hepatite aos farmacêuticos, empregados em hospitais e estabelecimentos de serviços de saúde, categoria profissional abrangida neste dissídio coletivo, tendo em vista a natureza da atividade desempenhada, que os expõe a maior risco de contágio de doenças, como a hepatite B.

Ou seja, a negociação coletiva pode administrar este grave problema de saúde pública relacionado à covid-19 e às vacinas, visto que a saúde está expressamente vinculada ao dado sensível contido no art. 5, inciso II, da LGPD. No caso, as negociações podem superar a questão de quem fornece e financia a vacina, e avançar pela Lei Geral de Proteção de Dados no sentido de como serão exigidas condutas e administrados os dados relacionados ao procedimento da vacinação e, mesmo, de que modo deverão ser tratados estes dados e com quais finalidades.

5. Negociação coletiva para assegurar outros direitos constantes da LGPD

Apontamos, por fim, um amplo espectro de ação sindical em negociação cole-

⁷ Disponível em: <https://epocanegocios.globo.com/Mundo/noticia/2021/03/italia-estuda-obrigatoriedade-de-vacina-para-profissionais-de-saude.html>

tiva a partir da LGPD, sendo que negociações poderiam conter os seguintes conteúdos e ações sindicais, segundo artigos da Lei 13.709/18:

a) explicitar cláusulas de transferência internacional de dados (art. 33 LGPD) para hipóteses de operações internacionais envolvendo dados de empregados de determinada categoria, embora para os padrões gerais deva-se aguardar a ANPD;

b) definir as boas práticas de governança de dados – tendente a criar códigos de ética e implementar selos de qualidade e estabelecer padrões de diálogo e informação aos trabalhadores, segundo o art. 50 da LGPD;

c) exercer o Habeas Data coletivo em favor de empregados associados, conforme artigo 5º, XXXIV, da Constituição Federal de 1988 combinado com o art. 114, inciso IV da Constituição Federal;

d) prever execução de ações para reparação de danos coletivos conforme art. 42, parágrafo 3º da LGPD, combinado com o art. 114, inciso VI, da CF/88 (ações de indenização por dano moral ou patrimonial, decorrentes da relação de trabalho);

e) fixar multas por descumprimento de normas de proteção à privacidade e intimidade dos empregados;

f) questionar decisões automatizadas que gerem discriminação para grupos de trabalhadores em processos de digitalização do trabalho, conforme art. 20 e 22 da LGPD;

g) definir regras sobre compartilhamento de dados entre empresas tomadoras e prestadoras em caso terceirização, bem como em caso grupo econômico, dando aos envolvidos transparência de informação;

h) conforme o artigo 46 da Lei nº 13.709/2018, definir responsabilidades específicas e setoriais pela implementação de medidas de segurança de dados por partes dos agentes;

i) explicitar responsabilidades constantes dos artigos 42 e 43 da LGPD, especialmente quando o operador designado pelo encarregado for empregado;

j) esclarecer os riscos e controles do empregados substituídos com relação ao *compliance* de dados e avaliação do impacto de dados;

k) atuar “*praeter legem*” no vazio legislativo (LGPD) e regulativo (ANPD);

l) atuar preventivamente na questão cultural, educacional e formativa na proteção de dados, tratando de temas como confiança, transparência e acesso à informação;

m) negociar garantia de emprego para o encarregado se este vier a ser empregado, bem como delimitar responsabilidades;

n) explicitar coletas tecnológicas de dados para proteção de direitos digitais.

O sindicato pode fiscalizar toda a lei com base na “*accountability*”: fazer denúncias para o DPO (encarregado) dentro da empresa, MPT e ANPD. Em síntese, o sindicato, numa visão de oportunidade e exercício de suas funções negociais constitucionais, está autorizado a retomar sua confiança, credibilidade e atuação com base nesta nova realidade de necessidade de proteção de dados.

Considerações finais

Num cenário de trabalho para os próximos anos, vale lembrar o centenário da

OIT, em sua Declaração, em 2019⁸, a qual menciona a necessidade de que o trabalhador tenha a proteção de seus dados pessoais e privacidade por meio do reforço das instituições. Essa proteção para o futuro do trabalho – proteção de dados, deve se dar de forma individual e mesmo de modo coletivo, com a participação sindical em negociações coletivas, visto que o sindicato é a instituição vocacionada para a defesa dos direitos individuais e coletivos dos representados,

Lendo-se os dispositivos legais que regulam negociações coletivas e, em especial, tomando-se a nova redação do art. 611 da CLT, parece-nos que há autorização da atuação sindical para defesa de direitos de proteção de dados de seus associados, considerando-se ainda as orientações principiológicas contidas no art. 8º da CF.

A negociação coletiva é uma ferramenta capaz de dar novo direcionamento normativo aos aspectos ainda não regulamentados suficientemente entre dados e trabalho, segundo a Lei 13.709/18. Negociação coletiva é o meio pelo qual se podem equilibrar necessidades e interesses de trabalhadores e empresas, esclarecendo condições de trabalho adequadas para a proteção de dados da pessoa natural do trabalhador em distintas realidades setoriais. Como ferramenta de diálogo, as negociações coletivas (acordos ou convenções coletivas) podem estabelecer cláusulas, direitos, obrigações, condutas, práticas, entendimentos em todas as fases do desenvolvimento do vínculo laboral, entre outros ajustes de interesses e comportamentos entabulados entre empresas e trabalhadores, especialmente num momento como este, de revisão do conceito de privacidade na sociedade informacional, com especiais repercussões nas relações laborais.

REFERÊNCIAS:

AGUIAR, Antonio Carlos. A proteção de dados no contrato de trabalho. **Revista LTr**: Legislação do Trabalho, São Paulo, v. 82, n. 6, p. 655-661, jun. 2018.

ARAÚJO, Adriane Reis de. A proteção da informação envolvendo empregados e suas dimensões no Direito do Trabalho. *In*: MIZIARA, Raphael; MOLLI-CONE, Bianca; PESSOA, André. **Reflexos da LGPD no Direito e no Processo do Trabalho**. São Paulo: RT, 2020.

ASENCIO, Antonio José Valverde. Protección de datos de carácter personal y derechos de información de los representantes de los trabajadores. **Revista andaluza de trabajo y bienestar social**, 119, p. 13-54, 2013.

BARZOTTO, Luciane Cardoso e CUNHA, Leonardo Stocker Pereira da. Proteção de dados pessoais e consentimento do empregado: jurisprudência trabalhista e a Lei Geral de Proteção de Dados (LGPD). *In*: **Inovações e Trabalho: o Direito do Trabalho em Tempos de Mudança**. BARZOTTO, Luciane Cardoso e DORNELLES, Leandro Dornelles de (org). Editora da UFRGS: Porto Alegre, 2020.

BIANCH, Alexandra Cristina Cypriano. A LGPD e as relações sindicais. Disponível em: <https://www.megajuridico.com/a-lei-geral-de-protecao-de-dados-pessoais-e-as-relacoes-sindicais/>

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites**

8 OIT- Declaração do centenário. Disponível em: https://www.ilo.org/wcmsp5/groups/public/---europe/---ro-geneva/---ilo-lisbon/documents/publication/wcms_706928.pdf

do consentimento. Rio de Janeiro: Forense, 2019.

BLUM, Renato Opice; LÓPEZ, Nuria. **Lei Geral de Proteção de Dados no setor público: transparência e fortalecimento do Estado Democrático de Direito.** Cadernos Jurídicos, São Paulo, v. 21, n. 53, p. 171-177, jan./mar. 2020. Disponível em: https://bdjur.stj.jus.br/jspui/bitstream/2011/142294/lei_geral_protecao_blum.pdf

BOLETIM de trabalho e emprego de Portugal. Disponível em: http://bte.gep.msess.gov.pt/completos/2021/bte2_2021.pdf.

BOMFIM, Vólia; PINHEIRO, Yuri. A lei geral de proteção de dados e seus impactos nas relações de trabalho. *In*: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. **Reflexos da LGPD no Direito e no Processo do Trabalho.** São Paulo: RT, 2020.

BRASIL. **Constituição Federal de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 23 mar. 2021.

BRASIL. **Decreto-Lei nº 5.452, de 1º de maio de 1943. Consolidação das Leis do Trabalho.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 23 mar. 2021.

BRASIL. **Lei nº 13.709/2018. Lei Geral de Proteção de Dados.** Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 23 mar. 2021.

CALCINI, Ricardo. Prática trabalhista: impactos da LGPD nas relações de trabalho. Disponível em: <https://www.conjur.com.br/2021-fev-11/pratica-trabalhista-impactos-lgpd-relacoes-trabalho>

CARLOTO, Selma. **Lei Geral de Proteção de Dados: enfoque nas relações de trabalho.** São Paulo: LTr, 2020.

CORREIA, Henrique e BOLDRIN, Paulo Henrique Martinucci. **Lei Geral de Proteção de Dados (LGPD) e o Direito do Trabalho.** Disponível em: <https://meusitejuridico.editorajuspodivm.com.br/2020/09/25/lei-geral-de-protecao-de-dados-lgpd-e-o-direito-trabalho/>

DERECHOS de información de los Representantes de los trabajadores. Sevilla: TEMAS LABORALES. **Revista Andaluza de Trabajo Y Bienestar Social.** n. 118/2013. p. 13-54. Disponível em: <https://idus.us.es/handle/11441/91056>. Acesso em: 5 abr. 2021

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de proteção de dados. 2ª ed. São Paulo: RT, 2019.

FERNANDEZ, Leandro. É possível negociação coletiva sobre dados pessoais? Palestra no youtube <https://www.youtube.com/watch?v=x2eoVzpXYBw&t=24408s>

GRANJA, Tatiana de Almeida. **O desafio da proteção aos dados pessoais do trabalhador:** breve exame do poder patronal. Direito & TI. 2016. Disponível em: Acesso em: 23 mar. 2021.

GUÍA de la protección de datos en las relaciones laborales de la propia Agencia Española de Protección de Datos. Disponível em: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_RelacionesLaborales.pdf.

GULARTE, Caroline de Melo Lima. **A Proteção de Dados Pessoais no Uso de Tecnologia na Relação de Emprego**: Efeitos do Compliance Trabalhista nas Negociações Coletivas. Dissertação (mestrado em Direito). PUCRS, 2020.

GUNTHER, L. E.; COMAR, R. T.; RODRIGUES, L. E. **A Proteção e o Tratamento dos Dados Pessoais Sensíveis na Era Digital e o Direito à Privacidade**: os Limites da Intervenção do Estado. Curitiba, 2020. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RIMA/article/view/3972>. Acesso em: 27 out. 2020.

ILO. Protection of workers' **personal data**. An ILO code of practice. Geneva, International Labour Office, 1997 /Code of practice/, /text/, /privacy/, /confidentiality/, /data protection/, /workers' rights/. 04.02.2 ISBN 92-2-110329-3. Disponível em: Acesso em: 19 mar.2021.

LIMA, Fabrício. A autodeterminação informativa e os limites do poder fiscalizatório do empregador. *In*: MIZIARA, Raphael; MOLLICONE, Bianca; PES-SOA, André. **Reflexos da LGPD no Direito e no Processo do Trabalho**. São Paulo: RT, 2020.

LIMBERGER, Têmis. **Cibertransparência** – informação pública em rede – a virtualidade e suas repercussões na realidade. Porto Alegre: Livraria do Advogado. 2016.

MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. Discriminação algorítmica à luz da Lei Geral de Proteção de Dados. *In*: MENDES, Laura Schertel; SARLET, Ingo; DONEDA, Danilo; RODRIGUES JR, Otávio Luiz et. al. (coord). **Tratado de Proteção de Dados**. Rio de Janeiro: Forense, 2021, p. 421-446.

MENKE, Fabiano e GOULART, Guilherme Damásio. Segurança da informação e vazamento de dados. *In*: MENDES, Laura Schertel; SARLET, Ingo; DONEDA, Danilo; RODRIGUES JR, Otávio Luiz et. al. (coord). **Tratado de Proteção de Dados**. Rio de Janeiro: Forense, 2021

PAMPLONA FILHO, Rodolfo; CONI JUNIOR, Vicente Vasconcelos. **A Lei Geral de Proteção de Dados Pessoais e seus impactos no Direito do Trabalho**. Direito Unifacs: debate virtual, Salvador, n. 239, p. 1-42, maio 2020. Disponível em: <https://revistas.unifacs.br/index.php/redu/article/view/6744/4066>

REIS, Beatriz de F. **O direito fundamental à proteção de dados pessoais e sensíveis do trabalhador frente às novas tecnologias da informação e comunicação**. 176 f. 2019. - Universidade do Extremo Sul Catarinense, Criciúma, 2019. Disponível em: <http://repositorio.unesc.net/handle/1/7469>. Acesso em: 27 out. 2020.

ROSSETO, Geralda Magela de Faria; QUINAN, Paulo Gustavo Magella de Faria. Verbetes LGPD- Lei Geral de Proteção de Dados. *In*: **Direito do Trabalho, tecnologia, fraternidade e OIT: compilação de verbetes**. RT Editora (Thomson Reuters): São Paulo, 2020. Coordenação: BARZOTTO, Luciane Cardoso; FITA, Fernando; FREDIANI, Yone; NAHAS, Thereza. p. 210-211.

SANKIEVICZ, Alexandre; PINHEIRO, Guilherme Pereira. Aspectos da proteção de dados nas relações de trabalho. *In*: MENDES, Laura Schertel; SARLET, Ingo, DONEDA, Danilo; RODRIGUES JR, Otávio Luiz et. al. (coord). **Tratado**

de Proteção de Dados. Rio de Janeiro: Forense, 2021, p. 421-446.

SARLET, Gabrielle Bezerra Sales; FERNANDES, Marcia Santana; RUARO, Regina Linden. A proteção de dados no setor de saúde em face do sistema normativo brasileiro atual. *In*: MENDES, Laura Schertel; SARLET, Ingo, DONEDA, Danilo; RODRIGUES JR, Otávio Luiz et. al. (coord). **Tratado de Proteção de Dados.** Rio de Janeiro: Forense, 2021.

SIGNES, Adrián Todolí. **La gobernanza colectiva de la protección de datos en las relaciones laborales** “big data”, creación de perfiles, decisiones empresariales automatizadas y los derechos colectivos. Valencia: Revista de derecho social, Nº 84, 2018, págs. 69-88

SZINVELSKI, Martín M; LIMBERGER, Têmis; SALDANHA, Jânia. Transnacionalização e selos de qualidade em proteção de dados: um novo campo de estudo na era digital. **Revista dos Tribunais**, v. 109, n. 1020, p. 143-162, out. 2020.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei geral de proteção de dados pessoais: e suas repercussões no Direito brasileiro.** 2. tir. São Paulo: Thomson Reuters Brasil, 2019.

UGUINA, Jesús R. Mercader e Ignacio García-Perrote Escartín. El protagonismo del convenio colectivo en el nuevo reglamento de protección de datos. Publicación: **Revista de Información Laboral** n.6, 2018, parte Editorial Editorial Aranzadi, S.A.U., Cizur Menor: 2018.

ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. *In*. **Tecnopolíticas da vigilância:** perspectivas da margem. Tradução Heloísa Cardoso Mourão. 1.ed. São Paulo: Boitempo, 2018.

29. O USO DO CONSENTIMENTO PARA TRATAMENTO DE DADOS DE EMPREGADOS

FERNANDA MASSOTE LEITÃO ALVARENGA¹

1. Introdução

Com a entrada em vigor da Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD), tornou-se necessário realizar alterações nas rotinas trabalhistas das empresas, para que estas se adequassem à nova legislação, garantindo transparência no uso de dados pessoais.

Importante esclarecer que o objetivo da LGPD é “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.”²

Em qualquer relação trabalhista são coletados e armazenados inúmeros dados dos trabalhadores e de terceiros. Dessa forma, não pairam dúvidas de que a LGPD deve ser observada pelos empregadores mesmo que não haja norma específica sobre a sua incidência no direito laboral:

Diversamente da GDPR, a lei brasileira não contempla expressa disposição sobre o direito do trabalho, mas sua incidência a ele é irrefutável, pois a relação de trabalho sequer teria como se iniciar e desenvolver sem a coleta, a recepção, o armazenamento e a retenção de dados pessoais dos empregados ou candidatos a empregos.³

A adequação à Lei Geral de Proteção de Dados, como elucidado pela Professora Selma Carloto⁴, inicia-se desde o anúncio da vaga de emprego, durante o processo seletivo, a execução do contrato de trabalho e até mesmo depois da rescisão.

1 Advogada trabalhista e Sócia do AM&M Advogados Associados. Graduada em Direito pela Pontifícia Universidade Católica de Minas Gerais, possui MBA em Direito do Trabalho pela Fundação Getúlio Vargas, Pós- Graduação em Novo Direito do Trabalho pela Pontifícia Universidade Católica do Rio Grande do Sul e Pós- graduação em Direito e Compliance Trabalhista pelo IEPREV. cursou Business Analytics: tomada de decisões a partir de dados, na Universidade de Cambridge. Colunista do Megajuridico, Conselheira da AMAT e Membro da Comissão de Direitos Sociais e Trabalhistas da OAB/MG (triênio 2019/2021). E-mail: f.massote@amassociados.adv.br.

2 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 out. 2021.

3 PINHEIRO, Iuri; BOMFIM, Vólia. **A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho**. Instituto Trabalho em Debate (ITD), 2020, p.49. Disponível em: <http://trabalhoemdebate.com.br/artigo/detalhe/a-lei-geral-de-protECAo-de-dados-e-seus-impactos-nas-relacoes-de-trabalho>. Acesso em: 17 set. 2021.

4 CARLOTO, Selma. **Lei Geral da Proteção de Dados: Enfoque nas relações de trabalho**. São Paulo: Editora LTR, 2020, p. 28.

O artigo 7º da LGPD traz as bases legais para tratamento de dados pessoais, enquanto o artigo 11º da mesma lei apresenta as hipóteses para tratamento de dados pessoais sensíveis.

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

§ 1º Nos casos de aplicação do disposto nos incisos II e III do caput deste artigo e excetuadas as hipóteses previstas no art. 4º desta Lei, o titular será informado das hipóteses em que será admitido o tratamento de seus dados. (Revogado pela Medida Provisória nº 869, de 2018)

§ 1º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)

§ 2º A forma de disponibilização das informações previstas no § 1º e no inciso I do caput do art. 23 desta Lei poderá ser especificada pela autoridade nacional. (Revogado pela Medida Provisória nº 869, de 2018)

§ 2º (Revogado). (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019) Vigência

[...]

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas

previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas “a” e “b” do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular.

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto

nas hipóteses de: (Redação dada pela Medida Provisória nº 869, de 2018)

I - portabilidade de dados quando consentido pelo titular; ou (Incluído pela Medida Provisória nº 869, de 2018)

II - necessidade de comunicação para a adequada prestação de serviços de saúde suplementar. (Incluído pela Medida Provisória nº 869, de 2018)

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019) Vigência

I - a portabilidade de dados quando solicitada pelo titular; ou (Incluído pela Lei nº 13.853, de 2019) Vigência

II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. (Incluído pela Lei nº 13.853, de 2019) Vigência

§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.⁵

O presente artigo pretende discutir acerca da utilização do consentimento para tratamento de dados de empregados, que é uma base legal para tratamento de dados, prevista tanto no artigo 7º quanto no artigo 11º da Lei nº 13.709, de 14 de agosto de 2018.

2. Dados pessoais e direitos de personalidade

Conforme Bruno Bioni, hoje tem-se uma sociedade em que “a categorização da pessoa, a partir de seus dados pessoais, pode repercutir nas suas oportunidades sociais, no contexto de uma sociedade e uma economia movida por dados.”⁶ São justamente tais projeções que autorizam que a proteção dos dados pessoais seja inserida dentro da categoria dos direitos da personalidade.

Dessa forma, o direito à exatidão dos dados confere ao cidadão proteção aos direitos da sua personalidade, uma vez que “os dados que influem na projeção

5 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 10 out. 2021.

6 BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2.ed. Edição. Rio de Janeiro: Editora Forense, 2020, p. 88.

de uma pessoa e na sua esfera relacional adequam-se conceitualmente como um novo direito de personalidade.⁷⁷

Nesse sentido, a LGPD veio disciplinar sobre o tratamento de dados pessoais, permitindo que o indivíduo tenha controle sobre seus dados pessoais, conforme bem pontuado pelos Professores Iuri Pinheiro e Vólia Bomfim:

Durante muito tempo acreditou-se que os dados das pessoas naturais faziam parte do patrimônio da empresa que os coletava. A valoração econômica da atividade empresarial, muitas vezes, correspondia ao quantitativo de dados que tratava. Após vazamentos e utilização indevida e muitas vezes abusiva, vem a lei para regular, e não impedir, o tratamento dos dados das pessoas físicas, dando ao seu titular, e só a este, o direito de informação, decisão e disponibilidade.⁸

3. Subordinação e a relação assimétrica

Vale lembrar que a CLT, em seus artigos 2º e 3º, é clara ao dispor que o elemento da subordinação é requisito indispensável para configurar o vínculo empregatício.

O professor Mauricio Godinho define a subordinação como:

7 BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2. ed. Edição. Rio de Janeiro: Editora Forense, 2020, p. 58.

8 PINHEIRO, Iuri; BOMFIM, Vólia. **A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho**. Instituto Trabalho em Debate (ITD), 2020. Disponível em: <http://trabalhoemdebate.com.br/artigo/detalhe/a-lei-geral-de-protecao-de-dados-e-seus-impactos-nas-relacoes-de-trabalho>. Acesso em: 17 set. 2021.

9 Art. 2º - Considera-se empregador a empresa, individual ou coletiva, que, assumindo os riscos da atividade econômica, admite, assalaria e dirige a prestação pessoal de serviço.

§ 1º - Equiparam-se ao empregador, para os efeitos exclusivos da relação de emprego, os profissionais liberais, as instituições de beneficência, as associações recreativas ou outras instituições sem fins lucrativos, que admitirem trabalhadores como empregados.

§ 2º - Sempre que uma ou mais empresas, tendo, embora, cada uma delas, personalidade jurídica própria, estiverem sob a direção, controle ou administração de outra, constituindo grupo industrial, comercial ou de qualquer outra atividade econômica, serão, para os efeitos da relação de emprego, solidariamente responsáveis a empresa principal e cada uma das subordinadas.

§ 2º Sempre que uma ou mais empresas, tendo, embora, cada uma delas, personalidade jurídica própria, estiverem sob a direção, controle ou administração de outra, ou ainda quando, mesmo guardando cada uma sua autonomia, integrem grupo econômico, serão responsáveis solidariamente pelas obrigações decorrentes da relação de emprego. (Redação dada pela Lei nº 13.467, de 2017) (Vigência)

§ 3º Não caracteriza grupo econômico a mera identidade de sócios, sendo necessárias, para a configuração do grupo, a demonstração do interesse integrado, a efetiva comunhão de interesses e a atuação conjunta das empresas dele integrantes. (Incluído pela Lei nº 13.467, de 2017) (Vigência)

Art. 3º - Considera-se empregado toda pessoa física que prestar serviços de natureza não eventual a empregador, sob a dependência deste e mediante salário.

Parágrafo único - Não haverá distinções relativas à espécie de emprego e à condição de trabalhador, nem entre o trabalho intelectual, técnico e manual. (BRASIL. DECRETO – LEI Nº 5.452, DE 1º DE MAIO DE 1943 . Aprova a Consolidação das leis do trabalho (CLT) 1943. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 15 out. 2021).

(...) a que se manifesta pela inserção do trabalhador na dinâmica do tomador de seus serviços, independentemente de receber (ou não) suas ordens diretas, mas acolhendo, estruturalmente, sua dinâmica de organização e funcionamento.¹⁰

Assim, em decorrência da subordinação, o empregado está sempre sujeito às ordens patronais, que podem ser rígidas (como exigência de cumprimento de horários de trabalho, submissão a controles do empregador e outros) ou decorrentes da subordinação estrutural¹¹. Por essa razão, nota-se que há um desequilíbrio entre as partes protagonistas da relação trabalhista.

4. Consentimento nas relações laboriais

No dicionário, **consentimento** significa anuência, ou seja, “Concordância de ideias, unanimidade de opiniões, acordo das partes envolvidas (em projeto, objetivo, decisões etc.)”

A LGPD (Lei n.º: 13.709/2018) traz o conceito de consentimento, no inciso XII, do artigo 5º, como “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”.¹²

Conforme foi demonstrado no item anterior, o traço distintivo do contrato de emprego é a subordinação. Se o empregado presta serviços sob a dependência do seu empregador e mediante salário, como descreve o artigo 3º da CLT, como é possível garantir que o seu consentimento, para tratamento de dados pessoais, será livre, informado e inequívoco?

Se a relação trabalhista tem um desequilíbrio contratual natural, como o trabalhador subordinado terá liberdade para consentir ou não acerca de seus dados pessoais, já que depende do seu empregador?

Insta esclarecer que a LGPD, em seu artigo 2º, elenca os fundamentos que disciplinam a proteção de dados. Dentre eles, está a autodeterminação informativa, que consiste no “controle pessoal sobre o trânsito de dados relativo ao próprio titular- e, portanto, uma extensão de liberdade do indivíduo”, como descreve Rony Vaizf¹³

10 DELGADO, Maurício Godinho. Direitos fundamentais na relação de trabalho. **Revista de Direito do Trabalho**, São Paulo, v.32, n. 123, jul./set. 2006. p 164

11 A ideia de subordinação estrutural supera as dificuldades de enquadramento de situações fáticas que o conceito clássico de subordinação tem demonstrado, dificuldades que se exacerbam em face, especialmente, do fenômeno contemporâneo da terceirização trabalhista. Nesta medida ela viabiliza não apenas alargar o campo de incidência do Direito do Trabalho, como também conferir resposta normativa eficaz a alguns de seus mais recentes instrumentos desestabilizadores – em especial a terceirização. (DELGADO, Maurício Godinho. Direitos fundamentais na relação de trabalho. **Revista de Direito do Trabalho**, São Paulo, v.32, n. 123, jul./set. 2006. p 164).

CONSENTIMENTO. In: **Dicionário Michaelis online**. Disponível em: <https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/consentimento/> Acesso em: 13 out. 2021.

12 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 10 out. 2021.

13 VAINZOF, Roiny. Capítulo I- Disposições Preliminares. In: MALDONADO, Viviane Nóbrega;

Para Bruno Ricardo Bioni¹⁴, “a prometida autodeterminação informacional é estrangulada em meio a uma relação assimétrica.” Nessa senda, percebe-se que o empregado, por ser considerado vulnerável, não possui condições de consentir de forma livre, informada e inequívoca no decurso do contrato de trabalho.

O consentimento livre só poderá ser aceito quando for possível saber o “poder de barganha”¹⁵ do trabalhador em relação aos seus dados pessoais, ou seja, é importante avaliar se serão disponibilizadas outras opções para o titular de dados.

Há situações peculiares que podem ensejar a adoção do consentimento para tratamento de dados pessoais do empregado, como o exemplo citado pela Professora Selma Carloto do Working Party 29:

Uma equipe de filmagem pretende filmar determinada parte de um escritório. O empregador solicita o consentimento de todos os trabalhadores que se sentam nessa zona do escritório para serem filmados, uma vez que podem aparecer em segundo plano nas filmagens do vídeo. Os trabalhadores que não quiserem ser filmados não serão de forma alguma penalizados, uma vez que serão colocados noutra local de trabalho equivalente numa outra zona do edifício enquanto durar a filmagem.¹⁶

No caso acima, o obreiro possuía livre-arbítrio para escolher se iria participar das gravações ou não, e sua escolha não implicaria nenhuma penalidade.

Nas lições de Bruno Ricardo Bioni:

A questão central é sempre chegar à existência de algum tipo de subordinação-assimetria de poder - que possa minar a voluntariedade do consentimento, devendo haver uma análise casuística para se concluir se o consentimento pode ser adjetivado ou não como livre.¹⁷

O artigo 9º¹⁸, da LGPD, demonstra que as informações deverão disponibiliza-

BLUM, Ópice (Coord). **LGPD- Lei Geral de Proteção de Dados Comentada**. São Paulo: Thomson Reuters Brasil. 2019, p.27.

14 BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**-2.ed. Rio de Janeiro: Editora Forense, 2020, p. 151.

15 BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**-2.ed. Rio de Janeiro: Editora Forense, 2020, p.185.

16 CARLOTO, Selma. **Lei Geral da Proteção de Dados Enfoque nas relações de trabalho**. São Paulo: Editora LTR, 2020, p.100-101.

17 BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**-2.ed. Rio de Janeiro: Editora Forense, 2020, p. 186.

18 Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;

das para o titular de dados de forma clara, para garantir que o consentimento seja informado. Por isso, “O consentimento informado tem correlação com o princípio da transparência¹⁹”.

Para evitar vício de consentimento, o consentimento deve ser granular, ou seja, específico para a finalidade informada pelo empregador. O adjetivo inequívoco, previsto no inciso XII, do artigo 5º, significa que “Qualquer declaração de vontade deve ter um direcionamento, já que não se consente no vazio e de forma genérica”²⁰.

Na legislação brasileira ainda não há nenhuma norma expressa que restrinja a utilização do consentimento para tratamento de dados de empregados. Já o Regulamento Geral de Proteção de Dados Europeu (GDPR) estabelece que o consentimento não deve ser utilizado caso exista um desequilíbrio manifesto entre o titular de dados e o responsável pelo tratamento:

A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferen-

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação do controlador;

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei. (BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 10 out. 2021).

19 CARLOTO, Selma. **Lei Geral da Proteção de Dados Enfoque nas relações de trabalho**. São Paulo: Editora LTR, 2020, p. 91.

20 BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2.ed.. Rio de Janeiro: Editora Forense, 2020, p.186.

tes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução.²¹

Como já foi informado anteriormente, o consentimento não é a única base legal para tratamento de dados pessoais. Dessa forma, tanto o artigo 6º quanto o artigo 11º da Lei nº 13.709, de 2018, apresentam, de forma taxativa, outras bases legais para tratamento de dados pessoais.

Por isso, nas situações em que a própria legislação dispensa o consentimento, o empregador deve utilizar outra hipótese legal para realizar o tratamento de dados de seus empregados, em decorrência da fragilidade do consentimento do empregado em uma relação assimétrica.

Conclusão

Para resguardar os direitos de privacidade e de liberdade, bem como para garantir o livre desenvolvimento da personalidade da pessoa humana²², a LGPD trouxe diversas normas, que devem ser respeitadas e cumpridas por aqueles que operam dados de pessoas físicas²³, aplicando-se, portanto, aos empregadores.

A autodeterminação informativa, prevista no inciso III do art. 2º da LGPD, garante ao titular dos dados o papel de protagonista na relação:

Assim, temos que o princípio da autodeterminação informativa confere ao titular dos dados a palavra final no que diz respeito às operações de tratamento dos seus dados pessoais, via de regra, e, mesmo quando não puder opor-se ao tratamento, nos casos em que este se der com base em outros interesses, confere ao menos o direito de informação sobre a limitação de finalidade desses dados e quanto à segurança conferida a eles.²⁴

Os artigos 6º e 11º da LGPD apresentam rol taxativo das bases legais para tratamento de dados pessoais, sendo o consentimento apenas uma delas.

Conforme foi demonstrado, o empregado, por ser um sujeito vulnerável na relação de emprego, não possui condições de consentir de forma livre, informada

21 UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679>. Acesso em: 14 out. 2021.

22 Art. 1º, da Lei nº 13.709, de 14 de agosto de 2018

23 Art. 3º, da Lei nº 13.709, de 14 de agosto de 2018

24 SALDANHA, João. **Fundamentos da LGPD**. A Autodeterminação Informativa. 9 jul. 2019. Disponível em: <https://triplait.com/a-autodeterminacao-informativa/>. Acesso em: 07 ago. 2021.

e inequívoca, conforme exige o inciso XII, do artigo 5º, da LGPD.

A ideia do presente artigo funda-se no reconhecimento da vulnerabilidade do trabalhador em um contrato de emprego, em que o seu “poder de barganha” contratual é corrompido, seja por conta da subordinação ou da dependência econômica.

Nesse diapasão, concluiu-se que o consentimento deve ser evitado para tratamento de dados pessoais nas relações de emprego, por ser a relação trabalhista assimétrica, resguardado a sua utilização para casos específicos, “quando o ato de recusar o consentimento não produzir consequências negativas ao titular dos dados.”²⁵ Nessas situações peculiares, o consentimento deverá ser colhido de forma granular, obedecendo os requisitos previstos no artigo 8º da LGPD²⁶ e os princípios que norteiam a LGPD²⁷.

25 CARLOTO, Selma. **Lei Geral da Proteção de Dados Enfoque nas relações de trabalho**. São Paulo: Editora LTR, 2020, p. 100.

26 Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração. (BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 out. 2021).

27 Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento

REFERÊNCIAS

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2.ed. Rio de Janeiro, 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 out. 2021.

BRASIL. DECRETO-LEI Nº 5.452, DE 1º DE MAIO DE 1943. Aprova a Consolidação das leis do trabalho (CLT) 1943. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 15 out. 2021

CARLOTO, Selma. **Lei Geral da Proteção de Dados Enfoque nas relações de trabalho**. São Paulo: Editora LTR, 2020.

DELGADO, Maurício Godinho. Direitos fundamentais na relação de trabalho. **Revista de Direito do Trabalho**, São Paulo, v.32, n. 123, jul./set. 2006.

DELGADO, Mauricio Godinho. **Curso de direito do trabalho**. 10. ed. São Paulo: LTr, 2011.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

PINHEIRO, Iuri; BOMFIM, Vólia. **A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho**. Instituto Trabalho em Debate (ITD), 2020. Disponível em: <http://trabalhoemdebate.com.br/artigo/detalhe/a-lei-geral-de-protecao-de-dados-e-seus-impactos-nas-relacoes-de-trabalho>. Acesso em: 17 set. 2021.

SALDANHA, João. **Fundamentos da LGPD**. A Autodeterminação Informativa. 9 jul. 2019. Disponível em: <https://triplait.com/a-autodeterminacao-informativa/>. Acesso em: 07 ago. 2021.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TX-?uri=CELEX:32016R0679>. Acesso em: 14 out. 2021

VAINZOF, Roiny. Capítulo I- Disposições Preliminares. In: MALDONADO, Viviane Nóbrega; BLUM, Ópice (Coord). **LGPD- Lei Geral de Proteção de Dados Comentada**. São Paulo: Thomson Reuters Brasil. 2019.

de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 out. 2021)

30. LGPD NAS RELAÇÕES DE TRABALHO: OS RISCOS DE UTILIZAÇÃO DO CONSENTIMENTO PARA O TRATAMENTO DOS DADOS DOS TRABALHADORES

FABRÍCIO LIMA SILVA¹

Resumo

O presente artigo pretende desenvolver uma reflexão jurídica sobre as bases para o tratamento dos dados pessoais nas relações de emprego. Serão abordadas, com fundamento na disciplina estabelecida pela Lei 13.709/2018 (LGPD), as hipóteses que autorizam o tratamento dos dados pessoais e os dados sensíveis, com a apresentação dos riscos de utilização do consentimento do titular como base de tratamento. Por se tratar de uma relação em que os contratantes não se encontram em patamar de igualdade, em razão da hipossuficiência do trabalhador, serão apresentadas razões para que o consentimento somente seja utilizado excepcionalmente.

Palavras-chave. Lei Geral de Proteção de Dados. Relações de Trabalho. Autodeterminação Informativa. Privacidade. Consentimento.

Abstract

This article aims to develop a legal reflection on the baselines about the processing of personal data in employment relationships. Based on the discipline established by the Law 13.709/2018 (Brazil's Data Law - LGPD), the hypotheses that authorize the processing of personal data and sensitive data will be approached, with the presentation of the risks of using the holder's consent as a basis for processing. As it is a relationship in which the contractors are not on the same level playing field, due to the employee's under-sufficiency, reasons will be presented so the consent can be used only exceptionally.

Keywords. General Data Protection Law. Workplace relationships. Informational self-determination. Privacy. Consent.

1. Introdução

Em 18 de setembro de 2020, entrou em vigor em nosso país a Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD).

A referida norma, fruto da necessidade de uniformização internacional de gestão, segurança e transferência de dados, estabeleceu diversos parâmetros para o tratamento de dados pessoais no território nacional e para transferências internacionais.

¹ Juiz do Trabalho do TRT da 3ª Região MG. Especialista em Direito Público, Direito Material e Processual do Trabalho. Doutorando em Direito Privado pela Universidade do Minho (Portugal). Mestrando em Constitucionalismo e Democracia pela Faculdade de Direito do Sul de Minas – FDSM. Professor de Direito e Processo do Trabalho em Cursos de Especialização. Formação em Compliance Laboral pela Wolters Kluwer (Espanha). Coautor do *Manual do Compliance Trabalhista*. Graduado pela Faculdade de Direito da Universidade de São Paulo (USP). Foi analista judiciário do TRT da 3ª Região, de 2004 até 2010.

A LGPD levou em consideração as regulamentações americanas e europeias, que foram concebidas com o foco na autodeterminação informativa e na regulamentação para proteção do fluxo de dados, ocasionando uma verdadeira ressignificação do direito à privacidade em nosso país.

A Organização Internacional do Trabalho, também preocupada com a questão já no ano de 1997, havia editado o Código de Boas Práticas sobre a Proteção de Dados Pessoais dos Trabalhadores (Code of Practice on the Protection of Workers' Personal Data)², estabelecendo orientações para o tratamento adequado dos trabalhadores.

Inicialmente, importante destacar a definição do conceito de tratamento.

Nos moldes do art. 5º, X, da LGPD, tratamento é:

toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

E com objetivo de ampliar a proteção da intimidade dos titulares dos dados e dos respectivos dados dos titulares, a referida legislação estabeleceu hipóteses justificadoras do tratamento pelos agentes descritos na lei, denominadas, pela doutrina, como “bases de tratamento”.

Além disso, foram previstos fundamentos, princípios e limitações para a realização de tais atividades.

A disciplina da proteção de dados em nosso país passou a ter como fundamentos: I) o respeito à privacidade; II) a autodeterminação informativa; III) a liberdade de expressão, de informação, de comunicação e de opinião; IV) a inviolabilidade da intimidade, da honra e da imagem; V) o desenvolvimento econômico e tecnológico e a inovação; VI) a livre iniciativa, a livre concorrência e a defesa do consumidor; VII) e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (art. 2º).

A mencionada legislação é voltada, principalmente, para os aspectos de atuação das empresas e do poder público, seja em relação aos dados de consumidores, usuários, parceiros de negócios, seja em relação aos dados de seus empregados/servidores.

E, considerando-se que, em uma relação de emprego, diversos dados de trabalhadores são coletados, armazenados e transferidos a terceiros, em um primeiro momento, tornou-se necessário que fossem encontradas bases legais para justificar o tratamento, objetivando-se o cumprimento da legislação e a adequação de procedimentos.

Além disso, o avanço disruptivo das novas tecnologias de informação e comunicação, além de ampliar a produtividade e a competitividade das empresas, potencializou as formas de fiscalização e controle das atividades laborais pelos empregadores, implicando, em determinados casos, em restrições à privacidade

2 OIT. Protección de los datos personales de los trabajadores. Disponível em: https://www.ilo.org/global/topics/safety-and-health-at-work/normative-instruments/code-of-practice/WCMS_112625/lang-es/index.htm. Acesso em: 01 de fevereiro 2021.

dos trabalhadores, a depender da intensidade e dos mecanismos adotados.

O videomonitoramento, a geolocalização, as gravações ambientais, a fiscalização do uso da Internet e das redes sociais podem, de certa forma, tornar possível o delineamento do perfil dos empregados ou de candidatos ao emprego, com controle de sua vida extralaboral ou utilização de práticas discriminatórias.

Em alguns casos, conforme destaca Uguina³, cogita-se sobre a existência de uma “empresa panóptica”, em referência ao modelo utópico de prisão, desenhado pelo filósofo e jurista inglês Jeremy Bentham em 1785, que permitiria que um único vigilante observasse todos os prisioneiros, induzindo aos detentos a sensação permanente de estarem sendo vigiados.

Foucault, em sua obra *Vigiar e Punir: Nascimento da prisão*, bem descreve o referido modelo:

O Panóptico de Bentham é a figura arquitetural dessa composição. O princípio é conhecido: na periferia uma construção em anel; no centro, uma torre: esta é vazada de largas janelas que se abrem sobre a face interna do anel; a construção periférica é dividida em celas, cada uma atravessando toda a espessura da construção; elas têm duas janelas, uma para o interior, correspondendo às janelas da torre; outra, que dá para o exterior, permite que a luz atravesse a cela de lado a lado. Basta então colocar um vigia na torre central, e em cada cela trancar um louco, um doente, um condenado, um operário ou um escolar. Pelo efeito da contraluz, pode-se perceber da torre, recortando-se exatamente sobre a claridade, as pequenas silhuetas cativas nas celas da periferia. Tantas jaulas, tantos pequenos teatros, em que cada ator está sozinho, perfeitamente individualizado e constantemente visível.⁴

Conforme destaca Miller, a prisão panóptica seria:

uma instância onividente, onipresente, onisciente, fechando os reclusos numa dependência de que não se aproxima nenhuma prisão ordinária, uma instância em que é mesmo preciso reconhecer um Deus artificial⁵.

Assim, percebe-se que o referido modelo é bem representado pela expressão “panóptico”, que significa: “o olho que tudo vê”, extrapolando a estrutura física das prisões, uma vez que demonstra uma verdadeira tecnologia de poder.

Bauman, ao tratar do modelo panóptico, como arquetípica do poder moderno feita por Michael Foucault, em sua obra *Modernidade Líquida*, destacou que:

3 UGUINA, Jesús Mercader. *Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica?* *Revista Relaciones Laborales*, n. 10, p. 2, 2001.

4 FOCAULT, Michel. 42. ed. *Vigiar e Punir: nascimento da prisão*. Tradução de Raquel Ramallete. Petrópolis: Vozes, 2014, p. 194.

5 MILLER, Jacques-Alain. A máquina panóptica de Jeremy Bentham. In: BENTHAM, Jeremy. *O panóptico*. São Paulo: Autêntica Editora, 2000, p. 89.

No Panóptico, os internos estavam presos ao lugar e impedidos de qualquer movimento, confinados entre muros grossos, densos e bem-guardados, e fixados a suas camas, celas ou bancadas. Eles não podiam se mover porque estavam sob vigilância; tinham que se ater aos lugares indicados sempre porque não sabiam, e nem tinham como saber, onde estavam no momento seus vigias, livres para mover-se à vontade. As instalações e a facilidade de movimento dos vigias eram a garantia de sua dominação; dos múltiplos laços de sua subordinação, a “fixação” dos internos ao lugar era o mais seguro e difícil de romper. O domínio do tempo era o segredo do poder dos administradores — e imobilizar os subordinados no espaço, negando-lhes o direito ao movimento e rotinizando o ritmo a que deviam obedecer era a principal estratégia em seu exercício do poder⁶.

Todavia, Bauman diz que, com o advento da pós-modernidade, houve uma mudança radical no arranjo do convívio humano e nas condições sociais sob as quais a política-vida é hoje levada, sendo que o poder se tornou extraterritorial, considerando-se a ampliação dos elementos de disrupção, afirmando que:

Isso dá aos detentores do poder uma oportunidade verdadeiramente sem precedentes: eles podem se livrar dos aspectos irritantes e atrasados da técnica de poder do Panóptico. O que quer que a história da modernidade seja no estágio presente, ela é também, e talvez acima de tudo, pós-Panóptica. O que importava no Panóptico era que os encarregados “estivessem lá”, próximos, na torre de controle. O que importa, nas relações de poder pós-panópticas é que as pessoas que operam as alavancas do poder de que depende o destino dos parceiros menos voláteis na relação podem fugir do alcance a qualquer momento — para a pura inacessibilidade. O fim do Panóptico é o arauto do fim da era do engajamento mútuo: entre supervisores e supervisados, capital e trabalho, líderes e seguidores, exércitos em guerra. As principais técnicas do poder são agora a fuga, a astúcia, o desvio e a evitação, a efetiva rejeição de qualquer confinamento territorial, com os complicados corolários de construção e manutenção da ordem, e com a responsabilidade pelas consequências de tudo, bem como com a necessidade de arcar com os custos⁷.

O pós-panoptico acaba tendo uma interconexão com o mundo distópico idealizado na obra de Orwell⁸, em que os cidadãos ficavam em constante vigilância do Grande Irmão, com o absoluto controle de tudo e todos, inclusive sobre os pensamentos dos indivíduos, sendo que até o pensamento poderia ser criminalizado (thoughtcrime), traduzido como “crimideia” ou “crimepensar”.

Na era do Big Data, faz-se referência ao denominado “trabalhador-transparente-

6 BAUMAN, Zigmund. **Modernidade Líquida**. Rio de Janeiro: Jorge Zahar Ed., 2001, p. 16.

7 *Id.*, 2001, p. 16.

8 ORWELL, George. **1984**. Tradução de Alexandre Hubner, Heloisa Jahn. São Paulo: Companhia das Letras, 2009.

te” ou “trabalhador de vidro”, na medida em que a automatização da captura de dados do empregado pode, em muitos casos, incidir sobre aspectos que fazem parte de sua privacidade e que, portanto, deveriam ser protegidos (MOREIRA, 2016). Tais considerações possuem origem histórica fundada nas práticas adotadas pela polícia secreta do partido nazista alemão (Gestapo), que pretendia transformar os homens no Gläserner Mensch (homem de vidro), transparente e sem segredos, atuando como importante ferramenta para o exercício do totalitarismo, com perseguições e injustas punições de grupos minoritários.

E, como o consentimento do titular é indicado, topograficamente, como a primeira base para tratamento de dados pessoais (art. 7º, I) e dos dados sensíveis (art. 11, I), por muitos, propagou-se a ideia de que, com a obtenção do mesmo, estaria resolvido o problema de justificação do tratamento dos dados nas relações de emprego.

Todas as hipóteses de tratamento, mesmo as mais invasivas e disruptivas, poderiam ser justificadas e fundamentadas na obtenção do consentimento pelo titular do dado, principalmente nas fases pré e pós-contratuais.

No presente artigo, pretende-se demonstrar quais são os riscos e inconvenientes advindos da referida postura e apresentar caminhos interpretativos que poderiam, a depender do caso, justificar o tratamento dos dados necessários para a formação, execução e extinção do contrato de trabalho, com a preservação da autodeterminação informativa do titular do dado.

2. Hipóteses legais para o tratamento de dados pessoais no Brasil

Para que ocorra o tratamento, é imprescindível que esteja presente ao menos uma das hipóteses autorizadoras.

Para os dados pessoais, aquelas previstas no art. 7º da LGPD:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

- I - mediante o fornecimento de consentimento pelo titular;
- II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
- III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
- IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por

profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

E, para os dados sensíveis, as descritas no art. 11 da LGPD:

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

- a) cumprimento de obrigação legal ou regulatória pelo controlador;
 - b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
 - c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
 - d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
 - e) proteção da vida ou da incolumidade física do titular ou de terceiro;
 - f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
 - g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
- Assim, verifica-se que existem várias hipóteses, diversas do consentimento, que podem ser utilizadas para a fundamentação do tratamento de dados na relação de emprego.

3. A precedente discussão europeia

Em 1976, Portugal foi o primeiro país a alçar a nível constitucional o direito fundamental à autodeterminação informativa, conforme o art. 35 do seu texto constitucional.

Por sua vez, na Espanha, em 1978, houve a previsão constitucional do referido direito (art. 18.4).

No ano de 2000, o art. 8º da Carta dos Direitos Fundamentais da União Europeia definiu que “todas as pessoas têm o direito à proteção dos dados de carácter pessoal que lhes digam respeito”.

Em 27 de abril de 2016, foi aprovado o Regulamento 2016/679, que revogou a Diretiva n.º 95/46 da CE, conhecida como GDPR (General Data Protection Regulation), compilando em uma única fonte as diretrizes pertinentes à proteção dos dados pessoais no velho continente.

Em seu art. 88, o GDPR tratou especificamente da questão trabalhista, prevenindo que os Estados-Membros poderiam adotar medidas adequadas e específicas para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados, com especial relevo para a transparência do tratamento de dados, a transferência de dados pessoais num grupo empresarial ou num grupo de empresas envolvidas numa atividade econômica conjunta e os sistemas de controle no local de trabalho.

Na Espanha, por sua vez, foi aprovada a Lei n.º 15.103/2018 (Ley Orgánica de Protección de Datos y garantía de los derechos digitales - LOPDGDD), que passou a estabelecer limites expressos aos poderes de controle empresarial com a finalidade de alcançar o devido respeito pelos direitos fundamentais dos trabalhadores.

Muitos dizem que a LGPD foi inspirada no Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation-GDPR) de 2016, na União Europeia (Regulamento 2016/679).

Entretanto, destaca-se que, na verdade, a legislação brasileira teve início de tramitação em 2012 (PL 4060/12), bem antes da vigência do regulamento europeu.

Importante salientar que a influência inicial da LGPD decorreu das disposições constantes da Diretiva 95/46/CE, que, desde 1995, já regulamentava o tratamento de dados pessoais e a livre circulação desses dados no âmbito da Comunidade Europeia.

As bases de legais de tratamento dos dados pessoais previstas na LGPD, em diversos aspectos, possuem um paralelo com as disposições dos artigos 7º e 8º da Diretiva 95/46/CE.

Desde o advento da Diretiva 95/46/CE, já se discutia no continente europeu a viabilidade da utilização do consentimento como base para o tratamento dos dados pessoais no âmbito da relação de emprego.

Sobre a questão, destaco o posicionamento manifestado pelo Grupo de Trabalho do Artigo 29 – GT29, órgão consultivo criado em razão da Diretiva n.º 95/46 da CE:

Dada a dependência que resulta da relação empregador/empregado, é improvável que o titular dos dados seja capaz de negar ao seu o empregador o consentimento para o processamento de dados sem sentir medo ou risco real de efeitos prejudiciais como resultado de uma recusa. É improvável que um funcionário seja capaz de responder livremente a uma solicitação para consentimento de seu empregador para, por exemplo, ativar sistemas de monitoramento, como observação por câmera em um local de trabalho, ou para preencher formulários de avaliação, sem sentir qualquer pressão para consentimento.

Portanto, o GT29 já considerava problemático o processamento de dados pessoais de empregados ou de futuros empregados com base no consentimento, uma vez que seria improvável que esse consentimento fosse livremente manifestado.

Sobre a legislação europeia e portuguesa, assevera o jurista Nascimento, in verbis:

Apesar de o consentimento poder ser a todo tempo revogado, ao abrigo do disposto no art. 81º, nº 2 do Código Civil, temos muitas dúvidas quanto à eficácia desta norma no âmbito do ambiente laboral, onde os direitos de personalidade se encontram especialmente comprimidos. Talvez tivesse sido mais eficaz que o legislador se limitasse a elencar as situações em que o tratamento de dados dos trabalhadores era permitido, ao invés de colocar a questão exclusivamente dependente de consentimento dos trabalhadores, os quais encontram numa posição especialmente desconfortável para negar essa pretensão ao empregador⁹.

No mesmo sentido, é o posicionamento defendido por Alves, professora da Universidade Autónoma de Lisboa:

No contexto laboral, por norma, o consentimento do trabalhador não é considerado um fundamento válido para o tratamento de dados pessoais, face à finalidade em causa e considerando a posição de dependência e subordinação do trabalhador; entende-se, pois, que este poderá não estar em posição de conceder o seu consentimento nos termos exigidos pelo RGPD, onde se prevê que tal consentimento seja prestado livremente e que seja tão fácil de retirar como de conceder, sem que daí advenham quaisquer consequências para o trabalhador.

O consentimento do trabalhador não é adequado como fundamento de legitimidade para permitir o tratamento de dados pessoais, o fundamento de legitimidade é conferido pela lei laboral, especificamente o n.º 2 do art.º 20.º do Código do Trabalho, que permite em certas circunstâncias a utilização de meios de vigilância à distância no local de trabalho.

A relação empregador-trabalhador é, de um modo geral, considerada uma relação de desequilíbrio, na qual o empregador possui supremacia em relação ao trabalhador. Uma vez que o consentimento tem de ser dado de livre vontade, e tendo em conta a natureza da relação laboral, o empregado não pode, na maioria dos casos, basear-se no consentimento para utilizar os seus dados¹⁰.

Quanto ao consentimento, já se pronunciou a Autoridade Helênica de Proteção de Dados, ao apresentar punição à empresa PricewaterhouseCoopers, em julho de 2019, já na vigência do GDPR, ao pagamento de uma multa de €150.000,00 pelo tratamento ilegal de dados pessoais dos seus empregados, sob o fundamento de que os funcionários da PWC teriam sido obrigados a consentir com o tratamento de dados pessoais.

Na referida autuação, ficou expressamente consignado que: “o consentimento dos titulares dos dados no contexto das relações de trabalho não pode ser considerado como dado livremente devido ao desequilíbrio evidente entre as partes”¹¹.

9 NASCIMENTO, André Pestana. *O impacto das novas tecnologias no direito do trabalho e a tutela dos direitos da personalidade do trabalhador*. Disponível em: https://www.uria.com/documentos/publicaciones/2242/documento/068apa.pdf?id=1948_pt. Acesso em: 05 out. 2020.

10 ALVES, Lurdes Dias. **Proteção de dados pessoais no contexto laboral**: o direito à privacidade do trabalhador. Coimbra: Almedina, 2020, p. 49.

11 Hellenic Data Protection Authority fines Price Waterhouse Coopers 150K for employees' data

Portanto, pode-se verificar que a discussão já possui certo delineamento no continente europeu.

4. A autodeterminação informativa e o consentimento

O primeiro estudo doutrinário que tratou da existência de um direito à privacidade foi escrito por Warren e Brandeis¹², nos idos de 1890, publicado na *Harvard Law Review*, e tinha o título de *The right to privacy*.

Em 1893, o referido direito foi reconhecido pela jurisprudência norte americana, no caso *Marks vs Joffra*, em um caso ajuizado por um estudante de direito contra um jornal que havia publicado uma foto sua sem sua autorização. No julgamento, restou reconhecido o direito à proteção da imagem, bem como o denominado “the right to be let alone” (o direito de ser deixado sozinho).

Não se pretende aqui tratar dos diversos aspectos e extensão do direito à privacidade, entretanto, para o desenvolvimento do raciocínio, importante destacar que, inicialmente, o referido direito foi concebido sob o viés negativo, no sentido de que os cidadãos apenas tinham o direito de não serem incomodados na sua intimidade/privacidade.

Entretanto, com a evolução dos meios tecnológicos e o surgimento de novos riscos, houve a ampliação dos conceitos de reserva à intimidade da vida privada, com a sua expansão como integrante do direito da personalidade, passando a ser oponível erga omnes e, principalmente, assumindo uma nova feição positiva, no sentido de impor um dever geral de respeito, impedindo o acesso a informações relativas à vida privada e proibindo a divulgação dos dados.

Por sua vez, em 1983, a Corte Constitucional da República Federal da Alemanha, no julgamento de uma ação em que se alegava a inconstitucionalidade de uma lei de recenseamento, reconheceu a existência de um direito fundamental à autodeterminação informativa (*Grundrecht auf informationelle Selbstbestimmung*).

Importante salientar que as inovações promovidas pela LGPD em nosso país foram concebidas para a defesa da autodeterminação informativa, implicando em verdadeira ressignificação do direito à privacidade em nosso país.

A autodeterminação informativa, nos dizeres de Canotilho e Moreira, pode ser definida como o direito conferido a cada pessoa de “controlar a informação disponível a seu respeito, impedindo-lhe que a pessoa se transforme em ‘simple objeto de informação.’”¹³.

É também conhecida como privacidade decisional e informacional.

Importantes são as lições de Navarro:

Pode-se falar, dessa forma, no direito à autodeterminação informativa como um direito oponível em face

breach. DataBreaches.net. 30.jul.2019. Disponível em: <https://www.databreaches.net/hellenic-data-protection-authority-fines-price-waterhouse-coopers-150k-for-employees-data-breach>. Acesso em: 31 mar. 2021.

12 BRANDEIS, Louis; WARREN, Samuel. *The right to privacy*. *Harvard Law Review*, v. 4, 1890. Disponível em: <http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm>. Acesso em: 20 jul. 2021.

13 CANOTILHO, José Joaquim Gomes; MOREIRA, Vital. *Constituição da República portuguesa anotada*. 4. ed. Coimbra: Coimbra Editora, 2007, p. 552.

do Estado, para a preservação de ações lesivas, por parte deste (direito de defesa), como também para exigir ações positivas. Com efeito, ‘los derechos a acciones positivas normativas son derechos a atos estatales de creación de normas’, consoante Robert Alexy¹⁴.

No mesmo sentido, Moreira¹⁵ destaca que, embora o direito à autodeterminação informativa tenha como origem a proteção de dados pessoais, é atribuída a ele uma extensão mais ampla, sendo considerado um verdadeiro direito a um controle da informação sobre a vida privada, que diz respeito não apenas à recolha de informação como também à sua divulgação.

Assim, a privacidade, partindo-se da concepção europeia, assume uma nova feição, sendo considerada como o direito de ter controle sobre as suas informações e de determinar a construção de sua própria esfera particular. Inclusive, há teorias que defendem a sua estrutura tridimensional, com a seguinte subdivisão pura: a) decisional; b) informacional; e c) espacial.

A privacidade, em seu aspecto decisional, diz respeito ao modo de vida do indivíduo, englobando, nos dizeres de Peixoto e Ehrhardt Júnior, “suas escolhas, seus gostos, seus projetos, suas características”, estabelecendo “um espaço de manobra no tráfego social que é necessário para a autonomia individual sem que haja interferência alheia”¹⁶.

E ainda, destacam que “a proteção da privacidade em sua dimensão decisional tem um ponto de encontro comum à dimensão informacional. Muitos assuntos que dizem respeito ao modo de viver da pessoa acabam virando dados, os chamados dados sensíveis, cuja proteção é uma das principais preocupações na chamada sociedade da informação”¹⁷.

Por sua vez, pela dimensão informacional, há uma preocupação com a coleta, o processamento, a disseminação e possível invasão de dados pessoais.

Por fim, pela dimensão espacial, o foco é direcionado ao aspecto mais tradicional da privacidade, dizendo respeito à “privacidade do lar, a privacidade de um cômodo da casa, de determinado local físico”¹⁸.

E, nesse contexto, o consentimento nada mais seria do que uma das formas de expressão legítima da autodeterminação informativa.

A LGPD define o consentimento como “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (art. 5º, XII).

14 NAVARRO, Ana Maria Neves de Paula. O direito fundamental à autodeterminação informativa. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=86a2f353e1e6692c>. Acesso em: 05 out. 2020.

15 MOREIRA, Teresa Coelho Alexandra. **Estudos de Direito do Trabalho**. v. 2. Coimbra: Almedina, 2016, p. 2010.

16 PEIXOTO, Erick Lucena Campos e EHRHARDT JÚNIOR, Marcos. Breves notas sobre a re-significação da privacidade. In: **Revista Brasileira de Direito Civil**, Belo Horizonte, v. 16. p. 35-56, abr/jun. 2018.

17 *Id.*, 2018.

18 *Id.*, 2018.

Tratando da legislação brasileira, afirma Maciel:

O consentimento sempre é visto, por muitos, como a panaceia para tratamento de dados pessoais. Com consentimento pode-se quase tudo. Bem verdade, o consentimento é a autorização expressa dada pelo titular ao controlador para que ele possa tratar os dados da forma desejada. No entanto, o consentimento só é válido se atender inúmeros requisitos legais, o que o torna um ônus desnecessário caso o tratamento possa ser validado em uma das outras nove bases previstas no artigo 7º, sem falar que ao titular é garantido o direito de revogação a qualquer tempo¹⁹.

Assim, destaca-se que, quando obtido o consentimento, se o controlador necessitar comunicar ou compartilhar dados pessoais com outros controladores, deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento (art. 7º, §5º).

O consentimento poderá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular (art. 8º, caput), sendo que, se fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais (art. 8º, §1º).

Além disso, cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com a lei (art. 8º, §2º).

A LGPD estabelece expresamente que é vedado o tratamento de dados pessoais mediante vício de consentimento e que deverá se referir a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas (art. 8º, §§3º e 4º).

Outro aspecto importante para a discussão é que o consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular (art. 8º, §5º).

E, se houver alguma alteração no tratamento, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração (arts. 8º, §6º e 9º, §2º).

Nas hipóteses em que o consentimento for requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca (art. 9º, §1º).

Nesse contexto, verifica-se que diversos direitos são atribuídos ao titular e inúmeras condições são impostas para o uso regular do consentimento como base de tratamento, não sendo adequado o seu uso, como padrão, nas relações trabalhistas.

Conforme destaca Delgado, o contrato de trabalho talvez seja “o mais eloquente exemplo de contrato de adesão fornecido pelo mundo contemporâneo, onde o

19 MACIEL, Rafael Fernandes. *Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais* (Lei nº 13.709/18), RM Digital Education, 1ª Edição. Goiânia – GO, 2019, p. 28/29.

exercício da liberdade e vontade por uma das partes contratuais — o empregado — encontra-se em polo extremado de contingenciamento²⁰.

E, diante de tal situação, percebe-se que, em diversos casos, o consentimento poderá não ser prestado de forma idônea.

Assim, seguindo o exemplo europeu, via de regra, não deve ser utilizado como fundamento para o tratamento de dados nas relações trabalhistas, considerando-se o desequilíbrio na relação entre empregador e empregado (imbalance of power).

Além disso, com já salientado, a maior parte dos dados coletados e armazenados em uma relação de emprego são necessários para a execução do contrato, para o cumprimento de obrigações legais ou para defesa em processo judicial ou administrativo.

Se solicitado o consentimento, mesmo quando existente outra hipótese legal de tratamento, poder-se-ia criar uma justa expectativa no trabalhador de que, se este for revogado, o tratamento deixaria de ser realizado.

Eventual modificação posterior da base de tratamento poderia ser considerada como violadora dos limites da boa-fé objetiva, em verdadeiro venire contra fatum proprium e também infringente do princípio da proteção.

A Organização Internacional do Trabalho, em seu Repertório de Recomendações Práticas sobre a Proteção de Dados Pessoais dos Trabalhadores²¹, não afasta a utilização do consentimento, mas destaca que esse deve ser explícito e documentado, devendo ser indicada a finalidade do tratamento dos dados, as fontes e os meios utilizados, o tipo de dados a serem coletados e as consequências, se houver, se o consentimento for negado.

Assim, mesmo que admitido, deverá ser utilizado residualmente, com a observância do regramento imposto pela LGPD, com a devida documentação e, se for o caso, com a garantia de recusa.

Observada alguma das hipóteses de tratamento, para que este seja considerado lícito, é importante que os propósitos sejam legítimos, específicos, explícitos e informados ao titular, sem a possibilidade de tratamento posterior de forma incompatível com essas finalidades (princípio da finalidade).

Precisa existir compatibilidade do tratamento com as finalidades informadas pelo titular, de acordo com o contexto do tratamento (princípio da adequação).

Mesmo quando admitido, o tratamento deve ser limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (princípio da necessidade).

Deve ser garantido o livre acesso aos titulares, com a possibilidade de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais (princípio do livre acesso).

Garantia da qualidade dos dados, com exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade

20 DELGADO, Maurício Godinho. **Curso de direito do trabalho**. 16. ed. São Paulo: LTr, 2017, p. 574.

21 ORGANIZAÇÃO INTERNACIONAL DO TRABALHO (OIT). *Protección de los datos personales de los trabajadores*. Disponível em: https://www.ilo.org/global/topics/safety-and-health-at-work/normative-instruments/code-of-practice/WCMS_112625/lang-es/index.htm. Acesso em: 01 fev. 2021.

de seu tratamento (princípio da qualidade dos dados).

As informações devem ser claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial (princípio da transparência).

Devem ser utilizadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (princípio da segurança), com a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (princípio da prevenção).

Os dados não podem ser utilizados com fins discriminatórios ilícitos ou abusivos (princípio da não discriminação).

E, por fim, deve ser demonstrada a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (princípio de responsabilização e prestação de contas).

Considerações finais

Diante desse contexto, pode-se verificar que o novo sistema imposto pela LGPD, embora tenha trazido várias balizas para o tratamento dos dados pessoais, não impediu que tais dados continuassem sendo coletados e utilizados na seara trabalhista.

A nova legislação inaugurou um modelo de responsabilidade e de conscientização sobre novos parâmetros para proteção da privacidade e dos dados em nosso país.

Assim, antes de se procurar obter o consentimento a qualquer custo, com a utilização de açodados aditivos contratuais, melhor seria que as empresas efetuassem um inventário dos dados tratados em suas atividades corriqueiras, procurando encontrar as bases legais justificadoras do tratamento.

E, se inexistente base legal diversa do consentimento, deveriam verificar a existência da efetiva necessidade de tratamento do dado e a adequação às finalidades apresentadas. Se não preenchidos tais requisitos, o dado deveria ser eliminado, uma vez que é grande a possibilidade de o dado ser discriminatório ou excessivamente invasivo, principalmente em se tratando de dados sensíveis.

Por fim, somente no caso de efetiva necessidade de tratamento, principalmente nos casos em que o tratamento possa trazer benefícios ao trabalhador, deveria ser obtido o consentimento do empregado, tomando todas as cautelas devidas para que a vontade seja manifestada livremente e com a devida documentação.

REFERÊNCIAS

ALVES, Lurdes Dias. Proteção de dados pessoais no contexto laboral: o direito à privacidade do trabalhador. Coimbra: Almedina, 2020.

BRANDEIS, Louis; WARREN, Samuel. The right to privacy. Harvard Law Review, v. 4, 1890. Disponível em: <http://faculty.uml.edu/sgallagher/Brandei-privacy.htm>. Acesso em: 20 jul. 2021.

CANOTILHO, José Joaquim Gomes; MOREIRA, Vital. Constituição da República portuguesa anotada. 4. ed. Coimbra: Coimbra Editora, 2007.

DELGADO, Maurício Godinho. Curso de direito do trabalho. 16. ed. São Paulo: Ltr, 2017.

FOCAULT, Michel. Vigiar e Punir: nascimento da prisão. Tradução de Raquel Ramallete. 42. ed. Petrópolis: Vozes, 2014.

MACIEL, Rafael Fernandes. Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18), RM Digital Education, 1ª Edição. Goiânia – GO, 2019.

MILLER, Jacques-Alain. A máquina panóptica de Jeremy Bentham In: BENTHAM, Jeremy. O panóptico. São Paulo: Autêntica Editora, 2000.

MOREIRA, Teresa Coelho Alexandra. Estudos de Direito do Trabalho. v. 2. Coimbra: Almedina, 2016.

NASCIMENTO, André Pestana. O impacto das novas tecnologias no direito do trabalho e a tutela dos direitos da personalidade do trabalhador. Disponível em: https://www.uria.com/documentos/publicaciones/2242/documento/068a-pa.pdf?id=1948_pt. Acesso em: 5 out. 2020.

NAVARRO, Ana Maria Neves de Paula. O direito fundamental à autodeterminação informativa. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=86a2f353e1e6692c>. Acesso em: 5 out. 2020.

ORGANIZAÇÃO INTERNACIONAL DO TRABALHO (OIT). Protección de los datos personales de los trabajadores. Disponível em: <https://www.ilo.org/global/topics/safety-and-health-at-work/normative-instruments/code-of-practice/WCMS_112625/lang-es/index.htm>. Acesso em: 01 fev. 2021.

HELLENIC Data Protection Authority fines Price Waterhouse Coopers 150K for employees' data breach. DataBreaches.net. 30.jul.2019. Disponível em: <<https://www.databreaches.net/hellenic-data-protection-authority-fines-price-waterhouse-coopers-150k-for-employees-data-breach>>. Acesso em: 31 mar. 2021.

UGUINA, Jesús Mercader. Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica? Revista Relaciones Laborales. n. 10, p. 2, 2001.

**31. DO DIREITO À PRIVACIDADE NO AMBIENTE DE
TRABALHO: PERSPECTIVAS A PARTIR DA LGPD**
*THE RIGHT TO PRIVACY IN THE WORKPLACE:
PERSPECTIVES FROM THE GENERAL DATA PROTECTION LAW*

CAROLINA LITVIN SCALETSKY¹

Resumo

A partir da evolução tecnológica e digital, proporcionada pela Indústria 4.0, são introduzidas novas técnicas utilizadas pelos empregadores para que possam exercer seu poder de fiscalização. Este, decorrente do poder diretivo e do direito à propriedade do empregador, muitas vezes se encontra em tensionamento com o direito à privacidade e à intimidade do trabalhador, figura vulnerável nesse tipo de relação. Diante disso, a presente pesquisa, por meio de um estudo doutrinário e jurisprudencial, pretende analisar situações em que a ponderação entre esses direitos foi realizada para solucionar a colisão existente, como no caso de revista íntima e pessoal, de monitoramento do correio eletrônico e da instalação de câmeras de vigilância no ambiente de trabalho. Ainda, considerando as disposições da Lei Geral de Proteção de Dados, objetiva-se verificar se estas são suficientes para a resolução desse conflito.

Palavras-chave: Direito à privacidade. Relação de trabalho. Lei Geral de Proteção de Dados.

Abstract

From the technological and digital evolution, provided by Industry 4.0, new techniques are used by employers, so that they can exercise their oversight power. This, due to the directive power and the employer's right to property, is often in tension with the employee's right to privacy and intimacy, the vulnerable figure in this type of relationship. Therefore, this research, through a doctrinal and jurisprudential study, intends to analyze situations in which the weighting between these rights was carried out to solve the existing collision, as in the case of an intimate and personal search, electronic mail monitoring and installation of surveillance cameras in the workplace. Still, considering the provisions of the General Data Protection Law, the objective is to verify whether these are sufficient to resolve this conflict.

Keywords: Right to privacy. Employment relationship. General Data Protection Law.

1. Introdução

A colisão entre direitos fundamentais assegurados sem qualquer tipo de hierarquia pela Constituição Federal é sempre uma questão que torna a ser discutida.

¹ Mestranda do Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Rio Grande do Sul - PUCRS. carolina.scaletscky@acad.pucrs.br. Lattes: <http://lattes.cnpq.br/2588580576964885>.

Assim, introduz-se a temática do direito à privacidade do trabalhador no ambiente de trabalho, que estabelece um conflito entre o direito à intimidade e à privacidade do empregado e o direito à propriedade do empregador.

Nesse sentido, utilizando-se do método de ponderação, pretende-se analisar alguns casos em que há o tensionamento entre esses direitos, estabelecendo, assim, um parâmetro razoável para a concretização da privacidade dentro dos limites do poder empregatício.

No que tange à abordagem teórica na elaboração deste trabalho, utilizar-se-á a forma dedutiva - de modo a aplicar as diferentes teorias estudadas aos casos concretos, partindo de uma premissa geral. As técnicas de pesquisa adotadas serão a revisão bibliográfica, de forma a apresentar os entendimentos doutrinários e legais existentes, e coleta de jurisprudência, de modo a verificar a posição do Tribunal Superior do Trabalho acerca do tema.

Sendo assim, em um primeiro momento, será apresentado o direito à privacidade, explicitando seu conceito e classificando-o como direito da personalidade. Posteriormente, será examinado o poder empregatício, de modo a verificar as suas espécies e os seus limites. Na sequência, serão estudados dois casos concretos julgados pelo Tribunal Superior do Trabalho, quais sejam: o monitoramento do correio eletrônico e a instalação de câmeras de vigilância no ambiente de trabalho. Por fim, abordar-se-á alguns aspectos da Lei Geral de Proteção de Dados, a fim de analisar se as suas disposições são suficientes para que haja a proteção de dados do trabalhador.

2. Do direito à privacidade nas relações trabalhistas à luz da LGPD

Atualmente, com a construção de uma Era Digital, as relações jurídicas têm se tornado cada vez mais complexas. Com o surgimento de novos instrumentos jurídicos - tal como o teletrabalho, o qual tem recebido grande adesão por parte das empresas, em especial a partir da situação de pandemia que se instaurou no país e no mundo em meados de março de 2020 -, houve uma mudança no panorama das relações contratuais trabalhistas até então existente.

Assim, os meios de controle e fiscalização do trabalho por parte do empregador foram adaptados para esse novo paradigma, de modo a haver o monitoramento eletrônico dos empregados - seja por meio da supervisão do correio eletrônico, seja por meio da instalação de um sistema de vigilância a distância. Ocorre que o direito fundamental à privacidade deve ser observado nas relações trabalhistas, de modo a impor algumas limitações à inspeção dos trabalhadores a fim de resguardar a sua esfera da vida íntima e privada - a ser analisada no próximo tópico.

2.1 Do direito à privacidade dos empregados

No plano constitucional, o direito à privacidade, considerado como um direito fundamental de primeira dimensão, encontra-se no inciso X, do artigo 5º (BRASIL, 1988), prevendo que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”.

Além disso, é considerado um direito da personalidade, previsto no artigo 21, do Código Civil (BRASIL, 2002): “Art. 21. A vida privada da pessoa natural é in-

violável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma”.

O Marco Civil da Internet (BRASIL, 2014b), nos artigos 10 e 11, faz menção à guarda e à disponibilização dos dados pessoais, devendo observar os direitos da privacidade, intimidade, honra e imagem das pessoas envolvidas.

Apesar dos artigos supracitados se referirem de forma distinta aos direitos à privacidade e à intimidade, cumpre ressaltar que esta é apenas uma decorrência daquela. Isto é, a vida íntima trata-se de uma esfera mais restrita do que a vida privada, mas ambas devem ser analisadas em conjunto, pois não podem ser dissociadas. (SARLET, 2020, p. 461-462).

O direito à privacidade pode ser definido, portanto, como um direito subjetivo inerente à pessoa, consistente na possibilidade de controlar suas informações pessoais e também de constranger terceiros que desrespeitarem sua esfera privada.

Ademais, esse direito pode se apresentar em diferentes categorias: a) a privacidade física; b) a privacidade do domicílio; c) a privacidade das comunicações; d) a privacidade decisional; e e) a privacidade informacional. (VIEIRA, 2007, p. 30-31).

A primeira categoria diz respeito ao direito de não se submeter a procedimentos de caráter invasivo, como, por exemplo, intervenções cirúrgicas, conforme previsão do artigo 15 do Código Civil. O segundo tipo trata da proteção do domicílio, que, via de regra, é inviolável, como prevê o inciso XI, do artigo 5º, da Constituição Federal. A terceira espécie se refere à inviolabilidade das comunicações em geral, de modo a garantir o sigilo das informações nelas constantes, assim como dispõe o inciso XII, do artigo 5º, da Constituição Federal. A quarta modalidade faz referência à possibilidade do indivíduo de tomar suas próprias decisões, a fim de resguardar aquilo que pertence ao seu foro íntimo. A última espécie, por sua vez, faz alusão à possibilidade do indivíduo de controlar e proteger suas informações e seus dados pessoais. (VIEIRA, 2007, p. 32-34).

Evidentemente, apesar de ser um direito fundamental, a privacidade está sujeita a restrições. Samuel Warren e Louis Brandeis (1990, p. 214-215) pontuam que a publicação de assuntos de interesse público ou geral não estaria proibida pela privacidade, uma vez que o objetivo desta é proteger as informações pessoais sobre as quais a sociedade não tem um interesse legítimo no seu conhecimento. Isto é, o objeto da tutela da privacidade é a sua invasão injustificada, que deve ser reprimida e impedida quando possível.

Pablo Stolze e Rodolfo Pamplona Filho (2020, p. 106) advertem acerca dos riscos trazidos pela rede mundial de computadores em relação ao direito à privacidade:

Com o avanço tecnológico, os atentados à intimidade e à vida privada, inclusive por meio da rede mundial de computadores (Internet), tornaram-se muito comuns. Não raro determinadas empresas obtêm dados pessoais do usuário (profissão, renda mensal, *hobbies*), com o propósito de ofertar os seus produtos, veiculando a sua publicidade por meio dos indesejáveis *spams*, técnica, em nosso entendimento, ofensiva à intimidade e à vida privada.

Dessa forma, apesar do direito à privacidade não constar de forma expressa no rol de direitos dos trabalhadores do artigo 7º, da Constituição Federal (BRASIL, 1988), sabe-se que este se trata de rol exemplificativo, de modo a reconhecer a existência de outros direitos que visem à melhoria da condição social do trabalhador. Além disso, o direito à privacidade é um direito fundamental garantido a toda e qualquer pessoa, razão pela qual se torna oponível também em face do empregador, ainda que o trabalhador labore a distância, fazendo uso de meios eletrônicos.

A legislação trabalhista, após sofrer alterações pela Lei 13.467, de 2017, acrescentou alguns dispositivos atinentes à responsabilização do empregador por eventuais danos extrapatrimoniais que ofendam a esfera moral ou existencial dos seus empregados, reconhecendo, no artigo 223-C, os bens juridicamente tutelados inerentes à pessoa física. São eles: “a honra, a imagem, a intimidade, a liberdade de ação, a autoestima, a sexualidade, a saúde, o lazer e a integridade física”.

Sendo assim, o principal desafio a ser enfrentado encontra-se na utilização de meios de fiscalização - ou até mesmo de utilização de dados ou informações pessoais - por parte do empregador mediante a autorização ou consentimento do empregado. Nesse sentido, o próximo tópico abordará o poder diretivo do empregador como um limitador do direito à privacidade do empregado.

2.2 Do poder diretivo do empregador

O poder empregatício ou intraempresarial, enquanto efeito próprio do contrato de trabalho, consiste em uma série de prerrogativas, por parte do empregador, capazes de ordenar a dinâmica da prestação laboral, no que tange à sua direção, regulamentação, fiscalização e disciplina (DELGADO, 2017, p. 749). Isto é, o modo como a atividade do empregado será exercida é determinado pelo empregador, tendo em vista ser este, via de regra, o detentor dos meios de produção.

O artigo 2º, da Consolidação das Leis de Trabalho (BRASIL, 1943), ao conceituar a figura do empregador, reconhece o poder de direção deste: “Art. 2º - Considera-se empregador a empresa, individual ou coletiva, que, assumindo os riscos da atividade econômica, admite, assalaria e dirige a prestação pessoal de serviço”.

Dessa forma, destaca-se o poder diretivo, consistindo este na manifestação do empregador no que diz respeito à organização e à orientação da prestação de serviços, sendo inerentes à relação contratual trabalhista as funções do empregador de “organizar, conduzir, estruturar, pois uma empresa desorganizada tem a sua produtividade e função social, como um todo, comprometidas” (ANDRADE, 2016, p. 207). Assim, torna-se possível visualizar os demais poderes do empregador - especialmente o regulamentar e o fiscalizador - como decorrência do poder de direção.

Ocorre que, assim como qualquer outro tipo de poder, o seu exercício deve ser moderado, de maneira a respeitar os limites impostos pelo ordenamento jurídico, tais como as previsões constitucionais, legais, contratuais e coletivas, observando os direitos fundamentais garantidos ao trabalhador. Nesse sentido, estabelece-se uma ponderação entre o direito de propriedade do empregador e o direito à privacidade do empregado, abrindo margem para debates constantes.

Para exemplificar a situação, cita-se o entendimento de que é vedada a revista íntima dos empregados, de modo a apalpar partes do corpo, com a finalidade de fiscalização, tendo em vista que tal prática é abusiva e enseja o pagamento de inde-

nização por danos morais. Veja-se:

RECURSO DE REVISTA. INTERPOSTO APÓS A ÉGIDE DA LEI 13.015/2014. INDENIZAÇÃO POR DANO MORAL. REVISTA ÍNTIMA. TOQUE NO CORPO DO TRABALHADOR PELOS VIGILANTES DA EMPRESA. CONFIGURAÇÃO. A relação de emprego não pode servir de fundamento para que o poder empresarial menospreze o balizamento constitucional relativo à preservação da intimidade. Constata-se ofensa à intimidade e procedimento abusivo atinente à revista pessoal, em que o trabalhador é constrangido a exhibir partes do corpo com apalpação pelos vigilantes. É permitido ao empregador utilizar todos os meios necessários à fiscalização de seu patrimônio, desde que não invada a intimidade dos empregados. O poder de direção previsto no art. 2º da CLT deve ser exercido sem abuso e com atenção ao art. 187 do Código Civil. Há precedentes. Recurso de revista conhecido e provido. (BRASIL. Tribunal Superior do Trabalho, 2019)

Em contrapartida, demonstra-se plenamente possível a revista pessoal feita nos pertences dos empregados, como em suas bolsas, sacolas e armários, desde que não haja contato físico e seja observado o princípio da razoabilidade. Isto é, a revista pessoal deve ser feita em caráter geral - de forma indiscriminada - e por motivo relevante. Veja-se:

AGRAVO DE INSTRUMENTO EM RECURSO DE REVISTA. PROCEDIMENTO SUMARÍSSIMO. INDENIZAÇÃO POR DANOS MORAIS. ASSÉDIO MORAL. RESTRIÇÃO AO USO DO BANHEIRO E REVISTAS PESSOAIS. [...] não há como concluir pela existência de danos morais passíveis de indenização, conforme sustentado pela reclamante, sendo que, especificamente em relação à revista pessoal, esta Corte Superior entende que a mera inspeção visual nos pertences do empregado, como bolsas e sacolas, realizada sem exposição vexatória, contato físico ou caráter discriminatório, hipótese dos autos, não configura, por si só, ato ilícito, constituindo, na realidade, exercício regular do direito do empregador, inerente ao seu poder de direção e fiscalização. Ilesos os dispositivos constitucionais apontados. Agravo de instrumento conhecido e não provido. (BRASIL. Tribunal Superior do Trabalho, 2020a)

Nesse sentido, a subordinação do empregado ao empregador, bem como o fato deste deter o poder diretivo, não constituem justificativa plausível para a ineficácia da tutela à intimidade no local de trabalho (BRASIL, 2014a, p. 242). Em verdade, o poder diretivo não existe em função de um capricho do empregador, uma vez que apresenta como fundamento a boa organização do trabalho na empresa. Dessa forma, as limitações a esse poder decorrem do princípio da dignidade da pessoa humana e dos direitos da personalidade do empregado. (RUARO; HAINZENREDER JÚNIOR, 2015, p. 611-612)

Há, contudo, situações em que se vislumbra verdadeiro conflito entre os direitos mencionados, a serem analisadas, a partir de casos concretos, no próximo tópico, sobretudo em função da evolução tecnológica e digital, que, cada vez mais, propicia novos meios de prestação do serviço - como é o caso do teletrabalho - e de fiscalização eletrônica - como é o caso do monitoramento de e-mails.

2.3 Do monitoramento eletrônico e o direito à privacidade

Tendo em vista a colisão entre os direitos fundamentais à privacidade e à pro-

priedade, serão analisados dois casos pontuais, a fim de que sejam traçadas algumas conclusões a respeito desse conflito: o monitoramento do correio eletrônico e a fiscalização do ambiente de trabalho por meio da instalação de câmeras de vigilância.

No que diz respeito ao monitoramento do correio eletrônico, em um primeiro momento, faz-se necessária a diferenciação entre e-mail pessoal e e-mail corporativo, para que, na sequência, sejam examinadas as possíveis soluções.

O e-mail pessoal do empregado, como o próprio nome sugere, é aquele voltado às suas comunicações diárias pessoais, ou seja, aquelas relacionadas aos seus amigos, familiares e relações amorosas (ARAUJO, 2002, p. 112). Sustenta-se, assim, que o e-mail pessoal tem natureza jurídica de correspondência, sendo constitucionalmente garantida, pelo inciso XII, do artigo 5º (BRASIL, 1988), a inviolabilidade do seu sigilo.

Nesse sentido, caso o empregador intente que seus empregados não utilizem o e-mail pessoal durante o horário de trabalho ou no ambiente deste, torna-se possível o bloqueio do acesso ao conteúdo indesejado por meio de programas de computador. Ademais, uma vez que isso seja acordado previamente e o empregado insista em desrespeitar essas limitações, o poder diretivo do empregador poderá se manifestar em sua vertente disciplinar, aplicando alguma penalidade em razão do descumprimento das regras do contrato de trabalho. (ALVARENGA, 2013, p. 30)

O e-mail corporativo, por sua vez, constitui instrumento de trabalho, sendo necessário para a realização de tarefas laborais, como a comunicação entre os funcionários ou entre estes e os seus superiores. Nesse caso, o e-mail geralmente é grafado com o domínio da empresa, de modo que o empregado apenas o utilizará para fins laborais, cessando o seu acesso no caso de desligamento da empresa (ARAUJO, 2002, p. 110). Dessa forma, o e-mail corporativo não é o ambiente adequado para que o empregado envie ou receba mensagens de cunho pessoal, relacionadas à sua esfera íntima ou privada.

Além disso, a empresa poderá ser responsabilizada por eventuais danos causados em virtude do encaminhamento de e-mails por seus empregados, conforme interpretação da Súmula 341, do Supremo Tribunal Federal (BRASIL, 1963): “É presumida a culpa do patrão ou comitente pelo ato culposo do empregado ou preposto”. No mesmo sentido, o inciso III, do artigo 932, do Código Civil (BRASIL, 2002), dispõe que será responsabilizado civilmente “o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele”. Assim, torna-se necessário o monitoramento do correio eletrônico por parte da empresa - como forma de evitar a responsabilização por culpa *in vigilando* ou *in eligendo* -, sendo a extensão dessa fiscalização a questão mais problemática.

Para tanto, sugere-se a necessidade de ciência prévia do empregado de que seu e-mail corporativo deve ser utilizado única e exclusivamente para fins profissionais, tendo a possibilidade deste ser monitorado. Nessa esteira, o poder disciplinar do empregador deve ser exercido em observância ao princípio da boa-fé, sendo razoável exigir que este informe os seus funcionários acerca dos limites objetivos do uso do correio eletrônico (AIETA, 2006, p. 66-67). O Tribunal Superior do Trabalho (BRASIL, 2015) já se manifestou nesse sentido, de modo a afastar a expectativa de privacidade do empregado quando este for previamente informado

acerca da fiscalização do e-mail corporativo:

AGRAVO DE INSTRUMENTO. RECURSO DE REVISTA. JUSTA CAUSA. PROVA ILÍCITA. Nenhum dos dispositivos declinados como violados, incluindo-se o art. 5º, XII, da CF, disciplina a matéria inerente à ilicitude da prova para que se possa reputar violado. Além disso, a ilicitude da obtenção da prova pressupõe inobservância de norma disciplinadora, o que não sucedeu. Sob o prisma de violabilidade do sigilo dos e-mails, tampouco há falar em violação do art. 5º, XII, da CF, por se tratar de e-mail corporativo e não privado, meio de comunicação disponibilizado pelo empregador apenas para uso profissional conforme normas internas de conhecimento do empregado e com “expressa previsão de gravação e monitoramento do correio eletrônico, ficando alertado que o colaborador não deve ter expectativa de privacidade na sua utilização (item 6.1 - fl. 176)”, conforme notícia o acórdão regional. [...]

No que tange à instalação de câmeras de vigilância no ambiente de trabalho, esta se dá como decorrência do poder fiscalizatório do empregador, geralmente com a finalidade de controle da atividade laboral e também por questões de segurança - a fim de resguardar o estabelecimento e as pessoas que nele se encontram -, podendo servir como prova em eventual demanda judicial. Contudo, a fiscalização jamais poderá ser efetivada no que diz respeito a aspectos íntimos dos empregados, tal como em banheiros ou vestiários, ou, ainda, em ambientes destinados ao descanso, como os refeitórios. O Tribunal Superior do Trabalho (BRASIL, 2020b) já se manifestou nesse sentido:

RECURSO DE REVISTA DA RECLAMADA. AÇÃO CIVIL PÚBLICA AJUIZADA PELO MINISTÉRIO PÚBLICO DO TRABALHO. TUTELA INIBITÓRIA. MONITORAMENTO DAS ATIVIDADES DOS EMPREGADOS POR MEIO DE CÂMERA. PODER FISCALIZATÓRIO DO EMPREGADOR. AUSÊNCIA DE ILICITUDE DA CONDUTA. 1. Trata-se de Ação Civil Pública em que o Ministério Público do Trabalho denuncia irregularidades praticadas pela reclamada, relativas à vigilância constante de seus empregados por meio de câmeras instaladas em suas dependências, com exceção dos banheiros. [...] 4. Contudo, o monitoramento dos empregados no ambiente de trabalho por meio de câmera, sem qualquer notícia no acórdão do Tribunal Regional a respeito de excessos pelo empregador, tais como a utilização de câmeras espãs ou a instalação de câmeras em recintos que fossem destinados ao repouso dos funcionários ou que pudessem expor partes íntimas dos empregados, como banheiros ou vestiários, não configura ato ilícito, inserindo-se dentro do poder fiscalizatório do empregador. 5. Nessa medida, não é possível exigir que a empregadora desative as câmeras de vigilância. 6. Configurada a ofensa ao art. 2º da CLT.

A fiscalização remota, decorrente da instalação de dispositivos tecnológicos de controle e rastreamento, por sua vez, torna-se ainda mais temerária quanto à violação aos direitos da privacidade e da intimidade, tendo em vista que, na maioria das vezes, o trabalhador sequer tem conhecimento do modo e por quem está sendo fiscalizado (BURMANN, 2011, p. 113). Dessa forma, a evolução tecnológica tem incrementado rapidamente os mecanismos de controle a distância, sobre os quais Maria Regina Gomes Redinha (2005, p. 2) pontua:

Tecnologias que vieram redefinir ou diluir as noções de tempo e local de trabalho e que ameaçam constantemente a conservação de uma esfera pessoal e até a integridade do trabalhador: lembremos actuais instrumentos de gestão tão invasivos como o *peeking*; os sensores de cadeira que medem e registam o tempo durante o qual o trabalhador permanece sentado no seu posto; os sensores do automóvel que indicam as distâncias percorridas, o consumo de combustível, paragens para descanso etc.; as placas de identificação com chip incorporado; ou testes tão agressivos da privacidade e reserva pessoal, como o mapeamento cerebral ou o rasteio genético.

Novamente, em qualquer caso, a ciência dos trabalhadores - por meio do reglamento da empresa ou instrumentos de negociação coletiva - de que estes estão sendo monitorados constitui requisito de legitimidade desse procedimento. Além disso, entende-se que a adoção de tal medida deveria se fundar em motivos relevantes, como a preservação do patrimônio e da integridade física daqueles que ambientam o local de trabalho, e não somente com o objetivo de vigiar o comportamento do trabalhador. (RUARO; HAINZENREDER JÚNIOR, 2015, p. 619).

Uma vez analisados alguns casos concretos em que há a colisão entre o direito à privacidade do empregado e o poder diretivo do empregador, passa-se a examinar as perspectivas de futuro a partir da Lei Geral de Proteção de Dados.

2.4 Da concretização do direito à privacidade a partir da Lei Geral de Proteção de Dados

Para que se tenha uma melhor compreensão acerca do tema, faz-se necessária a conceituação de dados pessoais. Sendo assim, primeiramente, cabe diferenciar informações pessoais de dados pessoais, visto que alguns autores tratam essas expressões de maneiras distintas.

As informações pessoais são aquelas referentes às características, como o nome ou domicílio, ou ações de uma pessoa, como opiniões ou hábitos de consumo, de modo a revelar algo sobre esta, por meio de um vínculo objetivo. Sendo assim, não são abarcadas por esse conceito as informações que não têm como objeto a própria pessoa, apesar de com esta terem relação, como, por exemplo, as opiniões de outrem sobre essa pessoa. (DONEDA, 2011, p. 93).

Diferentemente das informações pessoais - que têm como pressuposto uma etapa em que a elaboração do conteúdo de certa informação já foi iniciada -, os dados pessoais podem ser definidos como “pré-informações”, ou seja, informações referentes a uma pessoa suscetíveis de serem colhidas, arquivadas ou transferidas a terceiros. Isto é, os dados estão situados em uma etapa anterior às informações, uma vez que a interpretação e o processo de elaboração destas ainda não foi iniciado. (DONEDA, 2011, p. 94).

Com o advento da Lei Geral de Proteção de Dados (BRASIL, 2018), o conceito foi positivado no ordenamento jurídico brasileiro, no inciso I, do artigo 5º, sendo dado pessoal a “informação relacionada a pessoa natural identificada ou identificável”.

Faz-se menção, ainda, aos dados sensíveis - subcategoria de dados pessoais -, que são considerados aqueles cujo conteúdo, uma vez conhecido, apresenta mais riscos ao seu titular. São exemplos: dados referentes à religião, opinião política, raça, opção sexual, entre outros. Seu conceito encontra-se positivado no inciso II, do artigo 5º, da Lei Geral de Proteção de Dados (BRASIL, 2018):

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

No plano constitucional, a proteção do sigilo de dados apresenta respaldo no inciso XII, do artigo 5º (BRASIL, 1988):

XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

A proteção de dados, portanto, consiste no direito fundamental de um indivíduo ter resguardadas as informações relacionadas aos seus direitos de personalidade, que compreendem os direitos próprios, inerentes à pessoa, tanto físicos como morais - como a vida, o nome, a imagem e a honra.

Considerando que diversos são os mecanismos existentes para obter informações pessoais dos empregados e utilizá-las - por exemplo, como forma de facilitar a etapa de contratação pelo empregador ou então para fins de aferição da capacidade profissional do empregado (Accioly, 2018, p. 258) -, estas passam a ser tratadas como um bem jurídico, de modo a necessitar de uma tutela por parte do Estado.

Dessa forma, é possível vislumbrar a incidência da Lei Geral de Proteção de Dados em três momentos distintos: a) na fase pré-contratual; b) ao longo da relação de trabalho; e c) após o término da relação trabalhista.

No que tange à etapa de contratação, geralmente há a coleta e o armazenamento de dados dos candidatos a partir das entrevistas e da análise curricular. Assim, o tratamento de dados deve se limitar à finalidade para a qual se propôs inicialmente, de modo a se ater às informações que sejam necessárias para a avaliação da capacidade técnica do candidato para ocupar a vaga ofertada, bem como o seu atendimento aos requisitos exigidos para o cargo ou função, evitando-se a coleta de dados que possam estimular a discriminação (Giroldo; Machado, 2020, p. 115-116). Nesse sentido, necessária é a observância aos princípios da finalidade (de modo que o tratamento de dados atenda aos propósitos legítimos, específicos, explícitos e informados ao titular), da adequação (para que haja compatibilidade do tratamento com as finalidades informadas ao titular) e da necessidade (limitação do tratamento ao mínimo necessário para a realização de suas finalidades), previstos no artigo 6º da lei. (BRASIL, 2018).

No que diz respeito ao tratamento de dados durante a relação de emprego, a coleta e o armazenamento geralmente têm o intuito de aumentar a produtividade do trabalho. Além disso, a solicitação de outras informações pelo empregador, necessárias à manutenção do contrato de trabalho, tem respaldo legal no inciso II, do artigo 7º (BRASIL, 2018). São exemplos: o endereço eletrônico e o número de telefone do empregado (para fins de comunicação), bem como o número dos seus documentos pessoais (para fins de identificação e cadastramento).

Torna-se imperiosa a observância do princípio da não discriminação, que veda a utilização de dados para fins ilícitos ou abusivos. Com isso, pretende-se evitar distinções de tratamento entre funcionários, tendo em vista alguma informação

de caráter pessoal. Nesse sentido, não há como impedir o acesso pelo empregador, por exemplo, às redes sociais dos seus trabalhadores, visto que tais informações foram tornadas públicas por estes. Contudo, não se admite o uso dessas informações com o objetivo de tratar de forma distinta um trabalhador tão somente em virtude de suas convicções pessoais, uma vez que estas não guardam relação com a execução do serviço (Burmans, 2011, p. 110)

Outro aspecto importante reside no fato do trabalhador ter consentido ou não com o tratamento de seus dados, tendo em vista que este só será legítimo quando houver o seu consentimento, conforme disposição do inciso I, do artigo 7º, da lei protetiva (BRASIL, 2018). Ocorre que, por se tratar de figura vulnerável, o trabalhador muitas vezes cede às imposições do empregador com receio de sofrer represálias. Sendo assim, é necessária uma avaliação da validade do consentimento conferido, de acordo com os filtros constitucionais de interpretação dos direitos trabalhistas, uma vez que a LGPD, apesar de exigir o consentimento, não determina padrões objetivos para a aferição do consentimento válido. (Accioly, 2018, p. 261-262).

Por fim, em se tratando do período pós-contratual, a manutenção dos dados do trabalhador pelo empregador se justifica em caso de exercício de direito em processo judicial, administrativo e arbitral, devendo algumas informações serem mantidas em caráter permanente, tendo em vista que têm reflexo em direitos dos trabalhadores que podem vir a se manifestar anos após o término da relação trabalhista, como é o caso do direito à aposentadoria. (Giroldo; Machado, 2020, p. 118).

Por conseguinte, com base no que foi exposto, é possível constatar que a Lei Geral de Proteção de Dados estabeleceu diversos parâmetros para o tratamento legítimo dos dados pessoais, devendo tais disposições incidir sobre o direito do trabalho, embora ainda apresente algumas lacunas nesse sentido. Dessa forma, caberá à doutrina e à jurisprudência traçar uma definição mais restritiva desses conceitos - como no caso do consentimento válido -, de modo a adequá-los às relações de trabalho.

Considerações finais

Ante o exposto, viu-se que o direito à privacidade é um direito da personalidade que assegura o controle de informações pessoais e a possibilidade de constringer terceiros que desrespeitem a esfera privada do indivíduo. O avanço tecnológico, por sua vez, possibilitou a criação de novas técnicas utilizadas pelos empregadores, a fim de que estes possam melhor exercer o seu poder de fiscalização, decorrente do poder diretivo e do direito à propriedade que estes ostentam, por serem os detentores dos meios de produção.

Ocorre que, em diversas vezes, há a colisão entre esses direitos, por representarem interesses contrários. Assim, ao analisar alguns casos específicos, tornou-se possível a constatação de algumas considerações. No caso da revista dos trabalhadores, o entendimento é de que a revista íntima não é legítima, pois o fato de expor o corpo dos trabalhadores a uma inspeção constitui prática abusiva. Diferente é o caso da revista pessoal, realizada nos bens dos funcionários, como bolsas, sacolas e armários, sem contato físico, visto que faz parte da fiscalização pelo empregador.

Em se tratando de monitoramento do correio eletrônico, a solução se dá a partir da classificação deste como sendo pessoal ou corporativo. No primeiro caso

(e-mail pessoal), não há que se falar em fiscalização, tendo em vista que está protegido pelo direito à privacidade. Contudo, no caso do e-mail corporativo, tendo em vista que este pertence à empresa, sendo utilizado como instrumento de trabalho, esta tem o direito de exercer o poder fiscalizatório.

No que tange às câmeras de vigilância, a possibilidade de instalação reside na finalidade de segurança do estabelecimento e das pessoas que nele se encontram. Entretanto, a instalação em ambientes de repouso ou em locais em que presume-se a intimidade dos trabalhadores, como em banheiros e vestiários, resta proibida.

Em se tratando de um direito fundamental, que decorre de outros direitos da personalidade, a proteção de dados pessoais merece atenção principalmente no âmbito do direito do trabalho, tendo em vista a presença de uma parte vulnerável nesse tipo de relação.

Os dados pessoais, como já foi visto, diferenciam-se de informações pessoais. Estas têm como pressuposto uma etapa em que a elaboração do conteúdo de certa informação já foi iniciada, enquanto aqueles situam-se em uma etapa anterior. Isto é, os dados pessoais consistem em informações referentes a uma pessoa suscetíveis de serem colhidas, arquivadas ou transferidas a terceiros.

Ainda, é possível, segundo alguns autores, reconhecer a proteção de dados como um direito fundamental, de modo que essa classificação se dá a partir de uma interpretação conjunta de diversos princípios e diplomas normativos, tais como os direitos à intimidade e à vida privada, bem como a dignidade da pessoa humana.

Pretendeu-se, por fim, analisar a incidência da Lei Geral de Proteção de Dados em três momentos distintos: a) na fase pré-contratual, em que os dados são colhidos em entrevistas ou em análises curriculares; b) ao longo da relação trabalhista, em que os dados são armazenados para fins de identificação do trabalhador e aumento de sua produtividade; e c) após o término da relação contratual, em que a manutenção dos dados se justifica em caso de exercício de direito em processo judicial, administrativo e arbitral.

Em qualquer caso, torna-se necessária a observância dos princípios elencados pela lei, tais como a boa-fé objetiva, a não discriminação e a exigência de consentimento do trabalhador para que seus dados sejam colhidos, armazenados e mantidos. Ocorre que, por receio de sofrer represálias, o trabalhador muitas vezes cede às imposições do empregador, caso em que o consentimento nem sempre será dotado de autonomia.

Conclui-se, portanto, que a legislação vigente acerca do tema, apesar de conter disposições no sentido de tutelar a proteção de dados, ainda apresenta um certo risco para o trabalhador, principalmente no que tange ao consentimento quanto ao tratamento de seus dados pessoais, visto que a LGPD não determina padrões objetivos para a aferição do consentimento válido. Cumpre ressaltar que esta pesquisa não tem o intuito de exaurir as questões abordadas, e sim contribuir para o debate do tema estudado, promovendo, assim, uma reflexão acerca do direito à privacidade do trabalhador no ambiente de trabalho.

REFERÊNCIAS

ACCIOLY, Clara Lacerda. A proteção de dados do trabalhador: o direito do

trabalho constitucionalizado e seu diálogo com o direito à privacidade. **Revista Dos Estudantes De Direito Da Universidade De Brasília**, n. 15, p. 255 - 264, 2018.

AIETA, Vânia Siciliano. A violação da intimidade no ambiente de trabalho e o monitoramento eletrônico dos empregados. **Revista de Direito Constitucional e Internacional**, v. 55, p. 60-88, abr./jun. 2006.

ALVARENGA, Rúbia Zanotelli. Direitos da personalidade do trabalhador e correio eletrônico. **Revista do Tribunal Regional do Trabalho do Paraná**, v. 2, p. 8-36, 2013.

ANDRADE, Emanuela Machado. A revista pessoal no ambiente de trabalho em face das garantias que envolvem a relação de emprego. **Revista dos Tribunais**, v. 965, p. 201-224, mar. 2016.

ARAUJO, Luiz Alberto David. A correspondência eletrônica do empregado (e-mail) e o poder diretivo do empregador. **Revista de Direito Constitucional e Internacional**, v. 40, p. 96-121, jul./set. 2002.

BRASIL, Deilton Ribeiro. Proteção à intimidade e privacidade do empregado no ambiente de trabalho. In: MEZZAROBÀ, Orides. *et al* (coord.). **Direito do trabalho**. Curitiba: Clássica, 2014a.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 24 out. 2021.

BRASIL. **Decreto-Lei nº 5.452, de 1º de maio de 1943**. Aprova a Consolidação das Leis do Trabalho. Rio de Janeiro: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm>. Acesso em: 24 out. 2021.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm>. Acesso em: 24 out. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm>. Acesso em: 24 out. 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014b**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 24 out. 2021.

BRASIL. Supremo Tribunal Federal. **Súmula nº 341**. É presumida a culpa do patrão ou comitente pelo ato culposo do empregado ou preposto. Brasília, DF: Supremo Tribunal Federal, [1963]. Disponível em: <<https://jurisprudencia.stf.jus.br/pages/search/seq-sumula341/false>>. Acesso em: 24 out. 2021.

BRASIL. Tribunal Superior do Trabalho (6. Turma). **Recurso de Revista nº 10861-98.2013.5.03.0028**. Relator: Min. Augusto Cesar Leite de Carvalho. Brasília, 20 de novembro de 2019. Disponível em: <<https://jurisprudencia-backend.tst.jus.br/rest/documentos/1e0116d863ca71d6ec06702be4affbcd>>. Acesso em:

24 de out. 2021.

BRASIL. Tribunal Superior do Trabalho (8. Turma). **Agravo de Instrumento em Recurso de Revista nº 20633-39.2018.5.04.0204**. Relatora: Min. Dora Maria da Costa. Brasília, 24 de junho de 2020a. Disponível em: <<https://jurisprudencia-backend.tst.jus.br/rest/documentos/24818e23aff07bfc4097bb3e68931431>>. Acesso em: 24 de out. 2021.

BRASIL. Tribunal Superior do Trabalho (3. Turma). **Agravo de Instrumento em Recurso de Revista nº 1461-48.2010.5.10.0003**. Relator: Min. Alexandre de Souza Agra Belmonte. Brasília, 25 de fevereiro de 2015. Disponível em: <<https://jurisprudencia-backend.tst.jus.br/rest/documentos/274b3fbbee5e39de26a6b-c6edee7885f>>. Acesso em: 24 de out. 2021.

BRASIL. Tribunal Superior do Trabalho (1. Turma). **Recurso de Revista nº 21162-51.2015.5.04.0014**. Relator: Min. Hugo Carlos Scheuermann. Brasília, 26 de agosto de 2020b. Disponível em: <<https://jurisprudencia-backend.tst.jus.br/rest/documentos/208df9f1031ef78345c6c908dccb7e78>>. Acesso em: 24 de out. 2021.

BURMANN, Marcia Sanz. **A concretização da privacidade do empregado no ambiente de trabalho**. 2011. 159 f. Dissertação (Mestrado em Direito) – Faculdade de Direito. Universidade de São Paulo, São Paulo.

DELGADO, Maurício Godinho. **Curso de direito do trabalho**. 16. ed. São Paulo: LTr, 2017.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

GIROLDO, Andrea Gardano Bucharles; MACHADO, Daniela Cunha. A proteção da informação no âmbito das relações de emprego e o impacto da aplicação da LGPD aos contratos de trabalho no Brasil. **Revista de Direito e as Novas Tecnologias**, v. 6, p. 113-126, jan./mar. 2020.

REDINHA, Maria Regina Gomes. Os direito de personalidade no Código do Trabalho: actualidade e oportunidade da sua inclusão. In: _____. **A Reforma do Código do Trabalho**, Coimbra Editora, 2005.

RUARO, Regina Linden; HAINZENREDER JÚNIOR, Eugênio. Proteção da privacidade no contrato de trabalho: da normatização legal a situações de conflito. **Espaço Jurídico Journal of Law**, Joaçaba, v. 16, n. 2, p. 601-634, jul./dez. 2015.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. 9. ed. São Paulo: Saraiva, 2020.

STOLZE, Pablo; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil**. 22. ed. São Paulo: Saraiva, 2020.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. Porto Alegre: Sergio Antonio Fabris Editor, 2007.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **The Harvard Law Review Association**, Cambridge (The United States), v. 4, n. 5, p. 193-220, dec. 1890.

32. A RELAÇÃO TRABALHISTA SOB O VIÉS DA PROTEÇÃO DE DADOS E PRIVACIDADE: DUE DILIGENCE DE CANDIDATOS E EMPREGADOS, INCIDENTES COM DADOS PESSOAIS E POSSÍVEL REPARAÇÃO A DANOS

THE LABOR RELATIONSHIP UNDER THE BIAS OF DATA PROTECTION AND PRIVACY: DUE DILIGENCE OF CANDIDATES AND EMPLOYEES, INCIDENTS WITH PERSONAL DATA AND POSSIBLE REPAIR OF DAMAGE

FLÁVIA ALCASSA¹ E ADRIANNE LIMA²

Resumo

É objetivo geral deste artigo analisar os riscos, bem como pontuar possíveis medidas mitigadoras a empregadores decorrentes da vigência da Lei Geral de Proteção de Dados Pessoais - LGPD. Será realizada uma revisão de literatura e os dados serão interpretados pelo método qualitativo. Concluiu-se que é necessária a adoção de boas práticas para a governança de dados dos trabalhadores com o intuito de não os deixarem em uma posição de vulnerabilidade para evitar passivos trabalhistas, demandas perante o MPT e na Justiça do Trabalho, bem como eventuais sanções administrativas pela atuação da Autoridade Nacional de Proteção de Dados – ANPD. Também é importante que se registre que não há nenhuma intenção de esgotar o assunto, pois outros debates surgirão envolvendo questões de privacidade e aspectos da LGPD no âmbito laboral.

Palavras-chave: LGPD. Contrato de Trabalho. Justiça do Trabalho. Due Diligence.

Abstract

The general objective of this article is to analyze the risks, as well as to point out possible mitigating measures, to employers arising from the validity of the General Law on Personal Data Protection - LGPD. A literature review will be carried out and data will be interpreted by the qualitative method. It was concluded that it is necessary to adopt good practices for the governance of workers' data in order not to leave them in a position of vulnerability to avoid labor liabilities, demands before the MPT and the labor courts, as well as any administrative sanctions by the performance of the National Data Protection Authority – ANPD. It is also important to note that there is no intention to exhaust the subject, as other debates will arise involving privacy issues and aspects of the LGPD in the workplace.

Keywords: LGPD. Employment Contract. Work justice. Due Diligence.

1 Flávia Alcassa. Pós-graduada em Direito Digital e Proteção de Dados. Advogada, Sócia do escritório Alcassa & Pappert Advogados. Membro do comitê jurídico da ANPPD* Associação Nacional dos Profissionais de Privacidade de Dados, certificada pela EXIN Privacy and Data Protection. flavia@alcassapappert.adv.br

2 Adriane Lima. Mestre em Administração pela Mackenzie. MBA em Gestão pela ESALQ/USP. Advogada. Consultora em Proteção de Dados e Privacidade. Professora convidada na pós-graduação *lato sensu* na Universidade Mackenzie e PUC Campinas. Diretora do Comitê Jurídico da ANPPD. adriane.accl@gmail.com

1. Introdução

A proteção de dados é um direito humano que nasce vinculado à Declaração Universal dos Direitos Humanos, aprovada pela Assembleia Geral das Nações Unidas em 1948, com o objetivo de garantir a dignidade do ser humano e como instrumento de combate à opressão, impunidade e insultos à dignidade humana.

No Brasil, no panorama mundial de privacidade, encontramos a proteção da privacidade, da intimidade e da vida privada expressa na Constituição Federal em seu art. 5º, e em outras leis como o Marco Civil da Internet, Lei n.º 12.965/2014, com normas de proteção e segurança à privacidade de dados das pessoas. Com o avanço da tecnologia e necessidade de uma lei específica mais criteriosa, em 14 de agosto de 2018, após inúmeros debates e emendas foi publicada a Lei n.º 13.709 e alterações da Lei n.º 13.853, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). Buscou-se um equilíbrio na manutenção do desenvolvimento econômico e tecnológico, com a adoção da inviolabilidade dos direitos constitucionais dos cidadãos, representando um importantíssimo marco regulatório para o Brasil sobre o tema.

É objetivo geral deste artigo analisar a vigência da lei e os riscos da judicialização dos assuntos da Lei Geral de Proteção de Dados.

Em relação à estrutura, inicia-se com a introdução e a descrição do tema e dos objetivos da pesquisa. No capítulo 2, apresenta-se o desenvolvimento teórico do artigo. Por fim, serão apresentadas as conclusões obtidas e as referências bibliográficas utilizadas.

2. A relação trabalhista sob o viés da proteção de dados e da privacidade

O tratamento de dados pessoais ocorre quando há o recebimento e acesso a dados constantes em currículos de candidatos, na coleta de informações e documentos adicionais para o processo de admissão de um empregado, na manutenção do contrato de trabalho, até com o compartilhamento de dados pessoais de empregados com alguns órgãos públicos, como a Receita Federal ou devido a alguns programas, como o e-Social.

O empregador, muitas vezes, realiza uma atividade com dados pessoais de empregados não somente porque deseja compreender melhor com quem está lidando, mas também por uma questão de que a organização deve cumprir algumas obrigações legais, como a de recolhimento de imposto de renda na fonte, por exemplo.

O titular de dados pessoais, segundo a LGPD, é o empregado. Vale destacar que a Autoridade Nacional de Proteção de Dados Pessoais – ANPD (2021) já se posicionou afirmando que empregados, administradores e sócios não são agentes de tratamento, mas podem ser titulares, dependendo do tratamento de dados analisado:

Daí decorre que não são controladoras as pessoas naturais que atuam como profissionais subordinados a uma pessoa jurídica ou como membros de seus órgãos. É o caso de empregados, administradores, sócios, servidores e outras pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta. Nesse sentido, a de-

finição legal de controlador não deve ser entendida como uma norma de distribuição interna de competências e responsabilidades. De forma diversa, trata-se de comando legal que atribui obrigações específicas à pessoa jurídica, de modo que esta assume a responsabilidade pelos atos praticados por seus agentes e prepostos em face dos titulares e da ANPD.

Lima, Montes, Samaniego (*et al*, 2021, p. 127) sinalizam algumas boas práticas a empregadores para o cumprimento da LGPD, dentre elas:

No que concerne, por exemplo, à ficha de registro (que, por vezes, poderão conter dados pessoais sensíveis, tais como filiação a sindicato), por força da lei de proteção de dados brasileira, será necessário limitar o seu acesso e garantir que o seu armazenamento se dará de forma segura. O mesmo raciocínio se aplica aos atestados médicos, apesar da ausência de obrigatoriedade do preenchimento do CID (Classificação Internacional de Doenças), tendo em vista que sempre haverá a possibilidade de identificação da doença ou das razões que ensejaram o afastamento, demandando, dessa forma, uma política robusta que possa assegurar o sigilo desses dados, considerados sensíveis pela LGPD.

Outro ponto importante se refere à obrigatoriedade legal de exames periódicos. A NR7, ou Norma Regulamentadora nº 7.145, determina a obrigatoriedade de implementação, em todas as instituições e empresas, do Programa de Controle Médico de Saúde Ocupacional (PCMSO), cujo objetivo primordial reside na preservação da saúde dos colaboradores e funcionários, independentemente da quantidade, do grau de risco de trabalho e, ainda, do setor econômico envolvido.

Com cunho preventivo, o programa não deve acarretar quaisquer ônus para os trabalhadores e requer um plano de ação cuja execução deve se dar durante todo o ano exigindo, ainda, um relatório anual, que conterà a discriminação do número e da natureza dos exames médicos e, ainda, das avaliações clínicas e exames complementares requeridos.

Sobre a guarda e descarte, as autoras recomendam:

Com isso o suporte de recursos de tecnologia para a verificação dos principais processos (coleta, uso e guarda dos dados) é o meio mais adequado e seguro, da mes-

ma forma, seguir os normativos e regulamentos internos da organização trará maior segurança organizacional.

Quando falamos em manter os dados dos empregados ou parceiros, uma das primeiras ações é identificar quais são as informações que estão sob a responsabilidade e de que forma estão armazenadas na organização, bem como o tempo de guarda necessário destes dados. Isso porque, legalmente, por questões trabalhistas e previdenciárias é necessária a guarda de dados pessoais para resguardo de futuras solicitações administrativas e legais e, neste caso, o prazo mínimo de guarda das informações é de 5 anos.

A manutenção, obrigatória, de dados pessoais está prevista no artigo 16 da LGPD e, ainda que haja um pedido de exclusão de dados ou apagamento de colaboradores, parceiros ou ex-colaboradores, poderá ser justificada a recusa de conclusão do procedimento de exclusão ou apagamento, com base no artigo aqui indicado, desde que, de fato, haja a necessidade de manutenção desses dados sob o controle da organização e, neste caso, do controlador de dados.

2.1 O *due diligence* de candidatos e empregados

Segundo Leão (2012), o *due diligence* é realizado de maneira a abranger todas as áreas de uma empresa, principalmente as áreas societária, imobiliária, ambiental, contábil, jurídica, entre outras.

Dentre outros diversos exemplos, a organização pode criar processos internos para identificar se há, eventualmente, “caixa dois”, se os terceiros com quem vai se relacionar são “empresas de fachada”, se seus colaboradores adotam determinadas práticas que podem ser decorrentes pelo acesso de informação interna privilegiada, por exemplo.

Algumas dessas práticas de *due diligence* são chamadas de *know your customer* - KYC, *know your employee* - KYE e *know your partner* - KYP, em que são criados questionários e instruções para a solicitação ou análise de informações e evidências em relação a clientes, empregados e parceiros de negócio.

O *due diligence* é entendido como um serviço que melhora a qualidade de informações para os empresários tomarem suas decisões nos negócios, pois por meio dele a alta gestão cerca-se de informações que a ajuda a fazer a melhor escolha, evitando-se, assim, os maus negócios (Panosso, 2013).

Geralmente, as empresas também realizam controles e investigações internas como uma prática para evitar problemas futuros com prejuízos à imagem da organização, aos negócios ou, mesmo, a incidência de multas administrativas ou judiciais decorrentes de atos de corrupção ou concorrência desleal.

Ainda sobre as vantagens em se “estar em *compliance*”, segundo Bellinetti e Souza (2019, p. 12), “o *compliance* relacionado à seara laboral, além de estar em consonância com a função social e a responsabilidade socioambiental da empresa,

agrega valor à entidade empresarial e atrai consumidores, investidores e parceiros, proporcionando um aumento significativo do lucro”.

As investigações internas carregam uma certa problemática, isso porque pode ser difícil compreender quais situações são limítrofes à violação do direito à privacidade de pessoas, como exemplo: candidatos a trabalho, empregados, prestadores de serviço, sócios de organizações com as quais a empresa se relaciona, dentre outros.

O direito à privacidade encontra-se positivado na Constituição Federal em seu artigo 5º, X, que abrange o direito à intimidade, à vida privada, à honra e à imagem:

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

Não obstante a referida garantia constitucional, em situações de emprego a pessoa está sob o poder de direção do empregador, diante da subordinação. Por isso e diante da responsabilidade do empregador, por atos cometidos por seus empregados, constante no artigo 932, III, do Código Civil, são colocados em prática mecanismos de controle e investigação interna de trabalhadores.

Por não haver um limite claro e definido em lei sobre quais mecanismos são permitidos e quais não são em relações de trabalho, é recomendado que o empregador sempre informe seus empregados sobre as finalidades dos controles e investigações internas, seja ao concorrer a uma vaga de trabalho ou utilizar equipamentos da organização, bem como científicá-lo sobre a ausência de expectativa de privacidade.

Algumas informações são imprescindíveis à formalização do contrato de trabalho, como, por exemplo: nome completo, RG e CPF (para identificá-lo no contrato), endereço (para fins de vale-transporte), número e idade dos filhos (para fins do salário-família), experiência anterior e informações inerentes à atividade pretendida, com base no Código Civil e na Lei Geral de Proteção de Dados Pessoais – LGPD.

No entanto, a depender de cada contexto, poderá ser considerada conduta abusiva do empregador pedir informações ao candidato ao emprego relativas à sua religião, filiação política ou preferências sexuais ou pedir antecedentes dos pais ou parentes próximos (Felker, 1996).

Segundo João Teixeira Filho (1996),

Para obter maiores informações do candidato pode o empregador requerer que seja utilizada várias formas, como, por exemplo, análise de curriculum vitae, referências pessoais, entrevistas, testes grafológicos, exames médicos e psicotécnicos. Estes devem ser utilizados apenas para a seleção do candidato que será contratado, não podendo passar da razoabilidade e pertinência destas informações, caso contrário será caracterizado ofensa à honra, à intimidade e à moral do empregado, gerando com isto dano e direito a indenização.

Sobre a identificação de danos em relações de trabalho, o Tribunal Superior do Trabalho aponta no sentido de que:

O dano existencial nas relações do trabalho caracteriza-se pelo tolhimento da autodeterminação do indivíduo, inviabilizando a convivência social e frustrando seu projeto de vida, ocorrendo quando “o trabalhador sofre dano/limitações em relação à sua vida fora do ambiente de trabalho em razão de condutas ilícitas praticadas pelo empregador, impossibilitando-o de estabelecer a prática de um conjunto de atividades culturais, sociais, recreativas, esportivas, afetivas, familiares, etc”. (TST, Processo: RR 14439420125150010, Relatora Maria de Assis Calsing, Julgamento: 15.04.2015, 4ª Turma, DEJT 17.04.2015).

O Tribunal Superior do Trabalho – TST já se posicionou, em diversas oportunidades, com favorecimento à organização que é transparente a titulares em relação às suas práticas, inclusive de *due diligence*, isso é: um candidato a emprego deve conhecer quais serão os critérios que podem favorecer – ou não – a sua contratação, bem como a continuidade do seu contrato de trabalho. Também outro aspecto observado é a razoabilidade da informação utilizada, se faz sentido com o cargo que a pessoa exerce(rá) ou não.

Dessa forma, o ideal é observar o caso a caso, sempre prezando pelos princípios elencados no artigo 6º da Lei n.º 13.709/2018, bem como demais obrigações legais.

O importante é haver transparência nas práticas realizadas pelas organizações, desde o processo de seleção de candidatos até a continuidade na relação de trabalho. Assim, é garantida ao titular de dados a informação sobre quais métodos seus dados pessoais e perfil comportamental vão ser tratados – de forma automatizada ou não – pela organização, cabendo a este aceitar, ou não, fazer parte.

2.2 Da exposição dos dados pessoais nas relações de trabalho

A relação de trabalho constitui uma fonte inesgotável de dados pessoais, e no tocante à proteção de dados pessoais nas relações empregatícias um dos pontos que merecem maior atenção é o atinente à categoria dos dados pessoais sensíveis. A Constituição Federal do Brasil de 1988 protege os direitos da personalidade do trabalhador e a sua condição de dignidade:

Artigo 5º. [...] Inciso X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação; [...] (BRASIL, 1988).

No campo infraconstitucional do Direito do Trabalho brasileiro, o art. 1º, da Lei n.º 9.029/95, proíbe a adoção de qualquer prática discriminatória e limitativa para efeito de acesso à relação de emprego, ou sua manutenção, por motivo de sexo, origem, raça, cor, estado civil, situação familiar ou idade, ressalvadas, neste caso, as hipóteses de proteção ao menor, previstas no inciso XXXIII, do art. 7º, da Constituição Federal de 1988.

O direito à privacidade teria por objeto os comportamentos e acontecimentos

atinentes aos relacionamentos pessoais em geral, às relações comerciais e profissionais que o indivíduo não deseja que se espelhem ao conhecimento público. O objeto do direito à intimidade seriam as conversações e os episódios ainda mais íntimos, envolvendo relações familiares e amizades mais próximas (MENDES *apud* BRANCO, 2007, p. 367)

No tocante à Lei Geral de Proteção de Dados Pessoais (LGPD), o art. 5º considera que:

II - Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Os dados de saúde dos trabalhadores são considerados como dados sensíveis e, embora já protegidos pelo sigilo médico (código de ética médica, no art. 73), merecem muita atenção quanto ao armazenamento e divulgação de informações do quadro clínico, tais como: divulgação de doenças, atestados, exames médicos, divulgação de informações de compra de medicamentos, convênios e utilização do plano de saúde, por exemplo, além do armazenamento seguro das informações sensíveis por parte do empregador.

O Repertório de Recomendações Práticas de Proteção de Dados Pessoais do Trabalhador da Organização Internacional do Trabalho - OIT sugere que a coleta de dados médicos deve se restringir às informações que são necessárias para determinar se o trabalhador está apto para determinado posto de trabalho; se pode cumprir com os requisitos de segurança e saúde do trabalho; e, mais, se pode ter direito a prestações sociais.

2.3 Danos morais por vazamento de dados sensíveis

Como exemplo de prática ilícita de exposição de dados pessoais sensíveis de funcionários, cita-se a decisão de julho de 2020 dos julgadores da Segunda Turma do TRT-MG, que, sem divergência, mantiveram sentença proferida pela 24ª Vara do Trabalho de Belo Horizonte.

A juíza convocada Maria Cristina Diniz Caixeta entendeu que, pelas provas colhidas, ficaram claros os danos morais em virtude da exposição indevida da intimidade do trabalhador. A Justiça do Trabalho determinou que a empresa pague indenização por danos morais a um ex-empregado do setor administrativo que teve seus dados sigilosos expostos no sistema interno de informação da empresa. Um trabalhador da companhia confirmou no processo que, ao fazer pesquisa no sistema, deparou-se com o relatório médico do autor da ação, com a indicação de que ele tinha pensamentos suicidas e era usuário de cocaína. O empregado declarou que foi vítima de constrangimentos e humilhações. Ele relatou que, em 2015, passou por problemas pessoais com quadro de depressão e sofreu acidente fora do local de trabalho, resultando em afastamento do trabalho. Explicou que todos os relatórios e exames médicos privados estavam livres para acesso de qualquer em-

pregado. Na visão do trabalhador, ocorreu invasão de privacidade em decorrência da publicidade dos dados sigilosos. A própria empresa reconheceu a fragilidade do sistema. E que “qualquer empregado poderia pegar as informações sobre atestados e laudos médicos por meio de senha individual e que todos possuíam esse acesso”. Depoimento de testemunha comprovou que os atestados médicos ficavam em pastas de acesso público. Segundo ela, ao procurar sua própria pasta, acabou se deparando com o relatório do autor do processo. Ela informou, ainda, que comunicou o fato ao trabalhador e que enviou um e-mail à empresa questionando a exposição do documento, que posteriormente foi retirado do sistema. Para a juíza convocada Maria Cristina Diniz Caixeta, a conduta da empresa revelou o dano sofrido, já que a exposição de dados de cunho pessoal certamente causou dano moral ao autor (ITATIAIA, 2020, p.1).

E, diante das provas, a magistrada reforçou que não via elementos capazes de afastar o direito do reclamante à reparação por dano moral. A julgadora manteve o valor fixado para a indenização, de três salários do trabalhador, por entender que o montante atende à finalidade de atenuar as consequências da lesão jurídica e reveste-se de razoabilidade.

Notadamente, temos uma decisão reforçando a importância de boas práticas e governança de proteção de dados pessoais pelos empregadores, visando a proteção do empregado no âmbito laboral e mitigando o risco para os direitos e liberdades cuja probabilidade e gravidade podem ser variáveis nas operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação.

Importante destacar que a Justiça do Trabalho há muitos anos vem proferindo decisões que envolvem primordialmente as questões de privacidade dos empregados, sendo que a entrada da LGPD reforçará a importância deste tema no dia a dia das relações contendo exposição e uso indevido de dados pessoais.

Jurisprudência de uso indevido de dados pessoais:

DIVULGAÇÃO DE DADOS PESSOAIS PELO EMPREGADOR. INDENIZAÇÃO POR DANOS MORAIS. A exposição de dados pessoais do trabalhador pelo empregador, fora das hipóteses de permissão legal e dos limites da razoabilidade, gera constrangimentos decorrentes da imediata afetação da intimidade e vida privada do laborista, valores resguardados constitucionalmente (art. 5o, X, da CF), ensejando a indenização por danos morais pretendida (arts. 186 e 927 do CC). (TRT-3 - RO: 00116538520175030101 0011653-85.2017.5.03.0101, Relator: Sebastiao Geraldo de Oliveira, Segunda Turma).

RECURSO ORDINÁRIO - DANOS MORAIS - CONFIGURAÇÃO. 1. Apurado nos autos que o tomador de serviços, *in casu*, Estado de Pernambuco, foi o responsável pelo constrangimento sofrido pelo autor em razão

da divulgação de comunicado, por parte da Secretaria de Educação, exposto nos murais de escolas da rede estadual de ensino, contendo fotos e dados pessoais do demandante, atribuindo-lhe a prática de furto de componentes de computadores, sem qualquer prova cabal de sua autoria, deve este, unicamente, ser condenado no pagamento da indenização por danos morais, excluindo-se da relação processual a real empregadora Provider Soluções Tecnológicas Ltda. 2. Recurso ordinário parcialmente provido para deferir a indenização por danos morais. (TRT-6 - RO: 1056200701706005 PE 2007.017.06.00.5, Relator: Maria Clara Saboya A. Bernardino, Data de Publicação: 28/11/2008).

DIVULGAÇÃO DE CONTRACHEQUE EM SÍTIO ELETRÔNICO DA RECLAMADA, CONSTANDO NÃO APENAS A REMUNERAÇÃO E O CARGO DA AUTORA, MAS, TAMBÉM, DADOS PESSOAIS E PRIVADOS. EXTRAPOLAÇÃO DO QUE PREVÊ A LEI 12.527/2011, LEI DA TRANSPARÊNCIA. INDENIZAÇÃO POR DANOS MORAIS DEVIDA. O caso em epígrafe versa sobre pedido da autora, que é servidora pública municipal, de indenização por danos morais em razão de publicação feita pela municipalidade empregadora no site www.salesopolis.sp.gov.br/portal, de seu holerite constando não apenas a divulgação do seu cargo e valor de sua remuneração, mas, também, recibo de pagamento com dados bancários, descontos de farmácia, valor de empréstimos contratados, pensão alimentícia, entre outros. Matéria que se fulcra no conflito entre a disposição constitucional acerca da transparência dos atos públicos e o princípio da dignidade da pessoa humana, que a Lei nº. 12.527/11 dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do parágrafo 3º do art. 37 e no parágrafo 2º do art. 216 da Constituição Federal. Verificadas as normas constitucionais e legais que regem o tema e analisando o presente caso concreto, reputo que a forma como foi aplicada a Lei da Transparência (Lei 12.527/11) pelo Município reclamado extrapolou o regramento proposto e própria intenção do legislador, vez que o acesso dos usuários a registros sobre atos de governo não pode violar a intimidade do servidor, trazendo a público dados de sua vida privada, atingindo sua intimidade, sua honra, sua imagem e até mesmo a segu-

rança pessoal. Dessa forma, em tendo restado constatada a divulgação de dados pessoais e confidenciais, como detalhes do contracheque e débitos consignados em folha e outros encargos, juntamente com a divulgação do cargo e da remuneração da autora, evidencia-se que houve exposição indevida da intimidade da servidora, trazendo a público dados de sua vida privada, atingindo sua intimidade, sua honra e sua imagem, o que configura a conduta ilícita praticada pela ré, gerando para esta a obrigação de indenizar. (TRT-2 - RO: 00005472120145020373 SP 00005472120145020373 A28, Relator: MARIA ISABEL CUEVA MORAES, Data de Julgamento: 16/12/2014, 4ª TURMA, Data de Publicação: 16/01/2015)

O empregador, por sua vez, estará sujeito a inúmeros riscos com consequências, vejamos: uma ação trabalhista com pleito de obrigações de fazer ou não fazer por práticas discriminatórias na obtenção ou no uso da informação relativa ao empregado, ou dano moral individual ou coletivo por práticas discriminatórias quanto as que são de algum modo ilícitas (vazamento de dados pessoais sigilosos) poderá ser procedente com indenizações pecuniárias de danos morais e materiais, podendo inclusive a expedição de ofícios denunciativos pelo juiz para averiguação da conduta ilícita da empregadora pela Autoridade Nacional de Proteção de Dados (ANPD), que concomitantemente fará sua análise do descumprimento da LGPD, podendo aplicar multas de até 2% do faturamento da empresa (limitada a 50 milhões de reais), entre outras penalidades (advertência, suspensão, publicização etc). O Ministério Público do Trabalho poderá ser envolvido na hipótese de repercussão social com riscos aos empregados, podendo inclusive determinar a feitura de um Termo de Ajustamento de Conduta (TAC).

A LGPD afirma no *caput* de seu artigo 42:

O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

E no parágrafo 3º, os danos coletivos, sejam materiais ou morais:

As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do *caput* deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

O art. 5º, X, da Constituição da República prevê que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a

indenização pelo dano material ou moral decorrente de sua violação”. (BRASIL, 1988).

Tal previsão é justamente um conceito amplo a respeito da privacidade, que foi baseado na previsão genérica do art. 12 da Declaração Universal dos Direitos Humanos, que dispõe:

“Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.” (ONU, 2019, p.01).

Sobre a questão do próprio conceito de privacidade, Marcel Leonardi (2012) indica quatro acepções discutidas em sede doutrinária e jurisprudencial: o primeiro é de que a privacidade é relativa ao direito de ser deixado só (*right to be left alone*); o segundo é o resguardo contra interferências alheias; o terceiro, de que a privacidade seria equivalente a um segredo ou sigilo; e por fim, a tutela de privacidade seria o controle sobre informações e dados pessoais. Em que pesem tais conceitos unitários sobre privacidade, o autor propõe que a proteção da privacidade deve ser considerada pelo viés de direito de personalidade e como direito fundamental, cuja base é o princípio da dignidade da pessoa humana.

2.4 Encarregado de dados (DPO) – perigos do desvio ou acúmulo de função

Com o advento das leis de proteção de dados e privacidade (LGPD e GDPR), surge uma nova profissão, o encarregado de dados, nos termos da lei brasileira, um ponto que merece atenção, conhecido como Data Protection Officer (DPO) perante a GDPR na EU, peça chave para adequação e conformidade com atribuições nos termos da Lei, art. 41, § 2º e art. 50, que dita:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados.

Lima e Alves (2021, p. 114-115) ensinam que:

A LGPD não descreve a forma como a contratação pode – ou deve – ocorrer, sendo que, mais uma vez, é possível buscar referências internacionais de como é possível considerar no cenário de proteção de dados e privacidade.

O GDPR, conforme previsão do artigo 37º, n. 6, permite que o DPO seja uma pessoa empregada da controladora (responsável pelo tratamento), da operadora (subcontratante) ou exerça as suas atribuições com base em um contrato de prestação de serviços, ou seja, como um DPO externo – ou como é conhecido “*DPO as a service*”.

A terceirização do serviço também pode ser de parte do trabalho envolvido no contexto da proteção de dados e privacidade.

A LGPD não prevê, especificamente, sobre as relações de trabalho, mas a CLT dispõe que ocorre desvio de função quando o empregado exerce outra função, sem que haja o pagamento do salário respectivo. O desvio cria o direito ao pagamento das diferenças salariais enquanto houver o exercício da função.

Já o acúmulo de função ocorre quando o trabalhador, além de sua função, exercer outras funções de outros cargos, de forma habitual, imputando ao trabalhador novas tarefas que exigem o exercício de atividade de qualidade superior ao do cargo contratado. Só serão lícitas as alterações nos contratos de trabalho segundo o artigo 468 do CLT por mútuo consentimento, e mesmo assim não poderá gerar nenhum prejuízo ao empregado.

Art. 468 – Nos contratos individuais de trabalho só é lícita a alteração das respectivas condições por mútuo consentimento, e ainda assim desde que não resultem, direta ou indiretamente, prejuízos ao empregado, sob pena de nulidade da cláusula infringente desta garantia.

Em geral, as empresas têm nomeado seus encarregados internos. Resta saber se com adoção ou não de ajustes salariais, aditivos contratuais com a anuência do empregado para a mudança etc. O empregador, por cautela, deverá rever o contrato de trabalho com o indicado para a função de encarregado de dados (DPO), incluir e revisar as obrigações elencadas na LGPD e, se o caso do desvio for apontado, remunerá-lo de acordo com as práticas de mercado para profissionais da área de proteção de dados. A função de encarregado demanda alto nível de exigência, governança e boas práticas, razão pela qual o desvio de função sem nenhuma contraprestação, só o “ônus sem o bônus”, poderá ser judicializada.

A LGPD não possui uma definição clara quanto ao acúmulo de funções ou sobre conflito de interesses dos cargos de DPO. No mês de setembro do ano corrente,

em desconformidade com a GDPR, a Autoridade Belga de Proteção de Dados (DPA) tomou a decisão de multar uma empresa em 50 mil euros, por nomeação inadequada de seu Oficial de Proteção de Dados (DPO). Segundo a DPA, havia conflito de interesse nos papéis exercidos pelo profissional, constituindo violação do artigo 38.6 do GDPR.

Art. 38 GDPR - Posição do oficial de proteção de dados-6. O responsável pela proteção de dados pode cumprir outras tarefas e deveres. O responsável pelo tratamento ou processador deve assegurar que tais tarefas e deveres não resultem em conflito de interesses.

Devido a um incidente de segurança, a DPA realizou investigações quanto às práticas da empresa em relação a proteção de dados. Em conclusão, foi constatada a impossibilidade da acumulação de funções do Chefe de Conformidade, Risco e Auditoria, também nomeado DPO. Por ser a mesma pessoa exercendo as duas funções, ficaria impossibilitado ao DPO supervisionar independente das atividades de tratamento de dados pessoais realizada pelo chefe de conformidade.

A decisão da Autoridade Belga, apesar de ainda estar sujeita a recurso, abre precedente ao caso (GDPR e LGPD). Para as empresas menores, que por muitas vezes não têm a possibilidade de ter uma área autônoma para o DPO, fica o desafio de implementar mecanismos que possibilitem lidar com acúmulo de função e conflitos de interesse que poderão surgir.

Conforme citado acima, a multa da autoridade belga, elemento importante da estrutura da função do encarregado (DPO), é sobre a prevenção de conflitos de interesse. Por exemplo: o encarregado não pode ser responsável por monitorar a si próprio, por configurar parcialidade ou cumular suas funções com a de Gerente/ Diretor (TI, *Compliance*, etc.).

Lima, Peck, Alcassa *et al.* (2021) orientam que:

O ideal, seja DPO interno ou DPO *as a service*, é contar com um time híbrido que permita o desenvolvimento de atividades que demandam a análise técnica-jurídica, como: advogados, programadores, cientista de dados, DPO cyber com formação em Página 9 de 12 ciber segurança. Isso ocorre nos projetos relacionados ao *compliance* LGPD, mas também relacionados à proteção de patentes, *Big Data*, combate à fraude eletrônica, combate às *fake news*, entre outros, há também a colaboração da multidisciplinariedade desses profissionais para a análise de riscos e a elaboração de documentação técnica necessária para dar suporte ao diagnóstico e às recomendações jurídicas.

É comum, na prática jurídica, haver essa sinergia entre as diversas capacitações. Isso acontece, também, em

outras áreas, como o advogado especialista em direito tributário que conta com o suporte de equipe híbrida de contador e analistas financeiros, por exemplo.

No Brasil, a Autoridade Nacional de Proteção de Dados (ANPD) poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado (DPO), inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados. Uma empresa pode ter tanto um funcionário contratado como CLT ou contratar o serviço prestado por outra pessoa jurídica.

Cada contrato e situação poderá prever um determinado direito se não for corretamente verificado, dessa forma nota-se que no Brasil está ocorrendo uma evolução no que diz respeito à proteção dos dados pessoais, com novas funções e atribuições para o tratamento correto dos dados.

2.5 Rescisão indireta

A não observância de qualquer disposição da Lei Geral de Proteção de Dados implicará em responsabilidade exclusiva do EMPREGADOR, podendo inclusive ensejar nas penalidades de rescisão indireta pelo EMPREGADO nos termos do artigo 483 da CLT, d) não cumprir o empregador as obrigações do contrato.

Considerações finais

Concluiu-se que se fazem necessárias as adoções de boas práticas para a governança de dados dos trabalhadores com o intuito de não os deixarem em uma posição de vulnerabilidade para evitar passivos trabalhistas, demandas perante o MPT e fiscalizações da Autoridade Nacional de Proteção de Dados – ANPD.

Também é importante que se registre que não há nenhuma intenção de esgotar o assunto, pois outros debates surgirão na Justiça do Trabalho envolvendo questões de privacidade.

Encontraremos debates no âmbito da dupla penalidade quando da vigência da ANPD com penalidades na esfera administrativa e na esfera judicial. Nota-se que o foco das demandas trabalhistas está dirigido ao exercício dos poderes do empregador e aos direitos da personalidade do empregado, que indica o uso indevido, práticas discriminatórias e abusivas dos dados do trabalhador e diferenças salariais por acúmulo ou desvio de função.

Não pretendemos esgotar aqui esse assunto, acredita-se que a realização de uma pesquisa de campo poderá gerar resultados mais abrangentes.

REFERÊNCIAS

ANPD – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. 2021.

BELLINETTI, L; DE SOUZA, R. **Compliance trabalhista: uma análise a partir da função social da propriedade e da responsabilidade socioambiental da empresa**. Direitos Fundamentais & Justiça | Belo Horizonte, ano 13, n. 40, p. 221-238, jan. /jun. 2019 Disponível em: <http://dfj.emnuvens.com.br/dfj/article/>

LEÃO, Leandro. **Due diligence**: arma eficaz de prevenção jurídica para o empreendedor. São Paulo: Amorim & Leão Advogados, 2012.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012.

LIMA, A.; ALVES, D. **Encarregados - Data Protection Officer - DPOs exigidos pela LGPD - Lei Geral de Proteção de Dados**. São Paulo: Haikai Editora, 2021. ISBN: 978-65-86334-88-3. Disponível em: <https://haikaieditora.com.br/produto/encarregados-data-protection-officer-dpo/>

LIMA, A.; PECK, P.; ALCASSA, F.; *et al.* (2021). **Advogados - encarregados (DPO interno e DPO as a service) nos programas de governança em privacidade (LGPD)**. Migalhas. Disponível em: <https://www.migalhas.com.br/depe-so/345714/advogados--encarregados-dpo-interno-e-dpo-as-a-service>.

LIMA, A.; SAMANIEGO, D.; BARONOVSKY, T.; MONTES, Damarys; *et al.* **LGPD para Contratos: adequando contratos e documentos à Lei Geral de Proteção de Dados**. São Paulo, Editora Saraiva, 2021. ISBN: 978-65-5559-768-4. Disponível em: https://www.amazon.com.br/LGPD-para-contratos-Adequando-documentos-ebook/dp/B09BZNS4GG/ref=sr_1_1?__mk_pt_BR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&dchild=1&keywords=lgp-d+e+contratos&qid=1628523947&s=books&sr=1-1

PANOSSO, M. S. **Responsabilidade pré-contratual por omissão dolosa na realização da due diligence societária**. Porto Alegre: Universidade Federal do Rio Grande do Sul, 2013.

REGULAMENTO GERAL SOBRE PROTEÇÃO DE DADOS – 75. Disponível em: <https://www.privacyregulation.eu/pt/r75.htm>. Acesso em: 5 nov. 2020.

TEIXEIRA FILHO, João de Lima. **O dano moral no Direito do Trabalho. Trabalho e Doutrina**. São Paulo. Saraiva, n.10, 1996, p.28.

33. LEI GERAL DE PROTEÇÃO DE DADOS: RESPONSABILIDADE PATRONAL NO TRATAMENTO DE DADOS PESSOAIS E SENSÍVEIS DO TRABALHADOR

*GENERAL DATA PROTECTION LAW: EMPLOYER'S RESPONSIBILITY FOR
THE PROCESSING OF PERSONAL AND SENSITIVE DATA OF THE WORKER*

RODRIGO GOLDSCHMIDT¹ E MAX ANTÔNIO SILVA VIEIRA²

Resumo

O presente artigo científico tem como objetivo investigar as repercussões da Lei Geral de Proteção de Dados (Lei nº 13.709/18) no que se refere à responsabilidade civil do empregador pelo acesso e tratamento de dados pessoais e sensíveis dos trabalhadores. É notório que no decorrer da relação de emprego, até mesmo nos momentos anteriores à contratação, o empregado fornece inúmeros dados ao empregador, que figura como agente de tratamento de dados. A posição em que o empregado se encontra, submetido às ordens e ao poder patronal, por vezes impossibilita a negativa do fornecimento dos seus dados pessoais. Nesse sentido, a coleta, tratamento, destinação, modificação e exclusão não autorizada de dados pessoais dos trabalhadores representa potencial lesão a direitos de personalidade, como a privacidade e intimidade, entendidos como Direitos Fundamentais no ordenamento jurídico brasileiro. Desta forma, propõe-se que o instituto da responsabilidade civil, bem como os princípios e normas de Direito do Trabalho, possam conjuntamente com a Lei Geral de Proteção de Dados e outras normas correlatas, sem prejuízo da necessária evolução das tecnologias de comunicação e informações, construir um microsistema de proteção dos dados pessoais e sensíveis dos trabalhadores, prevenindo ou reprimindo eficazmente danos à intimidade e privacidade dos mesmos. Emprega-se, no presente estudo, o método dedutivo, conduzido pela técnica de procedimento monográfico subministrada pela pesquisa bibliográfica e documental.

Palavras-chave: Lei Geral de Proteção de Dados. Responsabilidade civil. Direitos da personalidade do trabalhador.

Abstract

This scientific article aims to investigate the repercussions of the General Data Protection Law (Law No. 13.709/18) with regard to the employer's civil liability for accessing and processing workers' personal and sensitive data. It is clear that during the employment relationship, even before hiring, the employee provides numerous data to the employer, who appears as a data processing agent. The position in which the employee finds himself, subject to orders and

1 Pós-Doutor em Direito pela PUC/RS. Mestre e Doutor em Direito pela UFSC. Professor e Pesquisador do Mestrado Acadêmico em Direito da UNESC - PPGD/UNESC. Membro pesquisador do NUPED/UNESC. Juiz do Trabalho Titular de Vara do TRT12. rodrigo.goldschmidt@trt12.jus.br

2 Mestrando em Direito pela UNESC. Especialista em Direito Previdenciário e do Trabalho pela UNICNEC/RS. Membro pesquisador do NUPED/UNESC. Advogado. Assessor Jurídico Municipal. adv.maxvieira@gmail.com

to the employer's power, sometimes makes it impossible to deny the provision of his personal data. In this sense, the unauthorized collection, processing, destination, modification and deletion of workers' personal data represents potential damage to personality rights, such as privacy and intimacy, understood as Fundamental Rights in the Brazilian legal system. In this way, it is proposed that the civil liability institute, as well as the principles and norms of labor law, may together with the General Data Protection Law and other related norms, without prejudice to the necessary evolution of communication and information technologies, build a microsystem to protect workers' personal and sensitive data, effectively preventing or repressing damage to their intimacy and privacy. In this study, the deductive method is used, conducted by the technique of monographic procedure provided by bibliographic and documentary research.

Keywords: General data protection law. Civil responsibility. Rights of the worker's personality.

1. Introdução

As relações socioeconômicas sofreram forte alteração nos primórdios do século 21 através do grande avanço tecnológico vivenciado de forma expressiva e contínua, em especial com o desenvolvimento de tecnologias digitais, que permitem a rápida transmissão de informação a nível global. As expressões "sociedade da informação" e "Big Data" foram cunhadas para descrever esse novo paradigma, onde a economia não mais se baseia nos insumos industriais, mas na coleta e tratamento contínuos de imensas quantidades de dados captados através da hiperconexão dos usuários das redes de comunicação e informação digital.

As inúmeras fragilidades desse novo sistema instigaram a proteção jurídica sobre a informação e sua matéria-prima: os dados. A coleta e processamento de dados, de forma não regulamentada, apresenta potencial risco aos direitos da personalidade, fundamentais e inerentes ao indivíduo, como a privacidade e a intimidade.

O principal modelo de legislação destinada a enfrentar o imenso desafio de proteger os bens jurídicos fundamentais frente a essa realidade nasceu na União Europeia. Em 2016 foi editado o Regulamento 2016/679, do Parlamento Europeu e Conselho da União Europeia, conhecido como Regulamento Geral sobre a Proteção de Dados (GDPR).

Inspirada nesse regulamento, no Brasil, foi promulgada a Lei n.º 13.709/2018, denominada Lei Geral de Proteção de Dados (LGPD), a qual tem o escopo de regulamentar o tratamento de dados pessoais, inclusive nos meios digitais. No seu bojo, instaura-se um novo microsistema de responsabilidade civil, alusivo aos eventuais danos causados a uma pessoa natural em face da ilicitude ou abusividade do tratamento de seus dados pessoais e sensíveis.

Ainda que o legislador tenha se mantido silente quanto ao tratamento de dados decorrentes de vínculos empregatícios, é evidente que os dispositivos presentes na LGPD são aplicáveis no âmbito das relações de trabalho, uma vez que, na prática, o empregador efetua a coleta e processamento de dados do empregado desde a fase pré-contratual até após o efetivo término do vínculo empregatício.

O enfoque do presente artigo é investigar como se opera a aplicabilidade do microsistema de responsabilidade civil, previsto na Lei Geral de Proteção de Dados (Lei nº 13.709/18) nas relações de trabalho, considerando a necessidade de amparo ao trabalhador, como sujeito hipossuficiente, de forma a garantir a proteção de seus direitos fundamentais de personalidade frente ao novo paradigma da sociedade da comunicação e informação, que torna recorrente a prática, por vezes ilícita ou abusiva, da coleta e processamento de seus dados pessoais e sensíveis.

Dito isso, o presente artigo tratará, no segundo tópico, do papel da Lei Geral de Proteção de Dados na defesa de direitos individuais para, no terceiro tópico, avançar para a natureza fundamental e personalíssima dos direitos à privacidade e intimidade do trabalhador. O quarto e último tópico adentrará no ponto culminante desta pesquisa, que abordará a responsabilidade civil do empregador pelo uso ilícito ou abusivo de dados do trabalhador.

O método utilizado nesta investigação é o dedutivo, partindo-se de considerações conceituais amplas para aplicá-las ao caso concreto. A técnica de procedimento é a monográfica, subministrado por pesquisa doutrinária e documental.

2. LGPD como instrumento de proteção de direitos individuais

As relações sociais vêm sendo travadas, de forma crescente, por intermédio de canais ou redes virtuais. Com a ascensão das tecnologias digitais, o ser humano tem vivido tempo expressivo de sua existência conectado à Internet. Por meio dessa hiperconexão, colhem-se inúmeros dados pessoais, que serão tratados, armazenados, analisados e comercializados.

O crescente fortalecimento das comunicações virtuais está fortemente atrelado às novas tecnologias da informação e comunicação. Para Teresa Moreira (2010), tais tecnologias compreendem o conjunto de inovações, baseadas na eletrônica, informática e telecomunicações, cuja finalidade é o aprimoramento dos mecanismos de armazenamento, recuperação, tratamento e transmissão de informações.

Os dados pessoais assumiram o papel que outrora pertenceu ao petróleo, isso é, são a maior fonte de recursos econômicos. Os dados são hoje não apenas, por si só, um grande objeto de mercado, mas também figuram como insumos essenciais para praticamente todas as atividades econômicas. Entretanto, o fenômeno não atinge apenas a seara econômica, repercute nas esferas individuais, afetando a estrutura das relações sociais e políticas (TEPEDINO; FRASÃO; OLIVA, 2019).

Os riscos desse cenário são inúmeros, abrangendo desde a clonagem de cartões até escândalos mundiais, como no caso “Cambridge Analytica”, onde foi realizada a coleta de dados pessoais de pelo menos 87 milhões de usuários do Facebook, que foram utilizados para produzir materiais políticos de forma direcionada e personalizada para a campanha eleitoral de Donald Trump, em 2016, e para a campanha pró saída do Reino Unido da União Europeia, movimento conhecido como Brexit. (FORNASIERM; BECKC, 2020).

O caso impulsionou o já ativo debate quanto à necessidade de regulamentar o uso e tratamento de dados pessoais.

No Brasil, esse debate se iniciou em 2010, com o lançamento de consulta pública sobre o tema pelo Ministério da Justiça. Primeiramente foi editada a lei

12.968/2014 (BRASIL, 2014), conhecida como Marco Civil da Internet, que disciplina o uso da Internet no país, com base na liberdade de expressão e garantia de direitos fundamentais (REIS, 2019).

Nos anos que se seguiram foram apresentados projetos visando a proteção dos dados pessoais, baseados no modelo europeu fundado no Regulamento Geral de Proteção de Dados, assinado em 2016 (DORNELES; BARZOTTO, 2020). Esses projetos culminaram na Lei nº 13.709, de 14 de agosto de 2018 (BRASIL, 2018), conhecida como Lei Geral de Proteção de Dados (LGPD). A nova legislação impôs regras sobre o tratamento de dados pessoais e, em sua essência, tem como objetivo proteger o direito à liberdade, à privacidade e ao livre desenvolvimento dos cidadãos.

O legislador buscou no texto legal construir um microsistema dentro do direito privado brasileiro, assim a LGPD é expressa em definir seus princípios, fundamentos, âmbito de incidência, terminologia e sistema de responsabilidade civil. (LIMA; SÁ, 2020).

Quanto à terminologia, a legislação, no seu art. 5º, estabelece conceitos que serão usados no decorrer do texto normativo. Para o debate que se pretende nesse artigo é relevante a análise da diferença ali estabelecida entre dado pessoal e dado pessoal sensível.

Enquanto o primeiro pode ser definido como informação de pessoa natural identificada ou identificável, o segundo se refere a uma informação igualmente capaz de indicar seu titular de forma direta ou indireta, mas que traz um conteúdo de intimidade mais profunda, como opinião política ou etnia. O titular mencionado é a pessoa natural a quem os dados se referem (BRASIL, 2018).

Outra definição relevante é a dada ao termo “tratamento”, que configura toda operação realizada com dados pessoais, desde sua coleta ou produção até a eliminação.

Nesse processo estão envolvidos os agentes de tratamento, pessoas físicas ou jurídicas, de direito público ou privado, que ocupam o papel de controlador ou de operador.

Controlador é aquele que passa a possuir os dados pessoais de outrem e a quem compete as decisões quanto ao tratamento destes dados, conforme estabelecido no art. 5º, inciso VI da LGPD. O operador, por sua vez, é aquele que realiza o tratamento de dados em nome do controlador (MEIRELES, 2021).

A lei prevê, ainda, a figura do encarregado, isso é, pessoa física indicada pelo controlador ou pelo operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados. Sua existência na cadeia de coleta e tratamento de dados é obrigatória (MEIRELES, 2021).

O art. 6º do diploma legal aqui apreciado estabelece como diretrizes do tratamento de dados a observância do princípio da boa-fé; adequação, proporcionalidade e necessidade deste tratamento para a finalidade legítima e específica informada ao titular dos dados e garantia do livre acesso do titular à forma e duração do tratamento, bem como dos dados utilizados, que devem manifestar exatidão, clareza e relevância. Além disso, impõe o emprego de medidas aptas a proteger os dados do conhecimento não autorizado, de perda e alteração acidental ou ilícita, e veda o tratamento de dados com fins discriminatórios, ilícitos ou abusivos. A não observância das diretrizes acima elencadas, que provocar dano patrimonial, moral, individual ou coletivo, gera responsabilidade solidária do controlador e do

operador que estiverem diretamente envolvidos.

O sistema de responsabilidade civil estabelecido pela LGPD, previsto nos arts. 42 a 45, é especial, configurando a mais relevante novidade trazida pelo diploma.

No âmbito do direito do trabalho, o empregador figura como controlador, enquanto o trabalhador é o titular dos dados. Nesse viés, considerando que o empregado, como cidadão, deve ter seus direitos fundamentais de personalidade preservados, bem como o grande acesso a dados propiciado pela relação de emprego, isto desde a etapa pré-contratual até a pós-contratual, faz-se necessário o estudo da aplicabilidade da LGPD nas relações de emprego, em especial a forma como a reparação dos danos ocorre nessa seara.

3. A privacidade e a intimidade do trabalhador com bens personalíssimos e fundamentais

A evolução tecnológica e as mudanças sociais que dela decorrem propiciam o surgimento de novos conflitos de interesse, inclusive na esfera do direito do trabalho. Se, antigamente, garantir ao trabalhador férias, limite da jornada e salário mínimo eram medidas suficientes para protegê-lo, hoje é preciso considerar a sociedade da informação para elencar novos direitos como básicos.

Nas relações de trabalho, a coleta e tratamento de dados é constante. Inicia-se na fase pré-contratual e estende-se até mesmo para depois do fim do contrato de trabalho. O cotidiano em uma relação de trabalho, com a convivência interpessoal entre o empregado, colegas de trabalho, clientes, terceiros e o empregador, possibilita o desrespeito dos limites da esfera pessoal.

Desta forma, é evidente a necessidade de proteger a privacidade e a intimidade do trabalhador, como direitos fundamentais que são, para que o empregador ou outros sujeitos participantes da relação de emprego não ultrapassem a esfera profissional, atingindo a personalidade do trabalhador, e ainda, potencialmente, maculando os seus direitos de proteção à vida privada.

A preocupação normativa quanto à proteção da privacidade e intimidade do ser humano remonta à Declaração Universal dos Direitos Humanos – DUDH – (1948). Elaborada pela Assembleia Geral das Nações Unidas, em 10 de dezembro de 1948, como norma comum a ser alcançada por todas as nações, configura legado de uma sociedade que presenciou as atrocidades da Segunda Guerra Mundial e buscou estabelecer limites a serem aplicados inclusive em momentos de conflito, reconhecendo que o ser humano possui direitos personalíssimos que, ao contrário daqueles vinculados ao patrimônio, não podem ser dispostos.

Dentro ditos direitos personalíssimos está o direito à privacidade. Nos termos do artigo 12 da referida Declaração, “ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques a sua honra e reputação. Todo o homem tem direito à proteção da lei contra tais interferências ou ataques.”(DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS, 1948).

No Brasil, o direito à intimidade e à vida privada possuem proteção expressa no texto constitucional. Conforme o disposto no art. 5º, X, da Constituição Federal: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas,

assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. (BRASIL, 1988).

Desta forma, o legislador constituinte não reconheceu apenas o direito à privacidade de forma genérica, mas escolheu referir proteção à privacidade e à intimidade como bens autônomos (SARLET; MARINONE; MITIDIERO, 2018).

Impõe-se, assim, uma diferenciação entre intimidade e privacidade. Embora a jurisprudência e algumas linhas doutrinárias não distingam a privacidade da intimidade, há também aqueles que entendem que o direito à intimidade faria parte do direito à privacidade, que seria mais amplo.

O direito à privacidade teria por objeto os comportamentos e acontecimentos atinentes aos relacionamentos pessoais em geral, às relações comerciais e profissionais que o indivíduo não deseja que se espalhem ao conhecimento público. Já o direito à intimidade seriam as conversações e os episódios ainda mais íntimos, envolvendo relações familiares e amizades mais próximas (MENDES; BRANCO, 2017).

Além disso, é relevante analisar a escolha do poder constituinte em elencar tal previsão dentro dos direitos fundamentais da personalidade, interligados ao princípio da dignidade humana, previsto no art. 1º, III, da Constituição Federal de 1988.

Como direitos fundamentais, os direitos à intimidade e à privacidade possuem características próprias. Ambos podem ser definidos como posições jurídicas, que do ponto de vista constitucional positivo foram retiradas da esfera de disponibilidade dos poderes constituídos, pois simbolizam decisões sobre a estrutura da sociedade com supremacia hierárquica no ordenamento jurídico (SARLET, 2018).

No ordenamento infraconstitucional, o Código Civil (2002) também tratou dos direitos da personalidade, do artigo 11 ao 21. Coube a ele a tarefa de delinear, através de regras objetivas, a tutela geral da dignidade humana (GOLDSCHMIDT, 2019).

Especificamente quanto à privacidade, a norma civilista dispôs no artigo 21 sobre a inviolabilidade da vida privada da pessoa natural, afirmando que o juiz, a critério do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário ao preceito (BRASIL, 2002).

Além disso, o Código Civil estabelece que os direitos da personalidade são intransmissíveis e irrenunciáveis. De acordo com o art. 11, o exercício destes direitos não pode sofrer limitação voluntária, exceto nos casos previstos em lei. Esta determinação pretende proteger a dignidade da pessoa humana de ações de seu próprio titular (GOLDSCHMIDT, 2019).

O Código de Direito Civil também prevê em seu art. 12 medidas a serem adotadas em casos de violação dos direitos da personalidade. Em um primeiro plano é possível que o indivíduo que tenha seu direito lesado ou ameaçado exija que a prática que afete seu direito seja obstada. Em um segundo plano é permitida a busca pela reparação civil dos danos decorrentes de tal lesão (GOLDSCHMIDT, 2019).

Conforme mencionado anteriormente, o cotidiano das relações de trabalho possibilita o desrespeito aos direitos da personalidade. Em virtude disso, a legislação trabalhista possui normas expressas sobre os direitos da personalidade, inseridas na Consolidação das Leis do Trabalho (CLT) a partir da entrada em vigor da Lei n.º 13.467/2017, conhecida como Reforma Trabalhista.

Importa dizer que uma das formas de proteção do direito à privacidade cons-

tante na CLT, mesmo antes da inclusão expressa de um título próprio para tratar da reparação de danos extrapatrimoniais, era efetivada através dos arts. 482, alínea “j”, e 483, alínea “e”, onde estabelecido como motivo justo para resolução do contrato de trabalho a lesão à honra e à boa fama (LEITE, 2019).

A Reforma Trabalhista veio a positivar a reparação do dano extrapatrimonial, inaugurando o novo “Título II-A”, que trata especificamente do assunto no decorrer dos arts. 223-A ao 223-G, temática que será melhor aprofundada no último capítulo do presente artigo.

Mais recentemente, a Lei Geral de Proteção de Dados trouxe diversos mecanismos de proteção aos direitos da personalidade. A nova lei possui mérito em dar maior concretude aos princípios constitucionais através de seu microsistema de proteção.

Apesar da LGPD não apresentar regulamentação específica para tratamento de dados decorrentes de relação empregatícia, a aplicação dela ao cotidiano do contrato de trabalho é inequívoca (LIMA; SÁ, 2020).

A privacidade do trabalhador, enquanto direito personalíssimo e fundamental, merece especial proteção do ordenamento jurídico. Entretanto é preciso considerar que na relação empregatícia o empregador exerce poderes patronais, que lhe permitem certas hipóteses de tratamento de dados dos empregados. Razão pela qual propõe-se o estudo do próximo tópico, que tratará acerca dos poderes patronais para tratamento de dados.

4. Responsabilidade civil do empregador pela utilização ilícita ou abusiva de dados dos empregados

A responsabilidade civil é um instituto jurídico destinado a recompor o equilíbrio social que foi quebrado pelo dano sofrido pela vítima, seja ele de caráter patrimonial ou extrapatrimonial. (MORAES; MORAES, 2017).

No art. 5º, X, da CF/88, o legislador constituinte estabeleceu que a violação dos direitos de privacidade, intimidade, honra e imagem gera o dever de reparar os danos que venham ocorrer em virtude desta violação, ainda que esses sejam de caráter extrapatrimonial. Mendes e Branco (2017) apontam que tal previsão não apenas encerra a discussão quanto à possibilidade de reparação civil de danos meramente extrapatrimoniais, mas também impõe limite à liberdade de expressão, na medida em que prevê sanções à violação dos direitos de personalidade.

O Código Civil de 2002 sofreu grande influência da atual Constituição Federal de 1988. A norma civilista teve sua estrutura modificada à medida que, buscando garantir o direito fundamental da dignidade da pessoa humana, passou a prescrever sobre os direitos da personalidade, cuidando de bens não patrimoniais. (GAGLIANO; PAMPLONA FILHO, 2019).

Afora a classificação quanto ao tipo de bem tutelado, também é possível classificar a responsabilidade civil quanto ao elemento culpa. O Código Civil vigente adota o sistema dualista, que aporta a responsabilidade civil subjetiva e a responsabilidade civil objetiva.

Em regra, para haver o dever de indenizar é preciso prova de conduta dolosa, ou, ao menos, culposa (negligência, imprudência ou imperícia). A espécie objetiva é prevista no parágrafo único do art. 927 do Código Civil, que estabelece a

obrigação de reparar o dano, independente da culpa, nos casos especificados em lei, ou quando o dano decorrer de atividade cuja natureza gere risco, que deve ser suportada por aquele que a exerce. Nesses casos excepcionais a culpa pode ser presumida pela lei ou prescindível, sendo analisado apenas o nexo de causalidade entre a ação e o dano. (MORAES; MORAES, 2017).

Moraes e Moraes (2017) apontam diversos princípios que norteiam a reparação civil do dano. Dentre eles destaca-se o princípio da reparação integral, com fundamento na justiça corretiva. Esse princípio sustenta que o ofendido deve ter o dano plenamente reparado, com base nas previsões constitucionais do art. 5º, particularmente no que refere o seu inciso V, que assegura a indenização por dano material, moral e à imagem, e o inciso X, que tutela a reparação integral pela violação à intimidade, vida privada, honra e imagem.

Na lei civil, a previsão deste princípio se localiza no art. 944, que dispõe que a indenização deve ser medida pela extensão do dano, de modo a garantir a reparação integral da lesão sem gerar enriquecimento injustificável do ofendido. A reparação integral também embasa a possibilidade de cumulação de indenizações por danos distintos oriundos do mesmo ato lesivo. (MORAES; MORAES, 2017).

Além de seguir os princípios, a responsabilidade civil deve corresponder a suas funções. Para além de reparar o dano patrimonial ou compensar o dano moral, o custo pago em indenização deve servir de punição e ensinamento ao ofensor. Isso porque, ao ter seu patrimônio atingido, o lesionador tende a refrear os seus impulsos antissociais. (GAGLIANO; PAMPLONA FILHO, 2019).

No que se refere à proteção aos direitos de privacidade e intimidade correlacionados aos dados pessoais, o ordenamento jurídico brasileiro não apresentava previsões específicas. Nos casos de abuso na utilização de dados, onde auferido dano, recorria-se ao disposto nos arts. 43 e 44 do Código de Defesa do consumidor, e aos dispositivos civis que versam sobre a proteção dos direitos da personalidade.

Essa lacuna foi preenchida pela Lei Geral de Proteção de Dados, que conforme aludido no segundo tópico desta pesquisa, instituiu um verdadeiro microsistema de reparação, baseado no fundamento da responsabilidade civil e nas excludentes de reparação, de modo que a aplicação de suas normas depende da completude do macrosistema de Direito Civil. (GODINHO; QUEIROGA; TOLÊDO, 2020).

Atualmente, nas lides trabalhistas, há dois regimes jurídicos para os danos. A reparação do dano patrimonial é fundada em cláusulas gerais e no princípio da reparação integral. Já os danos não patrimoniais são regulados pelo novo Título II-A da CLT (“Do Dano Extrapatrimonial), implementado pela Lei nº 13.467/2017. O título, composto pelos arts. 223-A ao 223-G, segue direção oposta ao sistema de reparação civil previsto no ordenamento jurídico brasileiro. (DELGADO, 2019).

Seguindo a literalidade da nova Lei, não cabe mais falar em dano estético, moral e correlatos, estes são unificados sob a terminologia de danos extrapatrimoniais. Em um primeiro plano, imperioso elucidar que a terminologia adotada na legislação não configura novo direito, nem mesmo altera o conteúdo já estabelecido na ciência jurídica. Ao utilizar o termo aqui destacado, o legislador buscou atingir todo e qualquer dano cuja natureza não seja patrimonial ou material. (DOS SANTOS; PEREIRA, 2020).

Os bens extrapatrimoniais juridicamente tuteláveis da pessoa natural são elencados no art. 223-C, como a honra, a imagem, a intimidade, a liberdade de ação, a autoestima, a sexualidade, a saúde, o lazer e a integridade física. Entretanto, Delgado (2019) aponta que o rol fixado neste artigo não é, de forma alguma, exaustivo, uma vez que a própria Constituição Federal, no art. 3º, IV, busca proteger de qualquer forma de discriminação, como etnia, cor, idade etc. E como lei hierarquicamente superior, não pode ser suprimida ou limitada.

O ponto mais controverso da lei se encontra no art. 223-G, cujo caput, bem como os doze incisos que o seguem, trazem a ideia de juízo de equidade ao estabelecer diretrizes para a aferição do dano e fixação da correspondente reparação, que apenas refletem a prática jurisdicional. Todavia, a nova lei não observou de forma integral a noção constitucional de equidade, uma vez que, no decorrer dos parágrafos que integram o dispositivo, o legislador optou por impor critério de tarifação do valor da indenização. (DELGADO, 2019).

O tarifamento está explicitado no art. 223-G, § 1º, incisos I, II, III e IV, e segue nos demais parágrafos. O primeiro parágrafo define cinco parâmetros da tarifação, que relacionam a natureza da ofensa a um valor da indenização ancorado no último salário contratual do ofendido.

A primeira crítica enfrentada pelo dispositivo diz respeito a vedação de cumulação dos parâmetros de grau de ofensa. Tal vedação encontra-se em dissonância com o princípio da reparação integral, mencionado anteriormente. Isso porque, nos casos em que a ofensa lesiona bens distintos em graus variados, apenas uma indenização poderá ser aplicada. (DOS SANTOS, 2020).

A segunda crítica se refere à aplicação do salário do ofendido como critério para o cômputo da indenização. Tal parâmetro fere o princípio da isonomia, uma vez que desconsidera as minúcias do caso concreto, e pode acarretar em situações onde um mesmo fato produz indenizações distintas. (GOLDSCHMIDT, 2019).

Imagine-se um caso concreto, onde ocorreu o vazamento de dados pessoais de dois empregados. Um deles ocupava o cargo de gerência, com salário de R\$10.000,00, enquanto o outro empregado percebia a quantia mensal de R\$1.000,00. Em sentença, o juiz reconhece que ocorreu dano à privacidade por culpa do empregador, e estabelece que este dano é de natureza média, cabendo assim indenização no montante de cinco salários. Desta forma enquanto o gerente receberá R\$ 50.000,00, o empregado terá direito a apenas R\$ 5.000,00.

Tal diferença é injustificável, uma vez que os dois empregados possuem a mesma dignidade, com base no direito constitucional, bem como no direito internacional comparado. De acordo com o artigo primeiro da Declaração Universal dos Direitos Humanos, todos os humanos nascem iguais em direito e dignidade, ainda, o art. 7º, inciso XXXII, da CF, proíbe expressamente a distinção entre trabalhadores que exercem atividade manuais técnicas e intelectuais (GOLDSCHMIDT, 2019).

A própria tarifação representa tema de debate, uma vez que flagrantemente inconstitucional, uma vez que o julgamento de indenização de dano extrapatrimonial deve ser feito com base na equidade, através dos princípios da razoabilidade e da proporcionalidade. O ordenamento jurídico brasileiro já presenciou o julgamento de fonte normativa de teor próximo. Através da ADPF 130/DF, em 2009,

o Supremo Tribunal Federal declarou a incompatibilidade da Lei nº 5.250/67, conhecida como Lei de Imprensa, com a CF/88, no que tange dispositivo que pretendia restringir a fixação de indenizações de dano moral (LEITE, 2017).

Atualmente existem quatro Ações Diretas de Inconstitucionalidade sobre a tarifação na lei trabalhista aguardando julgamento. A ADI 5.870, de 21 de dezembro de 2017, impetrada pela Anamatra, possui outras três ações apensadas: a ADI 6.050, de 19 de dezembro de 2017, igualmente proposta pela Anamatra, a ADI 6.069, de 5 de fevereiro de 2019, ajuizada pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB) e a ADI 6.082, de 25 de fevereiro de 2019, de autoria da Confederação Nacional dos Trabalhadores na Indústria (CNTI). As ações possuem, no geral, os mesmos argumentos, e questionam a constitucionalidade do parágrafo primeiro do art. 223-G, na medida em que esse, em tese, afronta princípios constitucionais e representa um retrocesso no âmbito do direito do trabalho.

Por fim, seria imprudente não mencionar que a nova legislação trabalhista, através do art. 223-A, pretende afastar a aplicação de outras normas que disciplinem o tema da reparação de danos extrapatrimoniais. Conforme sua redação (BRASIL, 2014): “223-A – Aplicam-se à reparação de danos de natureza extrapatrimonial decorrentes da relação de trabalho apenas os dispositivos desse título.”

O suposto afastamento pretendido está em dissonância com a própria lei trabalhista, que no seu art. 8º deixa claro que, em caso de omissão da CLT, o direito comum será fonte subsidiária do direito do trabalho. Percebe-se que esse afastamento representa retrocesso em avanços consolidados no direito, uma vez que a reparação por danos não patrimoniais possui amparo na Constituição Federal, que apresenta hierarquia superior à lei trabalhista, não sendo possível afastá-la ou limitar sua aplicação. (VIVEIROS, 2018).

Além da dissonância mencionada, o afastamento de outros diplomas legais pode produzir discriminação negativa do empregado na busca pela reparação de danos extrapatrimoniais.

Retomando o exemplo do caso hipotético já estudado, agora com uma pequena, mas expressiva variante, considere-se que os dados vazados pertenciam a clientes e empregados da empresa. Nesse caso, os dois grupos estariam sujeitos a regras diferentes: enquanto os primeiros se beneficiariam de um regime de responsabilidade civil que não impõe limites à indenização por dano extrapatrimonial, o segundo grupo se sujeita à limitação de sua indenização com base nos critérios de pré-tarifação dos danos extrapatrimoniais adotados na CLT.

Conforme o exposto até aqui, é nítido que a interpretação a ser aplicada ao novo Título II-A da CLT não pode ser literal. Em verdade, é preciso utilizar de métodos de interpretação jurídica, como o lógico-racional, o sistemático e o teleológico, para harmonizar os dispositivos inseridos na CLT pela reforma trabalhista com o conjunto jurídico mais amplo. (DELGADO, 2019).

Nesse sentido, a fim de evitar discriminação negativa na proteção dos dados pessoais do titular empregado, deve-se aplicar as normas do macrosistema de reparação civil para efetivação da reparação integral de danos advindos da violação de dados pessoais e sensíveis.

Assim, os julgamentos de lides que versem sobre vulneração de dados pesso-

ais do empregado só atingirão os objetivos da responsabilidade civil se efetuada a compatibilização entre as normas específicas de responsabilidade civil objetiva contidas na LGPD e o regime descrito na norma trabalhista, com os temperamentos decorrentes do macrossistema de reparação civil.

Considerações finais

O avanço das tecnologias de comunicação, e em decorrência, o grande fluxo de informações transportaram os dados pessoais para o centro do sistema econômico atual. Tal configuração social traz à tona diversas problemáticas, dentre elas, destaca-se a necessidade de proteção ainda maior aos direitos da personalidade, a exemplo da privacidade, intimidade e imagem.

Buscando prevenir a violação dos direitos de personalidade, o legislador brasileiro, inspirado em regulamento europeu, editou a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados – LGPD. A nova legislação inovou em diversos pontos, estabelecendo um verdadeiro microssistema de responsabilidade civil sobre a proteção de dados.

Constatou-se que no âmbito das relações de trabalho o fluxo de dados e informações é denso, está presente desde a etapa inicial de seleção de candidatos e se estende para além do encerramento do vínculo trabalhista. Desta forma, torna-se inegável a necessidade de aplicação das diretrizes da Lei Geral de Proteção de Dados ao tratamento de dados efetivado nestas relações, ainda que o diploma legal não traga previsão específica para sua aplicação nesse caso.

Nesse cenário, o empregador figura como controlador, e possui responsabilidade pela coleta, tratamento, armazenamento, compartilhamento e descarte dos dados pessoais do trabalhador.

O trabalhador, por sua vez, deve ter seus direitos de personalidade protegidos, na medida em que figuram direitos fundamentais inerentes a todos os indivíduos.

Convém mencionar que, em decorrência da configuração das relações de trabalho, o empregador possui certos poderes que colocam o empregado em posição de subordinação. Desta forma, torna-se crucial a defesa dos direitos de privacidade do trabalhador, uma vez que este pode não ser capaz de negar o tratamento de seus dados.

Conclui-se, portanto, que a fim de evitar danos à personalidade do obreiro, o tratamento de dados decorrentes de relações trabalhistas deve obedecer aos direitos dos titulares de dados previstos na LGPD: direito de acesso aos dados coletados, direito de retificação desses dados e o direito a negar a coleta de dados pessoais.

Todavia, se constatado o dano, o empregador deve sofrer as penas de acordo com o microssistema de reparação de danos, não apenas com a incidência das normas específicas previstas na Lei Geral de Proteção de Dados, mas também com a aplicação sistêmica da CLT, da Constituição Federal de 1988, o próprio do Código Civil, entre outras normas pertinentes à reparação integral do dano. Pois, em situação contrária, o trabalhador passaria por discriminação negativa frente aos demais papéis sociais.

REFERÊNCIAS

BRASIL. Código Civil. Lei nº 10.406, de 10 de janeiro de 2002. Brasília, DF.

Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 19 abr. 2021.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 20 mar. 2021.

BRASIL. Lei Geral de Proteção de Dados. Lei nº 13.709, de 14 de agosto de 2018. Brasília, DF. Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L3709.htm. Acesso em: 19 mar. 2021.

BRASIL. Marco Civil da Internet. Lei nº 12.968, de 6 de maio de 2014. Brasília, DF. Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12968.htm. Acesso em: 19 mar. 2021.

BRASIL. Reforma Trabalhista. Lei nº 13.467, de 13 de julho de 2017. Brasília, DF. Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13467.htm. Acesso em: 19 mar. 2021.

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS. Rio de Janeiro: UNIC, 2009 [1948]. Disponível em: <<http://www.dudh.org.br/wp-content/uploads/2014/12/dudh.pdf>> Acesso em: 26 abr. 2021

DELGADO, Mauricio Godinho. Curso de direito do trabalho: obra revista e atualizada conforme a lei da reforma trabalhista e inovações normativas e jurisprudenciais posteriores. 18. ed. São Paulo: LTr, 2019.

DORNELES, Leandro do Amaral D. de; BARZOTTO, Luciane Cardoso (org). Inovações e trabalho: o direito do trabalho em tempos de mudança [recurso eletrônico]. Porto Alegre: Editora da UFRGS, 2020. 288. Pdf

DOS SANTOS, Gesiane Luz; PEREIRA, Thaiana Araújo. O Dano extrapatrimonial regulamentado pela Reforma Trabalhista. Revista Científica Multidisciplinar do CEAP, v. 2, n. 2, p. 11-11, 2020. Disponível em: <http://periodicos.ceap.br/index.php/rcmc/article/view/48>. Acesso em: 22 abr. 2020

FORNASIER, M de O; BECK, C. Cambridge Analytica: escândalo, legado e possíveis futuros para a democracia. Revista Direito em Debate, v. 29, n. 53, p. 182-195, 26 maio 2020. Disponível em <https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/10033> Acesso em: 10 mar. 2021.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. Novo curso de direito civil, v. 3: responsabilidade civil. 17. ed. São Paulo: Saraiva Educação, 2019.

GOLDSCHMIDT, Rodrigo (org.). Direitos de personalidade do Trabalhador. Rio de Janeiro: Lumen Juris, 2019.

GOLDSCHMIDT, Rodrigo. Art. 223-G. In: LISBÔA, Daniel; MUNHOZ, José Lucio (org). Reforma trabalhista comentada por juizes do trabalho: artigo por artigo. 2. ed. rev. São Paulo: LTr, 2019. p. 141-146.

LEITE, Carlos Henrique Bezerra. Curso de Direito do Trabalho. 11. Ed. São Paulo: Saraiva Educação, 2019

LIMA, Taisa Maria Macena de; SÁ, Maria de Fátima Freire de. Microsistema de proteção de dados pessoais e contrato de trabalho: a reparação de danos decorrentes da violação dos direitos da personalidade do empregado. Revista Eletrônica de Direito do Centro Universitário Newton Paiva, Belo Horizonte,

n.40, p.110-116, jan./abr. 2020. Disponível em: <<https://revistas.newtonpaiva.br/redcunp/wpcontent/uploads/2020/10/DIR4006.pdf>>. Acesso em: 6 abril. 2021.

MEIRELES, Edilton (org). Direito e processo do trabalho entre reformas, indústria 4.0, negociação e proteção. Editora Paginæ: Salvador, 2021.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. 12. ed. rev. e aum. São Paulo: Saraiva, 2017.

MORAES, Carlos Alexandre; MORAES, Lilian Rosana dos Santos. Da responsabilidade civil: conceitos, constitucionalização, princípios, espécies, funções, pressupostos e do abuso de direito. 1. ed. Toledo (PR): Vivens, 2017.

REIS, Beatriz de Felipe. – A Proteção dos Dados Pessoais dos Trabalhadores na Defesa dos Direitos Fundamentais de Personalidade: os Riscos e Desafios à luz da nova LGPD. In: GOLDSCHIMIDT, Rodrigo (org.). Direitos da Personalidade do Trabalhador. Rio de Janeiro: Lumen Juris, 2019. p.137 -154

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. Curso de direito constitucional. 7. ed. – São Paulo: Saraiva Educação, 2018.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2019.

VIVEIROS, Luciano. CLT comentada pela reforma trabalhista (Lei nº 13.467/2017). 9 ed. Belo Horizonte: Fórum, 2018.

34. TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS LIGADOS A SAÚDE DO TRABALHADOR À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

MARINA RICHARD DE TOLEDO¹ E RODRIGO GOLDSCHMIDT²

Resumo: O presente artigo tem como objetivo analisar o tratamento de dados pessoais sensíveis ligados a saúde do trabalhador, observando os regramentos trazidos pela Lei Geral de Proteção de Dados Pessoais (LGPD). Para tanto, abordar-se-á sobre a valoração dos dados na atualidade. Posteriormente, os aspectos gerais da LGPD destacando seus princípios, fundamentos, dados pessoais e dados pessoais sensíveis. Por fim, pretende-se salientar a aplicação da LGPD nas relações de trabalho e o tratamento de dados sensíveis ligados a saúde do trabalhador. Nesse intento, utiliza-se do método de abordagem dedutivo e a técnica de pesquisa revisão bibliográfica pautada nas coletas de informações em legislações, obras, teses, dissertações e artigos científicos.

Palavras-chave: Direito do Trabalho. Lei Geral de Proteção de Dados Pessoais. Tratamento de Dados Pessoais Sensíveis. Direito à Privacidade.

1. Introdução

O avanço da sociedade e do acesso à informação intensificou a coleta de dados causando a necessidade de constante adaptação do Direito frente as novas realidades de proteção dos dados. Nesse campo, destaca-se o Direito do Trabalho, principalmente quando se trata de reforçar a proteção dos trabalhadores.

Em toda história do trabalho, há a prática de coleta de dados dos empregados, desde os registros feitos em papéis avulsos, fichas, livros, até os dias atuais em que os dados coletados são armazenados digitalmente. Tais dados são coletados, armazenados e compartilhados para fins de controle trabalhista, tributário e previdenciário.

O advento da lei n.º 13.709, de 14 de agosto de 2018, intitulada como Lei Geral de Proteção de Dados (LGPD) esclareceu a forma legalmente correta que a pessoa natural ou jurídica deve tratar os dados pessoais com o objetivo de proteger os direitos fundamentais da pessoa natural. Por se tratar de uma lei geral, seus efeitos incidem em diversas espécies de relações, em especial as relações de trabalho.

Dessa forma, o presente artigo visa analisar o tratamento de dados pessoais sensíveis ligados a saúde do trabalhador frente aos regramentos trazidos pela LGPD.

Para tanto, pretende-se, primeiramente, realizar uma breve introdução sobre a necessidade da lei de proteção de dados e seus aspectos gerais ressaltando seus

1 Mestranda em Direito pela UNESC. Pós-graduanda em Direito Notarial e Registral pelo CERS. Pós-graduanda em *Compliance*, LGPD & Prática Trabalhista pelo IEPREV. Advogada – OAB/SC 59.646.

2 Pós-Doutor em Direito pela PUC/RS. Mestre e Doutor em Direito pela UFSC. Professor e pesquisador permanente do PPGD/UNESC - Mestrado Acadêmico em Direito. Juiz Titular de Vara do Trabalho do TRT12.

princípios e fundamentos. Num segundo momento, verificar a diferenciação entre dados pessoais e os dados pessoais sensíveis conforme dispõe a lei. Por fim, pretende-se estudar sobre a aplicação da LGPD nas relações de trabalho e o tratamento de dados sensíveis ligados a saúde do trabalhador nessas relações.

Tendo em vista a relevância do tema, considera-se importante um estudo específico sobre o tratamento de dados sensíveis ligados a saúde do trabalhador para proteção de seus direitos fundamentais de liberdade e de privacidade, assim como livre desenvolvimento de sua personalidade no ambiente laboral.

Ademais, faz-se necessário ressaltar que em caso de descumprimento dos regramentos trazidos pela LGPD, serão aplicadas sanções administrativas que entrarão em vigor no dia 01 de agosto de 2021.

Para execução do presente artigo, utiliza-se o método de abordagem dedutivo, partindo-se da lei geral de proteção de dados pessoais para investigar o tratamento de dados pessoais sensíveis ligados a saúde do trabalhador. A técnica de pesquisa consiste na revisão bibliográfica pautada nas coletas de informações em legislações, obras, teses, dissertações e artigos científicos.

2. Aspectos gerais da LGPD

O desenvolvimento tecnológico trouxe consigo o intenso fluxo da coleta de dados através de plataformas utilizadas no dia a dia pela sociedade hiperconectada.

Pode-se dizer que os dados são considerados o principal insumo da atualidade devido à tamanha importância para a economia mundial. Argumenta-se, inclusive, que a sociedade global está pautada por uma nova religião, o dataísmo, segundo o qual “o Universo consiste num fluxo de dados e o valor de qualquer fenômeno ou entidade é determinado por sua contribuição ao processamento de dados” (HARARI, 2016).

Diante dessa análise massiva de dados, intensificou-se a necessidade de estabelecer proteção específica para o tratamento dos mesmos, nomeadamente diante do risco de lesão aos direitos fundamentais de personalidade.

No Brasil, os dados pessoais e sensíveis nunca estiveram em absoluta desproteção, visto que a Constituição Federal da República garante como direitos fundamentais a privacidade e intimidade. Ademais, existem outras manifestações infraconstitucionais a respeito, a exemplo a lei n.º 12.965/2014 (Marco Civil da Internet).

Entretanto, o país necessitava de uma legislação específica para a proteção de dados pessoais para a garantia da confiança dos países que já haviam estabelecidos regramentos próprios para tal matéria (SILVA; PINHEIRO; BOMFIM, 2021).

Dessa forma, veio à tona a lei n.º 13.709 (Lei Geral de Proteção de Dados Pessoais), publicada em 14 de agosto de 2018 com sua vigência programada para 16 de agosto de 2020, porém, a lei n.º 13.853 de 2019 prorrogou a entrada em vigor da LGPD por mais seis meses, ou seja, para agosto de 2020. Entretanto, a Medida Provisória n.º 959 de abril de 2020, trouxe o adiamento das novas regras para o dia 03 de maio de 2021.

Em 18 de setembro de 2020 a Medida Provisória n.º 959 foi convertida na lei n.º 14.058/2020 e o artigo que tratava da prorrogação para maio de 2021 foi excluído. Dessa forma, voltou a valer a data prevista na legislação anterior, a lei n.º

13.853/2019, que determinava agosto de 2020 para a entrada em vigor. Como a exclusão do artigo ocorreu em setembro de 2020 a lei passou a ter vigência imediata um dia após a lei n.º 14.058/2020, ou seja, a LGPD entrou em vigor oficialmente no dia 18 de setembro de 2020, exceto suas sanções administrativas, que entrarão em vigor somente em 01 de agosto de 2021 (RAMOS, 2020).

Tal lei versa sobre o tratamento de dados pessoais, nos meios digitais e físicos, por pessoa natural ou jurídica de direito público e privado e tem como objetivo garantir a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da pessoa natural. Entre seus fundamentos expostos no art. 2º da própria lei, ressalta-se a importância da autodeterminação informativa que assegura ao titular dos dados um maior controle sobre seus próprios dados pessoais (BRASIL, 2018).

A lei também dispõe expressamente em seu art. 6º os seus princípios, almejando a torná-la uma legislação didática, uma vez que os princípios são extremamente significantes para cumprimento da matéria tratada e para a garantia da proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Dentre eles, destacam-se os princípios da boa-fé, finalidade, adequação e necessidade dos dados que estão sendo tratados (VAINZOF, 2019).

O princípio da boa-fé é o norteador da LGPD. Impõe as partes uma atuação respeitando os deveres de lealdade, honestidade e informação. Os dados tratados devem restringir-se a finalidades específicas e legítimas a serem declaradas explicitamente aos interessados quando da coleta dos dados.

Além disso, conforme o princípio da adequação, os dados devem ser tratados de forma adequada, ou seja, devem ter compatibilidade com a finalidade declarada ao titular e serem necessários, sem excessos (BRASIL, 2018).

Analisar-se-á, em seguida, os conceitos de dados pessoais e dados pessoais sensíveis trazidos pela lei sendo o segundo objeto central do presente artigo.

3. Dados pessoais e dados sensíveis

Conhecer os principais conceitos trazidos pela LGPD é fundamental para aplicação do regramento ao caso concreto. Para o presente estudo, faz-se necessário diferenciar com clareza os dados pessoais e os dados pessoais sensíveis.

Primeiramente, ressalta-se que o tratamento dos dados consiste em toda operação realizada com dados pessoais, tais como coleta, utilização, armazenamento, compartilhamento, eliminação, etc. Tais operações podem ser automatizadas ou não.

Os dados pessoais são aquelas informações relacionadas a pessoa identificada ou identificável, ou seja, informações que levam diretamente a pessoa natural, a exemplo do nome, RG, CPF, idade, e-mail, endereço, número de telefone, entre outros.

Para esses dados a lei estabeleceu em seu art. 7º hipóteses nas quais é possível o seu tratamento, dentre elas, no presente estudo, destaca-se o fornecimento de consentimento do titular; cumprimento de obrigação legal ou regulatória pelo controlador; execução de contrato ou de procedimentos preliminares relacionados

ao contrato e exercício regular de direitos em processo judicial, administrativo ou arbitral (VAINZOF, 2019).

O dado pessoal sensível refere-se a informações que tratam de características da personalidade do indivíduo, tais como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2018).

Ressalta-se que diferentemente do dado pessoal, a LGPD dispõe em seu art. 11 que o tratamento de dados pessoais sensíveis só poderá ocorrer quando houver consentimento do titular ou seu responsável de forma específica e destacada para finalidade específica daquele tratamento. Entretanto, o mesmo artigo traz hipóteses em que os dados sensíveis poderão ser tratados sem fornecimento do consentimento do titular (LIMA, 2019).

Feita essa breve exposição acerca de alguns aspectos centrais da LGPD, passa-se a analisar a sua aplicação nas relações de trabalho, a fim de assegurar a proteção dos dados pessoais dos trabalhadores.

4. Aplicação da LGPD nas relações de trabalho

O atual estágio do desenvolvimento humano representa uma evolução tecnológica societária e consequente mudança no mercado de trabalho.

No ponto, colhe-se a lição de Dacheri (2019, p. 57):

O avanço da tecnologia tem modificado a estrutura e as modalidades das relações laborais, essencialmente com a substituição da força de trabalho humano manual pelo intelectual, que vem ocorrendo por meio da evolução das máquinas. O processo de globalização contribui com este avanço, pois age como um fator de diminuição das barreiras físicas da informação e da comunicação, facilita o contato entre as fronteiras e intensifica esta conexão existente entre o trabalho e a tecnologia.

A tecnologia tem o intuito de facilitar o labor humano e fomentar a produção, porém para sua perfeita funcionalidade, as plataformas digitais necessitam de dados cada vez mais específicos que geram insegurança para seus titulares.

Nas relações de trabalho percebe-se um intenso fluxo de dados pessoais e dados pessoais sensíveis entre trabalhadores, empregadores e terceiros envolvidos no processo. Diante desse fluxo, exige-se a aplicação dos regramentos trazidos pela LGPD nas relações de trabalho, visto que o uso desnecessário dos dados pode causar violação dos direitos fundamentais do trabalhador, em especial, os da personalidade, tais como o direito à honra, direito à imagem, direito à privacidade ou a vida privada (GOLDSCHMIDT, 2019).

Na mesma linha, Moreira (2010, p. 27) leciona:

A introdução das NTIC, traduzindo inúmeras vantagens para a empresa e para o empregador, comporta, também, riscos acrescidos para os direitos fundamentais dos trabalhadores, sobretudo para o direito à privacidade. Com estas novas tecnologias há um aumento desmesurado da capacidade de acumulação de informação e permite-se ao empregador reconstruir, a partir de dados aparentemente inócuos e *inofensivos*, o perfil do trabalhador, que poderá ser utilizado com os fins mais diversos. Desta forma, a informática permite um tratamento de dados pessoais do trabalhador de forma ilimitada e indiscriminada, desnudando-o *in totum*, tornando-o mais *transparente et, pour cause*, mais frágil.

Os dados dos trabalhadores são tratados durante todo seu contrato com a empresa, desde a fase pré-contratual, passando pela fase de execução contratual e, por fim, a fase pós-contratual. Em todo esse processo o empresário deverá se atentar sobre a finalidade, adequação e necessidade daqueles dados que estão sendo tratados seguindo uma severa política de privacidade sob um viés de um sistema de gestão de riscos (PINHEIRO; BOMFIM, 2020).

Essa gestão, pautada pelo princípio da boa-fé e por diretrizes éticas corporativas, num sistema interno de regras decorrentes do poder regulamentar do empregador, leva a contemporânea denominação de *compliance* trabalhista, que tem por objetivo:

[...] promover um ambiente de trabalho saudável, ético, íntegro que respeite os valores intrínsecos ao ser humano e que efetivamente busque o bem da coletividade. Pois, com a sua implementação, cria-se uma conscientização de integridade, de forma que o que é pregado pela alta direção, é de fato o que se pratica (JOBIM, 2018, p. 33).

O tratamento dos dados na fase pré-contratual engloba todo o processo seletivo e suas fases anteriores à celebração do contrato de emprego onde há o uso de diversos meios para selecionar e captar candidatos à vaga disponível.

Alguns meios utilizados são alimentados com informações que são capazes de traçar o perfil do empregado supostamente adequado para aquela empresa causando uma possível discriminação, visto que os dados pessoais recolhidos são desnecessários para fins de recrutamento. Dessa forma, o empregador deve ter cautela ao solicitar os dados ao candidato da vaga e requerer o consentimento dele para eventual armazenamento do currículo (RAMOS, 2020).

Após a escolha do candidato para a vaga de emprego inicia-se a fase da formalização do contrato na qual são coletados uma enormidade de dados pessoais e dados pessoais sensíveis para cumprimento de obrigação legal ou regulatória.

Inicia-se então a fase contratual marcada diariamente pelo tratamento de dados pessoais e dados pessoais sensíveis do trabalhador desde a sua chegada na empresa para controle de jornada podendo utilizar-se de dados extremamente sensíveis, tais como os dados biométricos para controle de ponto eletrônico.

Ressalta-se que essa fase exige cautela, pois são tratados diversos dados sensíveis como, por exemplo, atestados médicos, informações para geolocalização dos funcionários, câmeras de monitoramento, filiação a sindicato, etc. (CONI JUNIOR; PAMPLONA FILHO, 2020).

Com o término da relação de trabalho a coleta de dados do trabalhador cessa, porém se faz necessário manter por determinado período as informações já adquiridas relacionadas ao histórico laboral do trabalhador para fins de controle da empresa.

Apesar de LGPD dispor em seu art. 16 que após o término do tratamento, os dados pessoais deverão ser eliminados, a própria lei determina exceções como o cumprimento de obrigações legais e regulatórias, tal previsão que traz segurança para a parte contratante e o trabalhador (BRASIL, 2018).

Merece realce o prazo em que os dados pessoais deverão ser mantidos, visto que poderão ser necessários para produção probatória em eventual judicialização de um conflito.

Inicialmente, a manutenção desses dados poderia se dar por satisfeita pelo prazo prescricional trabalhista, entretanto, tal prescrição pode ser relativizada em determinados casos legais, como ações que tenham por objeto anotações para fins de prova junto à Previdência Social, conforme dispõe o art. 11, §1º, da Consolidação das Leis do Trabalho – CLT (BRASIL, 1943). Dessa forma, entende-se que tais dados devem ser mantidos além do prazo prescricional ou até mesmo por prazo indeterminado para fins de proteção jurídica da empresa (PINHEIRO; BOMFIM, 2020).

Posto isso, faz-se necessário analisar a utilização do consentimento como base legal para o tratamento de dados do trabalhador pelo empresário, uma vez que representa uma relação assimétrica entre as partes, em regra, marcada pela dependência econômica.

Para Doneda (2019) o consentimento representa a autonomia da vontade através de um instrumento de manifestação da escolha. Nesse contexto, ressaltam-se dois aspectos do consentimento, o primeiro que se trata de um elemento acessório de determinada situação, como por exemplo, um contrato de trabalho, no qual a possibilidade de não revelação dos dados pessoais pode causar certa rejeição pela parte contratante e segundo o consentimento apresentado de forma obscura, ou seja, suas consequências podem ser difíceis de serem identificadas.

Em decorrência do poder de comando imposto pelo empresário, normalmente, os dados dos trabalhadores são considerados de utilização unilateral. Entretanto, a LGPD afasta essa possibilidade, ao trazer como fundamento a autodeterminação informativa que determina ao titular o poder de controlar o trânsito dos seus dados.

Dessa forma, a LGPD garante o direito ao trabalhador de conhecer as formas de tratamento de dados utilizadas pela empresa. Além disso, a lei dispõe que a

utilização do consentimento como base legal para o tratamento deverá ser de forma livre, inequívoca e específica (VAINZOF, 2019).

Portanto, visando a prevenção de riscos, é recomendável evitar a utilização do consentimento como base legal de tratamento de dados nas relações de trabalho. Caso haja a utilização dessa base legal, ela deverá ocorrer de forma livre. Ressalta-se que a obtenção do consentimento pelo trabalhador não permite que o controlador compartilhe seus dados com terceiros (PINHEIRO; BOMFIM, 2020).

Considerando o exposto, é preciso levar em conta que além dos dados pessoais, há o tratamento de dados pessoais sensíveis nas relações de trabalho. Conforme já exposto acima, tais dados estão diretamente ligados a privacidade do trabalhador, como por exemplo, dados atinentes a sua saúde e por isso merecem ser tratados com cautela.

5. Tratamento de dados pessoais sensíveis ligados à saúde do trabalhador

Antes de analisar o tratamento de dados pessoais sensíveis ligados a saúde do trabalhador, faz-se necessário conhecer brevemente os agentes de tratamento dos dados, são eles o controlador e o operador, conforme dispõe o art. 5º, IX, da LGPD.

De acordo com a Autoridade Nacional de Proteção de Dados - ANPD (2021), o controlador pode ser pessoa física ou jurídica, de direito público ou privado, responsável pelas decisões referentes ao tratamento de dados pessoais. No geral, o controlador será uma pessoa jurídica, como por exemplo, o empresário que será responsável pelo tratamento dos dados do trabalhador.

O operador também poderá ser uma pessoa física ou jurídica, de direito público ou privado, responsável pelo tratamento dos dados em nome do controlador, ou seja, ele deverá seguir suas ordens quanto ao tratamento. Cabe-se destacar que o operador não poderá ser empregado, sócio ou servidor, deverá ser uma pessoa distinta do controlador (ANPD, 2021).

De acordo com LGPD, os agentes de tratamento são responsáveis pela reparação do dano patrimonial, moral, individual ou coletivo que causarem a outrem. Em regra, a responsabilidade é do controlador, porém, o inciso I, § 1º, do art. 42 da Lei dispõe que o operador responderá solidariamente pelos danos causados em razão do tratamento irregular dos dados, isto é, quando descumprir as obrigações da legislação ou quando não seguir as instruções do controlador (BRASIL, 2018).

Além dos agentes de tratamento citados acima, a LGPD determina que o controlador indique o encarregado pelo tratamento dos dados que será responsável pela comunicação entre o controlador, o titular dos dados e a ANPD.

Merece realce a figura do encarregado, pois ele será responsável pelas reclamações dos titulares, por prestar os devidos esclarecimentos e adotar as providências cabíveis, bem como orientar os funcionários da empresa a respeito das práticas de proteção de dados pessoais, conforme dispõe o art. 41, § 2º, da LGPD (BRASIL, 2018).

Nesse contexto, têm-se os agentes de tratamento dos dados, inclusive dados pessoais sensíveis. Para Doneda (2019) os dados sensíveis podem ser utilizados de forma discriminatória ou lesiva, por isso, a criação dessa categoria, visto que os efeitos da circulação desses dados possuem um elevado potencial lesivo em relação ao demais.

Dentre os dados sensíveis, destacam-se no presente artigo os dados ligados a saúde do trabalhador. Tais dados são coletados desde a fase pré-contratual, como por exemplo, perguntas referentes à saúde física e psíquica do trabalhador durante um processo seletivo para vaga, até a fase pós-contratual com as informações coletadas pelo exame demissional.

Além dos exemplos citados acima, durante a relação de trabalho há o tratamento de diversos outros dados, tais como informações para convênio e utilização do plano de saúde, atestados e exames médicos, medicamentos, entre outros que devem ser armazenados de forma segura pelo controlador.

Com relação ao tema, o Repertório de Recomendações Práticas de Proteção de Dados Pessoais do Trabalhador da OIT (1997) dispõe que os dados médicos do trabalhador só deverão ser coletados quando as informações forem necessárias para verificar se ele está apto para determinado posto de trabalho; se pode cumprir com os requisitos de segurança e saúde do trabalho; e, mais, se pode ter direito a prestações sociais (MACHADO; CALCINI, 2019).

No entanto, as empresas, a fim de obter o maior número de informações a respeito dos trabalhadores, acabam coletando uma quantidade massiva de dados desnecessários para a sua finalidade, desrespeitando, com tal conduta abusiva, os direitos de personalidade do trabalhador, em especial o direito de privacidade e intimidade. Ocorre que nessas relações marcadas pelo desequilíbrio entre as partes, tais como a relação de trabalho, o titular dos dados acaba não questionando sobre a coleta excessiva de seus dados.

Nessa linha, por relevante, cabe colocar em destaque a lição de Moreira (2010, p. 30):

O direito à privacidade é um direito que se encontra ligado à dignidade do trabalhador enquanto pessoa e, por isso, justifica-se a sua consagração ao nível do Direito do trabalho. O contrato de trabalho pressupõe o reconhecimento da dignidade do trabalhador, sendo que a execução das obrigações que dele decorrem não podem traduzir-se num atentando à dignidade de sua pessoa, devendo o ordenamento jurídico garantir-lhe os direitos fundamentais que tem enquanto pessoa e que não deixa de ter quando celebra um contrato de trabalho.

No atual cenário de pandemia causada pela disseminação do vírus SARS-CoV-2 (COVID-19) diversas medidas de prevenção estão sendo utilizadas no ambiente de trabalho, como a medição de temperatura e testes para diagnósticos. Contudo, tais medidas geram o tratamento de dados pessoais sensíveis por estarem ligadas a saúde do titular. Apesar de serem medidas necessárias para segurança de todos no ambiente laboral, esses dados devem seguir os regramentos da LGPD.

Dessa forma, a empresa deverá informar aos trabalhadores sobre o tratamento daqueles dados, tratá-los no limite da necessidade e armazená-los de forma segura para que não ocorra o vazamento dos dados e possíveis discriminações do trabalhador no ambiente laboral (CAMARGO; ZORZI, 2021).

Além das possibilidades citadas acima, a LGPD dispõe em seu art. 13, §4º, sobre a pseudonimização dos dados, isto é, um tratamento capaz de substituir as informações que identificam o titular, por um pseudônimo. Através desse tratamento, o dado perde a possibilidade de associação a um indivíduo, senão pela reversão do procedimento ou pelo uso de informação adicional mantida pelo controlador em ambiente seguro. Tendo em vista a vulnerabilidade dos dados sensíveis, tal técnica mostra-se ideal para garantir um tratamento controlado e seguro pelo controlador dos dados (BRASIL, 2018).

Portanto, como medida de segurança, todos os trabalhadores deverão ser informados e/ou treinados para o manuseio legalmente correto dos dados, em especial o descarte de documentos. Competem ao empresário (controlador) todas as precauções com os dados dos trabalhadores (PINHEIRO; BOMFIM, 2020).

Diante do exposto, percebe-se a importância da aplicação da LGPD nas relações de trabalho, tendo em vista o tratamento de diversos dados nessas relações. Ressalta-se a vulnerabilidade dos dados sensíveis ligados a saúde do trabalhador que deverão ser tratados com cautela pelo controlador. Preferencialmente, utilizando meios seguros para o seu armazenamento, dessa forma, assegurando o trabalhador contra possíveis violações a seus direitos fundamentais de personalidade.

Conclusão

Em um cenário de análise massiva de dados surge, em 2018, a Lei Geral de Proteção de Dados Pessoais com o objetivo de regular o tratamento de dados de pessoas naturais e assegurar os seus direitos fundamentais de liberdade e privacidade e o livre desenvolvimento de sua personalidade.

Na esfera das relações de trabalho, sua aplicação é inevitável a fim de conter o uso excessivo de dados dos trabalhadores. Para tanto, a LGPD fixa limites e procedimentos para o tratamento desses dados, bem como, dispõe sobre os princípios que podem ser considerados base da legislação, como os analisados no desenvolvimento deste artigo: princípios da boa-fé, finalidade, necessidade e adequação.

Deve-se ressaltar o tratamento e a utilização dos dados desde a fase pré contratual até a fase pós contratual da relação de trabalho com objetivo de reunir o maior número de informações dos trabalhadores e até mesmo traçar o seu perfil através desses dados causando uma possível discriminação.

Esses dados deverão ser tratados em conformidade com a legislação, isto é, sendo coletados apenas nos casos permitidos e dentro do limite necessário. Ademais, frisa-se que a lei tem como fundamento a autodeterminação informativa, ou seja, o trabalhador terá direito de saber como ocorre o tratamento dos seus dados pela empresa.

Como analisado, os dados podem ser diferenciados como dados pessoais e dados pessoais sensíveis, sendo que, o último deverá ser tratado com cautela, pois pode apresentar informações com elevado potencial discriminatório para seus titulares.

Dentre os dados sensíveis destacam-se os dados ligados a saúde do trabalhador. Tais dados são tratados em exames admissionais e demissionais, atestados médicos, cadastro para plano de saúde, medição de temperatura, resultados de diagnósticos, entre outros. Tendo em vista sua vulnerabilidade, eles deverão ser

tratados, bem como armazenados e controlados de forma segura.

Para tanto, aconselha-se a utilização de meios seguros para o armazenamento dos dados, como por exemplo, a utilização de criptografias e pseudonimização desses. Além disso, a empresa deve orientar os trabalhadores a terem cuidados com documentos que contenham dados pessoais, a fim de criar segurança no ambiente de trabalho.

Recomendável, do mesmo modo, que a empresa mantenha um programa de *compliance* trabalhista, estabelecendo regras internas claras, obrigando a todos os atores, no âmbito empresarial, a observar os estritos ditames da LGPD, com especial cautela no que se refere aos dados pessoais sensíveis ligados a saúde dos trabalhadores.

Conclui-se, portanto, que a efetiva aplicação da LGPD nas relações de trabalho garantirá maior segurança aos trabalhadores em relação aos seus dados e sua privacidade. Dessa forma, resta à empresa se adequar as regras estabelecidas pela legislação.

REFERÊNCIAS

ANPD. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e Encarregado**. Brasília, 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf. Acesso em: 08 jun. 2021.

BRASIL. **Decreto-Lei nº 5.452, de 1º de maio de 1943**. Consolidação das Leis do Trabalho (CLT). Disponível: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del5452.htm. Acesso em: 08 de jun. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 08 jun. 2021.

CAMARGO, Camila; ZORZI, Marco. Protocolos de acesso ao ambiente de trabalho e proteção dos dados pessoais. **Revista Consultor Jurídico**, 2021. Disponível em: <https://www.conjur.com.br/2021-mai-09/opiniao-acesso-ambiente-trabalho-protacao-dados>. Acesso em: 08 jun. 2021.

CONI JUNIOR, Vicente Vasconcelos; PAMPLONA FILHO, Rodolfo. *In*: MIZIARA, Raphael *et al.* (Org.). **Reflexos da LGPD no Direito e no Processo do Trabalho**. São Paulo: Revista dos Tribunais, 2020. p. 74-124.

DACHERI, Emanueli. **A eficácia horizontal dos direitos fundamentais de personalidade**: limites ao poder empregatício de controle e monitoramento tecnológico do trabalho humano. Rio de Janeiro: Lumen Juris, 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019.

GOLDSCHMIDT, Rodrigo. Direitos da Personalidade do Trabalhador: aproximações conceituais e tentativa de conformação de um microsistema trabalhista. *In*: GOLDSCHMIDT, Rodrigo (Org.). **Direitos da Personalidade do Trabalhador**. Rio de Janeiro: Lumen Juris, 2019. p. 1-36.

HARARI, Yuval Noah. **Homo Deus: uma breve história do amanhã**. São Paulo: Companhia das letras, 2016.

JOBIM, Rosana Kim. **Compliance e trabalho: entre o poder diretivo do empregador e os direitos inespecíficos do empregado**. Florianópolis: Tirant Lo Banch, 2018.

LIMA, Caio César Carvalho. Capítulo II – Do tratamento de dados pessoais. *In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). Lei Geral De Proteção De Dados comentada*. São Paulo: Revista dos Tribunais, 2019. p. 201-241.

MACHADO, Gustavo Carvalho; CALCINI, Ricardo Souza. Efeitos da Lei Geral de Proteção de Dados nas relações de trabalho. **Portal Colégio Registral Rio Grande do Sul**, Porto Alegre, 14 fev. 2019. Disponível em: <https://www.colegioregistrals.org.br/doutrinas/artigo-efeitos-da-lei-geral-de-protacao-de-dados-nas-relacoes-de-trabalho-por-gustavo-carvalho-machado-e-ricardo-souza-calcini/>. Acesso em: 08 jun. 2021.

MOREIRA, Teresa Alexandra Coelho. **A privacidade dos trabalhadores e as novas tecnologias de informação e comunicação: contributo para um estudo dos limites do poder de controlo eletrónico do empregador**. Coimbra: Almedina, 2010.

PINHEIRO, Iuri; BONFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. *In: MIZIARA, Raphael et al. (Org.). Reflexos da LGPD no Direito e no Processo do Trabalho*. São Paulo: Revista dos Tribunais, 2020. p. 48-72.

RAMOS, Lara Castro Padilha. **Lei Geral de Proteção de Dados Pessoais e seus impactos na garantia do direito fundamental à proteção de dados do trabalhador**. 2020. 100 f. Dissertação (Mestrado) - Curso de Direito, Universidade de Fortaleza, Fortaleza, 2020. Disponível em: <https://uol.unifor.br/oul/conteudosite/F10663420200925160712130871/Dissertacao.pdf>. Acesso em: 08 jun. 2021.

SILVA, Fabrício Lima; PINHEIRO, Iuri; BOMFIM, Vólia. **Manual do Compliance Trabalhista: teoria e prática**. 2. ed. Salvador: Juspodivm, 2021.

VAINZOF, Rony. Capítulo I – disposições preliminares. *In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). Lei Geral de Proteção de Dados comentada*. São Paulo: Revista dos Tribunais, 2019. p. 22-200.

35. O TRABALHO EM TEMPOS DE REVOLUÇÃO TECNOLÓGICA E DA PANDEMIA DE COVID-19: PROTEÇÃO DE DADOS PESSOAIS E PRECARIZAÇÃO LABORAL - SEGREGAÇÃO E/OU COOPERAÇÃO?

WORK IN TIMES OF TECHNOLOGICAL REVOLUTION AND THE COVID-19 PANDEMIC: PERSONAL DATA PROTECTION AND LABOR PRECARIZATION - SEGREGATION AND/OR COOPERATION?

GERALDA MAGELLA DE FARIA ROSSETTO¹
E ENDY DE GUIMARÃES E MORAES²

Resumo: A pandemia do COVID-19 deflagrou um novo cenário, no qual a tecnologia e demais categorias que lhes são conexas, tais como, a proteção de dados pessoais e uma figura importante às redes – no caso, a cooperação - tem impactado as relações laborais e redefinido a saúde, inclusive a pública. Em referida razão e contexto, o trabalho, em contraponto à tecnologia, é examinado na perspectiva da pandemia, tendo por fio condutor duas categorias, o teletrabalho e o home office, como também, a especial condição da saúde e vulnerabilidade humana em face da COVID-19. O Método a ser utilizado na fase de investigação foi o dedutivo.

Palavras-chave: Tecnologia; COVID-19; Proteção de Dados; Teletrabalho; Home Office.

Abstract: The COVID-19 pandemic has triggered a new scenario, in which technology and other related categories, such as personal data protection and an important feature in networks - in this case, cooperation - has impacted labor relations and redefined health, including public health. In this context, work, in counterpoint to technology, is examined in the perspective of the pandemic, with two categories, telework and home office, as the common thread, as well as the special condition of health and human vulnerability in light of COVID-19. The deductive method was used in this research.

Key-words: Technology; COVID-19; Data Protection; Telework; Home Office.

1. Introdução

Estas breves considerações têm como objetivo analisar a categoria do trabalho e de suas relações e “processos” estabelecidos, tendo como pano de fundo a proteção de dados, nestes dias em que a humanidade trava batalha contra o SAR-

1 Doutorado em Direito pela UFSC. Mestrado em Direito pela UNISINOS. Advogada. Procuradora Federal aposentada. Pesquisadora do Direito e Fraternidade; DataLab e NEJUSCA. Email: geraldamagella@gmail.com.

2 Doutoranda em Direito pela Fordham University; Mestrado em Direito pela Fordham University. Advogada e Diretora do Instituto sobre Religião, as Leis e os Advogados, Fordham University. Email: emoraes@law.fordham.edu.

S-CoV-2 (vírus que causa a doença COVID-19)³, sobretudo, dado que o avanço do contágio disseminou de tal forma que as relações sociais como as conhecíamos encontram-se sob ameaça e, somente com muita disposição, a ciência, a política e muita informação de qualidade, leitura e interpretação adequadas de dados, poderão corrigir o curso instalado por esse vírus e, assim, retomar as atividades sociais e de trabalho dentro de um cenário que, mesmo presente a precarização, não implique em tamanha insegurança e riscos como a instalada pelo Coronavírus.

A pandemia passou por várias fases, primeiramente acreditou-se que a letalidade resultasse da idade avançada, de grupos de riscos e da exposição, que muitos não acreditavam. Para os demais membros da população, o risco se apresentaria muito menor. Contudo, o resultado que se observou pelo número de mortes parece ter seguido padrão distinto.

O cenário atual predispõe uma série de mudanças e de necessárias medidas, das quais não escapou a categoria do trabalho⁴, independentemente de sua classificação, agenda, protocolos, diretrizes, regulações e regulamentações, podendo justificar, em nome da excepcionalidade e das circunstâncias decorrentes da pandemia, muitas alterações para as quais é preciso certas disposições cujo nome e atitude atende pelo avanço da pandemia, porque as mudanças poderão deixar de atender as conquistas sociais e laborais em nome das regras e interesses do mercado.

Neste estudo, a título de reflexão, toma-se em empréstimo duas importantes figuras, no caso a tecnologia e a proteção de dados, objetivando verificar o comportamento do trabalho em tempos da pandemia da Covid-19. Sobretudo, propõe-se verificar como o labor encontra sua “formatação”, tendo como pano de fundo a segregação (isolamento ou distanciamento social) e a cooperação, a fim de compreender a sua reconfiguração nestes tempos em que a normalidade escapou de nosso controle e passa a conhecer outras esferas.

Ainda, onde consta pandemia, em relação ao Direito, há disposição para a restrição de liberdades fundamentais. A respeito da vigilância epidemiológica e das disposições políticas levadas a determinações contidas em muitos dispositivos e regulamentos, também, variada autorregulamentação, a expressão significa a quarentena, a limitação de viagens, o fechamento das fronteiras, a restrição ou a supressão de reuniões, públicas ou privadas, o tratamento médico, o acesso aos leitos hospitalares, a responsabilidade pessoal e informacional – das mídias, além das questões pertinentes à privacidade.

No mais, examina-se a precarização do trabalho, e, para tanto, esta breve investigação contempla as temáticas seguintes, aptas que são a apresentar um panorama de suas questões cruciais e da estrutura de seus desafios e potencialidades, independentemente da ordem: concepções e perspectivas críticas sobre a precarização, suas atuais características e repercussões, reconfigurações individuais, institucionais, sociais, aspectos da saúde em sua dimensão coletiva, a indicar o grau de ma-

³ “A COVID-19 é uma doença infecciosa causada pelo novo coronavírus (SARS-CoV-2) e tem como principais sintomas febre, tosse seca. Uma em cada seis pessoas infectadas por COVID-19 fica gravemente doente e desenvolve dificuldade de respirar”. (OPAS BRASIL, 2021). Disponível em: <https://www.paho.org/bra/index.php?option=com_content&view=article&id=6101:covid19&Itemid=875>. Acesso em: 25 out 2021.

⁴ Formal ou informal; público ou privado; doméstico ou empresarial; nacional ou internacional.

turidade das relações de trabalho, tomadas no viés do Estado, das instituições, das empresas e do próprio ser humano.

A disposição para o tema encontra-se centrada na figura da proteção de dados pessoais, que é, por assim dizer, a razão do presente estudo, sendo que seu conceito no presente, trata-se de todo e qualquer assento ou registro ocorrentes em um determinado local ou em vários locais, mediante suporte eletrônico ou físico, por meio de papel ou não, com utilização ou não de imagens, de sons e/ou de figuras, que implique em transmissão de dados de cunho pessoal, ou submetido a meios de arquivos e tratamentos, referentes à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, a demandar a realização laborativa (ROQUE, 2019, p.3).

Também é importante levar em conta, que o reconhecimento do direito à proteção de dados, pertence à classe dos direitos fundamentais, qual seja, com eficácia direta e imediata, conforme consta dos ensinamentos de Sarmento, típica dessa categoria de direito, prevalecendo o condão de que sejam respeitados, não apenas e tão somente na relação entre Estado e sujeito(s), e igualmente entre particulares (SARMENTO, 2008, p. 107).

Para tanto, recorre-se a outras categorias que imprimem à relação de trabalho novas disposições, quais sejam, além da proteção de dados, conforme indicado, toma-se também a precarização laboral, e, no seu conjunto, referidas categorias são brevemente expostas pela dimensão da segregação e/ou da cooperação.

O desenvolvimento do estudo encontra-se assim distribuído, além da introdução, das considerações finais e das referências, inclusive bibliográficas e outras mais: o primeiro tópico temático tem como “mote” apresentar o cenário e a escalada da pandemia desencadeada pelo SARS-CoV-2; o segundo tópico expõe o isolacionismo ou a segregação e o papel da cooperação em sede de precarização laborativa, tendo em perspectiva a função da proteção de dados; e, por último, o terceiro tópico, retoma a tecnologia e seus efeitos na dimensão do trabalho, notadamente no teletrabalho e no home office.

A metodologia a qual se recorre para desenvolver o presente estudo, refere-se ao método de abordagem dedutivo, pelo procedimento monográfico e pela técnica de pesquisa bibliográfica, documental e, sobretudo, à análise de textos referenciais e bibliográficos, inclusive monográficos que tenham a temática em sua forma central ou transversal.

2. Cenário Experimentado e a escalada da pandemia desencadeada pelo SARS-CoV-2

Ao longo da História muitas sociedades enfrentaram episódios de riscos biológicos, dentre os quais, são ora citados como exemplos, a Peste Negra europeia ou Peste Bubônica (1347-1351); o impacto das doenças ‘europeias’ em populações nativas da América, em vários períodos e tempos da história⁵, e a Gripe Espanhola

5 A esse respeito Yuval Noah Harari (2020a) aponta que “Em março de 1520, um único hospedeiro da varíola — Francisco de Eguía — desembarcou no México. Na época, a América Central não tinha

(1918-1920); e, para não deixar de retratar a situação doméstica, significativa é a questão da varíola, a qual, no caso brasileiro, foi enfrentada nos inícios de 1900, que levou o então Presidente Rodrigues Alves, a enfrentar a Revolta da Vacina (1904) no Rio de Janeiro, na época Distrito Federal (SEVCENKO, 2018, p. 22), os quais acenaram as dificuldades enfrentadas, dignas da mais absoluta ignorância e desconhecimento científico⁶.

Todos esses fatos, antes declinados, dão conta de crises que tiveram por razão a questão da saúde, inclusive a pública, a indicar parâmetros de uma analogia histórica aberta a reflexão sobre a crise que ainda enfrentamos em 2021. Mas não é demais inferir, as condições do Coronavírus que, por si, dão azo às especificidades *sui generis*.

A respeito do conceito de pandemia, a Emergência de Saúde Pública de Importância Internacional (ESPII) é considerada, nos moldes do Regulamento Sanitário Internacional (RSI), “um evento extraordinário que pode constituir um risco de saúde pública para outros países devido a disseminação internacional de doenças; e potencialmente requer uma resposta internacional coordenada e imediata” (OPAS BRASIL, 2020).

A Organização Mundial da Saúde (OMS) declarou, em data de 30 de janeiro de 2020, que o surto do novo Coronavírus a desencadear a COVID-19 constituiu uma Emergência de Saúde Pública de Importância Internacional (ESPII) – o mais alto nível de alerta da Organização, conforme previsto no Regulamento Sanitário Internacional. Em 11 de março de 2020, a COVID-19 foi caracterizada pela OMS como uma pandemia (VENTURA, 2020, p. 6). Essa decisão buscou aprimorar a coordenação, a cooperação e a solidariedade global para interromper a propagação do vírus (OPAS BRASIL, 2020). Frente a cenários pandêmicos, mostra-se essencial a utilização da estrutura de gerenciamento de riscos de desastres em saúde e emergência da OMS para complementar as respostas atuais à COVID-19 e o risco de fenômenos semelhantes no futuro (RIYANTI, 2020).

Em podcast recente, o chefe interino do Grupo de Pesquisa em Biossegurança do Instituto Futuro da Humanidade da Universidade de Oxford apontou que é vital aprender com as lições desta pandemia e fornecer a nossos descendentes a segurança que desejamos a nós mesmos (LEWIS, 2020). Percebe-se que a COVID-19 é lembrete vívido de que somos vulneráveis a ameaças biológicas e estamos mal preparados para lidar com elas.

A condição de pandemia capitaneada pela Covid-19 está a esculpir aos dias

trens, ônibus, nem mesmo jumentos. No entanto, por volta de dezembro uma epidemia de varíola já devastava a América Central inteira, matando, de acordo com algumas estimativas, quase um terço de sua população”.

6 Digno de nota, tem-se a manifestação de Rui Barbosa, que apesar da enorme e significativa cultura e reconhecimento público, político conceituado, sobre a possibilidade da campanha de vacinação, levada a termo por Oswaldo Cruz, então diretor de Saúde Pública do Rio de Janeiro, assim se manifestou: “Não tem nome, na categoria dos crimes do poder, a temeridade, a violência, a tirania a que ele se aventura, expondo-se, voluntariamente, obstinadamente, a me envenenar, com a introdução no meu sangue, de um vírus sobre cuja influência existem os mais bem fundamentados receios e que seja condutor da moléstia ou da morte”. (SEVCENKO, 2018, p. 23). A tal respeito, encontra-se a firme posição de Müller: “Rui Barbosa, portanto, ampara seu posicionamento em relação à campanha de vacinação em uma junção de argumentos de caráter jurídico (‘crimes do poder’), político (‘tirania a que ele se aventura’), moral (o governo estaria, segundo ele, envenenando-o) e técnico (introdução de um vírus em seu sangue)”. (MÜLLER, 2020).

atuais a tônica de uma crise global, um hápax⁷ sem precedentes.

A tal respeito Harari (2020b) pontua que

[...] embora uma quarentena temporária seja essencial para deter epidemias, o isolacionismo prolongado conduzirá ao colapso econômico sem oferecer nenhuma proteção real contra doenças infecciosas. Muito pelo contrário. O verdadeiro antídoto para epidemias não é a segregação, mas a cooperação.

No âmbito internacional, porém, a dinâmica mais do que humanitária, é de animosidade. Será que se deveria esperar atitude outra, aquela da lição ética, de aprender profundos significados na vivência da dor e do sofrimento? Antes de avançar sobre as lições da cooperação, muitos adiantaram-se, e estão a militar o isolacionismo.

Ora, a proposta, mais do que de resistência, é simbólica de significados, sobretudo quando se volta para as experiências a que toda a humanidade, os países e suas gentes estão a experimentar. Esse algo que há de se resistir tanto a uma quanto a outra tendência, a dar conta de seu verdadeiro significado e lugar: a que se apoia em aprendizagens, ainda que menores, mas de que a história humana está repleta, e, assim dar passos ao que o conhecimento intelectual e científico deve premiar: o do conhecimento calcado no ideal humanista, a iluminar o caminho da humanidade na direção benfazeja do bem comum, e, assim, assegurar um valor primeiro à presença e desenvolvimento da existência do ser humano no planeta.

Nesse sentido, o mal provocado a quem quer que seja, quando atinge o ser humano, afeta a humanidade inteira, a dar conta de que o mal extremo que chega a um, em particular, igualmente chega a todos, em sua universalidade. É do legado da unidade que cabe a cada um tocar e cuidar, tal qual o presente mais valioso a que fomos destinados dedicar-se com responsabilidade e esmero.

3. O isolacionismo ou a segregação e o importantepapel da cooperação em sede de precarização laborativa: há lugar para a proteção de dados?

A chamada Revolução 4.0 – voltada precipuamente para a tecnologia e a expansão da automatização nos processos produtivos, notadamente quando se lança mão das potencialidades do uso de inteligência artificial - tem gerado impactos disruptivos em várias esferas, como ocorre, por exemplo, com a área do trabalho e a da saúde, seja substituindo mão de obra, seja mediando processos digitais para que os seres humanos produzam em larga escala e acentuada produção, além de obter significativa – pelo menos esperada – potencialidade na esfera medicamentosa.

Mais significativo que todos esses aspectos há a qualidade do dado pessoal, e sua capacidade de informação relacionada à pessoa natural identificada ou identificável. Ainda, na esfera da saúde, o dado pessoal sensível, diz respeito à informação sobre origem racial ou étnica, convicção religiosa, política, filiação a sindicato ou a organismo de caráter religioso, filosófico ou político, vida sexual, dado genético ou biomédico.

Se tomado o trabalho sob a perspectiva do dado da saúde, notadamente a pú-

⁷ O significado da palavra tem a ver com um único exemplo que se pode extrair até então.

blica, no cenário da Revolução 4.0, pode ser dito que referido contexto alterou o desenvolvimento tecnológico e, também, mudou o paradigma da saúde. Santos (2019), aponta que as mudanças são perceptíveis em várias dimensões, tais como, em processos de gestão, na medicina preventiva, assistiva, diagnóstica e terapêutica.

De qualquer modo, o aumento na capacidade do processamento de informações – em especial a redução de seus custos – representa um significativo passo para o desenvolvimento e capacidade de analisar uma grande quantidade de dados, de forma que o Big Data é tomado em relação ao tratamento de dados a utilizar um amplo volume e variedade de dados, por meio de uma alta velocidade (VERONESE, 2019).

Em todas essas situações o direito em si precisa fazer-se presente, a não ser que se admita a chegada dos deveres sem a sua condução correspondente, de tal forma que a construção de marcos jurídicos, tanto no direito internacional (em relação a legislação brasileira, pela influência, dá-se preferência ao direito europeu), e no direito nacional, o propósito é fornecer proteção de dados aos cidadãos⁸.

Contudo, na relação dos seres humanos com as máquinas, em como os humanos podem administrar outros humanos, é importante atentar para uma significativa problemática: é o caráter humano – e não a técnica – que está a fornecer soluções para os seres humanos, de onde decorre, a fundamentalidade da cooperação na esfera das relações humanas em sociedade.

Sendo mais específico,

A utilização de sistemas de captação de dados, que vão do prontuário eletrônico – com dados clínicos e laboratoriais – a dados coletados diretamente do indivíduo, no decorrer de suas atividades diárias, pelos chamados “wearables”, capazes de monitorar sinais vitais, atividade física, hábitos alimentares etc., que podem ser integrados, processados e analisados, já é uma realidade para um número significativo de pessoas no mundo (SANTOS, 2019).

Contudo, conceber a proteção de dados, quer em sua teoria e/ou prática, sobretudo, em suas leis gerais, enquanto condizentes com certos graus de aberturas aos direitos, como parte da empreitada de proteção dos direitos fundamentais, notadamente em face do direito ao trabalho e da própria organização e disposição do trabalho, é estar às voltas com discussões afeitas ao viés tecnológico, e, portanto, permeadas por valores, persuasão e negociação.

Agregadas a essas situações então apresentadas, a pandemia deixa uma exposição evidente: teremos de reaprender a difícil lição do isolamento, no que, o exercício da cooperação pode trazer um real significado aos relacionamentos – antes, o importar-se com o outro do que o discurso único do “venha a nós”.

Nesse sentido, a cooperação pode ser medida no apoio recíproco e, portanto, com a capacidade de entender e mostrar-se receptivo ao outro e agir em conjunto, uns com os outros, uns pelos outros e uns para os outros. Segundo Sennett, a

⁸ No Brasil, a Lei 13709, de 2018, qual seja, a Lei Geral de Proteção de Dados Pessoais, dispõe sobre o tratamento de dados.

cooperação pode ser definida, sucintamente, como uma troca em que as partes se beneficiam. Há cooperação para conseguir o que não pode ser alcançado sozinho (SENNETT, 2018, p. 21-22). Trazida para a esfera do trabalho, a cooperação volta-se às relações trabalhistas.

Parte-se do pressuposto de que a cooperação, não se trata de pensamento marginal, e sim de fonte inescapável dos dias que se seguem de forma que, muito mais que a segregação, é importante enaltece-la em nossas relações. Traduzi-la para o mundo do trabalho requer uma firme disposição que a pandemia, a custo de muita dor e pesado sofrimento, poderá nos obrigar a lições e aprendizados, de forma que, a cooperação voltada a linha da “cooperação social”⁹, e até mesmo a que se estabelece no âmbito do trabalho, tem amplos significados na capacidade de ouvir e trabalhar em sintonia com os outros.

De outro modo, em outro polo das relações, pode ser encontrada a precarização laborativa (LIMA, 2018), a qual, inobstante fenômeno da atualidade, articulada à tecnologia, produziram situações, as quais, voltam-se muito mais ao desprestígio do trabalho do que propriamente usufrui da condição de reconhecimento e destaque.

Examina-se a precarização do trabalho como sendo elemento compositivo da proposta tecnológica, sobretudo, porque igualmente produtor e pertencente à rede de proteção de dados, configurativa da nova realidade que emerge com a reestruturação e produção do trabalho. De sua pouca valorização e acentuado desprestígio, oportuniza-se a sua precarização e com ela a pouca qualidade e reconhecimento dos dados a lhes dar suporte e sentido (LIMA FILHO, 2020).

A respeito da precarização do trabalho, sua tradução tem depositado na flexibilização e na própria precarização do emprego – onde, tanto o trabalho temporário e o próprio desemprego usufruem de visibilidade ampla – a desafiar a própria configuração das relações de trabalho, a questionar o modelo de reconhecimento e qualificação do trabalho, mesmo que em sede de empresas com notória estabilidade. Sobretudo, ela deve ter como norte, ajustar a aplicação dos preceitos normativos às especificidades regionais, profissionais ou empresariais e, notadamente, em tempos de pandemia, precisa ser ajustada, adequando-se às exigências relativas à saúde pública e sua segurança.

Dentre as mudanças sociais, presentes na seara do trabalho, sobretudo as anunciadas pelo liberalismo a todo preço e custo, destaca-se a precarização do trabalho, como elemento a compor uma nova dimensão na esfera das relações trabalhistas e do trabalho em si, dando lugar para a intensificação e a ampliação da exploração e a espoliação da sua força.

Contudo, haveremos de ter clara consciência. É a cooperação antes que a segregação, ou até mesmo a precarização laborativa, antes que o reconhecimento do trabalho, os componentes da agenda que requer sejam repensados, no que não deixam desdizer os fenômenos de que estão cheios os dias atuais.

Aliás, quando se lança mão da cooperação, articulada às relações do trabalho,

⁹ Sennett a respeito da cooperação, refere a mesma como capacidade de entender e mostrar-se receptivo ao outro, para agir em conjunto. Nesse viés, trata a cooperação com atenção na receptividade aos outros, como acontece na capacidade de escuta em uma dada conversa, e, até mesmo, na receptividade do trabalho em uma comunidade. (SENNETT, 2018, p. 23).

as relações se enriquecem. Porém, tomada em contraponto ao segregacionismo, há terreno fértil para a prevaricação laboral. Seja qual for o caminho eleito e o trilho a seguir, é necessário que o trabalho passe a pensar em um “modelo” que nos dias contemporâneos atenda as implicações e os desafios relacionados ao Covid-19.

Nesse sentido, a demanda do trabalho requer adequar-se ao teletrabalho, ao home office, e ao cybertrabalho que então passam por uma reestruturação, cujo sentido impõe mais considerações como as que a seguir serão expostas.

4. A Tecnologia e seus efeitos no Teletrabalho e no Home Office

O surgimento e os desdobramentos da tecnologia levaram a profundas transformações na dinâmica da sociedade, inclusive, em suas relações de trabalho, tendo afetado de forma significativa as disposições laborativas, de onde despontou o teletrabalho e sua organização (ARAÚJO, 2020).

Em linhas gerais, a tecnologia permitiu o trabalho à distância e com ela nasceu o teletrabalho, de forma que, com a mesma audácia que atingiu a relação empregado versus empregador, também viabilizou formas de controle quase absolutas das atividades laborais, dispostas em um conjunto estruturado, com transmissão de dados, produzidos por meio de imagens, sons, escritos, estabelecido em um ou em vários locais, em suporte eletrônico ou físico, em tempo real ou submetido a meios de arquivos e tratamentos, a alterar o convívio pessoal, social, econômico e laboral, e até mesmo, a demandar operação e cumprimento de trabalho, a ser realizados, ou por realizar, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Com a mesma força que irrompeu as mudanças, a tecnologia em contato com o mundo do trabalho, também abriu para um novo e crescente ambiente laborativo, apresentando ao mundo a proposição disruptiva, a encerrar a ideia de trabalho a distância em que foram agregadas as modernas tecnologias da informação e da comunicação. Reside nesse particular a distinção que há entre o teletrabalho e a ideia tradicional do trabalho prestado em domicílio (ou trabalho em domicílio).

Assim, a configuração do teletrabalho requer o atendimento dos seguintes requisitos básicos: i) o empregado deve desenvolver suas atividades precipuamente fora das dependências de seu empregador e precisa utilizar tecnologias da informação ou da comunicação para levar a termo suas tarefas e atividades, servindo nesse caso de plataforma digital do empregador, a sua disposição e indicação.

A grosso modo o teletrabalho e o home office cumprem dinâmicas semelhantes, de forma que, em tradução literal, o teletrabalho pode transparecer uma espécie de home office, porém, o contrário não corresponde a realidade, de forma que, nem todo home office é teletrabalho. Uma consideração a ser levada em conta é o fato de que para efeitos de trabalho domiciliar, aqui indicada como sinônimas, como a própria expressão sugere, não há necessidade de estar conectado para realização das tarefas. Assim, diante dessa consideração, a realização de tarefas não necessariamente está dentro dos parâmetros do teletrabalho, mas tão somente, na hipótese de trabalho domiciliar – que, nos termos contidos no artigo 6º da CLT, se equipara ao trabalho tradicional desenvolvido na sede da empresa.

Outro aspecto a ser levado em conta, trata-se no fato de que há exigência legal para a realização do teletrabalho, a celebração de acordo formal (seja dispositivo contratual ou aditivo) para a instituição de tal regime, além da observância do prazo de 15 dias, para readaptação do empregado em caso de retorno ao serviço presencial, o que, na prática, pode tornar a medida pouco usual, nada objetiva, especialmente em situações excepcionais como está a demandar os tempos da COVID-19, ainda que se trate de uma pandemia, presente em toda a terra, certamente a usufruir de notoriedade global.

Há ainda uma terceira observação. É que a CLT, pós reforma de 2017, estabelece que os empregados quando submetidos ao teletrabalho, não são sujeitos ao controle de jornada. Essa condição confere aos mesmos total flexibilidade em relação aos horários de ativação, enquanto que o empregado em regime de home office (sem vínculo expresso com os requisitos do teletrabalho; não deve ocupar função externa e nem cargo de confiança), deve atender, cumprir e observar os mesmos horários do trabalho presencial, sendo de igual forma, esperada a fiscalização de horários e o controle que deve ser mantido na jornada cumprida em casa.

Cumpre também destacar, exatamente pela dimensão que alcança diretamente a saúde e a segurança do trabalhador e indiretamente, de toda a coletividade, ao tratar sobre o teletrabalho, a CLT dispõe a respeito da responsabilidade sobre esses temas, que são aplicáveis ao exercício da função realizadas fora da empresa, a dar conta da precaução necessárias para evitar doenças e acidentes.

Ao invés, quando se remete ao trabalho domiciliar, o home office, que não se enquadra na categoria anterior, são seguidas as mesmas disposições vigentes para os que trabalham durante todo o tempo junto ao seu empregador, sendo dele – e não do empregado – a responsabilidade quanto ao cumprimento das normas relativas à saúde e segurança. Percebe-se que a natureza dos riscos ocupacionais acompanha a aceleração da inovação, bem como o surgimento de novos fatores de risco e a transformação do trabalho (ESHW, 2009).

Todas essas questões quando submetidas às questões de proteção de dados podem ainda ser mais complexas, na medida em que, são acrescidas novas realidades e dispositivos de cumprimento, além do aspecto de que outros requisitos necessitarão de adoções. É que a esfera de resguardar e proteger os dados, igualmente dão conta de novos mecanismos e dispositivos que precisam ser resguardados.

Nessa perspectiva, o dado referente à saúde, o dado genético ou o biométrico, dentre outros, possuem a condição de dado sensível, consoante encontra-se disposto no art. 5º da Lei Geral de Proteção de Dados, a Lei 13709, de 2018, e, em razão da tutela da saúde, o seu tratamento, somente poderá ser realizado, conforme consta no art. 7º da LGPD, exclusivamente, em procedimento às expensas e realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

De qualquer modo o cenário de enfrentamento desse patógeno, onde, segundo Morin (2020), certas necessidades podem ter sido negadas, como a de usar uma máscara, apenas para esconder o fato de que não havia nenhuma, ou ao contrário, disseram também que os testes são inúteis, a camuflar que também não tínhamos testes. Seria humano reconhecer que os erros foram cometidos e que iremos corrigi-los em uma tarefa que precisa ser de cooperação, antes que se possa vencer o

individualismo, que virá em decorrência.

Nesse aspecto, o que não dizer da liberação para o trabalho a salvar a economia (VOMMARO, 2020). As dúvidas não param por aí. Em termos de restrições de liberdades, quando postas em contato com a proteção de dados, voltados à saúde e na presença da pandemia ocasionada pela COVID-19, desponta a regra do controle ou do monitoramento em massa, possível por diversos mecanismos que já fazem parte do cotidiano da humanidade, tais como câmeras, algoritmos, drones e até celular, que podem dar conta das condições de saúde dos cidadãos, tais como histórico médico, temperatura corporal, pressão, tipagem sanguínea, alergias, etc.

A respeito dessas regras restritivas convém o destaque quanto a Lei n. 13.979, de 6 de fevereiro de 2020, a qual dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do Coronavírus responsável pelo surto de 2019 e, dessa forma, a mesma passa a regular as medidas e processos de saúde pública relacionadas ao novo Coronavírus. A depender e no enfrentamento dessas “escolhas”, teremos retratado alto potencial restritivo de direitos fundamentais, inclusive a quarentena e o isolamento, a qual, ao lado da legislação epidemiológica em vigor, propõe medidas excepcionais, inclusive, as salvaguardas à sua implementação.

Significativa é a posição firmada por Harari, em que revela uma decisão a ser tomada: escolher entre vigiar a população de forma totalitária — esta é a primeira vez na história da humanidade em que a tecnologia permite monitorar todos o tempo todo — ou empoderar o público com boa informação como forma de preservar vidas (HARARI, 2020a).

As relações de trabalho presentes na atualidade, sobretudo as inseridas sob a marca da tecnologia, encontram-se cunhadas sob o manto da provisoriedade, impregnadas que estão pelo tom das tendências flexibilistas, da condição da derogabilidade e da alterabilidade dos ajustes da norma legal, incluindo protocolos, diretrizes, regulamentações. Contudo, é de se levar em consideração que medidas tomadas de forma apressada, sob o manto da provisoriedade, tendem a exercer profunda interferência e transfigurar-se sob o condão da definitividade.

Frente a urgência de medidas cobradas pela atuação em face do Coronavírus, não há espaço para decisões tardias. O lugar é sim para as questões apressadas, e que estão a traduzir a instantaneidade dos acontecimentos contemplados especialmente pela tecnologia, onde a urgência, a tomada de decisão e o instantâneo precisam dar conta do imediatismo que a Sars-Cov-2 disseminou no mundo.

Esse retrato deve moldar não somente os protocolos e as diretrizes de saúde, e até mesmo os sistemas de saúde, propriamente dito, mas também, deve reconfigurar as estruturas relativas ao sistema financeiro, a economia, a política, o sistema jurídico e a cultura propriamente dita — tudo isso com base em decisões urgentes, referendadas pelo selo da emergência, tomadas no calor dos fatos, rapidamente, em meio àquela que deverá ser a maior crise experimentada pela geração que encontra-se na terra — uma pandemia sem precedentes na história da humanidade a costurar processos históricos para que avancem com o imediatismo e a urgência tão necessários, por mais que “Tecnologias imaturas e até perigosas são colocadas em serviço porque os riscos de não fazer nada são maiores. Países inteiros servem

como cobaias em experimentos sociais em larga escala” (HARARI, 2020a) e estão a corroborar quanto à “definição” do ser humano.

Um ponto, contudo, merece destaque, quando submetido à realidade dos dias do Coronavírus: grandes contingentes de seres humanos, trabalhadores, não trabalhadores, e, em especial, desempregados, sobretudo aqueles a merecer especial proteção jurídica, tais como, os nominados pela Resolução nº. 01/20, da Comissão Interamericana de Direitos Humanos, que trata sobre Pandemia e Direitos Humanos nas Américas, que são os assim declarados “os grupos historicamente excluídos ou de especial risco, tais como: pessoas maiores e pessoas de qualquer idade que tem afecções médicas preexistentes, personas privadas de liberdade, mulheres, povos indígenas, pessoas em situação de mobilidade humana, meninos e meninas, crianças e adolescentes, pessoas LGBTI¹⁰, pessoas afrodescendentes, pessoas com deficiências, pessoas trabalhadoras, e pessoas que vivem na pobreza e pobreza extrema, especialmente pessoas trabalhadoras informais e pessoas em situação de rua; assim como as defensoras e defensores de direitos humanos, líderes sociais, profissionais de saúde e periodistas” (CIDH, 2020), os quais podem encontrar-se destituídos de meios de sobrevivência em seus locais de origem e até mesmos expostos, ou com saúde em comprometimento ou já comprometida, e que, portanto, vão requerer especial atenção a demandar medidas de atuação centradas nas suas respectivas pessoas.

Portanto, dificilmente serão incorporados ao sistema produtivo, nem tão pouco, mantidas as condições atuais, de típica alienação do trabalho, manterão qualquer tipo de relação de trabalho estável. É, pois, de particular relevância à atenção para com eles.

Nessa perspectiva, conforme disposto na referida Resolução, “no momento de emitir medidas de emergência e contenção frente a pandemia da COVID-19, os Estados da região devem brindar e aplicar perspectivas interseccionais e prestar especial atenção às necessidades e ao impacto diferenciado de ditas medidas dos direitos humanos dos grupos historicamente discriminados ou em especial vulnerabilidade” (CIDH, 2020).

Com efeito, os dados colhidos, precisam somar a esse anseio, e colaborar de forma cooperativa e não tipicamente como forma de controle e a serviço de interesses econômicos, centrados na segregação. É necessário que se compreenda melhor os fatores de risco da doença, a fim de que se possa proteger de maneira mais eficaz as pessoas mais vulneráveis (RESNICK,2020). Antes, sejam voltados à dignidade e aos interesses humanitários.

Considerações finais

A Revolução 4.0 vem ensejando inúmeras transformações nas relações da sociedade, na economia, na tecnologia, na saúde – inclusive a pública -, na política, na história e na esfera jurídica. Não sem razão, vem impactando também a esfera do trabalho que, por sua vez, reverbera nos processos formativos e informativos,

10 A expressão se reafirmou como LGBTQ+ e, atualmente, tem sido utilizada a sigla LGBTQI+ - uma versão reduzida de LGBTTT2QQIAAP. A sigla é dividida em duas partes. A primeira (LGB), diz respeito à orientação sexual do indivíduo, e contempla as iniciais de *lésbicas*, *gays* e *bissexuais*; e, a segunda parte, (TQI+), diz respeito ao gênero, e contempla as iniciais de *transsexuais*, *travestis* e *transgêneros*; e, também, as iniciais de *queer*; de *intersexuais*; e, alusivo ao “+”, diz respeito as outras mais categorias, tais como o “A” de *assexualidade* e o “P” de *pansexualidade*.

notadamente, no teletrabalho e no home office.

Ao passo que cresce a preocupação político-institucional, e os assuntos do COVID-19, estes se misturam aos de ordem econômica e à própria política, ocasião em que, muitas vezes são afastadas as questões relativas à pandemia e a própria ciência. Inquestionável é que os direitos estão a merecer atenção, em especial os relativos à tutela dos direitos à saúde. Bem por isso, constituem trabalhos cada vez mais árduo a proteção, a promoção e a defesa dos direitos.

Por outro lado, de modo crescente a tecnologia tem diminuído a atuação direta da força humana na produção e na própria dimensão laborativa, reduzindo os empregos e não repondo na mesma qualidade e proporção e, muito menos, mantendo os mesmos direitos.

As novas tecnologias, cada vez mais concentradas em poucas corporações econômicas e financeiras ou por indivíduos na área de serviços, destroem e incorporam concorrentes aumentando a concentração e estabelecem uma concorrência entre os próprios trabalhadores, a conferir exploração, expropriação e redução drástica de garantias e de direitos já conquistados.

Como se não bastasse esse cenário, outro desafio se apresentou: a chegada do novo Coronavírus, independentemente de ser ou não um divisor de águas para a nova realidade do mundo - a definir se o Sars-Cov-2 é um usurpador, um hóspede ou um morador - é certo que, a cultura de “estar juntos” encontra-se profundamente marcada pela nova onda de comportamentos que o “padrão de ser” do COVID19 está a implicar. A realidade do trabalho, já redimensionada pela tecnologia, encontra-se mais uma vez, às voltas com o padrão que a pandemia segue apregoando.

Ora, quando se toma em exame a pandemia do Sars-COV-2, a questão central a ser levada em consideração, diz respeito ao pleno respeito do direito à saúde (tomado em acepção e em conjunto com os direitos à vida e à integridade pessoal), de onde se extrai outros aspectos, dentre eles: i) o debate acerca dos dados, tem acompanhado a história da proteção de dados; ii) frente ao sistema de saúde – tomado este na acepção de medidas do seguro social e do acesso aos sistemas de saúde pública - no atual estágio, está tomado pela inexistência de conhecimento ou de intervenções farmacêuticas viáveis contra o Sars-Cov-2; iii) na perspectiva de facilitar o diagnóstico e o tratamento oportuno e exequível, o tratamento dos dados sensíveis, relativos à saúde, poderá estar às voltas com o interesse público, e, mesmo assim, prejudicar a privacidade; e iv) o trabalho que já tinha ganhado novas disposições com o acesso às novas tecnologias, sobretudo, o acesso aos produtos presentes em tempos de Revolução 4.0, acelerou e deu ênfase ao teletrabalho e ao home office – ainda que, cada um guarde suas especificidades.

Levando-se em consideração esses pontos, o foco primordial deste estudo, associou o trabalho, seus novos modelos e a proteção de dados em torno do direito à saúde, tomados todos em face da pandemia do COVID-19 – e não as tecnologias de tratamento e destruição, ou mesmo outros aspectos da gestão de resíduos de saúde, ou assistência médica, em que pese a evidência da cooperação de todas essas medidas e processos para auferir seus resultados.

Com o advento das mudanças que são feitas presentes na atualidade, sobretudo com a chegada da tecnologia em contato com o mundo do trabalho, um novo

mundo do trabalho descortinou-se, configurando processos disruptivos, em que o trabalho a distância passou a agregar modernas tecnologias, voltadas à informação e à comunicação. Reside nesse particular a distinção que há entre o teletrabalho e a ideia tradicional do trabalho prestado em domicílio (ou trabalho em domicílio).

A ideia associada de proteger o trabalho e, igualmente, o trabalhador, notadamente a sua saúde e seus dados, como é comum no pensamento constitucional, legal, tem implicações decisivas para a dinâmica das relações e o padrão de capacidades que se quer estabelecer. A Lei Geral de Proteção de Dados é um convite a esse estado protetivo, de forma a que cada pessoa, cada cidadão, cada ser humano, possa ter mais esse direito resguardado. Espera-se que não haja mais lugar para dispor das pessoas desse modo: colocando-as como meio, a fim de que seus respectivos empregadores as coloquem para trabalhar em condições abaixo de um mínimo, ou abaixo de um padrão decente, a fim de maximizar seu lucro e auferir vantagens.

Mesmo frente ao Coronavírus, a depender de que a pandemia do COVID19, possa ser a rota de passagem, a inaugurar um tempo de transição, verdadeira travessia da história humana, mesmo assim, referida doença requer aptidão de forma a contar a história do Século XXI, marcando-a com sua presença, por longo ou breve tempo, modificando costumes, culturas, estudos, organização, e Estado, seja, por quaisquer dos modos, sobretudo, é preciso proteger direitos, com implicações claras para as condições econômicas e de trabalho. Aliás, a lição das trocas cooperativas tem o condão de gerar fraternidade, tanto para aqueles que se parecem e para os indiferentes, indistintamente.

Diante desse contexto, a categoria do trabalho, em especial o teletrabalho e o home office parece caminhar rumo a um reconhecimento e a um espaço que até então vinha sendo criticado. É um dado, retirado das informações e das interpretações desses dados: enquanto pessoas deveremos adotar o compromisso de, também, cooperar com a Ciência até que venha finalmente uma resposta adequada, senão diretamente, pelo menos fazendo cada um a sua parte. Não se trata do tamanho da fé que poderá ser dedicado a esse esforço, mas sim, da combinação que o isolamento ou a cooperação está a exigir de todos. Empresas, fundações, corporações, universidades, pessoas e países precisarão estar abertos a essa nova proposta.

REFERÊNCIAS

ARAÚJO, Emilia. **Questões de tempo e espaço: Do teletrabalho, ao “ficar em casa”, passando pelo confinamento.** Communitas Think Tank – Ideias, 2020. Disponível em: <https://repositorium.sdum.uminho.pt/bitstream/1822/65536/1/2020_Araujo_Questoes-de-tempo-e-espa%C3%A7o.pdf>. Acesso em: 09 jun. 2020.

CIDH – Comissão Interamericana de Direitos Humanos. Resolução nº 1/2020: Pandemia e Direitos Humanos nas Américas (Adaptado pela CIDH, em 10 de abril de 2020). Disponível em: <http://www.oas.org/es/cidh/decisiones/pdf/Resolucion-1-20-es.pdf>. Acesso em: 11 abr. 2020.

DITCHEV, Ivaylo. In: DW Deutsche Welle. Coronavírus traz fronteiras de volta à Europa. Notícias Mundo. 21 abril 2020. Disponível em: <https://noticias.uol.com.br/ultimas-noticias/deutschewelle/2020/04/21/opiniao-coronavirus-traz-fronteiras-de-volta-a-europa.htm>. Acesso em: 29 abr. 2020.

EUROPEAN AGENCY FOR SAFETY AND HEALTH AT WORK (ESHW). Biological agents and pandemics: review of the literature and national policies. Luxembourg: Office for Official Publications of the European Communities, 2009. Disponível em: <<https://osha.europa.eu/en/publications/biological-agents-and-pandemics-review-literature-and-national-policies>>. Acesso em: 16 maio 2020.

HARARI, Yuval Noah. **'Guru' dos nossos tempos, Yuval Harari aponta os cenários pós-pandemia. (Breve Companhia, Ensaio)**. In: SAHD, Luiza, 2020a (atualizado em 01 abril de 2020). Disponível em: <https://tab.uol.com.br/noticias/redacao/2020/03/28/guru-dos-nossos-tempos-yuval-harari-aponta-os-cenarios-pos-pandemia.htm>. Acesso em: 09 abr. 2020.

HARARI, Yuval Noah. **Na batalha contra o Coronavírus, faltam líderes à humanidade (Breve Companhia, Ensaio)**. Tradução Odorico Leal. São Paulo: Companhia das Letras, 2020b.

LEWIS, G. Dr Greg Lewis on COVID-19 & catastrophic biological risks. [Entrevista concedida a] Howie Lempel. 80,000 Hours Podcast with Rob Wiblin. [s.l.]. 17 abr. 2020. Podcast. Disponível em: <<https://open.spotify.com/episode/1yAfMNDiGzDGQZkMLTMrys>>. Acesso em: 16 maio 2020.

LIMA, Fábíola Bessa Salmito; MELO, Sandro Nahmias. **Teletrabalho, meio ambiente do trabalho, redes Sociais e os reflexos na saúde mental do trabalhador**. Revista Nova Hileia. Vol. 5. Nº 3, julho-dezembro 2018. Disponível em: <<http://periodicos.uea.edu.br/index.php/novahileia/article/view/1698/1032>>. Acesso em: 09 jun. 2020.

LIMA FILHO, José Sarto Fulgência de; PEREIRA, Eddla Karina Gomes. **Precarização das relações laborais: análise crítica sobre as disposições do teletrabalho na lei 13.467/2017**. Revista de Direito. V.12. N.01. 2020. Disponível em: <<https://dialnet.unirioja.es/servlet/articulo?codigo=7404036>>. Acesso em: 09 jun. 2020.

Ministério da Saúde: DIRETRIZES PARA DIAGNÓSTICO E TRATAMENTO DA COVID-19. Brasília-DF, 06 de abril de 2020. Disponível em: <http://www.sbac.org.br/blog/2020/04/09/diretrizes-para-diagnostico-e-tratamento-da-covid-19/>. Acesso em: 17 de abr. 2020.

MORIN, Edgar. **As certezas são uma ilusão**. CNRS / Le Journal. In: Lecompte, Francis - 09.04.2020. Disponível em: <https://www.fronteiras.com/entrevistas/edgar-morin-as-certezas-sao-uma-ilusao>. Acesso em: 12 abr. 2020.

MÜLLER, Vinícius. **A linguagem republicana diante da crise: uma análise de A Revolta da Vacina, de Nicolau Sevcenko**. Boletim n. 7 - Ciências Sociais e Coronavírus. 28/03/2020. Ação conjunta que reúne a Associação Nacional de Pós-Graduação em Ciências Sociais (ANPOCS), a Sociedade Brasileira de Sociologia (SBS), a Associação Brasileira de Antropologia (ABA), a Associação Brasileira de Ciência Política (ABCP) e a Associação dos Cientistas Sociais da Religião do Mercosul (ACSRM). Disponível em: <<http://www.anpocs.com/index.php/ciencias-sociais/destaques/2314-boletim-n-3-as-ciencias-sociais-e-a-saude-coletiva-frente-a-Atual-epidemia-de-ignorancia-irresponsabilidade-e-ma-fe-5>>. Acesso em: 08 abr. 2020.

OPAS BRASIL (Organização Pan-Americana de Saúde) – OMS (Organização Mundial da Saúde): Folha Informativa – Covid-19. Disponível em: <https://www.paho.org/bra/index.php?option=com_content&view=article&id=6101:covid19&Itemid=875>. Acesso em: 08 abr. 2020.

RESNICK, B. **Scientists are trying to figure out why Covid-19 hits some young, healthy people hard.** Vox. 8 abr. 2020. Disponível em: <<https://www.vox.com/science-and-health/2020/4/8/21207269/covid-19-coronavirus-risk-factors>>. Acesso em: 15 maio 2020.

Resolução 01/2020: **Pandemia e Direitos Humanos nas Américas** (OEA e CIDH). Adotada pela Comissão Interamericana de Direitos Humanos – CIDH, em 10 de abril de 2020. Disponível em: <http://www.oas.org/es/cidh/decisiones/pdf/Resolucion-1-20-es.pdf>. Acesso em: 17 abr.2020.

RIYANTI, D. et al. **Building resilience against biological hazards and pandemics: COVID-19 and its implications for the Sendai Framework.** Elsevier Journal. vol. 6. 23 mar. 2020. p. 01-07. DOI: <https://doi.org/10.1016/j.pdisas.2020.100080>. Acesso em: 15 maio 2020.

ROQUE, André. **A tutela coletiva dos dados pessoais na Lei Geral de Proteção de Dados Pessoais (LGPD).** Revista Eletrônica de Direito Processual – REDP. Rio de Janeiro. Ano 13. v. 20. n. 2. Maio/Ago. 2019. Disponível em: <<https://www.e-publicacoes.uerj.br/index.php/redp/article/view/42138/30270>>. Acesso em: 09 jun. 2020.

SANTOS, João Vitor. In: **Impactos da Biologia Sintética na Revolução 4.0 e na Bioética.** Revista do Instituto Humanitas Unisinos – IHU on-line. Edição 544, de 04 de novembro de 2019. Disponível em: <http://www.ihuonline.unisinos.br/artigo/7707-impactos-da-biologia-sintetica-na-revolucao-4-0-e-na-bioetica>. Acesso em: 12 jun.2020.

SARMENTO, Daniel. **Direitos Fundamentais e Relações Privadas.** Rio de Janeiro: Editora Lumen Juris, 2008.

SENNETT, Richard. **Juntos.** Tradução Clóvis Marques. 4ª. ed. Rio de Janeiro – São Paulo: Editora Record, 2018.

SEVCENKO, Nicolau. **A Revolta da Vacina: mentes insanas em corpos rebeldes.** São Paulo: Editora Unesp, 2018.

VENTURA, Deisy de Freitas Lima. **Pandemias e Estado de Exceção.** In: CATTONI, Marcelo; MACHADO, Felipe (Coordenadores). **Constituição e Processo: a resposta do constitucionalismo à banalização do terror.** Belo Horizonte: Del Rey, 2009, p. 159-181.

VENTURA, Deisy de Freitas Lima; AITH, Fernando Mussa Abujamra; RACHED, Danielle Hanna. **A emergência do novo coronavírus e a “lei de quarentena” no Brasil.** Revista Direito e Práxis. Ahead of print, Rio de Janeiro, 2020. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/revistaceaju/article/view/49180/32876>. Acesso em: 09 jun. 2020.

VERONESE, Alexandre; SILVEIRA, Alessandra; LEMOS, Amanda Nunes Lopes Espínera. **Inteligência Artificial, Mercado único Digital e a postulação de um Direito às inferências justas e razoáveis: uma questão jurídica entre a ética e a técnica.** In: FRAZÃO, ANA; MULHOLLAND, Caitlin. **Inteligência Artificial e Direito: ética, regulação e responsabilidade.** São Paulo: Thomson Reuters Brasil, 2019.

VOMMARO, Pablo. **O mundo em tempos de pandemia: certezas, dilemas e perspectivas.** Revista Direito e Práxis. Ahead of print, Rio de Janeiro, 2020. Disponível em: <<https://www.e-publicacoes.uerj.br/index.php/revistaceaju/article/view/51001/33840>>. Acesso em: 09 jun. 2020.

36. A IMPORTÂNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS PARA O MEIO AMBIENTE DO TRABALHADOR

THE IMPORTANCE OF THE GENERAL DATA PROTECTION LAW FOR THE WORKER'S ENVIRONMENT

**CLÁUDIO JANNOTTI DA ROCHA¹, FÁBIO SIQUEIRA MACHADO²
E ALBERTO NEMER NETO³**

Resumo

O presente artigo visa demonstrar a importância da Lei Geral de Proteção de Dados – LGPD para o meio ambiente do trabalho saudável e seguro. A preservação da privacidade do trabalhador, incluindo o armazenamento e tratamento de seus dados, é fundamental para a sua integridade e desenvolvimento. Como metodologia de pesquisa, optou-se pelo método dedutivo, mediante consulta bibliográfica. Inicialmente, fez-se uma abordagem da LGPD e sua aplicabilidade às relações trabalhistas; em seguida, estudou-se o meio ambiente e o direito ambiental do trabalho; por fim, analisou-se a importância da LGPD para a preservação do meio ambiente do trabalho equilibrado.

Palavras-chave: Lei Geral de Proteção de Dados. Privacidade. Meio Ambiente do Trabalho.

Abstract

This article aims to demonstrate the importance of the General Data Protection Law – LGPD for a healthy and safe working environment. The preservation of the worker's privacy, including the storage and treatment of their data, is fundamental for their integrity and development. As research methodology, we opted for the deductive method, through bibliographical consultation. Initially, an approach was made to the LGPD and its applicability to labor relations; then, the environment and environmental labor law were studied; finally, the importance of the LGPD for the preservation of a balanced work environment was analyzed.

Keywords: General Data Protection Law. Privacy. Work Environment.

1 Professor Adjunto do Curso de Direito e do Programa de Pós-Graduação em Direito da Universidade Federal do Espírito Santo (UFES). Pós-Doutor em Direito pela Universidade Federal da Bahia (UFBA). Doutor e Mestre em Direito e Processo do Trabalho pela Pontifícia Universidade Católica de Minas Gerais (PUC Minas). Coordenador e Pesquisador do Grupo de Pesquisa Trabalho, Seguridade Social e Processo: diálogos e críticas (UFES-CNPq). Orcid: <https://orcid.org/0000-0003-2379-2488>

2 Mestrando em Direito pela Universidade Federal do Espírito Santo (UFES). Pesquisador do Grupo de Pesquisa Trabalho, Seguridade Social e Processo: diálogos e críticas (UFES-CNPq). Advogado e consultor jurídico.

3 Advogado e consultor jurídico. Advogado graduado pela Faculdade de Direito de Vitória – FDV, possui MBA em Direito do Trabalho e Processo do Trabalho pela Fundação Getúlio Vargas do Rio de Janeiro; especialista em Direito do Trabalho e Processo do Trabalho pela Escola Superior de Advocacia, representante dos Empregadores na 100ª Convenção da Organização Internacional do Trabalho – OIT / ONU (2019); representante dos Empregadores na 109ª Convenção da Organização Internacional do Trabalho – OIT / ONU (2021).

1. Introdução

A sociedade contemporânea é marcada pela massificação, digitalização e virtualização. O fornecimento e a troca de informações entre pessoas físicas e jurídicas são ininterruptos. Nesse contexto, foi editada em nosso país a Lei n.º 13.709/2018, que, com redação dada pela Lei n.º 13.853/2019, passou a ser denominada de Lei Geral de Proteção de Dados – LGPD.

A LGPD, que entrou integralmente em vigor no dia 15/08/2021, tem por objeto, conforme dispõe o seu artigo 1º:

“o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”.

O escopo protetivo da LGPD é a proteção dos direitos da liberdade e da privacidade, direitos fundamentais da personalidade, inerentes ao desenvolvimento humano, através da regulamentação do tratamento dos dados pessoais do indivíduo.

Nas palavras de Rúbia Zanotelli de Alvarenga, a tutela dos atributos da personalidade objetiva preservar a dignidade da pessoa humana⁴:

Por derradeiro, pode-se afirmar que os direitos da personalidade são inatos e inerentes à pessoa humana e a ela ligados de maneira perpétua e permanente. São direitos que nascem com a pessoa humana e a acompanham durante toda a sua existência, tendo como primordial a proteção aos atributos da personalidade e à dignidade da pessoa humana – em todos os aspectos (físico, psíquico, moral e intelectual). De tal modo, possuem uma concepção jusnaturalista, pois são pertencentes ao ser humano pela sua mera condição humana. Isso faz com que independam de previsão normativa.

Sendo direitos fundamentais de todo homem, resta fora de dúvida que possuem plena aplicabilidade aos trabalhadores, que devem ter sua personalidade mantida incólume, através da preservação de sua privacidade, de maneira que a LGPD é de plena aplicabilidade aos contratos de trabalho.

A necessidade de equilíbrio entre desenvolvimento econômico e proteção de direitos fundamentais tem destaque no meio ambiente do trabalho, sobretudo ao se considerar que as ações, tanto comissivas como comissivas geradoras de danos ao meio ambiente do trabalho, não se restringem aos trabalhadores diretamente afetados, mas a toda mão de obra disponível. Trabalhadores que não têm os seus

4 ALVARENGA, Rúbia Nanotelli. *Direitos da Personalidade do trabalhador e correio eletrônico*. Portal Jus.com.br. Dezembro de 2012. Disponível em: <https://jus.com.br/artigos/26273/direitos-da-personalidade-do-trabalhador-e-correio-eletronico>. Acesso: 28 set. 2021.

mais comezinhos direitos preservados, como o de laborarem em um meio ambiente laboral saudável e seguro, desempenham atividade com enorme potencial de deteriorar a sua integridade biopsíquica, desenhando o cenário perfeito para doenças e acidentes de trabalho, violando o direito fundamental ao meio ambiente do trabalho equilibrado.

Nessa esteira, a proposta deste trabalho é analisar a aplicabilidade da LGPD às relações de trabalho e sua importância para o meio ambiente equilibrado do trabalhador.

2. Da LGPD e sua aplicabilidade às relações trabalhistas

Influenciada pela legislação europeia (*General Protection Regulation 216/679*), a LGPD brasileira (Lei n.º 13.709/2018) estabelece os parâmetros dentro dos quais as pessoas físicas e jurídicas poderão realizar o tratamento de dados pessoais.

O *General Data Protection Regulation*⁵ dispõe, no considerando n.º 1, que a proteção dos dados pessoais é direito fundamental:

A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

Diferentemente da legislação brasileira, a norma europeia prevê, de forma expressa, o tratamento dos dados dentro da relação de emprego:

Art 88 – 1. Os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção dos bens do empregador ou do cliente e para efeitos do exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho.

⁵ General Data Protection Regulation. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=FR>. Acesso: 28 set. 2021.

Não obstante a ausência de menção específica às relações de trabalho, a LGPD brasileira não deixa dúvida de que sua aplicabilidade é irrestrita, quando, no artigo 3º, estabelece que qualquer operação de tratamento realizada em território nacional por pessoa física ou jurídica, seja de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, estará sujeita aos seus preceitos.

Soma-se a isso que, no artigo 2º, dispõe que possui como fundamentos, dentre outros: a) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (inciso VII); b) a inviolabilidade da intimidade, da honra e da imagem (inciso IV); c) o respeito à privacidade (inciso I); d) a autodeterminação informativa (inciso II).

De mais a mais, o artigo 4º, que trata das hipóteses taxativas de não aplicabilidade da lei, não faz qualquer menção às relações de trabalho.

Não há qualquer dúvida, portanto, de que a LGPD nacional é, excetuadas as hipóteses previstas na própria lei, integralmente aplicável a todo e qualquer tratamento de dados realizado no país, independentemente da relação havida entre as partes, eis que possui por objetivo a proteção de direitos da personalidade, inerentes e caros a todo ser humano.

O artigo 6º da LGPD dispõe que o tratamento de dados pessoais deverá observar a boa-fé e os seguintes princípios: a) finalidade, que implica no tratamento para propósitos legítimos, específicos, explícitos e informados ao titular; b) adequação, de maneira que o tratamento seja compatível com as finalidades informadas ao titular; c) necessidade, limitando o tratamento ao mínimo necessário às finalidades; d) livre acesso, garantindo aos titulares consulta facilitada e gratuita a respeito dos dados; e) qualidade dos dados, garantindo exatidão, clareza, relevância e atualização dos dados; f) transparência, conferindo informações claras, precisas e de fácil acesso aos seus titulares; g) segurança, conferindo proteção a acessos não autorizados; h) prevenção, a fim de prevenir a ocorrência de danos; i) não discriminação, impossibilitando a utilização para fins discriminatórios dos dados; j) responsabilização, de maneira que o agente deverá demonstrar a adoção de medidas objetivando o cumprimento das normas aplicáveis.

Merece destaque a utilização de dados biométricos, considerados de caráter pessoal sensível pelo artigo 5º, II, da LGPD. A biometria, é importante salientar, compreende não somente as impressões digitais, podendo ser extraídas, também, da íris, da face, da voz e até mesmo da forma de andar.

No contrato de trabalho, é comum a coleta de dados biométricos para o controle de jornada, considerado legítimo pela doutrina especializada, como se verifica da lição de Iuri Pinheiro e Vólia Bomfim⁶:

Uma forma frequente de utilização de dado biométrico na relação de emprego é para fins de registro de ponto.
O art. 74 da CLT estipula a necessidade de registro de

6 PINHEIRO, Iuri; BOMFIM, Vólia. *A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho*. Disponível em: <http://trabalhoemdebate.com.br/artigo/detalhe/a-lei-geral-de-protecao-de-dados-e-seus-impactos-nas-relacoes-de-trabalho>. Acesso em: 28 set. 2021.

ponto, admitindo que tal se dê por meio manual, mecânico ou eletrônico. A Portaria 1510/2009, do então Ministério do Trabalho, autorizou o registro de ponto biométrico de empregados.

O Princípio que pode suscitar dúvidas sobre a legitimidade de utilização desse tipo de dado é da Necessidade ou Minimização, já que existem outros meios supostamente menos invasivos e que permitem o controle de ponto (folha manual ou cartão magnético).

Conquanto seja possível, de fato, assinalar a jornada por outros meios diversos da biometria, não há meio tão eficaz quanto este para assegurar a integridade dos horários lançados nos respectivos registros e a autoria.

E a fidedignidade desses registros é essencial e extremamente saudável para ambas as partes, evitando alegações de desvirtuamento da jornada pela existência, por exemplo, de controle paralelo e permitindo a justa e real apuração do saldo de horas.

O tratamento do dado biométrico para fins de jornada estaria, assim, assegurado pelo cumprimento de obrigação legal pelo controlador (art. 11, II, a, da LGPD).

A novel legislação implica na necessidade de que a coleta e o tratamento de dados dos trabalhadores sejam realizados de forma responsável e adequada, de maneira que os empregadores deverão aprimorar suas práticas para que os dados fornecidos pelos trabalhadores o sejam de forma consentida e de legítima necessidade, sob pena de violação aos direitos da personalidade dos trabalhadores, especialmente sua privacidade.

O empregador que despreza os limites do tratamento de dados contraria o princípio da boa-fé objetiva, que consiste numa regra obrigatória do Direito do Trabalho, do qual emanam os deveres de cooperação, colaboração e lealdade entre as partes⁷.

3. O meio ambiente e o direito ambiental do trabalho

O meio ambiente é classificado em quatro aspectos: natural, que diz respeito à água, ao solo, ao ar, à flora e à fauna; artificial, ao espaço urbano construído; cultural, à formação e cultura de um povo; do trabalho, à forma direta e imediata como o ser humano exerce a atividade laboral em proveito de outrem. Fala-se, ainda, em meio ambiente virtual, a par das transformações tecnológicas que o mundo está experimentando. O Direito Ambiental, por sua vez, tem como objeto tutelar a vida saudável⁸.

7 ALVARENGA, Rúbia Nanotelli. *As revistas realizadas nos bens de uso pessoal do empregado e nos bens de propriedade da empresa*. Portal Jus.com.br. Abril de 2014. Disponível em: <https://jus.com.br/artigos/27514/as-revistas-realizadas-nos-bens-de-uso-pessoal-do-empregado-e-nos-bens-de-propriedade-da-empresa>. Acesso: 29 set. 2021.

8 MELO, Raimundo Simão de. *Direito Ambiental do Trabalho e a Saúde do Trabalhador*. São Paulo: LTr, 2006, p. 23-24.

Especificamente na esfera juslaboral, objeto da pesquisa proposta, o Meio Ambiente do Trabalho é conceituado pela doutrina como “a resultante da interação sistêmica de fatores naturais, artificiais, culturais e laborais que influencia as condições de vida, em todas as suas formas”⁹, evidenciando a sinergia existente entre o direito ambiental e o direito ambiental do trabalhador.

Dessa forma, a não violação aos direitos da personalidade, especialmente o respeito à privacidade do trabalhador, é elemento de suma importância para a existência de um meio ambiente do trabalho saudável e seguro. O trabalhador que não tem a sua intimidade preservada tem a sua honra e a sua moral violados, perde a confiança no empregador e fica sujeito à toda sorte de patologias psicossociais.

A Constituição Federal estabelece, no artigo 225, que todos têm direito ao meio ambiente ecologicamente equilibrado, de uso comum e indispensável à qualidade de vida saudável; no artigo 170, VI, que está assegurado a todos a defesa do meio ambiente, inclusive mediante tratamento diferenciado, enquanto que o art. 200, VIII, explicita a proteção constitucional ao meio ambiente do trabalho, evidenciando, dessa forma, o caráter transindividual do direito.

A par do que preceitua o artigo 3º, I, da Lei 6.938/1981, o meio ambiente é o conjunto de condições, leis, influências e interações de ordem física, química e biológica que permite, abriga e rege a vida em todas as suas formas, em consonância com o artigo 225 da CF, sua tutela é ampla, abrangendo os aspectos natural, artificial, cultural e do trabalho¹⁰.

A Constituição Federal consagra cinco princípios ambientais, quais sejam: a) o princípio da prevenção e da precaução, consagrado no art. 225, que implica no dever do poder público e da coletividade na defesa do meio ambiente equilibrado para as presentes e futuras gerações; b) o princípio do desenvolvimento sustentável (art. 170), segundo o qual o desenvolvimento econômico deve harmonizar-se com o desenvolvimento social, cultural, humano e ambiental; c) o princípio do poluidor-pagador (art. 225, §2º), que estabelece o dever de recuperação do dano ambiental ou indenização; d) o princípio da participação (art. 225), que prevê esforços comuns do poder público e da sociedade para preservação e a proteção do meio ambiente; e) o princípio da ubiquidade, que prevê que a responsabilidade relativamente ao meio ambiente é de todos.

O meio ambiente equilibrado é direito de terceira geração, fundamental, como registra Raimundo Simão de Melo¹¹:

“O meio ambiente é um direito de terceira geração, como, entre outros, reconhece Manoel Gonçalves Ferreira Filho (*Curso de Direito Constitucional*, p. 370). De primeira geração são os direitos civis e políticos – liberdades

9 MARANHÃO, Ney. *Poluição Labor Ambiental*. Abordagem conceitual da degradação das condições de trabalho, de organização do trabalho e das relações interpessoais travadas no contexto laborativo. Rio de Janeiro: Editora Lumen Juris, 2018, p. 49.

10 BRASIL. **Lei 6.938, de 31 de agosto de 1981**. Brasília, DF: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/ccivil03/leis/l6938.htm. Acesso em: 06 out. 2020.

11 MELO, Raimundo Simão de. *Direito Ambiental do Trabalho e a Saúde do Trabalhador*. São Paulo: LTr, 2006, p. 23.

públicas negativas perante o Estado. Depois de libertado o homem das garras deste, surgiram os direitos positivos, de segunda geração – os sociais, os econômicos e os culturais –, que servem para dotar o ser humano das condições materiais minimamente necessárias ao exercício de uma vida digna. De terceira geração são os direitos de solidariedade e fraternidade – a paz no mundo, o desenvolvimento econômico dos países, a preservação do meio ambiente, do patrimônio comum da humanidade e da comunicação. Essas gerações de direitos são imprescindíveis à condição humana e merecem proteção do Estado e da sociedade.

Para Ingo Wolfgang Sarlet, a Constituição Federal adotou um marco jurídico-constitucional socioambiental, formatando o “Estado Socioambiental de Direito”, incrementando novos valores e direitos ecológicos¹², que prima pela qualidade ambiental:

a ordem econômica constitucionalizada no art. 170 da Carta da República, com base também nos demais fundamentos constitucionais que lhe constituem e informam, expressa um *capitalismo socioambiental*, capaz de compatibilizar a livre-iniciativa, a autonomia privada e a propriedade privada com a proteção ambiental e a justiça ambiental (também social), tendo como o seu norte normativo “nada menos” do que a realização de uma vida humana digna e saudável (e, portanto, com qualidade ambiental) a todos os membros da comunidade estatal.

Dessa forma, o direito ao meio ambiente equilibrado revela-se como a próxima etapa do desenvolvimento na esteira do processo evolutivo enquanto sociedade justa e democrática, sobressaindo-se sobre as históricas conquistas liberais e sociais, mas sem extingui-las. Tais direitos são cumulativos e o arcabouço dos direitos humanos é ampliado com o direito a uma vida saudável, com qualidade ambiental, como elemento integrante e indissociável do princípio da dignidade da pessoa humana.

Raimundo Simão de Melo conceitua o Meio Ambiente do Trabalho como¹³:

o local onde as pessoas desempenham suas atividades laborais, sejam remuneradas ou não, cujo equilíbrio está embasado na salubridade do meio e na ausência de

12 SARLET, Ingo Wolfgang; FENSTERSEIFER, Tiago. Estado Socioambiental e Mínimo Existencial (Ecológico): algumas aproximações. In: FELICIANO, Guilherme Guimarães; SARLET, Ingo Wolfgang; MARANHÃO, Ney; FENSTERSEIFER, Tiago (org.). *Direito Ambiental do Trabalho* – apontamentos para uma teoria geral, volume 5. São Paulo: LTr, 2020. p. 22.

13 MELO, Raimundo Simão de. *Direito Ambiental do Trabalho e a Saúde do Trabalhador*. São Paulo: LTr, 2006, p. 24-25.

agentes que comprometam a incolumidade física dos trabalhadores, independentemente da condição que ostentam (homens ou mulheres, maiores ou menores de idade, celetistas, servidores públicos, autônomos, etc.).

A definição acima é das mais abrangentes, pois não se limita a tratar do assunto apenas em relação ao trabalhador classicamente conhecido como aquele que ostenta uma carteira de trabalho assinada. Isto é muito importante e está dentro do contexto maior asseguratório do meio ambiente equilibrado para todos, como estabelece a Constituição (art. 225, *caput*), uma vez que a definição geral de meio ambiente abarca todo cidadão e, a de meio ambiente do trabalho, todo trabalhador que desempenha alguma atividade, remunerada ou não, homem ou mulher, celetista, autônomo ou servidor público de qualquer espécie, porque realmente todos receberam a proteção constitucional de um ambiente de trabalho adequado e seguro, necessário à sadia qualidade de vida.

A doutrina aponta que são princípios fundamentais de Direito Ambiental do Trabalho: a) desenvolvimento sustentável; b) poluidor-pagador; c) prevenção; d) ubiquidade.

Rúbia Zanotelli de Alvarenga anota que, no Direito do Trabalho¹⁴:

o desenvolvimento é sustentável é respeitado quando o trabalho é decente, de modo a preservar não só a melhoria das condições de trabalho, mas também todos os aspectos inerentes à condição humana e aos direitos da personalidade do trabalhador, quais sejam: a) *integridade física*; b) *psíquica*; c) *moral*; d) *intelectual*; e) *direito à integração social*.

O princípio do poluidor pagador está estampado no artigo 225, §3º, da Constituição Federal, ao estabelecer que os causadores de danos ao meio ambiente estarão sujeitos a sanções penais e administrativas, sem prejuízo da obrigação de reparar o dano. Na esfera juslaboral, o princípio está relacionado ao pagamento adicional aos trabalhadores que desenvolvem atividades insalubres, penosas ou perigosas, conforme determina o artigo 7º, XXIII, da Constituição Federal.

O princípio da prevenção obriga a adoção de medidas tendentes a prevenir os riscos ambientais laborais a que os trabalhadores estejam sujeitos¹⁵.

O princípio da ubiquidade implica no dever de promover a eliminação e a

14 ALVARENGA, Rúbia Zanotelli. Princípios Fundamentais de Direito Ambiental do Trabalho. In: FELICIANO, Guilherme Guimarães; URIAS, João; MARANHÃO, Ney (coord). *Direito Ambiental do Trabalho*. Apontamentos para uma teoria geral. Volume 3. São Paulo: LTr, 2017. p. 70.

15 CAMARGO, Thaísia Rodrigues Lustosa; MELO, Sandro Nahmias. *Princípios de direito ambiental do trabalho*. São Paulo: LTr, 2013. p. 24-25.

minimização do risco de degradação que atinge e repercute de tal maneira na vida da coletividade e no equilíbrio ecológico, de maneira que, no local de trabalho, o princípio implica na obrigação de que seja retirado ou minimizado qualquer agente que possa desequilibrar o meio ambiente do trabalhador.

José Claudio Monteiro de Brito, em artigo no qual trabalha a aplicabilidade da teoria da justiça como equidade, de John Rawls, defende que a saúde do trabalhador deve ser vista com uma visão mais ampla¹⁶:

No caso dos trabalhadores, e ampliando a questão da saúde para uma visão mais ampla, de um meio ambiente do trabalho equilibrado, é forçoso entender que só podem os trabalhadores ter os direitos básicos que garantam o cumprimento de seus planos de vida se puderem trabalhar em ambiente que não comprometa a sua saúde, que não ofereça riscos à sua segurança, e em que possam atuar nas melhores condições ergonômicas possíveis.

O meio ambiente do trabalho equilibrado pressupõe o trabalho digno, decente, assim entendido aquele que respeita o ser humano em sua integralidade, ou seja, abrange os aspectos físico, psíquico, moral e intelectual.

Não basta, portanto, que a ausência de riscos seja limitada apenas ao aspecto físico, mas também ao psicológico e moral, englobando os direitos da personalidade, como a privacidade, especialmente, no que diz respeito ao presente trabalho, aos dados do trabalhador, que somente podem ser tratados nas hipóteses e dentro dos limites da LGPD.

A privacidade do trabalhador deve ser tutelada em prol de melhores condições laborais, pois o trabalho é essencial à dignidade do ser humano. Nesse sentido, são precisas as palavras de Gabriela Neves Delgado¹⁷:

“Porém, a identidade social do homem somente será assegurada se o seu trabalho for digno. A explicação deve ser compreendida por meio da contradição permanente que se desenvolve na sociedade civil: ao mesmo tempo em que o trabalho possibilita a construção da identidade social do homem, pode também destruir a sua existência, caso não existam condições mínimas para o seu exercício.

Se o obreiro ganha mal, se não existem condições mínimas de salubridade, por exemplo, não há espaço para a concretização da dignidade. O Direito será mera abs-

16 FILHO, José Claudio Monteiro de Brito. A proteção do meio ambiente do trabalho e a teoria da justiça como equidade de John Rawls. In: FELICIANO, Guilherme Guimarães; URIAS, João; MARANHÃO, Ney (coord). *Direito Ambiental do Trabalho*. Apontamentos para uma teoria geral. Volume 3. São Paulo: LTr, 2017. p. 473.

17 DELGADO, Gabriela Neves. *Direito Fundamental ao Trabalho Digno*. 2ª Edição. São Paulo: LTr, 2015.

tração. Compreender o trabalhador enquanto mero instrumento para a realização de determinado ofício, tônica da sociedade civil contemporânea, compromete o entendimento maior de que o homem deve ser um fim em si mesmo.

Para que o homem seja considerado um fim em si mesmo é necessário que o Estado garanta a efetividade do direito fundamental ao trabalho digno, por meio de práticas sociais de caráter interno e internacional.

Será por meio da promoção de direitos fundamentais que a dignidade será reconhecida como suporte de valor nas relações de trabalho. Eis, portanto, a importância do Direito do Trabalho enquanto “cânone de conduta e organização social.”

Trabalho, dignidade, identidade social e sustentabilidade são indissociáveis. Um não se mantém em pé sem o outro. Não há dignidade se os dados pessoais são indevidamente coletados, manipulados e compartilhados, pois tais práticas reduziram o trabalhador uma mera mercadoria.

4. Da importância da LGPD para o meio ambiente laboral equilibrado

Rosângelo Rodrigues de Miranda¹⁸, ao conceituar privacidade, destaca sua íntima correlação com a individualidade do homem:

[...] No mundo ocidental contemporâneo, o conceito de vida privada demarca, em essência, a individualidade do homem, não só frente aos outros indivíduos e à sociedade, mas também frente ao Estado; consubstanciando espaços nos quais as forças de criação e imaginação do homem estão livres, seja para reflexões introspectivas atinentes ao íntimo de cada qual, seja para manter intercâmbios sociais nos quais cabe a cada um, privativamente, escolher como, onde e quando atuar.

Para Fábio Ulhoa Coelho, o direito à privacidade protege um “conjunto de informações não-públicas sobre determinada pessoa, as quais esta deseja não ver divulgadas a ninguém”¹⁹.

No que diz respeito à privacidade no bojo do pacto laboral, Laert Mantovani Junior destaca a importância da proteção aos direitos da personalidade do trabalhador contra abusos do empregador²⁰:

18 MIRANDA, Rosângelo Rodrigues. *A Proteção Constitucional da Vida Privada*. São Paulo: Editora de Direito, 1996, p.82.

19 COELHO, Fábio Ulhoa. *Curso de Direito Civil*. São Paulo: Saraiva, 2003, v.1, p.193.

20 JUNIOR, Laert Mantovani. *O Direito Constitucional à Intimidade e à Vida Privada do Empregado e o Poder Diretivo do Empregador*. São Paulo: Ltr, 2010, p. 28.

As empresas primam cada vez mais pela qualidade e produtividade, utilizando-se de equipamentos sofisticados para o desenvolvimento de suas atividades, o que tem impacto direto no trabalho desenvolvido pelos empregados. [...]. Contudo, há que se observar que na relação do trabalho, o que se põe à venda é a força de trabalho e não o trabalhador em si, que deve ter seus direitos da personalidade protegidos contra eventuais abusos.

Cândido Anchieta Costa registra a obrigatoriedade do empregador manter incólume a integridade de seus empregados²¹:

Os direitos de personalidade, neles incluído o direito à privacidade, são a nítida projeção da dignidade da pessoa humana, sendo resguardados em todas as searas do ordenamento jurídico. Portanto, o empregador tem a obrigação de zelar pela incolumidade do direito à privacidade do empregado.

A Organização Internacional do Trabalho – OIT, através da Recomendação nº. 201, de 16 2011²², editou as seguintes resoluções acerca da privacidade e proteção de dados dos trabalhadores:

3. No momento de adotar medidas para a eliminação da discriminação em matéria de emprego e ocupação, os Membros, em conformidade com as normas internacionais do trabalho, deveriam, entre outras coisas:

(a) assegurar que os sistemas de exames médicos relacionados ao trabalho respeitem o princípio da **confidencialidade de dados pessoais e a privacidade dos trabalhadores** domésticos e estejam em consonância com o repertório de recomendações práticas da OIT, intitulado “Proteção de dados pessoais dos trabalhadores” (1997) e com outras normas internacionais pertinentes sobre proteção de dados pessoais (destacamos);

A confidencialidade de dados pessoais e a privacidade dos trabalhadores compõem o arcabouço de diretrizes acerca do trabalho decente, no bojo de um meio ambiente do trabalho saudável e seguro.

A Declaração da Filadélfia, de 1944, e a Constituição da OIT, de 1946, são do-

21 COSTA, Cândido Anchieta. *O controle dos websites acessados pelo trabalhador*. Portal Jus.com.br. Agosto de 2013. Disponível em: <https://jus.com.br/artigos/24724/o-controle-dos-websites-acessados-pelo-trabalhador/2>. Acesso: 29 set. 2021.

22 OIT. R201 – Sobre o Trabalho Doméstico Decente para as Trabalhadoras e os Trabalhadores Domésticos. Disponível em: https://www.ilo.org/brasil/temas/trabalho-domestico/WCMS_242769/lang-pt/index.htm. Acesso em: 01 out. 2021.

cumentos considerados fundadores dos princípios do mais importante organismo transnacional de proteção ao trabalhador e estabelecem que o trabalho não é uma mercadoria – não estando, portanto, sujeito às leis do mercado de oferta e demanda –, asseguram aos trabalhadores de todas as ocupações proteção adequada da vida e da saúde, com regulamentação das horas de trabalho, garantia de salário que assegura condições de existência convenientes²³.

Dessa forma, o trabalho precisa ser encarado como condição de promoção dos direitos humanos, efetivação de direitos e garantias universais do homem, de maneira que medidas objetivando conferir um meio ambiente equilibrado ao trabalhador, especialmente e inclusive quanto à privacidade e inviolabilidade de seus dados, são direitos universais de todo e qualquer trabalhador, independentemente de nacionalidade, sexo, raça, natureza jurídica da prestação laboral ou qualquer outra distinção.

A Convenção n.º 155, da OIT, promulgada pelo Decreto n.º 1.254/1994²⁴, estabelece, no artigo 3, alínea “e”, que o termo saúde, com relação ao trabalho, abrange não somente a ausência de sintomas ou doenças, mas inclui todos os elementos físicos e mentais que afetam a saúde e estão diretamente relacionados com a segurança e a higiene do trabalho.

A Convenção n.º 155, da OIT, também estabelece várias obrigações ao Estado, que exerce papel fundamental em matéria de segurança e saúde dos trabalhadores. O artigo 4, item 1, impõe a adoção e reexame periódico de política nacional; o artigo 5, determina a adoção de medidas legislativas e regulamentares para dar efetividade ao disposto no artigo 4, e o artigo 9 impõe a implementação de sistema de fiscalização do cumprimento de leis e regulamentos relativos à segurança, higiene e ao meio ambiente do trabalho.

Os direitos conquistados pelos trabalhadores ao longo de séculos consubstanciam-se em benefícios para toda a sociedade, que inadmitte o trabalho em ambiente não saudável ou inseguro. A tutela do trabalho digno é valor reconhecido e ratificado pela comunidade internacional, especialmente os membros da Organização Internacional do Trabalho, inclusive o Brasil, um de seus membros fundadores. É o que se extrai logo do preâmbulo da Constituição da OIT²⁵:

Preâmbulo

Considerando que a paz para ser universal e duradoura deve assentar sobre a justiça social;

Considerando que existem condições de trabalho que

23 OIT. Constituição da OIT e Declaração de Filadélfia, 1944. Disponível em: https://www.ilo.org/wcmsp5/groups/public/---americas/---ro-lima/---ilo-brasilia/documents/genericdocument/wcms_336957.pdf. Acesso em: 07 out. 2020.

24 BRASIL. Decreto n.º 1254 de setembro de 1994. Promulga a Convenção n.º 155 da Organização Internacional do Trabalho e o Meio Ambiente do Trabalho. Disponível em <https://www2.camara.leg.br/legin/fed/decret/1994/decreto-1254-29-setembro-1994-449674-publicacaooriginal-1-pe.html>. Acesso em: 07 out. 2020.

25 OIT. Constituição da OIT e Declaração de Filadélfia, 1944. Disponível em: https://www.ilo.org/wcmsp5/groups/public/---americas/---ro-lima/---ilo-brasilia/documents/genericdocument/wcms_336957.pdf. Acesso em: 07 out. 2020.

implicam, para grande número de indivíduos, miséria e privações, e que o descontentamento que daí decorre põe em perigo a paz e a harmonia universais, e considerando que é urgente melhorar essas condições no que se refere, por exemplo, à regulamentação das horas de trabalho, à fixação de uma duração máxima do dia e da semana de trabalho, ao recrutamento da mão-de-obra, à luta contra o desemprego, à garantia de um salário que assegure condições de existência convenientes, à proteção dos trabalhadores contra as moléstias graves ou profissionais e os acidentes do trabalho, à proteção das crianças, dos adolescentes e das mulheres, às pensões de velhice e de invalidez, à defesa dos interesses dos trabalhadores empregados no estrangeiro, à afirmação do princípio 'para igual trabalho, mesmo salário', à afirmação do princípio de liberdade sindical, à organização do ensino profissional e técnico, e outras medidas análogas;

Tais valores igualmente constam de nossa Carta Magna, que tem como fundamentos a dignidade da pessoa humana e o valor social do trabalho.

A saúde e a segurança têm importância epicentral na moral e na dignidade da relação de trabalho. O caráter coletivo da lesão potencializa o seus efeitos deletérios, na medida em que deprecia as condições de trabalho.

Conclusão

A LGPD objetiva a proteção dos direitos da liberdade e da privacidade, ambos fundamentos da personalidade, inerentes ao desenvolvimento humano, através da regulamentação do tratamento dos dados pessoais do indivíduo.

Não obstante a ausência de menção específica às relações de trabalho, a LGPD brasileira não deixa dúvida de que sua aplicabilidade é irrestrita, quando, no artigo 3º, estabelece que qualquer operação de tratamento realizada em território nacional por pessoa física ou jurídica, seja de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, estará sujeita aos seus preceitos.

Sendo direitos fundamentais de todo homem, possuem plena aplicabilidade aos trabalhadores, que devem ter sua personalidade mantida incólume, através da preservação de sua privacidade, de maneira que a LGPD é de plena aplicabilidade aos contratos de trabalho.

A LGPD estabelece a necessidade de que a coleta e o tratamento de dados dos trabalhadores seja realizada de forma responsável e adequada, de maneira que os empregadores deverão aprimorar suas práticas para que os dados fornecidos pelos trabalhadores o sejam de forma consentida e de legítima necessidade, sob pena de violação aos direitos da personalidade dos trabalhadores, especialmente sua privacidade.

O empregador que desrespeita os limites do tratamento de dados contraria o princípio da boa-fé objetiva, que consiste numa regra obrigatória do Direito

do Trabalho, do qual emanam os deveres de cooperação, colaboração e lealdade entre as partes

O trabalho precisa ser encarado como condição de promoção dos direitos humanos, efetivação de direitos e garantias universais do homem, de maneira que medidas objetivando conferir um meio ambiente equilibrado ao trabalhador, especialmente e inclusive quanto à privacidade e inviolabilidade de seus dados, são direitos universais de todo e qualquer trabalhador, independentemente de nacionalidade, sexo, raça, natureza jurídica da prestação laboral ou qualquer outra distinção.

Não basta, portanto, que a ausência de riscos seja limitada apenas ao aspecto físico, mas também ao psicológico e moral, englobando os direitos da personalidade, como a privacidade, especialmente, no que diz respeito ao presente trabalho, aos dados do trabalhador, que somente podem ser tratados nas hipóteses e dentro dos limites da LGPD.

Trabalho, dignidade, identidade social e sustentabilidade são indissociáveis. Um não se mantém em pé sem o outro. Não há dignidade se os dados pessoais são indevidamente coletados, manipulados e compartilhados, pois tais práticas reduziriam o trabalhador uma mera mercadoria.

As empresas que não respeitam a privacidade de seus trabalhadores e manipulam de forma ilegal seus dados pessoais não oferecem um meio ambiente de trabalho saudável e seguro, mas empurram ladeira abaixo as condições de vida de todos os seus subordinados.

REFERÊNCIAS

ALVARENGA, Rúbia Nanotelli. **As revistas realizadas nos bens de uso pessoal do empregado e nos bens de propriedade da empresa**. Portal Jus.com.br. Abril de 2014. Disponível em: <https://jus.com.br/artigos/27514/as-revistas-realizadas-nos-bens-de-uso-pessoal-do-empregado-e-nos-bens-de-propriedade-da-empresa>. Acesso: 29 set. 2021.

ALVARENGA, Rúbia Nanotelli. **Direitos da Personalidade do trabalhador e correio eletrônico**. Portal Jus.com.br. Dezembro de 2012. Disponível em: <https://jus.com.br/artigos/26273/direitos-da-personalidade-do-trabalhador-e-correio-eletronico>. Acesso: 28 set. 2021.

ALVARENGA, Rúbia Zanutelli. **Princípios Fundamentais de Direito Ambiental do Trabalho**. In: FELICIANO, Guilherme Guimarães; URIAS, João; MARANHÃO, Ney (coord). *Direito Ambiental do Trabalho*. Apontamentos para uma teoria geral. São Paulo: LTr, 2017. p. 70.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 18 abr. 2020.

BRASIL. **Lei 6.938, de 31 de agosto de 1981**. Brasília, DF: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/ccivil03/leis/l6938.htm. Acesso em: 06 out. 2020.

BRASIL. **Decreto n.º 1254 de setembro de 1994**. Promulga a Convenção n.º 155 da Organização Internacional do Trabalho e o Meio Ambiente do Traba-

lho. Disponível em <<https://www2.camara.leg.br/legin/fed/decret/1994/decreto-1254-29-setembro-1994-449674-publicacaooriginal-1-pe.html>>. Acesso em: 07 out. 2020.

CAMARGO, Thaísa Rodrigues Lustosa; MELO, Sandro Nahmias. **Princípios de direito ambiental do trabalho**. São Paulo: LTr, 2013. p. 24-25.

COELHO, Fábio Ulhoa. **Curso de Direito Civil**. São Paulo: Saraiva, 2003, v.1, p.193.

CONSELHO DA UNIAO EUROPEIA. **General Data Protection Regulation**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=FR>. Acesso em: 28 set. 2021.

COSTA, Cândido Anchieta. **O controle dos websites acessados pelo trabalhador**. Portal Jus.com.br. Agosto de 2013. Disponível em: <https://jus.com.br/artigos/24724/o-controle-dos-websites-acessados-pelo-trabalhador/2>. Acesso: 29 set. 2021.

DELGADO, Gabriela Neves. **Direito Fundamental ao Trabalho Digno**. 2ª Edição. São Paulo: LTr, 2015.

FILHO, José Claudio Monteiro de Brito. **A proteção do meio ambiente do trabalho e a teoria da justiça como equidade de John Rawls**. In: FELICIANO, Guilherme Guimarães; URIAS, João; MARANHÃO, Ney (coord). **Direito Ambiental do Trabalho**. Apontamentos para uma teoria geral. Volume 3. São Paulo: LTr, 2017. p. 473.

JUNIOR, Laert Mantovani. **O Direito Constitucional à Intimidade e à Vida Privada do Empregado e o Poder Diretivo do Empregador**. São Paulo: Ltr, 2010, p. 28.

MARANHÃO, Ney. **Poluição Labor Ambiental**. Abordagem conceitual da degradação das condições de trabalho, de organização do trabalho e das relações interpessoais travadas no contexto laborativo. Rio de Janeiro: Editora Lumen Juris, 2018, p. 49.

MELO, Raimundo Simão de. **Direito Ambiental do Trabalho e a Saúde do Trabalhador**. São Paulo: LTr, 2006, p. 23-24.

MIRANDA, Rosângelo Rodrigues. **A Proteção Constitucional da Vida Privada**. São Paulo: Editora de Direito, 1996, p.82.

ORGANIZAÇÃO INTERNACIONAL DO TRABALHO (OIT). **Constituição da OIT e Declaração de Filadélfia**, 1944. Disponível em: <https://www.ilo.org/wcmsp5/groups/public/---americas/---ro-lima/---ilo-brasilia/documents/genericdocument/wcms_336957.pdf>. Acesso em: 07 out. 2020.

ORGANIZAÇÃO INTERNACIONAL DO TRABALHO (OIT). **R201 – Sobre o Trabalho Doméstico Decente para as Trabalhadoras e os Trabalhadores Domésticos**. Disponível em: https://www.ilo.org/brasilia/temas/trabalho-domestico/WCMS_242769/lang--pt/index.htm. Acesso em: 01 out. 2021.

PINHEIRO, Iuri; BOMFIM, Vólia. **A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho**. Disponível em: <http://trabalhoemdebate.com.br/artigo/detalhe/a-lei-geral-de-protacao-de-dados-e-seus-impactos-nas-relacoes-de-trabalho>. Acesso em: 28 set. 2021.

SARLET, Ingo Wolfgang; FENSTERSEIFER, Tiago. **Estado Socioambiental**

e Mínimo Existencial (Ecológico): algumas aproximações. In: FELICIANO, Guilherme Guimarães; SARLET, Ingo Wolfgang; MARANHÃO, Ney; FENSTERSEIFER, Tiago (orgs.). *Direito Ambiental do Trabalho – apontamentos para uma teoria geral, volume 5*. São Paulo: LTr, 2020. p. 22.

37. LGPD E RELAÇÕES DE TRABALHO: A IMPORTÂNCIA DO TRATAMENTO DE DADOS SENSÍVEIS COMO FORMA DE COMBATE À DISCRIMINAÇÃO E PROTEÇÃO DOS TRABALHADORES LGBTIQ+

GDPL AND LABOUR RELATIONS: THE IMPORTANCE OF SENSIBLE DATA TREATMENT AS A FORM OF COMBAT AGAINST THE DISCRIMINATION AND PROTECTION OF LGBTIQ+ WORKERS

HELEN RODRIGUES DE SOUZA²⁶ E EYDIE CRISTINA DE SOUZA²⁷

Resumo

O escopo do presente artigo consiste em demonstrar como a Lei Geral de Proteção de Dados, Lei 13.709/2018, pode ser um importante instrumento no combate à discriminação no ambiente de trabalho, com foco na proteção das minorias integrantes da população LGBTIQ+. No que concerne à metodologia de pesquisa, adotou-se o método de abordagem hipotético-dedutivo, por meio de coleta bibliográfica de dados. De proêmio, foram tecidas considerações sobre aspectos gerais da LGPD, assim como sobre a sua incidência no âmbito das relações de trabalho. Outrossim, procedeu-se à análise de dispositivos da Lei que tratam dos dados e dos dados sensíveis, bem como foram abordadas as peculiaridades de tratamento impostas a essa última categoria. Cuidou-se, finalmente, da importância do reconhecimento dos dados relativos à orientação sexual e à identidade de gênero como dados sensíveis, conferindo-lhes tratamento apropriado a tal categoria como forma de promoção da igualdade e de combate à discriminação no ambiente de trabalho.

Palavras-chave: Lei Geral de Proteção de Dados. Dados Sensíveis. Direitos LGBTIQ+. Orientação Sexual e Identidade de Gênero. Direito à igualdade e à não discriminação. Privacidade.

Abstract

The scope of this article is to demonstrate how the General Data Protection Law, Law 13.709/2018, can be an important instrument for combating discrim-

26 Pós-Graduação Lato Sensu-Especialista em Direito e Processo do Trabalho pelo Instituto Brasileiro de Mercado de Capitais de São Paulo (IBMEC-SP). Extensão universitária em Direitos Sociais pela Escola de Lisboa da Faculdade de Direito da Universidade Católica Portuguesa (UCP). Extensão universitária em Temas Avançados de Direito Público e Privado pela Universidade de Santiago de Compostela (USC). Certificação de DPO pelo Complexo de Ensino Renato Saraiva (CERS). Pós-graduação do Master in Business Administration de Gestão Tributária pela USP/Esalq. Advogada cível. helenhrs@hotmail.com.

27 Pós-Graduação Lato Sensu - Especialista em Direito Público pela Universidade de Direito Damásio de Jesus. Possui extensão universitária em Temas Avançados de Direito Público e Privado pela Universidade de Santiago de Compostela. Oficial de Justiça Avaliadora Federal do TRT15. eydiecristina@gmail.com

ination in the work environment, focusing on the protection of minorities that integrate the LGBTIQ+ population. Regarding the research methodology, the method of hypothetical-deductive approach was adopted, through the collection of bibliographic data. As first, considerations were made about the general aspects of the GDPL, as well as its impact on labor relations. Furthermore, some articles of the Law that deal with data and sensitive data were analyzed, as well as the treatment peculiarities imposed on this category. Finally, attention was given to the importance of recognizing as sensitive data those related to sexual orientation and gender identity, giving them the appropriate treatment to this category as a way of promoting equality and combating discrimination in the work environment.

Keywords: General Data Protection Law. Sensitive Data. LGBTIQ+ Rights. Sexual Orientation and Gender Identity. Right to equality and non-discrimination. Privacy.

1. Introdução

É cediço que, diante da intensa globalização e aceleração do desenvolvimento da sociedade, a privacidade, tanto na seara física quanto digital, tornou-se uma das principais demandas e cerne das discussões no âmbito das relações humanas.

A troca de dados mostra-se como um ato inerente aos relacionamentos pessoais, seja por razões de comunicação, trabalho ou, ainda, promoção pessoal, uma vez que os dados podem ser considerados como uma extensão da própria personalidade de seus titulares.

Conforme se verá adiante, o tratamento de dados pessoais no âmbito das relações de trabalho mostra-se como uma das principais vertentes da proteção da privacidade, porquanto o fornecimento de dados, nestes casos, se dá como condição indispensável à própria relação de trabalho, não havendo, na hipótese, o consentimento nos mesmos moldes em que há, por exemplo, nas relações existentes nas redes sociais, de consumo de produtos e serviços, dentre outras formas de relacionamento pessoal, onde o titular de dados voluntariamente escolhe se vai divulgar suas informações ou não. De fato, nas relações de trabalho, naturalmente pautadas pelo desequilíbrio entre as partes, há que se ter um olhar diferenciado do consentimento concedido pelo trabalhador.

De toda forma, tem-se que a privacidade de dados é uma demanda em ascensão na sociedade moderna, é um valor essencial que não pode ser negligenciado.

Neste âmbito, observa-se um movimento legislativo crescente no cenário internacional e nacional que visa à regulamentação das operações que envolvem a privacidade.

Nessa conjuntura, em 14 de agosto de 2018 foi editada a Lei 13.709/2018, conhecida como LGPD (Lei Geral de Proteção de Dados), sendo alterada pela Medida Provisória 869/2018 e pela Lei n.º 13.853/2019, tendo entrado em vigência apenas em 17.09.2020. A LGPD inspirou-se na lei europeia de proteção de dados, denominada General Data Protection Regulation - GDPR (Regulation 2016/679), possuindo como principal objetivo a proteção de dados de pessoas naturais.

No Brasil, o direito à privacidade já contava com previsão constitucional, con-

substanciada no direito fundamental previsto no art. 5º, X, da Constituição Federal de 1988, e possuía mecanismos de proteção.

Muito embora a LGPD tenha configurado grande avanço no que tange à proteção da privacidade, notadamente quanto à segurança de dados pessoais, tem-se que a legislação pátria contava com outros diplomas normativos que foram editados visando instituir mecanismos legais de proteção, tais como a Lei n. 12.965/2014 (Marco Civil da Internet), a Lei n. 8.078/1990 (Código de Defesa do Consumidor), a Lei n.º 12.527/2011 (Lei de Acesso à Informação), a Lei n.º 9.507/1997 (Lei do Habeas Data) e o Decreto n.º 7.963/2013 (Decreto do Comércio Eletrônico), o Decreto n.º 6.523/2008 (Decreto do Serviço de Atendimento ao Consumidor), Decreto n.º 6.425/2008 (Decreto do Censo Anual da Educação) e o Decreto n.º 6.135/2007 (Decreto que regula o cadastro único para programas sociais do Governo Federal).

Isto é, a privacidade, no Brasil, já há tempos mostra-se como objeto de proteção, tanto pela Lei Maior quanto pela legislação ordinária, isso uma vez que o ordenamento jurídico brasileiro, antes mesmo da edição da LGPD, já possuía normas que buscavam conferir proteção à privacidade, estendendo-se os mecanismos protetivos aos dados pessoais, por meio de uma interpretação sistemática das normas. Os supramencionados diplomas legais individualmente enunciavam alguns dos princípios inerentes à proteção de dados, o que foi fator indispensável para a sistematização das normas no âmbito da LGPD.

Desta forma, tem-se que a grande novidade trazida pela LGPD consiste no fato de que esta prevê mecanismos, procedimentos e, ainda, penalidades relacionadas especificamente à proteção de dados pessoais, o que se distingue da proteção da privacidade em si.

O referido diploma legal promoveu, inclusive, governança, tendo-se em vista a criação da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDP), estruturas ligadas à Presidência da República e exclusivamente dedicadas ao tema.

Contudo, a LGPD vem sendo alvo de muitos debates, tendo-se em vista que traz à baila conceitos e terminologias completamente inéditas, ensejando dúvidas e discussões acerca da extensão de aplicação da norma.

Desse modo, no presente artigo será realizada análise de ponto ensejador de debate, afeito à aplicação da LGPD no âmbito das relações de trabalho, especificamente no que concerne à abrangência das informações relativas à orientação sexual e identidade de gênero como dados sensíveis, merecedores de maior proteção por meio de mecanismos de segurança específicos.

Conforme adiante se verá, houve lacuna normativa no que se refere à aplicabilidade da LGPD às relações de trabalho, diferentemente do que se observa no regulamento europeu (GDPR), que disciplina expressamente o assunto.

Por conseguinte, buscar-se-á na presente análise apontar argumentos favoráveis à aplicação da Lei Geral de Proteção de Dados às relações de trabalho, pretendendo-se, outrossim, demonstrar a relevância da adoção de vertente interpretativa que inclua os dados relativos à orientação sexual e identidade de gênero como dados pessoais sensíveis, posto que são informações que integram a privacidade

e intimidade dos indivíduos, estando sob o manto protetivo próprio dos direitos fundamentais. Demais disso, abordar-se-á o elevado potencial ensejador de tratamento discriminatório no ambiente de trabalho contido nos referidos dados a justificar a sua inclusão dentre os dados sensíveis, à luz da Lei 13.709/2018.

É certo que, até a consolidação doutrinária e jurisprudencial dos posicionamentos sobre a aplicação da LGPD, muitos de seus aspectos serão alvo de discussão em instâncias diversas, buscando-se com o presente estudo contribuir para o debate concernente ao nevrálgico tema do tratamento como dados sensíveis das informações relativas à identidade de gênero e orientação sexual a fim de se proteger trabalhadores LGBTIQ+ contra condutas discriminatórias no meio ambiente laboral.

2. Aspectos gerais da LGPD. Dados e dados sensíveis

Antes de adentrar à questão dos mecanismos de proteção instituídos pela LGPD no âmbito dos dados sensíveis, é de rigor, para melhor compreensão do tema, realizar breve análise sobre alguns dos conceitos essenciais trazidos pela referida Lei.

Pois bem, tem-se que as disposições gerais da LGPD são tratadas em seu Capítulo I, nele estando contidas as definições de novos termos e princípios aplicáveis.

No artigo 1º do referido diploma legal, é estabelecida a proteção de direitos fundamentais como a liberdade, a privacidade e o direito ao desenvolvimento de pessoas naturais, havendo posição majoritária que defende, com base neste dispositivo, que a LGPD seria aplicável apenas ao tratamento de dados de pessoas físicas, excluindo-se, neste caso, as pessoas jurídicas.

No artigo 4º da referida lei, há previsão acerca das atividades excluídas de seu escopo, dispondo expressamente que não se aplica aos dados tratados por pessoa natural sem finalidade econômica; dados utilizados para fins artísticos, jornalísticos e acadêmicos; dados utilizados para fins de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão a infrações penais, bem como de dados que tenham origem fora do Brasil, sem qualquer compartilhamento, tratamento ou transferência no território nacional.

O artigo 2º da LGPD traz os fundamentos da proteção de dados, deixando cristalino que, a despeito da proteção na esfera privada, particular, os dados também possuem grande importância e influência em âmbito externo, de desenvolvimento econômico e social da própria sociedade.

Importante destacar que, no contexto do presente estudo, imperioso se faz analisar as conceituações trazidas pela lei em seu artigo 5º, isto é, dentre os conceitos mais relevantes, denota-se:

Art. 5º Para os fins desta Lei, considera-se²⁸:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem

28 BRASIL. Lei n.º 13.709. Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 20 out. 2021.

racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019) Vigência

IX - agentes de tratamento: o controlador e o operador;

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei nº 13.853, de 2019).

Observa-se que os incisos V, VI, VII, VIII e XIX do artigo supratranscrito tratam dos sujeitos envolvidos nas relações de tratamento de dados, hipótese na qual

interessa ao presente estudo compreender que, no âmbito das relações de trabalho, o titular de dados, no caso o empregado ou trabalhador, possui seu consentimento contaminado pela subordinação existente na relação jurídica, o que denota ainda mais a necessidade de proteção dos dados coletados consoante se verá na sequência.

No que se refere à denominação legal acerca dos dados, tem-se que os incisos I, II e III do artigo supramencionado diferenciam os tipos de informação coletada. Isto é, os dados pessoais seriam qualquer tipo de informação coletada de pessoa natural, que, analisada de forma isolada ou juntamente com outras informações, viabiliza a identificação do titular de dados. Na qualidade de categoria dos dados pessoais, a lei define os dados pessoais sensíveis como aqueles que exprimem informações específicas descritas no inciso II artigo em comento sobre a pessoa natural titular e, noutra categoria, os dados anonimizados seriam os referentes a pessoas naturais sem que seja possível a sua identificação.

No que tange aos dados sensíveis, tem-se que tal nomenclatura decorre do potencial claro de discriminação social que advém das informações coletadas, de modo que o tratamento desses dados deve ser realizado de forma mais restritiva, com padrões mais elevados de segurança.

Sobre o tema, destaque-se o artigo 51 da GDPR²⁹, lei europeia que serviu de inspiração para a edição da LGPD, veja -se:

(51) Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais.

Neste sentido, os dados sensíveis merecem maior proteção, motivo pelo qual a LGPD, em seu artigo 11, restringe as hipóteses de tratamento, relacionando, em sua maior parte, a possibilidade de acesso pelo operador e controlador de dados condicionada ao consentimento do titular.

Observa-se que, em comparação ao artigo 7º da LGPD (que define as bases legais para tratamento de dados pessoais), há exclusão das hipóteses de tratamento de dados sensíveis com base na execução de contrato, interesse legítimo e proteção ao crédito, permanecendo, portanto, as demais bases, ainda que com restrições.

Conforme já mencionado, no âmbito das relações de trabalho há problemática envolvendo a questão do consentimento, tendo-se em vista o natural desequilíbrio de poder existente entre as partes a afetar o momento da coleta de dados.

De todo modo, a empresa/empregador, na posição de controlador/operador, ao coletar os dados de seus empregados/trabalhadores, deve sempre prezar pela adoção das melhores práticas e políticas de segurança, de modo a garantir a proteção legal conferida no Capítulo III da LGPD (que trata dos direitos do titular de

29 UNIÃO EUROPEIA. General Data Protection Regulation. Bruxelas, Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 20 out. 2021.

dados), sob pena de responsabilização e aplicação das penalidades previstas nos moldes dos Capítulos IV, VIII e IXI.

Em suma, tem-se que o tratamento de dados pessoais sensíveis deve ser precedido de maiores cautelas, visando sempre à proteção dos direitos dos titulares, tendo-se em vista que o vazamento de dados dessa natureza pode trazer consequências mais gravosas à esfera de privacidade e intimidade dos titulares, dando azo, inclusive, a condutas discriminatórias, conforme se verá adiante.

3. Orientação sexual e identidade de gênero como dados sensíveis: igualdade e não discriminação

A aplicação da Lei Geral de Proteção de Dados - LGPD, Lei 13.709/2018, às relações de trabalho decerto constitui instrumento regulatório relevante a incrementar o instrumental normativo de combate à discriminação na seara laboral, atuando como manto protetivo de dados que possam expor grupos considerados *outsiders*.

Nesse contexto, exsurge a temática envolvendo as questões atinentes à identidade de gênero e à orientação sexual, haja vista a reconhecida maior vulnerabilidade das pessoas que integram a população LGBTIQ+, do que emana a necessidade de atenção especial ao tratamento de dados com potencial de ensejar tratamento discriminatório no meio ambiente de trabalho.

Vale lembrar que o combate à discriminação e a busca contínua por tratamento isonômico para a população LGBTIQ+ hoje ocupam assento central no âmbito dos direitos humanos e fundamentais, em que pese o longo período pretérito de obscurantismo no tocante aos direitos desses indivíduos. A marcha evolutiva dos direitos humanos, sempre pautada pela historicidade em sua construção, é irrefreável.

De fato, os Direitos LGBTIQ+ somente foram, pela primeira vez, declarados como Direitos Humanos pela Organização das Nações Unidas em junho de 2011, no bojo da Resolução do Conselho de Direitos Humanos da ONU, de nº L9, na Assembleia Geral. A partir de então, cabível a interpretação no sentido de que o país negligente no cumprimento de suas obrigações de cuidado também em relação aos seus cidadãos LGBTIQ+ estará desrespeitando Tratados Internacionais de Direitos Humanos³⁰.

Hodiernamente, farto arcabouço legislativo internacional confere suporte normativo ao tratamento isonômico no que tange às oportunidades em geral e nas relações de trabalho e emprego para os integrantes do grupo LGBTIQ+, valendo mencionar os Princípios de Yogyakarta sobre Aplicação da Legislação Internacional de Direitos Humanos em Relação a Orientação Sexual e Identidade de Gênero (2006), o Pacto Internacional sobre Direitos Civis e Políticos, em seus artigos 2º, 1 e 26, o Pacto de São José da Costa Rica, em seus artigos 1, 3, 7.1, 11.2 e 18, a Convenção Americana sobre Direitos Humanos, a Convenção Interamericana sobre Toda Forma de Discriminação e Intolerância, dentre outros.

30 GORISGH, Patricia Cristina Vasques de Souza. *O reconhecimento dos direitos humanos LGBT: de stonewall à ONU*. Disponível em <https://pt.scribd.com/book/405704128/O-reconhecimento-dos-direitos-humanos-lgbt-de-stonewall-a-onu>. Acesso em: 19 out. 2021.

Com efeito, os Princípios de Yogyakarta³¹ n.º 06 e n.º 12 preconizam:

PRINCÍPIO 06

DIREITO À PRIVACIDADE Toda pessoa, **independente de sua orientação sexual ou identidade de gênero, tem o direito de desfrutar de privacidade**, sem interferência arbitrária ou ilegal, inclusive em relação à sua família, residência e correspondência, assim como o direito à proteção contra ataques ilegais à sua honra e reputação. **O direito à privacidade normalmente inclui a opção de revelar ou não informações relativas à sua orientação sexual ou identidade de gênero**, assim como decisões e escolhas relativas a seu próprio corpo e a relações sexuais consensuais e outras relações pessoais. (grifo nosso)

Os Estados deverão:

(...) **Assegurar o direito de todas as pessoas poderem escolher, normalmente, quando, a quem e como revelar informações sobre sua orientação sexual ou identidade de gênero, e proteger todas as pessoas de revelações arbitrárias ou indesejadas**, ou de ameaças de revelação dessas informações por outras pessoas. (grifo nosso)

PRINCÍPIO 12

DIREITO AO TRABALHO Toda pessoa tem o direito ao trabalho digno e produtivo, a condições de trabalho justas e favoráveis e à proteção contra o desemprego, **sem discriminação por motivo de orientação sexual ou identidade de gênero**. (grifo nosso)

Os Estados deverão:

a) Tomar todas as medidas legislativas, administrativas e outras medidas necessárias para **eliminar e proibir a discriminação com base na orientação sexual e identidade de gênero no emprego público e privado**, inclusive em relação à educação profissional, recrutamento, promoção, demissão, condições de emprego e remuneração; (grifo nosso)

b) Eliminar qualquer discriminação por motivo de orientação sexual ou identidade de gênero para assegurar emprego e oportunidades de desenvolvimento iguais em todas as áreas do serviço público, incluindo todos os níveis de serviço governamental e de emprego em funções públicas, também incluindo o serviço na polícia e nas

31 Princípios de Yogyakarta. Brasília, DF. Disponível em: http://www.dhnet.org.br/direitos/sos/gays/principios_de_yogyakarta.pdf. Acesso em: 20 out. 2021.

forças militares, fornecendo treinamento e programas de conscientização adequados para combater atitudes discriminatórias.

Outrossim, da Convenção Interamericana Contra Toda Forma de Discriminação e Intolerância³² extraem-se importantes noções, *in verbis*:

Artigo 1. Para os efeitos desta Convenção:

1. **Discriminação é qualquer distinção, exclusão, restrição ou preferência, em qualquer área da vida pública ou privada**, cujo propósito ou efeito seja anular ou restringir o reconhecimento, gozo ou exercício, em condições de igualdade, de um ou mais direitos humanos e liberdades fundamentais consagrados nos instrumentos internacionais aplicáveis aos Estados Partes. A discriminação pode basear-se em nacionalidade, idade, sexo, **orientação sexual, identidade e expressão de gênero**, idioma, religião, identidade cultural, opinião política ou de outra natureza, origem social, posição socioeconômica, nível educacional, condição de migrante, refugiado, repatriado, apátrida ou deslocado interno, deficiência, característica genética, estado de saúde física ou mental, inclusive infectocontagioso, e condição psíquica incapacitante, ou qualquer outra condição. (grifo nosso)

Semelhantes preceitos são apresentados pela Convenção 111 da Organização Internacional do Trabalho, que trata da Discriminação em Matéria de Emprego e Ocupação³³, *in verbis*:

Art. 1 — 1. Para os fins da presente convenção o termo “discriminação” compreende:

a) toda distinção, exclusão ou preferência fundada na raça, cor, **sexo**, religião, opinião política, ascendência nacional ou origem social, que tenha por efeito destruir ou alterar a igualdade de oportunidade ou de tratamento em matéria de emprego ou profissão; (grifo nosso)

b) **qualquer outra distinção, exclusão ou preferência que tenha por efeito destruir ou alterar a igualdade de oportunidades ou tratamento em matéria de emprego**

32 Convenção Interamericana Contra Toda Forma de Discriminação e Intolerância. Disponível em https://www.oas.org/en/sla/dil/docs/inter_american_treaties_A-69_Convencao_Interamericana_discriminacao_intolerancia_POR.pdf. Acesso em: 20 out. 2021.

33 Convenção n.º 111 da Organização Internacional do Trabalho – Discriminação em Matéria de Emprego e Ocupação, disponível em: https://www.ilo.org/brasil/convencoes/WCMS_235325/lang-pt/index.htm. Acesso em: 20 out. 2021.

ou profissão que poderá ser especificada pelo membro interessado depois de consultadas as organizações representativas de empregadores e trabalhadores, quando estas existam, e outros organismos adequados. (grifo nosso)

No estuário normativo nacional, a Constituição Federal traz em seu preâmbulo a igualdade como valor supremo de uma sociedade fraterna, pluralista e sem preconceitos. Elenca, outrossim, os valores da igualdade e da não discriminação no rol dos objetivos fundamentais da República Federativa do Brasil (artigo 3º, I, III e IV, CF), além de prever a dignidade da pessoa humana como um de seus fundamentos (artigo 1º, III, CF). A Lei Maior insere, ainda, dentre os direitos sociais dos trabalhadores a proibição de diferenças no tocante a critério de admissão, exercício de quaisquer funções ou diferenças salariais embasadas em motivo relacionado a sexo (artigo 7º, XXX, da Constituição Federal). Nessa linha, ganha destaque a isonomia como direito fundamental (artigo 5º, *caput*, da CF), valendo lembrar a possibilidade de ampliação do rol dos direitos fundamentais por normas mais benéficas internacionais ratificadas pelo Brasil, conforme cláusula de abertura constante do artigo 5º, § 2º, CF. O artigo 4º, II, da Constituição Cidadã elenca, ainda, como princípio fundamental a reger a República Federativa do Brasil em suas relações internacionais a prevalência dos direitos humanos.

Na seara infraconstitucional, importantes diplomas compõem o conjunto normativo destinado a dar forma ao molde isonômico e não discriminatório traçado pela Lei Maior, tais como Lei 9.029/95, artigo 1º, e a CLT, artigo 461. O Decreto 9.571/2008, por seu turno, trata das diretrizes nacionais sobre empresas e direitos humanos e traz duas importantes previsões em seu artigo 3º, XII e XIII, ao estabelecer o “combate à discriminação nas relações de trabalho e promoção da valorização da diversidade”, além de determinar a adoção de medidas que visam a evitar a discriminação e a fomentar práticas inclusivas, fazendo menção expressa a “incentivos para a contratação de grupos vulneráveis”.

Como é cediço, a discriminação pode ocorrer em diversos núcleos sociais que compõem a vida de uma pessoa, dentre eles o laboral, podendo apresentar-se em suas dimensões direta, quando externalizada por meio de um ato de cunho discriminatório claramente ofensivo ao tratamento isonômico que deve reger as relações num Estado Democrático de Direito, ou, ainda, indireta, essa consistente num tratamento com estampa isonômica, porém cujos resultados ensejam segregação.

Por outro lado, é indubitável que os direitos fundamentais à igualdade e à não discriminação devem ser observados não apenas nas relações entre o Estado e o indivíduo (eficácia vertical), mas também entre particulares (eficácia horizontal), portanto nas relações familiares, contratuais, sociais e, especialmente, naquelas em que há desequilíbrio de poder, como é típico das relações de trabalho. Na lição sempre presente de Beltrameli³⁴, ao tratar dos direitos fundamentais nas relações entre particulares, a “doutrina majoritária nacional, com pequenas variações de condução metodológica, alinha-se, claramente, com a teoria dos efeitos diretos ou imediatos, como consequência do perfil social da Constituição Federal”.

34 NETO, Silvio Beltramelli. *Direitos Humanos*. Salvador: Editora Juspodivm, 2014. p. 180.

Nesse contexto, a seara laboral constitui um dos núcleos mais relevantes na composição da identidade social de um indivíduo, a merecer especial atenção do Estado no tocante à temática da não discriminação, devendo ser adotadas medidas legislativas, administrativas e quaisquer outras necessárias³⁵ não apenas a afastar a discriminação negativa, mas também que possam promover uma escala inclusiva crescente da população LGBTIQ+.

Nesta trilha, resta evidente a contribuição da Lei Geral de Proteção de Dados, Lei 13.709/2018, que, em seu artigo 5º, incisos I e II, estabelece dados considerados sensíveis, os quais demandam tratamento diferenciado:

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - **dado pessoal sensível**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, **dado referente à saúde ou à vida sexual**, dado genético ou biométrico, quando vinculado a uma pessoa natural; (grifo nosso)

Da análise do precitado dispositivo infere-se que o legislador nacional fez menção a dados referentes à **saúde** e à vida sexual, quedando-se silente no tocante à orientação sexual e identidade de gênero.

Em breve parênteses, cabe esclarecer que os conceitos de sexo, identidade de gênero e orientação sexual não se confundem. Com efeito, sexo refere-se à dimensão biológica e binária (masculino ou feminino) aferida quando do nascimento. O conceito de identidade de gênero, por seu turno, está relacionado a uma percepção subjetiva e interna do indivíduo em relação ao seu próprio corpo, podendo coadunar-se com a sua conformação sexual, situação em que o indivíduo identifica-se e aceita o próprio sexo (cisgênero), ou, ser divergente, quando o sujeito não se identifica com o seu sexo biológico, podendo recorrer, por livre escolha, à adoção de meios médicos, cirúrgicos ou outros para fins de alteração de sua aparência ou função corporal, hipótese na qual se incluem os indivíduos transexuais. Já no tocante à orientação sexual, extrai-se clara lição dos Princípios de Yogyakarta, *in verbis*:

Entendemos orientação sexual como uma referência à capacidade de cada pessoa de ter uma profunda atração emocional, afetiva ou sexual por indivíduos de gênero diferente (heterossexual), do mesmo gênero (homossexual) ou de mais de um gênero, assim como ter relações íntimas e sexuais com essas pessoas³⁶.

35 Princípios de Yogyakarta. Princípio 12, “a”. http://www.dhnet.org.br/direitos/sos/gays/principios_de_yogyakarta.pdf, Acesso em: 18 out. 2021.

36 Princípios de Yogyakarta. Princípio 12, “a”. http://www.dhnet.org.br/direitos/sos/gays/principios_de_yogyakarta.pdf, Acesso em: 18 out. 2021.

Não se pode olvidar, outrossim, dos indivíduos que se identificam pelo termo “queer”, definidos como avessos a categorizações, ou seja, aquele que “está incessantemente em desacordo com o normal, a norma, seja a heterossexualidade dominante ou a identidade gay/lésbica. É categoricamente excêntrico, anormal”.³⁷

O silêncio acerca das expressões “identidade de gênero” e “orientação sexual” no inciso II do artigo 5º da LGPD trazem à baila a discussão sobre a inclusão ou não dessas informações no rol dos dados pessoais sensíveis, mercedores de tratamento diferenciado.

Nesta senda e considerando a forte inspiração da Lei 13.709/2018 na legislação europeia, a General Data Protection Regulation (GDPR)³⁸, uma percutiente análise de alguns de seus dispositivos pode colaborar para que se traga luz quanto a tal questionamento interpretativo:

General Data Protection Regulation (GDPR) – art.71:

A fim de assegurar um tratamento equitativo e transparente no que diz respeito ao titular dos dados, **tendo em conta a especificidade das circunstâncias e do contexto em que os dados pessoais são tratados**, o responsável pelo tratamento deverá utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis, aplicar medidas técnicas e organizativas que garantam designadamente que os fatores que introduzem imprecisões nos dados pessoais são corrigidos e que o risco de erros é minimizado, **e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios** contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou **orientação sexual**, ou a impedir que as medidas venham a ter tais efeitos. A decisão e definição de perfis automatizada baseada em categorias especiais de dados pessoais só deverá ser permitida em condições específicas.

Como se denota do dispositivo supramencionado, a legislação europeia utiliza-se de terminologia alinhada com outros diplomas internacionais e afasta qualquer dúvida quanto à inclusão da orientação sexual no rol de dados pessoais sensíveis.

Diversamente disso, a Lei 13.709/2018, em seu artigo 5º, II, faz alusão a “vida

37 SPARGO, Tamsin. Foucault e a teoria queer: seguido de Ágape e êxtase: orientações pós- seculares. Tradução Heci Regina Candiani. 1. Ed. Belo Horizonte: Autêntica Editora, 2017. Disponível em: <https://pt.scribd.com/read/405829894/Foucault-e-a-teoria-queer-seguido-de-Agape-e-extase-orientacoes-pos-seculares>. Acesso em: 20 out. 2021.

38 UNIÃO EUROPEIA. General Data Protection Regulation. Bruxelas, Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 20 out. 2021.

sexual”, opção terminológica que não encontra correspondência nos conceitos internacionalmente firmados de sexo, identidade de gênero ou orientação sexual, exigindo maior esforço interpretativo.

A par e com respeito a interpretações no sentido de que dados alusivos a orientação sexual e identidade de gênero não estariam abarcados pelo manto protetivo mais denso que recobre os dados pessoais sensíveis na legislação pátria (LGBT), desvela-se como melhor linha interpretativa, afeita aos propósitos fundamentais de existência do próprio dispositivo, a compreensão de que tais informações estão abrangidas pelo artigo 5º, II, da LGBT, e merecem tratamento mais criterioso e diferenciado, próprio dos dados sensíveis. Conclusão diversa caminha de encontro a normas internacionais que tratam do tema e reconhecem como fatores passíveis de ensejar tratamento discriminatório os dados concernentes a “orientação sexual, identidade e expressão de gênero”, como expresso no artigo 1, 1, da Convenção Interamericana Contra Toda Forma de Discriminação e Intolerância, e, ainda, nos Princípios de Yogyakarta, n.º 06 e n.º 12.

Realmente, um vácuo conceitual exsurge quando se tenta interpretar, na legislação brasileira, o sentido do termo “vida sexual” caso excluídos os conceitos de orientação sexual e identidade de gênero. A quais dados estaria o legislador se referindo? Caso pretendesse restringir a proteção meramente ao aspecto biológico (masculino e feminino), poderia ter-se valido do termo mais restritivo “sexo”, o que não fez. Dessa forma, tratando-se de informação inegavelmente relacionada a uma das esferas mais íntimas da personalidade, que tangencia direitos fundamentais como a intimidade, a privacidade e a dignidade, parece descaber ao intérprete realizar uma restrição conceitual na análise terminológica do dispositivo brasileiro (art. 5º, II, LGPD). Desta sorte, poder-se-ia entender que “vida sexual” abarca a dimensão biológica, portando, o sexo do indivíduo, e também a sua dimensão interna, subjetiva, mental e psicológica, consubstanciada na sua orientação sexual e identidade de gênero.

Dúvidas não restam de que a exposição contra a vontade do titular de informações que digam respeito à sua orientação sexual e/ou identidade de gênero são passíveis de provocar perturbações em seu ambiente de trabalho, seja em virtude do elevado potencial de gerar condutas segregacionistas, seja pelo desconforto íntimo, subjetivo, psicológico, enfrentado pelo indivíduo. Em ambas as hipóteses, restam maculadas a dignidade da pessoa humana, o direito à intimidade, à igualdade e à não discriminação.

Por diversos ângulos de análise, o tratamento de informações relativas à orientação sexual e identidade de gênero como dados que demandam maior critério em sua coleta e armazenamento, mediante a observância da sistemática diferenciada própria dos dados sensíveis à luz da Lei 13.709/2018, afigura-se necessário à consecução dos direitos fundamentais que regem um Estado Democrático de Direito. Desta sorte, como alhures demonstrado, tais dados cabem dentro do molde conceitual traçado pela expressão “vida sexual”. Não obstante, ainda que assim não fosse, decerto tratar-se-ia de questão passível de enquadramento no termo “saúde” constante do inciso II, do artigo 5º, da LGPD.

Mister se faz ressaltar que a saúde deve ser compreendida de modo amplo,

abarcando tanto a ausência de moléstias que se manifestam na dimensão física, como também abrange os elementos psíquicos, mentais, que possam influenciar a saúde de um indivíduo.

Tanto é assim que a Convenção 155 da Organização Internacional do Trabalho, que trata da segurança e saúde dos trabalhadores³⁹, é expressa ao afirmar a incidência nas relações laborais dessa interpretação ampliativa do termo saúde, *in verbis*:

Art. 3 — Para os fins da presente Convenção:

e) o termo ‘saúde’, com relação ao trabalho, abrange não só a ausência de afecções ou de doenças, mas também os elementos físicos e mentais que afetam a saúde e estão diretamente relacionados com a segurança e a higiene no trabalho.

Tenha-se presente, outrossim, ser inegável a pressão psicológica sofrida por trabalhadores LGBTIQ+ em virtude da exposição de sua orientação sexual e/ou identidade de gênero no ambiente de trabalho, seja em virtude do temor de experienciar os deletérios efeitos psíquicos decorrentes de condutas desrespeitosas e segregacionistas advindas de colegas ou superiores, seja devido ao receio de terem, de plano, reduzidas ou até mesmo extirpadas as suas chances de ascensão profissional em virtude da velada, porém bastante presente, política de determinadas empresas consistente em evitar o preenchimento de cargos de comando ou de representação empresarial por pessoas que integram o grupo populacional LGBTIQ+.

Corroboram essa assertiva matérias jornalísticas sobre o tema, a exemplo de publicações realizadas pelo jornal O Globo, intituladas, respectivamente, “1 em cada 5 empresas não contrataria homossexuais, diz estudo”, e “40% dos profissionais LGBTs já sofreram discriminação no trabalho”, da quais se transcrevem alguns trechos:

Empresas estão preocupadas com a sexualidade de seus empregados.

11% não contratariam gays para cargos executivos.

Pesquisa feita pela Elancers, empresa de sistemas de recrutamento e seleção, com 10 mil empresas, mostra que 1 em cada 5 não contrataria homossexuais para determinados cargos. Entre as empresas consultadas, cerca de 1.500 responderam a pesquisa online, envolvendo 2.075 recrutadores. Os profissionais ouvidos são essencialmente mulheres - 75% do total, e 44% têm idade entre 26 e 35 anos.

(...) Quando 11% dizem que não contratariam homossexuais para determinados cargos, eles se referem essencialmente a cargos executivos que, via de regra, representam a empresa em público. Somados aos 7% que

39 Convenção 155 da OIT sobre Segurança e Saúde dos Trabalhadores. Disponível em https://www.ilo.org/brasil/convencoes/WCMS_236163/lang--pt/index.htm. Acesso em: 22 out. 2021.

dizem que não contratariam homossexuais de modo algum, temos um cenário onde quase um quinto das empresas não contrataria homossexuais no Brasil”, diz Cezar Tegon, presidente da Elancers.⁴⁰ (grifo nosso)

61% têm medo de escolher companhia que não aceite sua orientação.

47% revelam a orientação, sendo 32% para o chefe e 2% para o RH.

Levantamento realizado pela consultoria de engajamento Santo Caos com 230 pessoas com idades entre 18 e 50 anos, de 14 estados do Brasil, mostra que 40% dos entrevistados já sofreram discriminação no trabalho por conta da orientação sexual. Ainda de acordo com os dados, 61% dos entrevistados declararam ter alta ou média influência ao escolherem uma vaga em determinada companhia com medo da empresa não aceitar sua orientação.

(...) O executivo revela que o medo de exposição é tão grande que de uma a cada três pessoas recusou-se a responder a entrevista. **“Mais de um terço das pessoas que gostaríamos de ter entrevistado não quis se expor por medo da instituição que trabalha reconhecer sua orientação sexual e, por conta disso, sofrer algum tipo de represália, mesmo que psicológica”**, comenta. (grifo nosso)

Além disso, a pesquisa também mostrou que em apenas 52% das empresas a postura era favorável à diversidade. **“Quase metade das companhias brasileiras mostrou ter uma postura neutra ou desfavorável quanto à orientação sexual do candidato.** Em hipótese alguma o gestor deve medir a capacidade do profissional por causa de sua orientação sexual, identidade ou expressão de gênero. Esse número é muito alto e mostra o quão atrasados estamos”, afirma.⁴¹ (grifo nosso)

Vale lembrar, ainda, especialmente no tocante aos transexuais, grupo que sofre preconceito ainda mais acentuado dentro da população LGBTIQ+, que a transição de sexo não ocorre de modo imediato, tratando-se, na realidade, de um processo

40 1 em cada 5 empresas não contrataria homossexuais, diz estudo: empresas estão preocupadas com a sexualidade de seus empregados. 11% não contratariam gays para cargos executivos. Disponível em: <http://g1.globo.com/concursos-e-emprego/noticia/2015/05/1-em-cada-5-empresas-nao-contrataria-homossexuais-diz-estudo.html>. Acesso em: 20 out. 2021.

41 40% dos profissionais LGBTs já sofreram discriminação no trabalho: 61% têm medo de escolher companhia que não aceite sua orientação. 47% revelam a orientação, sendo 32% para o chefe e 2% para o rh. G1. São Paulo, maio 2015. Disponível em: <http://g1.globo.com/concursos-e-emprego/noticia/2015/04/40-dos-profissionais-lgbts-ja-sofreram-discriminacao-no-trabalho.html>. Acesso em: 20 out. 21.

lento e bastante delicado, tanto do ponto de vista fisiológico, como mental e psíquico. Durante esse processo, o indivíduo necessita de suporte psicológico, sendo fato notório que a sua expressão profissional constitui um dos pilares de maior relevância para assegurar-lhe as bases que propiciarão o atingimento da transição de sexo de modo saudável, transição essa, vale frisar, que se consubstancia em um direito humano fundamental, diretamente relacionado com a dignidade da pessoa humana.

A garantia do direito ao trabalho, e ao trabalho em ambiente hígido para integrantes do grupo LGBTIQ+, são temas da máxima relevância, pois afetam tanto a autoidentidade, o autorreconhecimento de valor social, o senso de pertencimento do indivíduo, como também interferem na sua capacidade econômica, em sua garantia de sustento, de tal sorte que a esfera laboral da vida de uma pessoa revela-se área de importância ímpar para assegurar uma vida digna. Resta evidente que um desequilíbrio nessas questões pode contribuir para a desestabilização da saúde do indivíduo, afetando-o profundamente em seu espectro psíquico e mental. E isso parece ser tão mais premente quanto maior a vulnerabilidade do indivíduo no seio social, no que se inserem, a toda evidência, as pessoas que decidem realizar a transição de sexo.

Nesta senda, ressalta à evidência que a exposição involuntária de dados concernentes à orientação sexual e identidade de gênero de uma pessoa pode causar-lhe séria perturbação e sofrimento psicológico, além da existência de um risco concreto de preterição quanto à ascensão profissional ou, em casos mais extremos, perda do próprio emprego, com comprometimento da fonte básica de sustento. Fato é que apenas a possibilidade desses eventos já é o bastante para dar azo a abalo psicológico, de tal sorte que toda e qualquer exposição passível de ensejar risco de tratamento discriminatório deve ser evitada, como meio de proteção à saúde do indivíduo, concretização da dignidade da pessoa humana e atendimento ao direito fundamental a não discriminação.

Destarte, imperioso o reconhecimento de que os conceitos de orientação sexual e identidade de gênero estão abrangidos pela especial proteção atribuída a dados sensíveis na LGPD, artigo 5º, II, seja pelo seu enquadramento no termo “vida sexual”, seja no termo “saúde”, não se podendo descuidar de atenção e cuidados com a população LGBTIQ+, sob pena de ofensa a direitos fundamentais assegurados pelo Estado Democrático brasileiro e, ainda, desrespeito a direitos humanos previstos em diplomas internacionais.

Considerações finais

Diante de todo o exposto, observa-se que a LGPD, a despeito de sua incipiente aplicação no ordenamento jurídico brasileiro, vez que entrou em vigor há pouco mais de um ano, mostra-se como instrumento indispensável para a promoção de segurança e garantia dos direitos à privacidade, intimidade, igualdade, não discriminação, notadamente quanto aos mecanismos inovadores e previsão acerca de procedimentos e boas práticas no âmbito da proteção de dados pessoais.

Conforme analisado no presente estudo, muito embora a LGPD não trate expressamente sobre sua aplicabilidade às relações de trabalho, as análises normativas, inclusive da GDPR (lei europeia que serviu como inspiração para a lei bra-

sileira), evidenciam a incidência dos mecanismos e instrumentos de proteção de dados no âmbito trabalhista.

Ademais, denota-se a importância de tais instrumentos quando analisado o tratamento de dados sensíveis no âmbito das relações de trabalho, posto que essas informações, por si só, possuem o condão de ensejar eventual tratamento segregacionista na hipótese de divulgação indiscriminada.

É neste âmbito que a LGPD estabelece limites normativos diversos para o tratamento de dados sensíveis, restringindo as bases legais de acesso a estas informações e colocando maior enfoque na questão do consentimento.

Conforme alhures mencionado, o consentimento fornecido nas relações de trabalho merece especial atenção, posto que existe um desequilíbrio de forças entre o titular de dados (empregado/trabalhador) e o controlado/operador (empresa/empregador), podendo haver contaminação da livre manifestação de vontade, vez que o fornecimento de dados pessoais surge como condição inerente à própria contratação e prestação de serviços.

Desse modo, sabe-se que o fornecimento de dados para a execução do contrato de trabalho deve ser regulado pelas disposições e procedimentos da LGPD, todavia, o tratamento de dados pelas empresas/empregadores deve ser realizado com ainda mais rigor quando há a coleta e gerenciamento de dados considerados sensíveis.

No presente estudo, utilizou-se como base de análise a questão dos indivíduos integrantes da comunidade LGBTIQ+, que, infelizmente, ainda são alvo de tratamento discriminatório por grande parte da sociedade.

Como se sabe, inúmeros prejuízos podem advir do vazamento de dados pessoais, contudo, tais danos podem ser ainda mais gravosos na hipótese aqui analisada, que seria a divulgação não autorizada das informações relativas à orientação sexual e/ou à identidade de gênero de eventual indivíduo no ambiente laboral.

Como é notório, muitos indivíduos integrantes da comunidade LGBTIQ+ hesitam em divulgar ou até escondem a sua identidade de gênero ou orientação sexual no ambiente de trabalho por receio de sofrerem tratamento discriminatório que possa obstar a sua ascensão profissional e, em casos extremos, ensejar a precoce ruptura contratual.

Lamentavelmente, a sociedade brasileira ainda se encontra contaminada por ideais discriminatórios que atuam em desfavor dos grupos minoritários, sendo os integrantes da comunidade LGBTIQ+, dentre os grupos considerados *outsiders* (portadores de deficiência, pretos, mulheres, idosos, obesos, dentre outras minorias), parcela das mais severamente atingidas e que sofre com o tratamento diferenciado em razão de suas idiosincrasias.

Certamente ainda ocorrerão inúmeras discussões e embates jurídicos acerca dos limites e forma de aplicação da LGPD. No entanto, é indubitável que a sua edição configura grande avanço para o ordenamento jurídico pátrio, sendo um mecanismo de suma importância para a garantia dos direitos fundamentais à privacidade, intimidade, igualdade e não discriminação, consubstanciando-se, outrossim, em ferramenta assecuratória da promoção, em análise última, da própria dignidade da pessoa humana, fundamento do Estado Democrático Brasileiro.

REFERÊNCIAS

BARZOTTO, Luciane Cardoso. **Trabalho E Igualdade**: tipos de discriminação no ambiente de trabalho. Porto Alegre: Livraria do Advogado, 2012. 367 p.

BUCHAIN, Luiz Carlos. **A Lei Geral de Proteção de Dados**: noções gerais. Revista

Eletrônica do Tribunal Regional do Trabalho da 9ª Região, Curitiba, v. 10, n. 93, p. 51-66, mar. 2021. Disponível em: <https://juslaboris.tst.jus.br/handle/20.500.12178/186013>. Acesso em: 21 out. 2021.

CARLOTO, Selma. **Lei Geral da Proteção de Dados**: enfoque nas relações de trabalho. 2. ed. São Paulo: LTr, 2021. 254 p.

CORREIA, Henrique; BOLDRIN, Paulo Henrique Martinucci. **Lei Geral de Proteção de Dados (LGPD) e o Direito do Trabalho**. Disponível em file:///C:/Users/User/Downloads/Lei%20Geral%20de%20Protec%CC%A7a%C-C%83o%20de%20Dados%20-%20LGPD%20-%20e%20o%20Direito%20do%20Trabalho.pdf. Acesso em: 21 out. 2021.

GORISGH, Patricia Cristina Vasques de Souza. **O reconhecimento dos direitos humanos LGBT: de Stonewall à ONU**. Disponível em <https://pt.scribd.com/book/405704128/O-reconhecimento-dos-direitos-humanos-lgbt-de-stonewall-a-onu>. Acesso em: 19 out. 2021.

MENKE, Fabiano; DRESCH, Rafael de Freitas Valle. **Lei Geral da Proteção de Dados**: aspectos relevantes. Indaiatuba: Editora Foco, 2021. 751 p. Disponível em: <https://pt.scribd.com/read/499850050/Lei-geral-de-protecao-de-dados-Aspectos-relevantes#>. Acesso em: 20 out. 2021.

MULHOLLAND, Caitlin. **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020. 593 p. Disponível em: <https://pt.scribd.com/read/496828562/A-LGPD-e-o-novo-marco-normativo-no-Brasil>. Acesso em: 20 out. 2021.

NETO, Silvio Beltramelli. **Direitos Humanos**. Salvador: Editora Juspodivm, 2014. p. 180.

PINHEIRO, Iuri; BOMFIM, Vólia. **A Lei Geral de Proteção de Dados e seus Impactos nas Relações de Trabalho**. Disponível em <http://trabalhoemdebate.com.br/artigo/detalhe/a-lei-geral-de-protecao-de-dados-e-seus-impactos-nas-relacoes-de-trabalho>. Acesso em: 21 out. 2021.

SARLET, Gabrielle Bezerra Sales; TRINDADE, Manoel Gustavo Neubarth; MELGARÉ, Plínio. **Proteção de dados**: temas controvertidos. Indaiatuba: Editora Foco, 2021. 762 p.

SPARGO, Tamsin. **Foucault e a teoria queer**: seguido de Ágape e êxtase: orientações pós-seculares. Tradução Heci Regina Candiani. 1. ed. Belo Horizonte: Autêntica Editora, 2017. Disponível em <https://pt.scribd.com/read/405829894/Foucault-e-a-teoria-queer-seguido-de-Agape-e-extase-orientacoes-pos-seculares>. Acesso em: 20 out. 2021.

TEIXEIRA, Ana Carolina Brochado; MENEZES, Joyceane Bezerra de. **Gênero, Vulnerabilidade e Autonomia: repercussões jurídicas**. 2. ed. Indaiatuba: Editora Foco, 2021. 568 p.

38. O IMPACTO DA LGPD NO CONTROLE DE PONTO POR RECONHECIMENTO FACIAL

THE IMPACT OF LGPD ON POINT CONTROL BY FACIAL RECOGNITION

MARIANA RUZZI⁴²

Resumo

O presente artigo tem como objetivo analisar a necessidade e a (in)segurança do uso do controle de ponto por reconhecimento facial e os impactos da LGPD em virtude desta prática nas relações de trabalho.

Palavras-chave: Reconhecimento facial. Dados pessoais sensíveis. Relação trabalhista.

Abstract

This article aims to analyze the need and (in) security of the use of time attendance by facial recognition and the impacts of LGPD due to this practice in labor relations.

Keywords: Facial recognition. Sensitive personal data. Labor relationship.

1. Introdução

Com a Lei Geral Proteção de Dados (LGPD - Lei 13.709/18) já em vigor, muitas empresas tiveram ou ainda estão tendo que rever seus processos internos. Um dos setores afetados pela LGPD é o setor de Recursos Humanos, vez que trata diretamente de dados pessoais e dados pessoais sensíveis de seus colaboradores e dependentes.

Dentre os processos administrados pelo setor de Recursos Humanos está o controle de ponto, exigência legal para empresas que possuem mais de 20 (colaboradores), através de registro manual, mecânico ou eletrônico. Além da obrigatoriedade de anotação de horário de entrada e saída - após regulamentado pelo antigo Ministério do Trabalho e Emprego -, também é obrigatória a impressão do comprovante de registro de ponto, documento por vezes descartado no ambiente de trabalho que contém inúmeros dados pessoais do colaborador.

Sendo assim, o presente artigo abordará os pontos para os quais a empresa deve atentar no tratamento de dados pessoais de seus colaboradores, especialmente em relação ao ponto eletrônico quando utilizar-se da tecnologia de coleta de biometria por reconhecimento facial.

A fim de construir uma linha lógica de raciocínio, buscar-se-á trazer os principais conceitos de privacidade e proteção de dados. Posteriormente, o foco passará a ser o tratamento dos dados pessoais dos colaboradores no processo de controle de ponto através da tecnologia de reconhecimento facial.

⁴² Especialista em Direito Empresarial pela Faculdade Legale. Advogada. marianaruzzi@hotmail.com

2 Lei Geral de Proteção de Dados

2.1 Trajetória normativa até a publicação da LGPD

Viktor Mayer-Scönberger divide a evolução das normativas sobre proteção de dados pessoais em quatro gerações (DONEDA, 2011). No que tange à primeira geração, o contexto vincula-se a um processamento intenso de dados pessoais voltados para a construção do Estado Moderno e de concentração de bancos de dados governamentais, sendo que os regulamentos voltavam-se mais a questões de tecnologia para introdução de padrões democráticos (MENDES, 2014).

Na segunda geração, a proteção dos dados fica a cargo do próprio titular dos dados pessoais, uma vez que através do consentimento o indivíduo determina suas escolhas em relação ao uso, coleta e compartilhamento dos dados, dando a autonomia para o próprio titular (BIONI, 2018). Neste ponto, é importante esclarecer que a proteção de dados vincula-se diretamente às questões de privacidades e liberdades individuais (MENDES, 2014).

A terceira geração envolve o indivíduo continuamente em todos os processos de tratamento de seus dados, e não somente na coleta, uso e compartilhamento, ampliando, portanto, etapas não previstas na geração anterior (BIONI, 2018). No entanto, a autodeterminação informativa ainda não é alcançada de forma plena nesta geração.

Somente na quarta geração é que a autonomia do titular sobre o tratamento de dados foi realmente ampliada, relativizando o poder de troca que os dados pessoais tinham (DONEDA, 2011). Em suma, esta última geração formaliza normas como a Lei Geral de Proteção de Dados, que garantem ao titular maior controle sobre seus próprios dados pessoais (MENDES, 2014).

2.2 Conceitos importantes

A Lei Geral de Proteção de Dados Pessoais (LGPD - Lei n.º 13.709/2018) foi baseada em diversos aspectos da General Data Protection Regulation (GDPR), normativa do direito europeu que também dispõe sobre privacidade e proteção de dados pessoais. A LGPD institui diversas regras às quais entidades públicas e privadas devem se submeter para tratamento de dados pessoais de pessoas físicas identificadas ou identificáveis para finalidades econômicas (ENJISMAN e LACERDA, 2019).

Evidente, portanto, que é indispensável, em virtude da Lei Geral de Proteção de Dados, a proteção do grande volume de informações que possuem características de dados pessoais (MALDONADO, 2019). Antes, para compreensão deste artigo, é fundamental a noção conceitual de dados pessoais, dados pessoais sensíveis, tratamento de dados pessoais, finalidades e bases legais.

O tratamento de dados pessoais, nos termos do art. 5º, X, da LGPD, é conceituado da seguinte forma:

Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Sendo assim, não restam dúvidas de que o tratamento de dados pessoais tem um conceito extremamente amplo propositalmente, a fim de abarcar tudo o que é realizado com o dado pessoal.

Já dados pessoais, pelo artigo 5º, I, da LGPD, são uma “informação relacionada a pessoa natural identificada ou identificável”. A noção de dado pessoal requer a vinculação da informação a um indivíduo, caso contrário, são tidas como informações abstratas e genéricas e não se enquadram no conceito deste artigo legal.

Por sua vez, dados pessoais sensíveis, nos moldes do art. 5º, II da LGPD, são definidos como:

Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Os dados sensíveis são dados mais íntimos da vida do indivíduo e seu tratamento deve ser realizado de forma rigorosamente cuidadosa, já que um incidente de segurança envolvendo essa categoria de dados pessoais pode trazer consequências mais graves para os direitos e liberdades individuais, como discriminação, por exemplo (LIMA, 2021).

Também é necessário entender o conceito de finalidade previsto no art. 6º, I, da LGPD, que nada mais é do que “a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.”

Por fim, as bases legais são hipóteses previstas na legislação que legitimam o tratamento dos dados pessoais e são taxativas nos artigos 7º e 11º da LGPD, a depender se são dados pessoais ou dados pessoais sensíveis.

Feitas essas considerações iniciais sobre os principais conceitos que serão utilizados neste artigo, passar-se-á a tecer comentários no próximo tópico sobre a sociedade da informação e a relação com os dados pessoais para o desenvolvimento da economia, visando assim entender os motivos pelos quais as empresas optam por sistemas de ponto eletrônico por reconhecimento facial.

3. Sociedade da informação e dados pessoais para o desenvolvimento da economia

Ao longo dos tempos, a economia se desenvolveu a depender de um elemento central que embasou questões estruturais e estabeleceu marcos históricos. Atualmente, a informação é este elemento nuclear que embasa o desenvolvimento da economia e (re)organiza a sociedade, alicerçada na evolução tecnológica (BIONI, 2019).

Em decorrência da virtualização da informação, as informações passaram a ser desmaterializadas em bits, o que possibilitou que todas as informações pudessem ser digitalizadas, inclusive imagens (fotos e vídeos), aumentando de forma considerável a quantidade de informações processadas (BIONI, 2019).

Conforme dispõe Bruno Ricardo Bioni: “A informação em si não é o que ala-

vanca eficiência na atividade empresarial, mas o seu processo-organização a ser transformado em um conhecimento aplicado” (BIONI, 2019, p.11). Por isso, pode-se concluir que na questão relacionada ao setor de Recursos Humanos, os dados pessoais dos colaboradores transformam-se em um fator de suma importância para o funcionamento da empresa, tanto para questões relacionadas para cumprimento de obrigação legal quanto considerando o colaborador como a própria engrenagem do negócio.

Portanto, é importante mencionar que a tutela jurídica dos dados pessoais está baseada no fato de que esses dados e as informações geradas a partir deles refletem a figura do titular de dados, representando uma parcela de um direito já tutelado pelo Código Civil: a personalidade do indivíduo.

4. Ponto eletrônico por meio de biometria e reconhecimento facial

Calcados na ideia de que a tutela dos dados pessoais pode ir além, refletindo também nos direitos da personalidade e da privacidade, inicia-se este tópico para abordar a marcação do ponto eletrônico por meio de biometria e por reconhecimento facial.

O artigo 74 da Consolidação das Leis do Trabalho (CLT) dispõe sobre a obrigatoriedade de registro de ponto nos estabelecimentos com mais de 20 (vinte) trabalhadores:

Art. 74. O horário de trabalho será anotado em registro de empregados.

§ 2º Para os estabelecimentos com mais de 20 (vinte) trabalhadores será obrigatória a anotação da hora de entrada e de saída, em registro manual, mecânico ou eletrônico, conforme instruções expedidas pela Secretaria Especial de Previdência e Trabalho do Ministério da Economia, permitida a pré-assinalação do período de repouso.

Sendo assim, não restam dúvidas de que existem uma finalidade específica e uma base legal, já que o tratamento de dados pessoais do colaborador será realizado para cumprimento de uma obrigação legal.

A Portaria nº 1.510 do Ministério do Trabalho e Emprego entrou em vigência para complementar ao artigo 74 da CLT e dispõe sobre a obrigatoriedade de impressão do comprovante de registro de ponto para que o empregado possa acompanhar, a cada marcação, o controle de sua jornada de trabalho, contendo neste papel alguns dados pessoais do trabalhador como nome, CPF, local de trabalho, PIS, entre outros.

Não é porque existe uma obrigação legal que a empresa pode se descuidar com o tratamento dos dados pessoais.

Frisa-se que, se o colaborador descartar o comprovante com todos esses dados em um lixo da empresa, a empresa será responsável final pelo descarte e, portanto, deve preocupar-se com a trituração do papel para que não ocorra nenhum incidente com os dados pessoais dos colaboradores.

No controle de ponto, a empresa, conforme dispõe a legislação, pode optar pelo registro manual, mecânico ou eletrônico.

Conforme elucida José Augusto Fontoura Costa (2021, p. 89): “As novas tecnologias digitais de informação vêm abrindo campo para sensíveis melhoras, pois possibilitam incrementar a eficiência da realização dos mais diversos processos.”

Não seria diferente nos processos de negócios. As empresas têm cada vez mais optado por automatizar os processos utilizando-se de inteligência artificial. Um dos exemplos é a implementação de registros de ponto eletrônico com coleta de biometria utilizando-se a impressão digital ou ainda através de reconhecimento facial

Com isto, as grandes empresas conseguem tratar uma enorme quantidade de dados de forma bem mais rápida.

Ocorre que, como bem se sabe, tanto a impressão digital quanto o reconhecimento facial são dados pessoais sensíveis no conceito trazido pela Lei Geral de Proteção de Dados, e portanto, o tratamento deve ser precedido de cuidados maiores já que um incidente de segurança envolvendo tais dados pode trazer consequências gravosas aos direitos e liberdade fundamentais dos titulares (LIMA, 2021).

Sendo assim, caso a empresa opte por tratar dados pessoais sensíveis no registro de ponto eletrônico através da coleta de biometria (impressão digital ou reconhecimento facial) ao invés da utilização do crachá, por exemplo, é indispensável que a empresa elabore o Relatório de Impacto à Proteção de Dados (RIPD).

Conforme dispõe Rony Vaizof:

O relatório de impacto à proteção de dados (RIPD) é um instrumento, de responsabilidade do controlador, pelo qual, em qualquer operação que envolva o tratamento de dados pessoais, que possa gerar riscos às liberdades civis e aos direitos fundamentais, será realizada a descrição dos processos para mitigação de riscos, e concomitantemente, de responsabilidades (VAIZOF, 2021, p. 133).

Sendo assim, caso a empresa opte por utilizar a marcação de ponto automática por meio de reconhecimento facial ou por coleta de impressão digital, antes mesmo de iniciar o tratamento, deverá elaborar o relatório de impacto à proteção de dados.

O uso de reconhecimento facial não é proibido pela legislação em vigor, mas a empresa deverá ter cuidados redobrados em virtude do tratamento de dados sensíveis.

5. Os cuidados da empresa na proteção de dados pessoais sensíveis do colaborador

Em um caso hipotético, uma empresa (controladora) com 2.000 (dois mil) colaboradores contrata uma empresa de tecnologia (operadora) que trabalha com prestação de serviço de instalação e gestão de pontos eletrônicos por reconhecimento facial.

O software fará o registro de ponto dos colaboradores através do reconhecimento facial, visando assim a mitigação das fraudes de colaboradores passando o

crachá em nome de outro colaboradores que eventualmente tenham se ausentado da jornada laboral.

Assim como exige a legislação, há a impressão do registro de pontos com os principais dados dos colaboradores.

Ocorre que, nesta situação hipotética, os colaboradores descartam esse comprovante do registro de ponto em um lixo que fica ao lado do relógio e a empresa descarta esse material sem qualquer cuidado.

Além disso, ainda neste caso hipotético, a empresa operadora não possui padrões e tampouco medidas administrativas e tecnológicas aptas a proteger os dados sensíveis da empresa controladora de acessos não autorizados, o que pode causar incidentes com os dados de dois mil colaboradores desta empresa.

Sendo assim, caso ocorra um incidente, o impacto aos direitos e às liberdades fundamentais desses colaboradores será muito mais gravoso, pois ao invés de vazarem dados cadastrais vinculados a um crachá, haverá vazamento de dois mil dados sensíveis.

A LGPD dispõe, em seu art. 46, que:

Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Deste modo, caso o colaborador opte por não armazenar o comprovante de ponto para conferência e descarte nas dependências da empresa, deve-se viabilizar a trituração deste material para que não haja nenhum incidente de segurança devido ao incorreto descarte que possa vir a gerar uma demanda judicial em face da empresa.

No que tange às medidas técnicas e administrativas no âmbito digital, a LGPD não impôs nenhum padrão específico, o que poderá vir a ser regulamentado posteriormente pela ANPD, conforme artigo 46, § 1º da LGPD.

Embora não existam recomendações específicas em termos técnicos e administrativos, é desejável que as empresas que tratam desses dados implantem medidas que garantam a confidencialidade, a integridade e a disponibilidade das informações através de controles de acesso lógico, de acesso a dados, de segregação, de transferência, de anonimização e criptografia, entre outros.

6. Base legal para o tratamento de dados sensíveis

A Lei Geral de Proteção de Dados dedica atenção especial ao tratamento de dados pessoais sensíveis e este poderá ser realizado em oito hipóteses.

Denota-se que os dados pessoais sensíveis têm maior potencial de ferir os direitos humanos básicos (SANDER, 2019).

Conforme dispõe Caio Cesar Carvalho Lima:

[...] o tratamento de dados sensíveis deve ser precedido de cautelas ainda maiores (com atenção aos princípios da lei e direitos dos titulares), uma vez que eventual in-

cidente de segurança com os dados em referência pode trazer consequências mais gravosas aos direitos e às liberdades dos titulares (LIMA, 2021, p. 209).

No mesmo sentido, dispõe Silva e Silva (2013, p.6): “[...] deve haver cautela redobrada quando se trata de dados sensíveis, seja no momento do recolhimento, seja quanto à segurança em seu armazenamento, a fim de garantir que seu uso não se dissocie da finalidade para a qual foi obtida”.

Em virtude desta necessidade de especial proteção que se requer em relação aos dados sensíveis é que a LGPD determina alguns controles maiores, por exemplo, caso haja coleta de consentimento, este deve ser feito de maneira clara e expressa. Deve-se atentar que a LGPD autoriza o tratamento em algumas situações especiais sem a obrigatoriedade da coleta de consentimento, visando garantir o exercício plenos dos direitos fundamentais pelos titulares.

Sobre isso, dispõe Mulholland:

Por isto que a regulação da coleta, uso, tratamento e compartilhamento de dados pela Lei Geral de Proteção de Dados torna-se de suma importância, devendo tais atividades serem realizadas de tal forma a respeitar os princípios previstos na mesma, enfatizando-se, no caso de dados sensíveis, o uso dos mesmos de maneira que atente ao princípio da igualdade e não gere uma discriminação. O princípio da não discriminação deve ser refletido em todas as circunstâncias em que o uso de dados, sejam sensíveis ou não, gere algum tipo de desvalor ou indução a resultados que seriam inequívocos. Esse princípio deve servir como base de sustentação da tutela dos dados sensíveis, especialmente quando estamos diante do exercício democrático e do acesso a direitos sociais, tais como o direito ao trabalho, à saúde e à moradia. (MULHOLLAND, 2018, p. 68).

Postas essas observações, as bases legais que legitimam o tratamento de dados pessoais sensíveis são:

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir de forma específica e destacada, para finalidades específicas;

II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

Cumprimento de obrigação legal ou regulatória pelo controlador;

Tratamento compartilhado de dados necessários à

execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral [...];

Proteção da vida ou da incolumidade física do titular ou de terceiro

Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária, ou;

Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto nos casos de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

Neste ponto, a análise específica que cabe a este artigo é se é possível a utilização da biometria e do reconhecimento facial para registro de ponto de colaboradores, vez que são dados pessoais sensíveis e precisam de uma base legal específica.

Para tanto, primeiramente deve-se verificar qual a necessidade em instituir um processo que coletará dados sensíveis. Desta análise, pode-se extrair que supostamente 60% (sessenta por cento) dos colaboradores têm se ausentado do trabalho e os colegas passam o cartão marcando como se a pessoa que praticou a fraude tivesse ido ao trabalho naquele dia.

Desta forma, denota-se que, no caso hipotético em questão, a empresa realmente necessita implantar um processo que garanta que não há fraude no processo de identificação, o que estava ocorrendo.

Sendo assim, há a possibilidade de aplicação do art. 11, II, alínea “g”, vez que o processo será utilizado para uma finalidade específica, qual seja, de garantir que o colaborador realmente tenha ido trabalhar e que nenhum colaborador está indevidamente marcando o horário de ponto em nome de outrem.

Para fim de se resguardar, caso a empresa opte por adotar essa opção, em face na necessidade da empresa em prevenir a ocorrência de fraude na marcação de ponto de seus colaboradores, recomenda-se que sejam armazenadas evidências, tais como a lista de presenças assinada manualmente por todos do setor daquele indivíduo na data em que o colaborador supostamente estava presente de acordo com a marcação de ponto, mas na realidade não estava.

O importante para verificar se o tratamento está adequado é sempre questionar se o processo ocorreria da mesma forma se fosse realizado de outra maneira, com menos dados e sem a coleta de dados sensíveis.

Para esta análise, recorrer-se-á a alguns dos princípios da Lei Geral de Proteção de Dados, conforme disposto no tópico abaixo.

7. Princípios da Lei Geral de Proteção de Dados

Além da necessidade de adequar o tratamento de dados pessoais em uma finalidade e de acordo com uma base legal, também é indispensável a observância de princípios, que são, segundo Newton de Lucca, normas jurídicas que são determinantes em relação a outras normas subordinadas, que as pressupõem e desenvolvem e especificam preceitos anteriores em direções mais específicas (LUCCA, 2015).

É importante ressaltar que os princípios devem ser cumpridos, independentemente das bases legais elencadas nos artigos 7º e 11º da LGPD para o tratamento de dados pessoais (LIMA, 2021).

Sendo assim, comentar-se-á os incisos do artigo 6º da LGPD para análise, mas sem a pretensão de esgotar o tema, apenas para relacionar ao tema deste artigo.

O inciso I dispõe sobre o princípio da finalidade, que possui grande relevância na prática, pois através dele: “é garantido ao titular, mediante informação prévia, as fronteiras da legalidade do tratamento de seus dados, delimitando os propósitos do tratamento, desde que lícitos, e de terceiros que poderão ou não ter acesso aos dados. Visa mitigar o risco de uso secundário à revelia do titular” (LIMA, 2021, p. 145).

Em resumo, o princípio da finalidade visa garantir que o motivo da coleta esteja de acordo com o objetivo final do tratamento dos dados (DONEDA, 2015).

O inciso II prevê que “o tratamento de dados pessoais somente pode ser realizado quando houver compatibilidade com as finalidades informadas ao titular” (LIMA, 2021, p. 149). Ou seja, está intimamente ligado ao princípio anterior.

Já o inciso III dispõe sobre o princípio da necessidade e ressalta “a limitação do tratamento ao mínimo necessário para se atingir a finalidade pretendida” (LIMA, 2021, p. 151).

O inciso IV viabiliza, através do princípio do livre acesso, que o titular de dados tenha acesso aos seus dados e que possa acompanhar a utilização com o controlador.

O inciso V está em linha com o inciso anterior, pois, para que o titular possa fazer as alterações em seus dados pessoais de forma que sempre estejam condizentes com a realidade, é necessário que ele tenha controle sobre os dados.

Outro princípio muito importante previsto no inciso VI é o da transparência, que visa disponibilizar ao titular de dados informações sobre o agente de tratamento, sobre as características do tratamento de forma simples, clara e acessíveis (LIMA, 2021, p. 157).

O princípio previsto no inciso VII é o da segurança, que requer dos controladores e operadores medidas técnicas e administrativas que garantam a proteção dos dados pessoais.

O inciso VIII trata do princípio da prevenção, que, entre os aspectos, visa “modificar a cultura no tratamento de dados pessoais para que riscos sejam mitigados desde antes do tratamento, evitando-se ao máximo qualquer hipótese, sempre presente, de violação de dados pessoais” (LIMA, 2021, p. 164).

O princípio da não discriminação disposto no inciso IX prevê a “impossibilidade do tratamento de dados para fins discriminatórios, seja de forma automatizada ou não, justamente visando impor limites e permissões no processamento de dados, de modo a mitigar o risco do determinismo tecnológico” (LIMA, 2021, p. 168).

Por fim, o artigo menciona no inciso X o princípio da responsabilização e prestação de contas, que dispõe que não basta o cumprimento da lei pelos agentes de tratamento, mas estes também devem ser capazes de comprovar que as medidas adotadas são eficazes.

Feitas essas considerações iniciais, é fácil identificar os motivos pelos quais **há divergência no entendimento sobre o uso de biometria por impressão digital e por reconhecimento facial**.

O principal princípio que estaria sendo ignorado ao coletar biometria por impressão digital e reconhecimento facial seria o princípio da necessidade disposto no inciso III retro mencionado. Isto porque, conforme dispõe Lima, é necessário analisar antes do início do tratamento a proporcionalidade em relação aos riscos a que os titulares estariam sendo expostos, com base nas espécies de bases tratadas, toda a operação e os resultados que se pretende alcançar com o tratamento (LIMA, 2021).

Ainda segundo Lima, algumas perguntas podem auxiliar na resposta ao enquadramento do princípio da necessidade antes do início do tratamento:

A finalidade pretendida pode ser atingida de outro modo, sem a utilização de dados pessoais? Se a resposta for negativa, quais espécies de dados realmente são essenciais ao tratamento? Finalmente, superadas todas essas questões, mesmo utilizando as espécies de dados essenciais, no menor volume possível, é proporcional a realização desse tratamento diante dos potenciais riscos aos titulares (LIMA, 2021, p. 151).

Sendo assim, não há necessidade em implementar uma tecnologia que visa somente dar agilidade ao processo, quando não há qualquer indicio de fraude neste procedimento na empresa. A utilização de tecnologia que trata dados pessoais sensíveis pode colocar em risco os titulares de dados pessoais e existem inúmeras outras formas de se atingir a finalidade pretendida, como o próprio crachá. Os dados essenciais ao tratamento se resumem às credenciais do colaborador, conforme dispõe a CLT.

Qualquer coleta a mais trata-se de coleta excessiva e vai além da finalidade pretendida, estando em desacordo com o princípio da finalidade.

Considerações finais

A sociedade da informação, com a evolução da tecnologia, tem desenvolvido e modificado diversos processos internos no ambiente empresarial. É cada vez mais comum, por exemplo, a empresa buscar formas de automatizar, tornar mais rápido e eficiente os processos de negócios.

Dessa tendência nasce uma tensão, contraponto, de um lado os benefícios de se automatizar e evitar a fraude na marcação do ponto através da instituição de uma tecnologia por reconhecimento facial, e de outro, os riscos inerentes aos tratamentos dos dados sensíveis.

Sendo assim, deve-se sopesar, por meio dos princípios da necessidade (ou minimização de dados) e dos demais princípios da LGPD, se é realmente indispensável a coleta de dados sensíveis aptos a justificar aquele tratamento, ou se seria possível fazer o registro de uma forma que traga menos riscos para os titulares de dados.

REFERÊNCIAS

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2018

BIONI, Bruno Ricardo. Regulação de dados é uma janela de oportunidade. 2019. Disponível em: <https://dataprivacy.com.br/regulacao-de-dados-e-uma-janela-deoportunidade/>. Acesso em: 25 out. 2021.

BLUM, Rita Peixoto Ferreira. **O direito à privacidade e à proteção de dados do consumidor**. São Paulo: Almedina, 2018.

BRASIL. **Lei Geral de Proteção de Dados Pessoais**. Lei n.º 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 16 out. 2021

BRASIL. **Marco Civil da Internet**. Lei n.º 12.414, de 9 de junho de 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm>. Acesso em: 16 out. 2021

DONEDA, Danilo. O Papel Regulatório da Autoridade Nacional de Proteção de Dados: desafios e perspectivas. *In*: SEMINÁRIO REFLEXOS DA LGPD NAS RELAÇÕES DE TRABALHO em 25/10/2021. Disponível em <https://www.youtube.com/watch?v=x2eoVzpXYBw&t=25032s>.

DONEDA, Danilo. Princípios de Proteção de Dados Pessoais. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto; Lima, Cintia Rosa Pereira de (coord.). *Direito & Internet III: Marco Civil da Internet*. Quartier Latin, 2015. T. I. p.378.

EJNISMAN, Marcela Waksman; LACERDA, Maria Eugenia. O consentimento na Internet na nova Lei Geral de Dados Pessoais. Jota, 2019. Disponível em: <<https://www.jota.info/opiniao-e-analise/colunas/coluna-do-tozzinifreire/lei-geral-de-dados-pessoais-01012019>>. Acesso em: 23 out. 2021.

LIMA, Caio Cesar Carvalho de Lima. Capítulo II – Do tratamento de Dados Pessoais. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord). **LGPD: Lei Geral de Proteção de Dados pessoais comentada**. São Paulo: Thomson Reuters Brasil, 2021.

LUCCA, Newton de. Marco Civil da Internet. Uma visão panorâmica dos principais aspectos relativos às suas disposições preliminares. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira de (coord.). *Direito & Internet III: Marco Civil de Internet*. Quartier Latin, 2015. T. I. p. 39.

MENDES, Thomas. LGPD: Entenda sobre anonimização de dados. Disponível em: <https://w3lcome.com/pt/lgpd-dados-anonimizados/>. Acesso em: 16 out. 2021

MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Revista Direitos e Garantias Fundamentais**, Vitória, v. 19, n. 3, p. 167 set./dez. 2018. Disponível em: <http://sisbib.emnuvens.com.br/direitosegarantias/article/>

view/1603. Acesso em: 22 out.2021.

SANDER, Guilherme. Principais conceitos da LGPD. 2019. Disponível em: <https://sisqualis.com.br/conceitos-lgpd/>. Acesso em: 16 out. 2021

SILVA, Rosane Leal; SILVA, Letícia Brum. **A proteção jurídica de dados pessoais na Internet**: análise comparada do tratamento jurídico do tema na União Europeia e no Brasil. Direito e novas tecnologias. Florianópolis: FUNJAB, 2013. Disponível em: 58 <http://www.publicadireito.com.br/artigos/?cod=e4d-8163c7a068b65>. Acesso em: 24 out. 2021.

VAISOFF, Rony. Capítulo I – Disposições Preliminares. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord). **LGPD: Lei Geral de Proteção de Dados pessoais comentada**. São Paulo: Thomson Reuters Brasil, 2021.

39. O RECONHECIMENTO DA PEJOTIZAÇÃO E OS REFLEXOS NAS RELAÇÕES DE TRABALHO DIANTE DA LGPD

THE RECOGNITION OF PEJOTIZAÇÃO AND THE REFLECTIONS ON LABOR RELATIONS BEFORE THE LGPD

JULIANA BORTONCELLO FERREIRA⁴³

Resumo

A contratação de pessoa jurídica por outra, normalmente denominada como “pejotização”, pode se constituir em fraude quando tal contratação visa burlar a lei, especialmente obreira. Para entender melhor o instituto, neste artigo são feitas ponderações a respeito no primeiro capítulo, seguidas de breves considerações acerca da Lei Geral de Proteção de Dados (LGPD), de nº 13.709/2018, no segundo tópico. Isso porque, reconhecida a fraude da pejotização pela Justiça do Trabalho, faz-se necessária a adoção de providências pelas empresas reclamadas e condenadas, desde a assinatura da Carteira de Trabalho e Previdência do Social do anterior prestador de serviços, e agora empregado, até a observância dos preceitos contidos na lei referida, no tocante à relação de emprego, a fim de resguardar os dados pessoais do titular (trabalhador).

Palavras-chave: Pejotização. LGPD. Relações de Trabalho.

Abstract

The hiring of a legal entity by another, commonly known as “pejotização”, may constitute fraud when such hiring aims to cheat the law, especially for workers. In order to better understand the institute, in this article considerations are made in the first chapter, followed by brief considerations on the General Data Protection Law (LGPD) nº 13.709 / 2018 in the second topic. This is because, once the fraud of “pejotização” is recognized by the Labor Court, it is necessary to take measures by the defendant and convicted companies, from the signing of the Work and Social Security Card of the previous service provider, and now employed, until the observance of the precepts contained in the applicable law, not related to the employment relationship, in order to safeguard the personal data of the holder (employee).

Keywords: Pejotização. LGPD. Work relationships.

1. Introdução

A Lei n.º 13.709/2018, denominada Lei Geral de Proteção de Dados (LGPD), foi publicada no ano de 2018, entretanto a maioria dos seus dispositivos passaram a vigorar apenas em agosto de 2020.

43 Procuradora do Trabalho. Vice-Coordenadora da Coord. Nacional de Combate às Fraudes nas Relações de Trabalho - PRT 4ª Região. Especialista em Direito e Proc. do Trabalho, em Mercado de Trabalho e Formação de Professores para a Educação Superior Jurídica. juliana.bferreira@mpt.mp.br

Por essa razão, tal norma ainda é recente no ordenamento jurídico brasileiro, estando, especialmente as empresas, atualizando-se às determinações lá contidas. O pouco tempo de vigência ainda repercute no cenário nacional, pois há várias dúvidas ainda existentes, dentre elas os reflexos da fraude decorrente de pejetização nas relações de trabalho, em vista da atual existência da LGPD.

No primeiro capítulo, são tecidas breves considerações a respeito do instituto da pejetização, quanto às suas características, dúvidas geradas, especialmente com a entrada em vigor da reforma trabalhista no ano de 2017; ilicitude; consequências negativas aos trabalhadores atingidos pela fraude; bem como os impactos da pejetização na arrecadação da Previdência Social.

Em um segundo momento, é dado enfoque à Lei Geral de Proteção de Dados e sua aplicação às relações de trabalho. Nesse contexto, são abordados os objetivos da norma; reflexões acerca do tratamento dos dados das pessoas naturais, inclusive sobre a necessidade de consentimento dos titulares e, ao final, há um apanhado sobre a inafastabilidade da aplicação da Lei nº 13.709/2018 às relações de trabalho.

O terceiro capítulo, por fim, aborda os reflexos do reconhecimento da pejetização nas relações de trabalho diante da LGPD, eis que quando constatada tal fraude pelo Poder Judiciário, é declarada a existência de vínculo de emprego entre as partes, sendo necessário, de plano, que o empregador passe a adotar as providências de registro da CTPS do trabalhador, além das medidas cautelosas de tratamento dos dados deste, de acordo com a Lei Geral de Proteção de Dados. Como exemplo, está a obtenção do consentimento e a indicação pela empresa de quem será o encarregado pelo tratamento. Outrossim, a Lei prevê a responsabilização do empregador e, inclusive, a possibilidade de sanções a serem aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD).

Com o estudo, visa-se acender a luz para um olhar mais atento aos reflexos da pejetização nas relações de trabalho, e que, diante de eventual reconhecimento pela Justiça Obreira, há diversas consequências às empresas e providências a serem adotadas, na esteira do que está previsto na LGPD, com vistas à proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, nesse caso, dos trabalhadores.

2. Breves considerações a respeito do instituto da pejetização

Com vistas a dar o pontapé inicial neste artigo, faz-se importante enfrentar o tema da pejetização, para que, com a análise preliminar do instituto, possa-se fazer o elo com os capítulos seguintes.

Nesse contexto, pode-se afirmar que a pejetização se trata da contratação de pessoa jurídica, normalmente enquadrada como MEI (Microempreendedor Individual) ou no Simples Nacional (cujo regime tributário é destinado às microempresas ou empresas de pequeno porte), por outra pessoa jurídica. O termo advém da sigla “PJ”, referente à pessoa jurídica.

O instituto tem sido analisado e assim é denominado/vinculado, normalmente, quando da constatação pela Justiça do Trabalho da existência de fraude na relação de emprego.

Isso porque, com o fim de burlar a legislação trabalhista, previdenciária e tri-

butária, com vistas à economia em eventuais custos, empresas contratantes têm se utilizado de pessoas jurídicas, constituídas por um sócio específico ou um ou mais trabalhadores convenientemente escolhidos, para lhe prestarem serviços com a presença dos requisitos da relação de emprego, dentre eles a subordinação.

Ao constatar a fraude, a Justiça do Trabalho determina o registro do contrato de trabalho na CTPS do empregado, bem como o pagamento de diferenças salariais devidas, e ainda o cumprimento de outras providências pertinentes às relações de emprego.

Trata-se de tema ainda pouco explorado pela doutrina, mas já constatado inúmeras vezes pela Justiça Obreira em reclamationárias individuais ou ações coletivas propostas pelo Ministério Público do Trabalho, por exemplo.

Este órgão, inclusive, através de sua Coordenadoria Nacional de Combate às Fraudes nas Relações de Trabalho (CONAFRET) debruçando-se sobre o assunto, sintetizou consistir a pejetização na “[...] contratação de trabalhador subordinado como sócio ou titular de pessoa jurídica, mecanismo voltado a mascarar vínculo empregatício por meio da formalização contratual autônoma, em fraude à relação de emprego” (CONAFRET, 2017, p. 139).

Entretanto, inobstante o caráter fraudulento, a reforma trabalhista que deu ensejo à Lei n.º 13.467/2017 trouxe dúvidas acerca da possibilidade de contratação nos referidos moldes, eis que, em uma leitura açodada da Lei, a partir de tal momento houve quem entendesse pela licitude na conduta, especialmente diante da inclusão do art. 442-B à CLT, bem como da alteração feita pela reforma no art. 4ª-A⁴⁴, da Lei n.º 6.097/74.

Baixada a poeira da entrada em vigor da Lei n.º 13.467/2017, foi possível aferir que não houve modificações significativas quanto ao tema.

Veja-se que o *caput* do art. 4ª-A referido deixa claro que a pessoa jurídica contratada deve possuir capacidade econômica compatível com a execução dos serviços, o que, de plano, já demonstra a incompatibilidade com o trabalho prestado por um trabalhador que constituiu uma empresa e entrega, basicamente, a sua força de trabalho; em que, nessa relação, não se está entregando/transfere a execução de uma dada atividade, mas sim, visando apenas a força de trabalho do efetivo “empregado”, normalmente escolhido especificamente.

Ademais, o art. 4ª-B da Lei n.º 6.097/74 estabelece requisitos que devem ser observados para o funcionamento de uma empresa de prestação de serviços a terceiros, que incluem desde a inscrição no CNPJ, passando pelo registro na Junta Comercial e, por fim, um capital social mínimo, legalmente determinado no

44 Art. 40-A. Considera-se prestação de serviços a terceiros a transferência feita pela contratante da execução de quaisquer de suas atividades, inclusive sua atividade principal, à pessoa jurídica de direito privado prestadora de serviços que possua capacidade econômica compatível com a sua execução. (Redação dada pela Lei n.º 13.467, de 2017).

§ 1º A empresa prestadora de serviços contrata, remunera e dirige o trabalho realizado por seus trabalhadores, ou subcontrata outras empresas para realização desses serviços. (Incluído pela Lei n.º 13.429, de 2017).

§ 2º Não se configura vínculo empregatício entre os trabalhadores, ou sócios das empresas prestadoras de serviços, qualquer que seja o seu ramo, e a empresa contratante. (Incluído pela Lei n.º 13.429, de 2017).

respectivo inciso III, que vai desde R\$ 10.000,00 (dez mil reais) a, ao menos, R\$ 250.000,00 (duzentos e cinquenta mil reais).

Sabe-se que a maioria dos contratos de prestação de serviços tidos como fraudulentos pela Justiça Obreira apresentam, como uma das partes, empresa que possui por trás um sócio ou um trabalhador sem condições financeiras de, realmente, constituir uma pessoa jurídica. Esta é constituída apenas para a realização do contrato específico, sob a égide de todas as características típicas de um vínculo empregatício, com o fim único de fraudar a lei.

A interpretação do §1º do art. 4º-A leva à mesma conclusão. Isso porque, se é a empresa prestadora que contrata, dirige e remunera os trabalhadores, configurando-se os típicos requisitos de uma relação empregatícia, mas havendo subordinação efetiva à contratante, com o controle da atividade por esta, possivelmente restará caracterizada a pejetização.

Ainda, o §2º do art. 4º-A referido, aparentemente, colaboraria ou estimularia a fraude. No entanto, examinando-se o conjunto das normas que foram acrescentadas à Lei que dispõe sobre o trabalho temporário nas empresas urbanas, fica evidente que a pejetização não está enquadrada no que se chama “prestação de serviços”. Isso porque essa modalidade exige a transferência do serviço para a contratada, sendo a autonomia um elemento a ela intrínseco (MINISTÉRIO PÚBLICO DO TRABALHO, 2018, p. 16).

A ilicitude da pejetização e sua proibição pelo ordenamento jurídico brasileiro fica também evidente quando da leitura dos arts. 5º-C e 5º-D, ambos inseridos pela Lei n.º 13.467/2017 à Lei n.º 6.097/74, eis que passaram a prever uma quarentena de 18 (dezoito) meses para contratação pela empresa contratante de ex-empregados a fim de prestarem serviços, assim como de pessoas jurídicas prestadoras que tenham, como titulares ou sócios, pessoas que prestaram serviços à contratante na qualidade de empregado ou trabalhador sem vínculo empregatício.

Da mesma forma que os dispositivos acima, o art. 442-B⁴⁵, inserido na Consolidação das Leis do Trabalho (CLT) pelo art. 1º da Lei n.º 13.467/2017, trouxe dúvidas, inicialmente, acerca da possibilidade legítima de se demitir empregados e recontratá-los por meio de pessoas jurídicas por eles constituídas.

Mas quaisquer dúvidas restam ou restaram sanadas quando da análise sistemática do ordenamento jurídico brasileiro.

Não se pode esquecer, de início, que o próprio art. 3º da CLT permanece vigente e que, se constatados existentes os requisitos de uma relação de emprego, somado à subordinação, haverá forte indício de fraude.

Não bastasse isso, a CLT ou outro diploma normativo não esclarecem, definem o que seriam as “formalidades legais” a que menciona o art. 442-B. E assim, “[...] não obstante o fato de as inovações legislativas mitigarem o risco, apenas a realidade vivenciada entre as partes num caso concreto poderá atestar a inexistência de subordinação entre PJs e a empresa contratante” (SCHIOSER, 2019, p.36).

Feitas essas considerações sobre a impossibilidade de se exigir que trabalhado-

45 Art. 442-B. A contratação do autônomo, cumpridas por este todas as formalidades legais, com ou sem exclusividade, de forma contínua ou não, afasta a qualidade de empregado prevista no art. 3º desta Consolidação. (Incluído pela Lei n.º 13.467, de 2017).

res (antes empregados das empresas tomadoras, ou que mesmo não tendo sido) constituam pessoas jurídicas para a efetivação de prestação de serviços, camuflando-se real relação de emprego, ainda faz-se pertinente abordar os malefícios da pejotização para a sociedade brasileira.

Isso porque há inúmeras consequências negativas aos trabalhadores atingidos, os quais, para verem reconhecidos seus direitos e receberem as verbas devidas, precisam ingressar com uma reclamação trabalhista na Justiça do Trabalho, sujeitando-se a todos os trâmites processuais. Quanto a estes, tendo em vista a constituição de uma pessoa jurídica, ainda precisam arcar com os ônus do correto encerramento da empresa.

Mas aqui, entende-se ainda pertinente trazer à tona o impacto da pejotização na arrecadação da Previdência Social, para que a sociedade possa entender através dos números a necessidade de se coibir e denunciar a prática.

Em estudo publicado, Welle, Arantes, Mello e Rossi (2019, p. 142) esclarecem:

[...] que, se um trabalhador com carteira assinada sai do mercado de trabalho, ele deixa de contribuir, em média, com R\$ 1.600,50 ao ano para o RGPS. Se esta posição não é repostada com outro trabalhador com carteira assinada, o empregador deixa de contribuir, em média, com R\$ 2.671,62 ao ano. Ou seja, diante da saída de um trabalhador representativo ocorre, em média, uma **perda de arrecadação total da Previdência de R\$ 4.272,11 por ano**. Evidentemente, por se tratar de um trabalhador médio, a análise deve levar em consideração que o valor de perda é maior nas categorias com maior renda e menor nas categorias de menor renda. (grifo nosso)

Em complemento, levando-se em conta as contribuições de pessoas jurídicas pelo chamado Simples Nacional ou de um vínculo MEI, através de cálculos, os citados autores informam (2019, p. 142):

Considerando os dados da RAIS para os valores das rendas acima do teto, que migrariam para o Simples, a contribuição média por vínculo de emprego, calculada pela soma das contribuições sobre o faturamento e sobre o pró-labore, foi de R\$ 3.264,56 ao ano. Por sua vez, a contribuição de um vínculo MEI é de 5% do salário mínimo por mês, o que representa R\$ 39,40 considerando o ano de 2015 como referência. Supondo 10 meses de contribuição no ano, este vínculo trará uma **arrecadação de R\$ 394,00 no ano**. (grifo nosso)

Por fim, fazendo-se o arremate, concluem Welle, Arantes, Mello e Rossi (2019, p. 143) que, **para cada trabalhador** que deixa de trabalhar como empregado e

com a regular assinatura da CTPS, passando a constituir uma pessoa jurídica, seja via Simples Nacional ou MEI, **a Previdência Social, em média, deixa de arrecadar R\$ 3.661,71 (três mil e seiscentos e sessenta e um reais e setenta e um centavos) anualmente.**

Com esses números que refletem boa parte dos significativos prejuízos à sociedade brasileira com o cometimento de fraude via pejetização, parte-se para o segundo capítulo deste artigo, que tratará da Lei Geral de Proteção de Dados (LGPD), aplicada aos contratos de trabalho.

Ver-se-á que as noções preliminares sobre pejetização foram fundamentais para se fazer o link quanto à aplicação da LGPD nos referidos contratos, especialmente após o reconhecimento da fraude pela Justiça do Trabalho.

3. A LGPD aplicada aos contratos de trabalho

A Lei Geral de Proteção de Dados (LGPD), de n.º 13.709/2018, traz os preceitos gerais sobre a proteção de dados e o tratamento destes no tocante às pessoas naturais identificadas ou identificáveis. Portanto, não abrange pessoas jurídicas, patentes ou outros documentos que não sejam pertinentes às pessoas naturais, pois quanto àquelas a tutela legal correspondente é dada a partir dos diversos diplomas normativos que se espraiam no ordenamento jurídico, a exemplo da Lei n.º 9.279/1996, acerca da propriedade industrial e da Lei n.º 9.610/1998, que regula os direitos autorais.

Isso não significa que a LGPD não seja aplicada às pessoas jurídicas, pois tanto estas, de direito público ou privado, quanto as pessoas físicas devem observância aos preceitos, conforme redação do seu art. 1^o⁴⁶.

Feitas essas considerações preliminares, outra conclusão a que se chega é a de que, não fazendo a Lei n.º 13.709/2018 distinção quanto ao tipo de relação jurídica tutelada, esta abrange, também as relações de trabalho. Nesse contexto, de acordo com o referido art. 1º, e sendo o objetivo da norma a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, devem os empregadores se adequar à Lei e atentar para o correto tratamento dos dados de seus trabalhadores.

O tratamento, por sua vez, não se refere apenas a condutas apropriadas com os documentos dos empregados durante o contrato de trabalho. Engloba uma série de providências que devem ocorrer desde a fase pré-contratual até o momento pós encerramento do vínculo.

De acordo, por exemplo, com Aguiar (2018, p. 656, *apud* BARZOTTO; CUNHA, 2020, p. 251), a coleta de dados, antes mesmo do início da relação de trabalho, se dá na entrevista do candidato ao emprego, isso porque passam por esse estágio perguntas pessoais e que, por vezes, vão além daquilo a que necessária e obrigatoriamente deveria o empregador ter acesso.

46 Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios (grifo nosso).

Sobre o tratamento, o art. 5º, X da LGPD, dispõe tratar-se de:

[...] toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Assim, depreende-se que o tratamento engloba o manuseio dos dados, de forma física ou digital e, também, a coleta, a transmissão e o próprio arquivamento. Por isso, a importância de se entender com mais cautela o referido dispositivo e as hipóteses em que o tratamento está autorizado.

Com base no art. 7º da Lei Geral de Proteção de Dados, há necessidade de o empregador obter o consentimento do titular, ou seja, do empregado para obtenção dos seus dados (inc. I), que deve ser, no mínimo, livre, informado (ter o titular recebido todas as informações claras e de forma prévia sobre as finalidades do tratamento dos seus dados) e inequívoco.

De outro lado, a hipótese de tratamento para o cumprimento de obrigação legal ou regulatória pelo controlador está permitida (inc. II); assim como para a execução de políticas públicas pela administração pública (inc. III); para a realização de estudos por órgão de pesquisa (inc. IV); quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular (nesse caso o trabalhador), a pedido deste (inc. V); para o exercício regular de direitos em processo judicial, administrativo ou arbitral (inc. VI), em consonância ao art. 5º, XXXV e LV, da Constituição Federal; para proteção da vida ou da incolumidade física do titular (trabalhador) ou de terceiro (inc. VII), pois o direito à vida e à saúde são inafastáveis, consoante regramento constitucional; e para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (inc. VIII).

O art. 7º elenca, outrossim, que o tratamento de dados pessoais poderá ser realizado quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular (nesse caso, do trabalhador) que exijam a proteção dos dados pessoais (inc. IX). Sobre esse tópico, entretanto, prevalecem controvérsias, já que o art. 10, da LGPD, frisa que “o legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas”. Portanto, tal qual defende Borelli *et al.* (2021, p. 198), tal inciso deve ser analisado com cautela, diante da indefinição que existe na legislação, e que deve ser solucionada com o passar do tempo, a partir da aplicação prática da norma.

Finalmente, o inciso X elenca a hipótese de tratamento para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Analisadas, brevemente, as situações em que permitido o tratamento de dados pessoais, inclusive acerca da necessidade de consentimento do trabalhador

no âmbito dos contratos de trabalho, há que se ressaltar que, em vista de a LGPD ainda ser relativamente nova no ordenamento jurídico brasileiro, cabe às empresas investir em treinamentos para se adequarem concretamente aos preceitos legais, bem como buscar os meios necessários para o seu fiel cumprimento nas relações de trabalho.

A Organização Internacional do Trabalho (OIT), inclusive, possui um Repertório de Recomendações Práticas de Proteção de Dados Pessoais do Trabalhador, datado do ano de 1997, e em que, como frisam Barzotto e Cunha (2020, p. 253), “[...] é traçado um guia sobre aquisição, proteção, conservação, utilização, comunicação de dados de empregados e ainda quais os direitos individuais e coletivos envolvidos [...]”.

Como exemplo, sugere o Repertório que a coleta de dados médicos se restrinja às informações que são necessárias para determinar se o trabalhador está apto para determinado posto de trabalho (item 6.7), bem como que, realizado um exame médico, o empregador apenas seja informado das conclusões relevantes para a decisão específica em matéria de emprego (item 10.8).

Portanto, inafastável a aplicação da Lei nº 13.709/2018 às relações de trabalho, não havendo mais que se falar, inclusive, em decisões unilaterais pelos empregadores quanto a documentos exigidos de futuros e atuais empregados, tampouco da manutenção dos seus dados pessoais de forma definitiva, eis que a LGPD trouxe regras claras e limitadoras que envolvem o tratamento de dados nas relações de trabalho, havendo a necessidade, dentre vários outros requisitos, que o empregado emita seu consentimento, permitindo-se a este participar de todo o processo que envolve seus direitos de personalidade.

4. Os reflexos do reconhecimento da pejetização nas relações de trabalho diante da LGPD

Aplicável a LGPD às relações de trabalho, necessariamente se verifica que, reconhecida eventual fraude em decorrência de pejetização, haverá reflexos nos contratos e que deverão ser observados pelas empresas.

Sobre o assunto, ainda pendem estudos mais aprofundados e, inclusive, determinações específicas e expressas pelos juízes e tribunais pátrios, eis que a Lei ainda é recente e a maioria de seus dispositivos somente entrou em vigor em agosto de 2020. De todo o modo, cotejando-se o disposto na Lei n.º 13.709/2018 com as demais normas regedoras das relações de trabalho, principalmente da Constituição Federal de 1988, que prevê direitos e garantias fundamentais, faz-se possível avançar no tema.

Inicialmente, cabe ponderar que, constatada a pejetização pelo Poder Judiciário e assim declarada a existência de vínculo de emprego entre as partes, será necessário, de plano, que o empregador passe a adotar as providências de registro da CTPS do trabalhador, além das medidas cautelosas de tratamento dos dados deste, de acordo com a LGPD.

Isso porque a relação de direito civil que antes havia entre as partes passa a ser de trabalho, fazendo-se necessárias providências específicas, até em razão da disparidade das partes na relação.

Ao fazer a coleta dos dados – que nesse caso não se dará em uma fase pré-contratual, ante ao fato de que a relação de emprego foi declarada pela Justiça -, a empresa precisa obter o consentimento do trabalhador com o fornecimento dos dados (art. 8º da LGPD), o qual deverá ser fornecido por escrito (nesse caso através de cláusula destacada das demais cláusulas contratuais) ou por outro meio que demonstre, inequivocamente, a intenção do trabalhador. O consentimento, como dito em linhas anteriores, precisa ser, no mínimo, livre, informado (ter o titular recebido todas as informações claras e de forma prévia sobre as finalidades do tratamento dos seus dados) e inequívoco.

No caso de reconhecimento de fraude mediante pejetização e que envolva trabalhador menor de idade, ao proceder ao tratamento, as empresas necessitam de um consentimento específico fornecido por, pelo menos, um dos pais ou pelo responsável legal, o qual contenha todas as informações a respeito, na esteira do disposto no art. 14 da LGPD.

Em um olhar ligeiro sobre a matéria, poderia parecer impossível a ocorrência da pejetização envolvendo menores de idade, mas não é o caso, eis que existentes hipóteses de constituição de pessoas jurídicas com o fim de fraudar a lei, em que constam maiores de idade no seu quadro societário, mas que possuem como trabalhadores outras pessoas físicas, inclusive com idades entre 16 e 18 anos. Além disso, a Instrução Normativa nº 81, de 10 de junho de 2020, do Diretor do Departamento Nacional de Registro Empresarial e Integração, prevê a possibilidade de constituição de Eireli por menores de 18 anos, desde que emancipados (item 3.1 do Anexo II, Capítulo II, Seção I), bem como que figurem como sócio com idade inferior a 16 anos, desde que não atuem como administradores (item 3.2, I, do Anexo II, Capítulo II, Seção I, da referida IN), e estejam representados pelos seus responsáveis legais, consoante art. 1.690 do Código Civil.

Sendo assim, a atenção deve ser redobrada quanto a contratos que, porventura, precisem ser registrados com trabalhadores menores de idade.

Seguindo-se, outro reflexo do reconhecimento da pejetização nas relações de trabalho diante da LGPD é a necessária indicação pela empresa de quem será o encarregado pelo tratamento de dados pessoais do trabalhador, cuja identidade e informações de contato devem ser divulgadas publicamente, conforme art. 41 da Lei Geral de Proteção de Dados.

Trata-se do pleno conhecimento a que o titular tem o direito de obter, até porque o encarregado, de acordo com o que dispõe o art. 5º, VIII, da LGPD, é a pessoa indicada que atuará como canal de comunicação entre o controlador dos dados, os titulares destes e a Autoridade Nacional de Proteção de Dados (ANPD).

Nesse contexto, cabe frisar que o acesso aos dados dos titulares compete apenas às pessoas autorizadas, razão pela qual cabe aos empregadores adotar as medidas de segurança necessárias a proteger tais dados. Tal proteção envolve não somente o cuidado com acessos não autorizados, como também eventos inesperados ou atos ilícitos, de alteração, perda e destruição, por exemplo, dos dados dos prestadores, agora empregados, diante de determinação judicial.

O reconhecimento do vínculo de emprego em vista da pejetização gera ainda às empresas, para fins de atendimento à LGPD, uma atenção ao fornecimento dos

dados do “novo” empregado para consultorias contratadas, para empresas responsáveis por planos de saúde fornecidos por estas, assim como de seguros de vida, eis que nesses casos e, também, de filiação a sindicatos, por exemplo, deve haver a expressa autorização do empregado quanto ao compartilhamento de seus dados pessoais.

Isso porque, como ensina Chehab (2012, p. 1077), em razão do direito fundamental à privacidade, o consentimento do empregado para o fornecimento, reprodução, acesso e também circulação de seus dados deve ser a regra, já que, somente a lei, conforme determina o art. 5º, II, da Constituição Federal de 1988, pode, em princípio, excepcionar a regra geral.

Em retrospecto, como bem salientam Dias e Alves (2021), a partir do reconhecimento da pejetização pela Justiça do Trabalho, deve o processo de conformidade regulatória ser revisto, a fim de que haja a readequação dos controles, premissas e autorizações para o tratamento dos dados dos trabalhadores, assim como para que haja o redimensionamento dos riscos ao titular dos dados, em vista da mudança no espectro de responsabilização dos agentes de tratamento.

Quanto à responsabilização, há que se lembrar que, independentemente de condenação às empresas pela Justiça Obreira de assinar a CTPS dos trabalhadores e adotar as medidas daí consequentes, quando constatada a fraude em comento, devem os causadores ressarcir os danos causados aos efetivos empregados, assim reconhecidos em decisão judicial, consoante capítulo VI, seção III, da Lei n.º 13.709/2018.

Ainda, a partir do conhecimento do *decisum* pela Autoridade Nacional de Proteção de Dados (ANPD), o que poderá se dar a partir de envio de ofício pela Justiça do Trabalho, aquela poderá aplicar sanções administrativas às empresas reclamadas e condenadas, nos termos do que definido no capítulo VIII, seção I, da LGPD, eis que, a partir do dia 1º de agosto de 2021, os artigos 52, 53 e 54 da referida norma entraram em vigor.

Posto isso, verifica-se que a prática de fraude mediante pejetização também repercute nas relações de trabalho no que tange à aplicação da Lei Geral de Proteção de Dados, eis que tal norma é aplicada em âmbito geral às relações havidas entre pessoas naturais e jurídicas, o que é o caso aqui analisado.

De outro lado, havendo a constatação de pejetização pela Justiça do Trabalho e as consequências de condenação daí advindas, as empresas estão obrigadas a adotar todas as providências definidas em lei para a proteção dos dados pessoais dos seus trabalhadores.

Considerações finais

A pejetização não se trata de um novo instituto, pois já há tempos é de conhecimento dos aplicadores do Direito, especialmente do Poder Judiciário. Entretanto, com a reforma trabalhista que deu ensejo à Lei n.º 13.467/2017, os estudos acerca do tema passaram a ser revisitados, a fim de que os estudiosos pudessem se debruçar sobre as diferentes interpretações a respeito da possibilidade de contratação nos referidos moldes, eis que, em uma leitura açodada da Lei, a partir de tal momento houve quem entendesse pela licitude na conduta, especialmente diante

da inclusão do art. 442-B à CLT, bem como da alteração feita pela reforma no art. 4^a-A⁴⁷, da Lei n.º 6.097/74.

Dúvidas esclarecidas e mantido o posicionamento pela maioria da doutrina e jurisprudência, foi possível aferir que não houve modificações significativas quanto ao tema, sendo que a ilicitude da pejetização e sua proibição pelo ordenamento jurídico brasileiro ficam também evidentes quando da leitura atenta dos dispositivos da Lei n.º 13.467/2017, em comunhão com a Lei n.º 6.097/74 e com as demais normas do ordenamento jurídico, especialmente a Consolidação das Leis do Trabalho e a Constituição Federal de 1988.

Inobstante a isso, com a chegada ao ordenamento jurídico brasileiro da Lei Geral de Proteção de Dados, passou-se a questionar sobre a sua aplicabilidade nas relações de trabalho, e então, também, sobre eventuais reflexos nos casos de declaração de pejetização pela Justiça Obreira em processos trabalhistas, tendo em vista a necessidade de assinatura da CTPS dos trabalhadores pelas empresas condenadas, bem como outras medidas daí decorrentes.

Sobre o ponto, no segundo capítulo deste artigo, foi possível observar que, realmente, a Lei Geral de Proteção de Dados aplica-se às relações de trabalho, eis que destinada a todas as pessoas naturais e, neste caso em específico, aos trabalhadores. Portanto, necessária a observância da norma pelas empresas quando da condenação por pejetização, a efetivar a contratação direta de trabalhadores que vinham prestando serviços na condição de sócios ou trabalhadores de outras pessoas jurídicas, mas de forma escusa.

E sendo assim, há reflexos decorrentes da contratação mesmo que apenas após a decretação da existência da fraude, eis que, de fato, os trabalhadores já vinham despendendo sua força de trabalho às empresas, com os requisitos de uma relação de emprego. Apenas, deverão ser adotadas todas as providências a partir de então, desde a assinatura das Carteiras de Trabalho e Previdência Social, até outras providências decorrentes dos novos vínculos, e ainda, de todas as medidas cautelosas previstas na LGPD para a proteção dos dados pessoais dos agora empregados.

REFERÊNCIAS

BORELLI, Alessandra *et al.* **LGPD**: Lei Geral de Proteção de Dados Pessoais comentada. MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). 3. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2021.

BARZOTTO, L. C.; CUNHA, L. S. P. Proteção de dados pessoais e consentimento do empregado: jurisprudência trabalhista e a Lei Geral de Proteção de

47 Art. 40-A. Considera-se prestação de serviços a terceiros a transferência feita pela contratante da execução de quaisquer de suas atividades, inclusive sua atividade principal, à pessoa jurídica de direito privado prestadora de serviços que possua capacidade econômica compatível com a sua execução. (Redação dada pela Lei n.º 13.467, de 2017).

§ 1o A empresa prestadora de serviços contrata, remunera e dirige o trabalho realizado por seus trabalhadores, ou subcontrata outras empresas para realização desses serviços. (Incluído pela Lei n.º 13.429, de 2017).

§ 2o Não se configura vínculo empregatício entre os trabalhadores, ou sócios das empresas prestadoras de serviços, qualquer que seja o seu ramo, e a empresa contratante. (Incluído pela Lei n.º 13.429, de 2017).

Dados (LGPD). *In: Inovações e trabalho: o direito do trabalho em tempos de mudança*. DORNELES, L. A. D.; BARZOTTO, L. C. (org.). Porto Alegre: Editora da UFRGS, 2020.

BRASIL. **Lei n.º 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, 15 ago. 2018, republicado parcialmente em 15 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 17 out. 2021.

CHEHAB, Gustavo Carvalho. **A proteção dos dados pessoais e sensíveis do empregado**. São Paulo: Revista LTr, v. 76, nº 09, 2012.

CONAFRET. **Prestação de Serviços a Terceiros e Figuras Associadas: análise face à nova regulamentação**. Brasília: Gráfica Movimento, 2017.

DIAS, B.; ALVES, F. M. **Pejotização e LGPD: terceirização e riscos**. Disponível em: <<http://www.obinoadvogados.com.br/conteudo/pejotizacao-e-lgpd-terceirizacao-e-riscos/>>. Acesso em: 19 out. 2021.

MINISTÉRIO PÚBLICO DO TRABALHO. *Hermenêutica infraconstitucional da Lei n.º 13.467/2017- Reforma Trabalhista*. Brasília: Gráfica Movimento, 2018.

ORGANIZAÇÃO INTERNACIONAL DO TRABALHO. **Práticas de Proteção de Dados Pessoais do Trabalhador da OIT**. Genebra: OIT, 1997. Disponível em: https://www.ilo.org/global/publications/ilo-bookstore/order-online/books/WCMS_PUBL_9221103293_EN/lang--en/index.htm. Acesso em: 18 out. 2021.

SCHIOSER, André Rodrigues. Posso “pejotizar” meus atuais empregados? *In: Perguntas e respostas sobre a lei da reforma trabalhista: obra coletiva por ocasião dos 2 anos da Lei n. 13.467/2017*. CALCINI, R.; MENDONÇA, L. E. A. (coord). São Paulo: LTr, 2019.

WELLE, A.; ARANTES, F.; MELLO G.; ROSSI P. Os impactos da pejotização e da formalização no financiamento da Previdência Social: uma simulação pautada pela reforma trabalhista. *In: Revista Eletrônica do Tribunal Regional do Trabalho do Paraná*. Curitiba: Ano VIII, nº 80, jul. 2019.

40. O USO DE INTELIGÊNCIA ARTIFICIAL NA DESPEDIDA DO TRABALHADOR

ANA PAULA ÁVILA⁴⁸, LUCIANA ARANALDE⁴⁹ E MÁRCIA SANTANA FERNANDES⁵⁰

Resumo

Este trabalho trata da aplicação de Inteligência Artificial para seleção de trabalhadores em processos de despedida em massa. Parte-se do exame de um caso de aplicação da tecnologia por empresa russa para, em seguida, apresentar o contexto e os modelos de Inteligência Artificial. Analisam-se também os principais pontos do debate em torno das decisões automatizadas, passando pela opacidade dos algoritmos e por sua comparação em face das decisões humanas. Como um contrapeso à opacidade possível em ambos os casos, aborda-se a ideia de devido processo algorítmico e suas estratégias para a mitigação dos riscos e vieses das decisões automatizadas, com foco nos direitos à explicação e à revisão por pessoa natural como forma de tornar o processo de demissão em massa um processo mais justo e respeitoso da dignidade do trabalhador.

Abstract

This article analyzes the use of Artificial Intelligence in selecting workers in massive lay-offs. We start by examining a case of use of this technology by a Russian company, and then we present the context and models of Artificial Intelligence. The main points of debate around automated decisions are also analyzed, going through the opacity of algorithms and their comparison with human decisions. As a counterbalance to the possible opacity in both cases, we address the idea of “algorithmic due process” and its strategies for mitigating possible risks and biases of automated decisions, focusing on the rights to an explanation and to a revision by a natural person as means to make the process of mass dismissal fair and more respectful of the worker’s dignity.

1. Introdução

Em 03 de agosto de 2021, ganhou grande repercussão na mídia nacional e in-

48 Mestre e Doutora em Direito pela UFRGS; Mestre em Global Rule of Law pela Universidade de Genova, Itália; Formação em Gestão de Crise pelo MIT, Estados Unidos. Sócia Coordenadora da área de Compliance do Silveiro Advogados.

49 Mestre em Direito pela PUC/RS. Pós-Graduada em Processo Civil (ULBRA). Pós-Graduada em Direito do Trabalho e Processo do Trabalho (UNISC). Pós-Graduada em Resolución de Conflictos (UCLM/Espanha). Mediadora e Instrutora Judicial capacitada pelo CNJ. Negociadora com diversos cursos de atualização e formação, incluindo ICFML - Instituto De Certificação De Mediadores Lusófonos e Cmi Interser - Theory and Tools of The Harvard Negotiation Project.

50 Doutora em Direito pela UFRGS. Pós-Doutora em Medicina pela UFRGS. Professora do Mestrado Profissional em Pesquisa Clínica e Pesquisadora do Laboratório em Pesquisa em Bioética e Ética na Ciência (LAPEBEC) do Hospital de Clínicas de Porto Alegre – HCPA. Professora Colaboradora do PPG/Direito da PUCRS. Advogada Sócia do escritório Santana Fernandes Advocacia e Consultoria.

ternacional a circunstância de uma empresa russa que fornece soluções e pagamentos de outros serviços para a indústria de jogos, a Xsolla, que despediu 150 pessoas com base em uma análise de *big data* quanto à produtividade. A notícia foi veiculada inicialmente pelo site Game World Observer⁵¹, divulgando publicamente o e-mail enviado pelo CEO aos funcionários afetados da sede da empresa em Perm, Rússia. De acordo com as informações desta reportagem, as despedidas foram baseadas na análise da equipe de *big data* da Xsolla sobre os dados concernentes às atividades de cada funcionário nas seguintes plataformas: Gmail, Jira, Confluence, além de vários chats, documentos e dashboards⁵². O conteúdo do e-mail enviado aos trabalhadores apontou que eles estavam “não envolvidos e improdutivos”, ressaltando que a análise de suas atividades evidenciou que nem sempre estavam presentes no local de trabalho, especialmente quando estavam na modalidade de trabalho a distância.

Esta notícia apresenta um sintoma da era digital, que é o uso, pelas empresas, da chamada “people analytics” (análise de pessoas) como meio de avaliar sistematicamente seu capital humano, com o fim de aumentar o valor corporativo. Um grande número de funcionários é afetado pela utilização dessas ferramentas em sua vida profissional e trata-se de uma tendência crescente. A pandemia de covid-19 intensificou, sem precedentes, o trabalho remoto e não surpreende que o empregador deseje monitorar o rendimento dos funcionários em seus escritórios domésticos.

Ulrich Beck, ao cunhar a expressão *Sociedade de Risco* – título da obra publicada em 1986 –, destacou que “a flexibilização espacial” descentralizou o trabalho assalariado com o “trabalho eletrônico em casa”, transferindo aos próprios trabalhadores “os riscos que o trabalho oferece à saúde física e psicológica”, conjugando a isso a precarização e o subemprego, assim como outras formas de controle. Segundo o autor,

(...) progresso e miséria se entrelaçam de novas maneiras. Os ganhos de produtividade das empresas são acompanhados por problemas de controle. Os trabalhadores trocam uma parcela de liberdade em relação ao trabalho por novas compulsões e incertezas materiais.⁵³

Enquanto as empresas enaltecem os benefícios da análise de pessoas, tais como mais transparência e justiça nas decisões de pessoal, melhor desempenho, redução de custos ou aumento da inovação, os riscos do emprego deste tipo de tecnologia muitas vezes permanecem sem solução. Esses riscos podem envolver violações da privacidade e dos dados pessoais dos funcionários, estresse relacionado ao mi-

51 Disponível em <https://gameworldobserver.com/2021/08/04/xsolla-fires-150-employees-using-big-data-and-ai-analysis-ceos-letter-causes-controversy>. Acesso em: 24 out 2021.

52 *Dashboards* são ferramentas de gestão da informação que ajudam no acompanhamento e exibição de indicadores chave de performance (KPIs), métricas e dados que indicam a saúde de um negócio, setor ou processo.

53 BECK, Ulrich. **Sociedade de risco** – rumo a uma modernidade. 2ª edição em tradução em português, traduzida por Sebastião Nascimento. São Paulo: Editora 34, 2011. p. 209. A primeira edição da obra é de 1986.

crogerenciamento e a discriminação baseada em algoritmos. Com a análise de pessoas, os empregadores acumulam dados e conhecimento, ganhando poder sobre seus funcionários em uma extensão sem precedentes. Essa dinâmica, ao que tudo indica, acentua o desequilíbrio de poder na relação jurídica, algo típico das relações de trabalho.

Com sensores e dispositivos cada vez menores, como telefones celulares ou computadores portáteis que podem acompanhar um funcionário 24 horas por dia, os dados podem ser coletados em todos os lugares (de forma onipresente) e ainda os vários sistemas de processamento de dados são interoperáveis, o que permite combinar conjuntos de dados e obter novos *insights* sobre o funcionário que antes não eram visíveis. Por último, uma infraestrutura computacional cada vez mais poderosa é capaz de processar dados em tempo real, antecipar o futuro com análises preditivas e cumprir tarefas não repetitivas graças à crescente inteligência artificial.

A sociedade que reconhecemos como atual, com *pixels*, dados, algoritmos, máquinas inteligentes, relações de trabalho em constantes transformações, teve seu marco inaugural na década de 1950, com a chamada Terceira Revolução Industrial⁵⁴, com consideração ao surgimento do computador pessoal e da Internet.

Luciano Floridi, ao tratar da temática da sociedade da informação como a Quarta Revolução, destaca a importância de refletir, pesquisar e compreender, em sentido amplo, os impactos da Inteligência Artificial na vida dos seres humanos, individual ou coletivamente. É necessário compreender o ambiente da informação e sua transformação, conhecer o que Floridi denominou *Infosfera* (*Infosphere*, neologismo a partir de biosfera), pois a informação está presente no mundo vivo e em tudo que corresponde ao humano.^{55,56} E para compreender a natureza intrínseca da informação e sua transformação, também é necessária uma *reontologia* (*re-ontology*), isto é, uma forma radical de reengenharia; que transforma a natureza intrínseca, sua ontologia, ou seja, o próprio ser.⁵⁷

Na mesma linha, Klaus Schwab⁵⁸ entende que a sociedade da Quarta Revolução Industrial é marcada pelo custo decrescente da computação e de dispositivos conectados, pela facilidade de implementação de algoritmos de Inteligência Artificial e pela queda no preço do sequenciamento genético, citados como fatores determinantes dessa nova fase. Enfim: vive-se em uma sociedade marcada pela presença maciça de Inteligência Artificial (IA) em praticamente todas as áreas: transportes, moradias, compras, marketing, saúde, educação, trabalho, direito.

54 RIFKIN, Jeremy. **Sociedade com Custo Marginal Zero**. São Paulo: M. Books do Brasil, 2016.

55 FLORIDI, Luciano. **The Fourth Revolution: How the infosphere is reshaping human reality**. Oxford: Oxford University, 2014

56 FLORIDI, Luciano. Group privacy: a defence and an interpretation. In: FLORIDI, Luciano TAYLOR, Linné; VAN DER SLOOT, Bart (Eds.). *Group privacy: new challenges of data technologies*. New York: Springer International Publishing, 2017, pp. 83-100; FLORIDI, Luciano. *The ethics of information*. Oxford: Oxford University Press, 2013.

57 FERNANDES, Márcia S. Privacidade, sociedade da informação e Big Data. In: **Direito, Cultura e Método - Leituras da obra de Judith Martins-Costa**. BENETTI, G.; CORREA, A. R.; FERNANDES, M.S.; NITSCHKE, G. C. M.; PARGENDLER, M.; VARELA, L. B (org.). 1ª ed., Rio de Janeiro: GZ Editora, 2019, v.1, p. 182-210.

58 SCHWAB, Klaus. **A quarta revolução industrial**. 2016. World Economic Forum. All rights reserved.

Compreender essa realidade implica uma série de entendimentos, tais como: a) o uso da tecnologia não deve se tornar um substituto para a justiça, sem qualquer tipo de questionamento; b) conceitos como violação da lei precisam ser (re) estruturados frente às possibilidades de aplicação digital, especialmente se considerarmos a necessidade dos empregadores, no exercício do seu poder diretivo de despedir, minimamente fundamentar suas decisões; (c) em princípio, não se poderia admitir que um processo de pontuação algorítmica seja mantido em segredo, dificultando a contestação de seus principais aspectos. Salienta-se que a matéria se torna mais complexa no setor privado, uma vez que sustentado o segredo comercial de determinado software, pode-se lidar com a impunidade graças à opacidade dos sistemas de classificação; d) há a necessidade premente de ser assegurado um direito à explicação e à possibilidade de os trabalhadores contestarem as decisões algorítmicas, pois o direito ao conhecimento de como e por que o algoritmo ponderar diferentes pontos e dados é a base do princípio do devido processo legal e seus desdobramentos: contraditório e ampla defesa.

Uma vez que os dados estão em jogo, a LGPD é indispensável para um tratamento adequado dos riscos incorridos pelo uso de softwares de gestão de análise de pessoas. Assim, em um cenário no qual a frequência de tomadas de decisão está vinculada à operação algorítmica, deve-se investigar a compatibilidade entre a despedida por decisão automatizada com os direitos fundamentais dos empregados, notadamente o princípio do devido processo legal, assim como estratégias que atenuem as críticas quanto à opacidade dos critérios empregados pelos algoritmos. Diante disso, este trabalho ocupa-se desses pontos em três seções: a primeira, apresentando conceitos necessários à compreensão da inteligência artificial; a segunda aborda pontos em que uma maior reflexão é necessária, considerando vantagens e desvantagens na comparação entre decisões automáticas e decisões humanas; e a terceira, em que se apresentam estratégias de harmonização das decisões automatizadas com os direitos individuais das pessoas por elas afetadas. Em síntese conclusiva, demonstramos como esses parâmetros forneceriam os elementos necessários para a construção de um processo de desligamento mais justo e humanizado.

2. Inteligência Artificial: contexto e definições

2.1 Contexto

A definição clássica de Inteligência Artificial foi dada por John McCarthy, Marvin Minsky, Nathaniel Rochester e Claude Shannon, na “Proposta para o Projeto de Investigação de Verão de Dartmouth sobre Inteligência Artificial”. Trata-se de documento fundador que estabeleceu o campo de estudo em IA, em 1955:

Para o presente propósito, o problema da inteligência artificial é fazer com que máquinas se comportem de forma que seriam chamadas de inteligentes se um ser humano se comportasse assim. (Citação da reedição de 2006 em McCarthy et al. 2006)⁵⁹

59 FLORIDI, Luciano. What the Near Future of Artificial Intelligence Could Be. *In*: BURR, Chris-

A Inteligência Artificial (IA) e seus modelos, que serão tratados na sequência, impõem uma avaliação dos riscos e oportunidades associados à sua incorporação na vida e no viver dos seres humanos. O tema incorpora velhas-novas questões, como bem pontuou Ulrick Beck em *A Sociedade de Risco* (1986)⁶⁰, posteriormente desenvolvidas em *Mundo em Risco* (2007)⁶¹, ao debate envolvendo o impacto da tecnologia na vida dos seres humanos, qual seja:

Por trás de todas as reificações⁶², cedo ou tarde emerge a questão da aceitação e, como ela, a velha nova questão: como queremos viver? O que há de humano no ser humano, de natural na natureza, que é preciso proteger? (...) Estas velhas-novas questões - que é o ser humano? como seguir adiante com a natureza? - podem ser jogadas para lá e para cá entre o cotidiano, a política e a ciência. No estágio mais avançado do processo civilizatório, elas voltam a gozar de prioridade na ordem do dia - também ou *justamente* nos momentos em que se revistam com a camuflagem das fórmulas matemáticas e das controvérsias metodológicas.⁶³ (BECK, p. 34, 1986).

Estas velhas-novas questões têm sido cerne das discussões envolvendo IA e a tomada de decisão. Nesta perspectiva, Floridi, Cowls, Beltrametti e outros, em texto publicado em 2018⁶⁴, sustentam que a AI é uma realidade sem retorno e por esta razão é necessário formar reflexões em prol de uma Sociedade de AI para o bem (*Good AI Society*). O artigo identifica as oportunidades e riscos para proteger a dignidade da pessoa humana e prover o seu desenvolvimento e como proposta apresenta 20 recomendações específicas para minimizar riscos e inadequações na utilização de AI. As recomendações devem estar permeadas pelos princípios da beneficência, não maleficência, autonomia e justiça (tradicional da bioética),

topher; MILANO, Silvia (ed). The 2019 Yearbook of the Digital Ethics Lab. Oxford Internet Institute. Springer Nature Switzerland AG 2020

(eBook) <https://doi.org/10.1007/978-3-030-29145-7>

60 BECK, Ulrich. **Sociedade de risco** – rumo a uma modernidade. 2ª ed. São Paulo: Editora 34. 2011.

61 BECK, Ulrich. **World at Risk**. Translated by Ciaran Cronin. Cambridge: Policy Press, 2009. A primeira edição da obra é de 2007.

62 Reificação – termo empregado para designar o fenômeno, ressaltado por Marx, de que, na economia capitalista, o trabalho humano torna-se simples atributo de uma coisa. (Abbagnano, Nicola. Dicionário de Filosofia. São Paulo: Editora Martins Fontes, 200, p. 841.) Houaiss exemplifica: encarar algo abstrato como uma coisa material ou concreta, coisificar, isso é, qualquer processo em que uma realidade social ou subjetiva de natureza dinâmica e criativa passa a apresentar determinadas características de um objeto inorgânico, perdendo sua autonomia e autoconsciência. (HOUAISS, Antônio; VILLAR, Mauro de Salles; MELLO FRANCO, Francisco Manoel de Mello. Dicionário Houaiss da língua portuguesa. Rio de Janeiro: Editora Objetiva, 1ª Edição, 2001, p. 2419)

63 BECK, Ulrich. **Sociedade de risco** – rumo a uma modernidade. 2ª ed. São Paulo: Editora 34. 2011, p. 34.

64 FLORIDI, Luciano; Cowls, Josh; Beltrametti, Monica et. al. AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*, volume 28, pages 689–707 (2018). Disponível em: <https://link.springer.com/article/10.1007/s11023-018-9482-5>. Acessado em: 24 out. 2021.

além do princípio da explicabilidade (*explicability*), e são divididas em quatro pontos centrais para ações: avaliações, desenvolvimento, incentivo e apoio.

As recomendações, igualmente, vêm sendo desenvolvidas por países e organizações, destacando-se a recomendação proposta pela Comissão Europeia, em 2020, no “White Paper – On Artificial Intelligence – An European approach to excellence and trust”, com a finalidade de estabelecer os caminhos políticos para buscar o uso adequado da IA. Neste documento, a Comissão recomenda o estabelecimento de normas e orientações para o investimento na área de AI, visando dois objetivos centrais: promover a adoção da IA e abordar os riscos associados a certas utilizações desta nova tecnologia.⁶⁵ A Comissão também criou um Grupo de Peritos de Alto Nível que publicou Diretrizes sobre IA fidedigna em abril de 2019, compostos de sete requisitos-chave: respeito à dignidade da pessoa humana; sistemas técnicos e de segurança robustos; gestão de privacidade e de dados; transparência; respeito à diversidade; não discriminação e equidade; bem-estar social e ambiental e prestação de contas.⁶⁶

2.2 Modelos de IA

Operações algorítmicas, análise de dados, análise preditiva são aplicações do que conhecemos por Inteligência Artificial (AI), tendo seus primeiros estudos datados de 1950, liderados pelo matemático e criptoanalista Alan Turing. Na busca por desenvolverem soluções artificiais que simulem, e superem, a capacidade humana de raciocínio, ressaltam-se as técnicas como o *machine learning*⁶⁷ (aprendizado de máquina) e o *deep learning*⁶⁸ (aprendizagem profunda), exemplos de “tecnologia que aprende a partir da experiência (dados) para prever o comportamento futuro de indivíduos a fim de gerar melhores decisões.”⁶⁹

Os modelos de Inteligência Artificial, conforme descrição no documento da Organização para a Cooperação e Desenvolvimento Econômico (OCDE)⁷⁰, são:

Um modelo de IA é uma representação computacional de processos, objetos, ideias, pessoas e/ou interações do mundo real que incluem suposições sobre a realidade. As características principais desta dimensão incluem as características do modelo; como o sistema é construído (por exemplo, utilizando conhecimentos especializados, aprendizagem de máquinas ou ambos); e como é utilizado (por exemplo, para que objetivos e

65 Comissão Europeia. White Paper – On Artificial Intelligence – An European approach to excellence and trust. 19 de fevereiro de 2020. Disponível em: https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en. Acesso em: 24 out. 2021.

66 *Op. cit.*

67 *Machine learning* é uma técnica de análise preditiva, por meio da análise de uma grande quantidade de dados. Destaca-se a desnecessidade de reprogramação, cabendo à própria máquina o desenvolvimento de algoritmos para a reprodução de resultados confiáveis e repetitivos. Deste método, pode-se inferir, por exemplo, a análise da repercussão geral de recursos

68 Por exemplo, *Deep Learning* é a tecnologia base para ferramentas como o Google Translate (Google Tradutor) e a Cortana (assistente personalizado da Microsoft).

69 SIEGEL, Eric. 2017, p. 13.

70 OECD Framework for the classification of AI systems – public consultation on preliminary findings.

utilizando que medidas de desempenho).

(...)

Os modelos de IA são representações computacionais de processos, objetos, ideias, pessoas, e/ou interações que ocorrem no contexto (ou no ambiente). Os modelos de IA seguem procedimentos concebidos pelo homem para representar, e interagir com processos do mundo real ou artificial.⁷¹

Conforme informações da OCDE, o sistema de IA utilizado está descrito pelo ambiente socioeconômico, isto é, o contexto em que o sistema de AI será utilizado e implantado (*por exemplo, cuidados de saúde, finanças, indústria*); a sua função comercial; natureza crítica; escala de implantação; partes interessadas afetadas; utilizador(es); impactos nos direitos humanos, e no bem-estar e no seu operador.⁷²

Os modelos de AI podem ainda ser agrupados por suas características⁷³:

1- Modelos simbólicos de IA (ou seja, modelos de IA que utilizam representações geradas pelo homem): a IA simbólica usa representações lógicas para deduzir uma conclusão a partir de um conjunto de restrições. Incluem regras, ontologias e algoritmos de pesquisa e dependem de descrições explícitas de variáveis. Os modelos simbólicos são expressos em linguagens tais como lógica e fórmulas matemáticas.

2- Modelos estatísticos de IA (por exemplo, algoritmos genéticos, redes neuronais e aprendizagem profunda): os modelos estatísticos de IA identificam padrões baseados em dados em vez de conhecimentos especializados. Estes modelos estatísticos eram anteriormente utilizados principalmente para fins de reconhecimento (por exemplo, traduzir a escrita em cheques em código legível por máquina), e mais recentemente são também utilizados para

71 OCDE Framework for the classification of AI systems – public consultation on preliminary findings. 2021. Disponível em: https://aipo-api.buddyweb.fr/app/uploads/2021/06/Report-for-consultation_OECD.AI_Classification.pdf. Este documento tem como finalidade tratar dos diferentes tipos de sistemas de IA que levantam oportunidades e desafios políticos muito diferentes. O Quadro de Classificação dos Sistemas de IA da OCDE ajuda os decisores políticos e outros a classificar os sistemas de IA de acordo com o seu impacto potencial na política pública em áreas abrangidas pelos Princípios de IA da OCDE. A secção I fornece um quadro para avaliar o impacto dos sistemas de IA sobre as políticas. Acesso em: 24 out. 2021.

72 OCDE- Framework for the classification of AI systems – public consultation on preliminary findings. 2021. Disponível em: https://aipo-api.buddyweb.fr/app/uploads/2021/06/Report-for-consultation_OECD.AI_Classification.pdf. Acesso em: 24 out. 2021.

73 OCDE- Framework for the classification of ai systems – public consultation on preliminary findings. 2021. p.25. Disponível em: https://aipo-api.buddyweb.fr/app/uploads/2021/06/Report-for-consultation_OECD.AI_Classification.pdf Traduzido com a utilização do sistema DeepL Tradutor, que aliás o faz com a ajuda de AI. Acesso em 24 out. 2021.

tarefas como a geração (por exemplo, sistemas que podem sintetizar e gerar imagens, ou áudio). Os modelos que dependem de dados são concebidos para serem capazes de extrair e representar eficazmente o conhecimento de dados, em vez de conterem conhecimento explícito.

3- Modelos híbridos de IA: Várias aplicações combinam modelos de IA simbólicos e estatísticos, ou seja, são modelos “híbridos”. Por exemplo, os algoritmos de processamento de linguagem natural combinam frequentemente abordagens estatísticas baseadas em grandes quantidades de dados e abordagens simbólicas que consideram questões como as regras gramaticais.

Percebe-se nesses modelos enorme variedade de aplicações, apresentando múltiplos desafios éticos, legais e sociais. Os sistemas de IA envolvidos com processos de percepção foram incorporados com as novas tecnologias de imagem e tratamento de sinais. Da mesma forma, os sistemas de IA na área de comunicação têm permitido realizar interações antes inexistentes e facilitar o acesso a dados e informações. A maior preocupação envolve as áreas de planejamento, conhecimento e raciocínio, pois os sistemas de IA se associam diretamente ao processo de tomada de decisão.⁷⁴

O *White Paper* editado pela Comissão Europeia relaciona, ainda, as características específicas de muitas tecnologias de IA, incluindo a opacidade, o “efeito caixa preta” (*effect back box*), a complexidade, a imprevisibilidade e o comportamento parcialmente autônomo como desafios que podem dificultar o cumprimento e efetividade das normas destinadas a proteger os direitos fundamentais. Por isso, os responsáveis pela aplicação da IA e as pessoas afetadas podem não dispor dos meios para verificar os critérios algorítmicos empregados na tomada de decisão e, por conseguinte, se esses critérios consideraram os direitos fundamentais e de personalidade dos envolvidos.⁷⁵

Quanto às questões relacionadas à *regulação das decisões algorítmicas*, envolvidas na IA, recomenda-se que sejam demonstrados os aspectos conceituais centrais, os possíveis impactos e vieses, os impactos éticos e jurídicos, envolvidos em decisões que têm como substrato os algoritmos. Os indivíduos e as pessoas jurídicas devem ser informados dos critérios e formas de organização e composição dos algoritmos para que o acesso à justiça, em situações em que tais decisões os possam afetar negativamente, não seja restrito.⁷⁶

74 FERNANDES, Márcia S. e GOLDIM, José Roberto. Inteligência Artificial e Processo de Tomada de Decisão em Saúde: riscos e oportunidades, capítulo em desenvolvimento para publicação internacional, em 2022.

75 Comissão Europeia. *White Paper – On Artificial Intelligence – A European approach to excellence and trust*. 19 de fevereiro de 2020. Disponível em https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en. Acesso em 24 out. 2021.

76 Comissão Europeia. *White Paper – On Artificial Intelligence – An European approach to excellence and trust*. 19 de fevereiro de 2020. Disponível em https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en. Acesso em 24 out. 2021.

A utilização de algoritmos, como afirma Luciano Floridi, não é uma má notícia para os seres humanos, pois eles podem ser agregados no desenvolvimento de projetos e processos em seu benefício. Entretanto, precisamos de sistemas de controle, transparência e responsabilidade que sejam supervisionados por seres humanos - *há muito trabalho inteligente para o ser humano fazer no futuro*.⁷⁷ A arquitetura desses sistemas será crucial para harmonizar a tecnologia com os direitos humanos e passará, necessariamente, por pontos relevantes de reflexão relacionados ao modo de superação da opacidade das decisões algorítmicas e às garantias ao indivíduos que tenham suas liberdades e escolhas de vida desproporcionalmente prejudicadas por tais decisões.

3. Pontos necessários de reflexão

O uso de algoritmos justifica-se em razões de eficiência e economicidade e é uma das respostas oferecidas pela tecnologia aos desafios inerentes à massificação social, já que decisões individualizadas para cada decisão demandam tempo e recursos humanos e financeiros. Em questão de eficiência, deve-se ponderar o atributo “capacidade”, pois, por um lado, a inteligência artificial é capaz de detectar padrões e oferecer análises preditivas que escapam à capacidade humana. Por outro lado, as decisões algorítmicas enfrentarão limites quando se exigem respostas para questões éticas, pois não há evidências de que as máquinas possam resolver questões morais e políticas que envolvam a definição de prioridades e distribuição. A par disso, em algumas áreas vemos tecnologias avançadas lutando para desempenhar atividades que “para os humanos são absolutamente triviais”⁷⁸, como a fala, a escrita e o reconhecimento de objetos.

O modelo de análise por AI para obter eficiência na predição de eventos futuros nada mais é do que a aplicação de um modelo estatístico, em que se busca o reconhecimento de padrões, somado ao possível aprendizado da máquina. Como modelo estatístico, padece da incompletude comum às estatísticas, podendo direcionar decisões inverossímeis com a realidade concreta em que vive o indivíduo. Assim, um desafio a enfrentar será esta inaptidão para a identificação de situações individuais particulares que se distinguem dos padrões usuais e levem a decisões inadequadas ou injustas.

Outra questão frequentemente debatida acerca do uso de algoritmos diz respeito à sua opacidade, à medida que os critérios empregados nas decisões algorítmicas não são visíveis e a justificativa dessas decisões é complexa e operacionalmente imprevisível⁷⁹, já que os algoritmos são comumente associados ao “machine learning” e se desenvolvem de modo autônomo, ou seja: a tecnologia evolui com autonomia a partir do programa inicialmente ajustado pelo programador. As decisões algorítmicas são consideradas mais opacas e por isso mais difíceis de explicar que as decisões humanas, porque a aprendizagem da máquina “envolve processos

77 Floridi, Luciano. The rise of the algorithm need not be bad news for humans. Financial Times Ltda, May 4th, 2017. Disponível em <https://www.ft.com/content/ac9e10ce-30b2-11e7-9555-23ef563ec-f9a?mhq5j=e2>. Acesso em 24 out. 2021.

78 Huq, Aziz Z. *A Right to a Human Decision*, 106 Va. L. Rev. 611-688 (2020), p. 640.

79 Huq, *op. cit.*, p. 638.

que não são explicáveis em linguagem humana”⁸⁰.

Em extenso trabalho em que compara as decisões automatizadas com as decisões humanas, Aziz Huq oferece alguns argumentos que nem sempre são lembrados. Ele reconhece que a questão da opacidade tem sido particularmente debatida, mas questiona se a maior impenetrabilidade das decisões algorítmicas em relação às decisões por pessoas tem de fato fundamento, argumentando que as decisões humanas são permeadas por distorções heurísticas (erros de percepção, avaliação e julgamento), vieses, preconceitos e ruídos. De modo semelhante, a aprendizagem da máquina também é vulnerável a dados poluídos e requer escolhas normativas na elaboração de regras classificatórias que, se malversadas, podem resultar em instrumentos de predição que podem apresentar vieses discriminatórios e exacerbar a exclusão de certos grupos sociais. No entanto, a construção dessas regras dentro de padrões adequados pode resultar em predições com um grau de acurácia inatingível pelas pessoas⁸¹.

De fato, as decisões humanas são também permeadas por fatores inconclusivos e refratários a uma justificativa sempre racional⁸². Nas palavras de Anupam Chander, pesquisador da Universidade da Califórnia, “the ultimate black box is the human mind”, e os preconceitos que atuam dentro desta caixa preta nem sempre são escritos ou revelados⁸³. Ele não acredita que programadores manipulem os algoritmos, deliberadamente, para exacerbar a discriminação social, especialmente porque a programação exige um processo consciente e plenamente registrado do que é feito na composição das regras; soma-se a isso o fato de que a discriminação, em geral, é estrutural e inconsciente, sendo muito mais provável que habite na mente dos responsáveis pela tomada de decisões do que nos algoritmos que os substituem⁸⁴.

80 Zarsky, Tal Z. *Transparent Predictions*. University of Illinois Law Review (p.1503 et. seq.), 2013, p. 1568.

81 *Id.*, *ibid.*

82 Nessa linha argumentativa, Aziz Huq sustenta que “a mente dos outros é tão obscura quanto as ferramentas de aprendizagem da máquina. Há evidências científicas de que nós tomamos decisões que nem mesmo nós compreendemos inteiramente e dificilmente conseguimos explicar os motivos racionais pelos quais chegamos a uma conclusão. Entender a mente do outro e seus processos cognitivos pode ser um mistério e, claro, alguém pode até revelar justificativas para uma decisão, mas problemas de sinceridade são abundantes neste tema [...]”. *Op. cit.*, p. 644. (tradução nossa)

83 “A maior caixa-preta é a mente humana”. CHANDER, Anupam. *The Racist Algorithm? In: 115 Mich. L. Rev. 1023-1045 (2017)*, p. 1030. A frase é um contraponto à obra de Frank Pasquale, que apresentou a metáfora da “black box society” (sociedade da caixa preta) para ilustrar a falta de transparência dos algoritmos empregados em decisões automatizadas que definem a vida do cidadão com frequência cada vez maior (Pasquale, Frank. *The Black Box Society: The secret algorithms that control money and information*; London, HUP, 2015).

84 E segue desenvolvendo seu raciocínio: “A discriminação inconsciente tem muito menos probabilidade de se manifestar por meio do processo de programação do que por meio do processo de tomada de decisão. A programação requer um processo de escrita passo a passo que depende de uma compreensão consciente do que se busca. Não apenas o programador deve instruir o computador com grande precisão, mas as práticas de programação modernas também exigem que o programador documente (ou anote) o que o programa está fazendo. Por causa de um processo de programação que requer tanto a escrita de instruções explícitas quanto a documentação do que o código específico faz, a discriminação inconsciente ou subconsciente tem menos probabilidade de se manifestar na

Contudo, parece não haver dúvidas de que o preconceito da máquina é inerente ao criador do código e ou dos usuários que a alimentam. Tomemos por exemplo a ascensão do robô racista da Microsoft, Tay, que, após um dia na rede social Twitter, aprendeu com seus usuários e passou a escrever mensagens antissemitas. Portanto, quando alimentamos as máquinas com dados baseados em nossos próprios preconceitos, até que ponto podemos confiar em decisões algorítmicas?⁸⁵ Essa desconfiança não tem o poder de frear o inevitável avanço tecnológico, mas no mínimo exigirá que o emprego dessas tecnologias seja acompanhado de garantias às pessoas afetadas.

Em razão disso, na visão de Huq, ignorar os benefícios que as decisões algorítmicas podem trazer à sociedade é um erro tão grande quanto ignorar os riscos envolvidos no design e programação das ferramentas preditivas, e na equação entre esses dois equívocos surge a necessidade de responder se as falhas no algoritmo não são mais fáceis de identificar e remediar do que as falhas nas decisões tomadas por pessoas. Se não houver razão para acreditarmos que os erros das máquinas são irremediáveis e os humanos não são, não haveria razão para a preferência pelas decisões humanas.⁸⁶ Dito de outro modo, se existe a possibilidade de sindicância das decisões algorítmicas, “não parece correto dizer *a priori* que as máquinas são mais opacas que as pessoas”⁸⁷.

Se essas razões pendem em favor das decisões algorítmicas, cabe lembrar que a decisão automatizada para a despedida dos empregados implica na perda do emprego do trabalhador, do seu direito ao trabalho e de sua fonte de sustento; sendo assim, como em todas as decisões que atingem direitos, é necessário pensarmos em salvaguardas que possam ser oferecidas aos indivíduos afetados para que possam se proteger contra situações arbitrárias.

4. Garantias aos indivíduos afetados

4.1 Transparência Algorítmica

No debate sobre o devido processo algorítmico, um ponto que sobressai é o da transparência algorítmica, i.e., o direito ao conhecimento dos critérios empregados nas decisões automatizadas - algo nem sempre fácil de estabelecer. Primeiro, porque um direito à transparência deve ser compatibilizado com os direitos de propriedade intelectual do criador do processo automatizado. Não por outra razão, a Lei n.º 13.709/2018 – LGPD – estabeleceu que o princípio da transparência deverá observar os segredos comercial e industrial (art. 6º, inc. VI; art. 20, §1º;

programação de computador do que na tomada de decisão humana”. CHANDER, *op. cit.*, p. 1028-9 (tradução nossa). A questão é amplamente debatida, havendo, além do famoso caso de discriminação racial pelo sistema COMPAS, do precedente *State vs. Loomis* julgado no Estado de Wisconsin - EUA, outros casos já evidenciados de discriminação algorítmica. HAMILTON, Melissa. The Biased Algorithm: evidence of disparate impact on Hispanics. *In: American Criminal Law Review* n. 56, v. 4, pp. 1553-1578 (2019).

85 BURANYI, Stephen. Rise of the racist robots – how AI is learning all our worst impulses. *In: The Guardian*. Disponível em: <https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses>. Acesso em: 24 out 2021.

86 Huq, *op. cit.*, p. 639-640.

87 Casey, Anthony J.; Niblett, Anthony. A Framework for the New Personalization of Law. *University of Chicago Law Review* n. 86 (2019), p.355-56, p. 333.

entre outras disposições), ligado ao princípio da boa-fé objetiva, assegurando que a composição sequencial do algoritmo não seja revelada.⁸⁸

Uma grande dificuldade está em que a compreensão da dinâmica do algoritmo é complexa. O processo de decisão automatizada nem sempre se funda num código lógico explícito, resultando mais da função dinâmica de uma “rede neural” do que de uma sequência de cálculos. Na lição de Huq, “de uma perspectiva *ex post*, há a sensação de que os algoritmos podem não ser transparentes porque é impossível reconstruir os fundamentos com base nos quais a decisão foi construída”⁸⁹.

Sabe-se, contudo, que a criação do código sequencial é passível de registro, por isso, *ex ante*, é possível assegurar um registro inviolável da sequência das ações desempenhadas pelo algoritmo, de modo que ações falhas possam ser detectadas. Diante disso, a construção de estratégias para o devido processo algorítmico em contextos de avaliação do indivíduo passa por estabelecer avisos que as pessoas afetadas devam receber quando os sistemas tomem decisões desfavoráveis sobre elas. Para Pasquale e Citron, de acordo com a cláusula do devido processo, tais avisos devem ser “razoavelmente calculados” para informar os indivíduos dos critérios empregados contra eles. A suficiência do aviso depende de sua capacidade de informar os indivíduos afetados sobre as questões a serem decididas, as evidências que apoiam a decisão e o processo de decisão do órgão. Um aviso claro diminui a probabilidade de que as decisões do órgão se baseiem em “premissas factuais incorretas ou enganosas ou na aplicação incorreta de regras”.⁹⁰ Por isso, concordam que o devido processo tecnológico exige que os sistemas automatizados incluam “trilhas de auditoria imutáveis”, de modo a garantir que os indivíduos recebam avisos sobre os fundamentos das decisões que lhes sejam contrárias.⁹¹

Na conclusão de Huq cabe, portanto, ao programador do sistema estabelecer uma “arquitetura” que permita o fornecimento de explicações *post hoc* a respeito dos resultados obtidos. Deste modo, “a falta da capacidade de gerar explicações que permitam a avaliação dos efeitos das decisões algorítmicas no mundo real é meramente uma questão de escolha no design do sistema, e não uma inevitabilidade decorrente da complexidade de grandes sistemas”⁹². Ao lado desta arquitetura, pode-se pensar também no direito à revisão da decisão por pessoa natural como um contrapeso às decisões automatizadas, conforme veremos em seguida.

4.2 Direito à revisão por pessoa natural

O Regulamento da União Europeia, em vigor desde 25 de maio de 2018, em seu art. 22⁹³, dispõe que o tratamento automatizado de dados deve ser sempre excepcional, sendo admitido tão somente nas exceções legalmente autorizadas, ressaltando sempre o direito à revisão humana. O ordenamento jurídico norte-americano ainda não apresenta regulamentação federal sobre a matéria, especial-

88 Para estudos aprofundados sobre o princípio da boa-fé objetiva, ver: MARTINS-COSTA, Judith. *A Boa-Fé no Direito Privado* – critérios para sua aplicação. São Paulo: Marcial Pons, 2015.

89 Huq, *op. cit.*, p. 641.

90 Citron, Danielle Keats; Pasquale, Frank. *The Scored Society: Due Process for Automated Predictions*. *Washington Law Review* 89, no. 1, 2014 (p.1-34), p.27.

91 *Idem*, p. 28.

92 Huq, *op. cit.*, p. 642-3.

93 General Data Protection Regulation (Regulamentação Geral de Proteção de Dados - RGPD)

mente sobre responsabilidade e transparência algorítmica⁹⁴.

A literatura jurídica norte-americana, de uma perspectiva europeia, tentou resolver os problemas de governança algorítmica sem reconhecer um “direito a uma explicação” fundamentada em proteção de dados. O trabalho pioneiro de Crawford e Schultz, com base nos trabalhos de Citron, propõe uma série de adaptações à bem conhecida cláusula do “*due process*” (devido processo), que podem incluir: a) educação extra sobre os preconceitos e falácias da automação para órgãos governamentais que se utilizam de sistemas automatizados; b) agências para contratar “auditores” para explicar em detalhes sua dependência dos resultados de tais sistemas para tomar decisões administrativas, incluindo quaisquer “fatos gerados por computador ou constatações legais”; c) agências devem ser obrigadas a testar regularmente os sistemas em busca de erros e outros erros; d) trilhas de auditoria a serem emitidas pelos sistemas e aviso aos sujeitos de que foram usadas para tomar decisões, de modo que a revisão judicial seja possível.⁹⁵

A tensão gerada pela crescente substituição das decisões humanas por decisões automatizadas ficou evidente no art. 22(1) do GDPR (Regulamento Geral de Proteção dos Dados), o qual estabeleceu o direito de o indivíduo não ser submetido a decisões baseadas em processos exclusivamente automáticos de decisão, inclusive a perfilamento que possa produzir efeitos jurídicos sobre ele. O art. 22(3) também estabelece o direito à que o controlador de dados pessoais disponibilize a intervenção humana como uma garantia de proteção aos direitos, liberdades e interesses legítimos dos titulares, a fim de que tenham suas razões e pontos de vista considerados⁹⁶.

94 A discussão sobre opacidade ganhou importante relevância no caso em que um acusado, em processo criminal, não obteve acesso ao código fonte que fixou sua condenação. No caso *State v. Loomis*, a Suprema Corte de Wisconsin sustentou que o uso de uma ferramenta proprietária de avaliação de risco chamada COMPAS não violava o princípio do devido processo legal. A partir daí, surgiram algumas regulamentações em âmbito estadual.

95 Tradução livre. *In*: Lilian Edwards and Michael Veale, *Slave to the Algorithm? Why a ‘Right to an Explanation’ is Probably Not the Remedy You are Looking For*, 16 *Duke L. & Tech. Rev.* 18 (2017), available at SSRN.

96 Article 22 - Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests; or

(c) is based on the data subject’s explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests are in place.

Em que pese a circunscrição territorial da GDPR limitada à União Europeia, seu impacto em outros Estados soberanos é inegável, tanto pela manutenção das relações comerciais com os países da comunidade europeia – exigindo a conformidade às normas de proteção da privacidade de todos os parceiros comerciais –, quanto pela enorme influência que esse diploma exerceu nas legislações adotadas para a proteção dos dados fora do continente europeu.

No Brasil não foi diferente, e a redação do projeto original da LGPD estabelecia que uma *decisão automatizada* deveria ser revisada por uma pessoa física, quando solicitado pelo titular dos dados. No entanto, uma medida provisória, a MP 869/2018, manteve o direito à revisão de decisões automatizadas, todavia, suprimiu a previsão de que essa revisão fosse feita por pessoa natural. O Projeto de Lei de Conversão 7/19 da MP 869/2018 tentou reverter, por meio de seu art. 2º, essa alteração ao sugerir ao §º3 do art. 20 a seguinte redação: “A revisão de que trata esse *caput* deverá ser realizada por pessoa natural, conforme previsto em regulamentação da autoridade nacional, que levará em consideração a natureza e o porte da entidade ou o volume de operações de tratamento de dados”. No entanto, o dispositivo foi vetado pelo Presidente da República, e posteriormente o veto foi mantido pelo Congresso pela diferença de apenas um voto. O veto foi motivado com a seguinte justificativa:

A propositura legislativa, ao dispor que toda e qualquer decisão baseada unicamente no tratamento automatizado seja suscetível de revisão humana, contraria o interesse público, tendo em vista que tal exigência inviabilizará os modelos atuais de planos de negócios de muitas empresas, notadamente das startups, bem como impacta na análise de risco de crédito e de novos modelos de negócios de instituições financeiras, gerando efeito negativo na oferta de crédito aos consumidores, tanto no que diz respeito à qualidade das garantias, ao volume de crédito contratado e à composição de preços, com reflexos, ainda, nos índices de inflação e na condução da política monetária.

Diante disso, ao contrário do Regulamento Geral de Proteção de Dados (RGPD), que é explícito quanto à obrigatoriedade de intervenção humana na revisão de decisões automatizadas, hoje a legislação brasileira não prevê a revisão de todas as decisões automatizadas por pessoa natural, mas também não proíbe que essa revisão ocorra em determinadas situações. É importante levar em consideração que a motivação do veto foi pela desnecessidade de revisão por pessoa natural “de toda e qualquer decisão automatizada”, o que não impede que a Autoridade Nacional de Proteção de Dados (ANPD) regulamente a possibilidade de revisão humana em determinadas situações em que tal intervenção se faça necessária para evitar violações desproporcionais a direitos e liberdades fundamentais. Em nosso juízo, manter a possibilidade de revisão por pessoa natural em casos de restrições a direitos fundamentais originadas em processos de decisão automática é uma

exigência ligada ao direito fundamental do devido processo [algorítmico] previsto na Constituição Federal de 1988.

O sistema jurídico brasileiro adota o princípio do devido processo. A Constituição Federal de 1988 manifesta de forma explícita, no artigo 5º, no rol dos Direitos e Garantias Fundamentais, em seu inciso LIV, que “ninguém será privado da liberdade ou de seus bens sem o devido processo legal” (grifo nosso). A liberdade é apresentada, em forma singular, no *caput* do artigo 5º, pluralizando-se em diversas formas de escolhas, tais como a liberdade de pensamento, liberdade religiosa, liberdade de expressão etc. Não incorreria em erro a afirmação de que essas escolhas e liberdades podem ser colocadas em risco em um cenário onde máquinas preveem determinados comportamentos humanos, onde a análise preditiva de dados em massa pode acabar por expor intimidades, desejos e pensamentos sem o conhecimento ou autorização do titular desses dados, terminando por excluí-lo de oportunidades necessárias ao pleno desenvolvimento de sua personalidade. Uma contrapartida mínima seria a concessão da possibilidade de contestação das decisões automáticas tomadas com base nesses dados mediante o exercício do direito à revisão humana.

Considerações finais

Devido processo, somado à segurança jurídica, são direitos humanos que requerem previsibilidade. Na era do *Big Data*, essa necessidade de previsibilidade quanto à consequência das nossas ações, por ser algo fundamental e indispensável ao exercício consciente das nossas escolhas, traz consequências ao processo de inovação tecnológica e de uso da inteligência artificial.

No caso das decisões automatizadas, calculadas a partir de algoritmos capazes de coletar, processar e analisar uma quantidade enorme de informações a respeito de um indivíduo, para fornecer como resultado uma decisão em que oportunidades lhe são concedidas ou negadas e afetam suas escolhas de vida, parece razoável conceder-lhe salvaguardas que lhe permitam o direito de defesa contra situações iníquas.

Se as vantagens na adoção de processos automatizados de decisão se impõem por razões de eficiência e acurácia, também é certo que os algoritmos, ao carregarem vieses imputados pelos programadores e se desenvolverem com certa autonomia, poderão apresentar falhas que levem à discriminação e exclusão de grupos, causando prejuízos desproporcionais aos seus direitos e liberdades. Fatos noticiosos multiplicam-se para apontar iniquidades nas decisões por algoritmos.

Conforme vimos, tanto as decisões humanas quanto as algorítmicas estão sujeitas a falhas e vieses. No caso das decisões humanas, o sistema conta com mitigadores desses riscos: decisões legislativas que são tomadas por uma pluralidade de indivíduos devem ser democraticamente debatidas e passar por um processo transparente de formação de consenso para que possam passar a condicionar a vida do indivíduo; às decisões judiciais impõe-se o dever de fundamentação, pois são coercitivas e condicionam a vida dos sujeitos por elas afetados. No caso das decisões automatizadas, parece razoável que o risco do viés discriminatório também seja minimizado pelo fornecimento de explicações “post hoc”, que permita a identificação de eventuais falhas. Isso faz parte das estratégias para se reconhecer

o devido processo algorítmico nos contextos de avaliação do indivíduo, para que, em nome da previsibilidade e da correção, sejam estabelecidas explicações às pessoas afetadas quando os sistemas tomem decisões desproporcionalmente desfavoráveis sobre elas.

Essas informações devem ser “razoavelmente calculadas” para tornar visíveis aos indivíduos os critérios empregados contra eles e as evidências que apoiaram o processo de decisão. Com isso, seria recomendável que nos processos de despedida em massa baseados em decisões algorítmicas fossem indicados os critérios utilizados na seletividade dos trabalhadores, permitindo-lhes aferir em que medida de fato se enquadram nos critérios selecionados.

Frente a sinalizações de possíveis ocorrências de tratamento legalmente inadequado, ferindo direitos básicos, como os direitos à liberdade e à isonomia, faz-se necessário e urgente desenvolver os principais fundamentos de um devido processo de decisão algorítmica, dando a conhecer como e por que o algoritmo pondera diferentes dados, e permitindo-se a revisão por pessoa natural nos casos em que as inadequações puderem ser demonstradas. Se os critérios forem mantidos totalmente em segredo, será impossível contestar seus principais aspectos. E a impossibilidade de contestar uma decisão ofende o princípio do devido processo e seus desdobramentos do contraditório e da ampla defesa, previstos no artigo 5º, inciso LV da CF/88.

Da mesma forma, ao submeter uma operação algorítmica ao arcabouço principiológico do devido processo legal, especificamente, confrontando opacidade com a exigência de maior transparência, haverá a possibilidade de obter elementos que assegurem ao indivíduo um devido processo algorítmico. É certo que tais precauções não têm o poder de evitar a despedida dos trabalhadores, já que temos também um direito do empregador em despedir, mas poderão assegurar que essas despedidas por decisão algorítmica ocorram mediante um processo justo, correto, igualitário e que preserve a dignidade da pessoa humana.

REFERÊNCIAS

BECK, Ulrich. **Sociedade de risco** – rumo a uma modernidade. 2ª ed. Tradução de Sebastião Nascimento. São Paulo: Editora 34, 2011.

BECK, Ulrich. **World at Risk**. Translated by Ciaran Cronin. Cambridge: Policy Press, 2009.

BURANYI, Stephen. Rise of the racist robots – How AI is learning all our worst impulses. *In*: The Guardian. Disponível em: <<https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses>>. Acesso em: 24 out 2021.

CASEY, Anthony J.; NIBLETT, Anthony. A Framework for the New Personalization of Law. **University of Chicago Law Review**, n. 86. 2019.

CHANDER, Anupam. The Racist Algorithm? *In*: 115 Mich. L. Rev. 1023-1045, 2017.

CITRON, Danielle Keats; PASQUALE, Frank. The Scored Society: Due Process for Automated Predictions. **Washington Law Review** 89, no. 1 (p. 1-34), 2014.

COMISSÃO EUROPEIA. White Paper – On Artificial Intelligence – An European approach to excellence and trust”. 19 de fevereiro de 2020. Disponível em: https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en. Acesso em 24 out. 2021.

FERNANDES, Márcia S. Privacidade, sociedade da informação e Big Data. *In: Direito, Cultura e Método - Leituras da obra de Judith Martins-Costa*. BENNETTI, G.; CORREA, A. R.; FERNANDES, M.S.; NITSCHKE, G. C. M.; PAR-GENDLER, M.; VARELA, L. B. (org.) 1ª ed. Rio de Janeiro: GZ Editora, 2019, v.1, p. 182-210.

FERNANDES, Márcia S. e GOLDIM, José Roberto. Inteligência Artificial e Processo de Tomada de Decisão em Saúde: riscos e oportunidades, Capítulo em desenvolvimento para publicação internacional, em 2022.

FLORIDI, Luciano. **The Fourth Revolution** – How the infosphere is reshaping human reality. Oxford: Oxford University, 2014.

FLORIDI, Luciano. Group privacy: a defence and an interpretation. *In: FLORIDI, Luciano; TAYLOR, Linnet; VAN DER SLOOT, Bart (ed.). Group privacy: new challenges of data technologies*. New York: Springer International Publishing, 2017, p. 83-100; FLORIDI, Luciano. *The ethics of information*. Oxford: Oxford University Press, 2013.

FLORIDI, Luciano. The rise of the algorithm need not be bad news for humans. Financial Times Ltda, May 4, 2017. Disponível em: <https://www.ft.com/content/ac9e10ce-30b2-11e7-9555-23ef563ecf9a?mhq5j=e2>. Acesso em 24 out. de 2021.

FLORIDI, Luciano. What the Near Future of Artificial Intelligence Could Be. *In: The 2019 Yearbook of the Digital Ethics Lab*. BURR, Christopher; MILANO, Silvia. Oxford Internet Institute. Springer Nature Switzerland AG 2020 (eBook) <https://doi.org/10.1007/978-3-030-29145-7>

FLORIDI, Luciano; COWLS, Josh; BELTRAMETTI, Monica et. al. AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*, volume 28, p. 689–707 (2018). Disponível em: <https://link.springer.com/article/10.1007/s11023-018-9482-5>. Acesso em 24 out. 2021.

HAMILTON, Melissa. The Biased Algorithm: evidence of disparate impact on Hispanics. *In: American Criminal Law Review*, n. 56, v. 4, p. 1553-1578, 2019.

HUQ, Aziz Z. **A Right to a Human Decision**. 106 Va. L. Rev. pp. 611-688, 2020.

KAMINSKI, Margot. Ther GDPR's Version of Algorithmic Accountability. *In: EDWARDS, Lilian e VEALE, Micheal*. Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You are Looking For. 16 Duke L. & Tech. Rev. 18 (2017), available at SSRN.

OCDE- *Framework for the classification of ai systems – public consultation on preliminary findings*. 2021. Disponível em: https://aipo-api.buddyweb.fr/app/uploads/2021/06/Report-for-consultation_OECD.AI_Classification.pdf. Acesso em 24 out. 2021.

PASQUALE, Frank. **The Black Box Society**: The secret algorithms that control money and information; London, HUP, 2015.

RIFKIN, Jeremy. **Sociedade com Custo Marginal Zero**. São Paulo, 2016. M. Books do Brasil.

SCHWAB, Klaus. **A quarta revolução industrial**. 2016. World Economic Forum.

ZARSKY, Tal Z. **Transparent Predictions**. University of Illinois Law Review (p.1503 et. seq.), 2013.

41. LEI GERAL DE PROTEÇÃO DE DADOS – ANÁLISE JURISPRUDENCIAL DAS DECISÕES EMANADAS DA JUSTIÇA DO TRABALHO

GENERAL DATA PROTECTION LAW – ANALYSIS OF BRAZILIAN CASE LAW PUT TOGETHER BY THE BRAZILIAN LABOUR COURTS

RICARDO CALCINI⁹⁷ E FELIPE CAMARGO DE ARAÚJO⁹⁸

Resumo

O objetivo deste artigo é identificar as decisões de forma a vislumbrar possíveis tendências de entendimento da Justiça do Trabalho quanto à LGPD, bem como trazer à tona a inegável importância desta lei em matéria trabalhista.

Palavras-chave: Justiça do Trabalho. Proteção de dados. LGPD.

Abstract

The purpose of this article is to identify the decisions in order to glimpse possible trends in the understanding of the Labor Court regarding the LGPD, as well as to bring to light the undeniable importance of this law in labor matters.

Keywords: Labor Justice. Data Protection. LGPD.

1. Introdução

A LGPD, consoante seu artigo 1º, trata sobremaneira do direito à liberdade, bem como do direito à privacidade, notadamente direitos fundamentais de primeira geração ou dimensão. Seu principal objetivo, desta forma, é a proteção de dados pessoais, seja por meio físico ou digital.

Não restam dúvidas de que o direito ao trabalho é o mais importante entre todos os direitos, equiparando-se, inclusive, aos direitos à vida e à saúde, pois é por meio do trabalho que o indivíduo reunirá recursos aptos a alcançar outros direitos fundamentais, tais como lazer, saúde, educação, alimento, entre outros. Não pode ser o direito ao trabalho, entretanto, uma salvaguarda do empregador de forma a aviltar os direitos de liberdade e privacidade do empregado. Bem se sabe da impossibilidade de o empregador exigir informações privadas do candidato ao emprego como condição da contratação, como exames de saúde, antecedentes criminais⁹⁹.

A LGPD, desta forma, vem à tona como uma importante salvaguarda do empregado perante o poderio econômico do empregador, o qual somente poderá

97 Mestre em Direito pela PUC/SP. Professor de Direito do Trabalho da FMU. Membro do Comitê Técnico da Revista Síntese Trabalhista e Previdenciária. Coordenador Trabalhista da Editora Mizuno. rcalcini@gmail.com

98 Especialista em Direito e Processual do Trabalho pela EPD. Especialista em Direito Previdenciário pela EPD. Membro do grupo de estudos de Direito do Trabalho do IASP. Advogado. lippe_araujo@yahoo.com.br

99 Admissível somente em casos de contratação de empregado doméstico e atividades que envolvam segurança patrimonial.

exigir determinadas informações de cunho pessoal do empregado se houver exigência legal para tanto. Do contrário, estará configurado abuso do direito e estará o empregador sujeito a multas e outras sanções administrativas. O presente artigo tem a finalidade de trazer um breve cenário acerca da evolução da jurisprudência, ainda que pouco numerosa, acerca da aplicação da LGPD ao Direito do Trabalho.

2. O Tribunal Superior do Trabalho e a LGPD

Embora o Processo Judicial Eletrônico – PJE – tenha acelerado sobremaneira o trâmite das reclamações trabalhistas em âmbito nacional, é certo que o lapso temporal entre a entrada em vigor da LGPD e a chegada do tema ao Tribunal Superior do Trabalho (TST) é demasiado curto, não havendo ainda ampla discussão do tema pela Corte superior da Justiça Especializada.

Contudo, trataremos de observar alguns posicionamentos do TST em matéria de LGPD, de forma a observar como as turmas vêm se posicionando no enfrentamento do tema, bem como para observar como utilizam a LGPD ao fundamentar suas decisões/acórdãos.

No processo n.º ES 1000537-22.2021.5.00.0000, julgado em 16/08/2021 pela Seção Especializada em Dissídios Coletivos (SDC) do TST, tratando sobremaneira da legitimidade de arguir direitos ou violações de direitos com base na LGPD: no caso em tela, foi negada legitimidade do sindicato profissional em substituir os empregados na defesa de direitos baseados na LGPD, entendendo a SDC que a legitimidade é pessoal de cada empregado¹⁰⁰:

A Lei Geral de Proteção de Dados - LGPD (Lei 13.709/2018) dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O sujeito principal da LGPD é o titular dos dados pessoais, ou seja, a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, a teor do art. 5º, I e V, razão pela qual não há falar em legitimidade do sindicato patronal no caso, quer para defender os interesses de trabalhadores do respectivo setor, quer para buscar a proteção de empregadores.

Não bastasse isso, verifica-se que a Lei n.º 13.709/2018 enuncia, em seu art. 7º, dez hipóteses autorizadoras do uso dos dados pessoais, dentre as quais destacam-se aquelas previstas nos incisos II a IV e IX:

[...]

Esta última hipótese permite o uso de dados para fi-

100 Processo n.º ES 1000537-22.2021.5.00.0000 – TST – SDC – Rel. Maria Cristina Irigoyen Peduzzi – Julgamento em 16/08/2021 – Publicado em 10/09/2021.

nalidades outras daquelas regulamente previstas, quando, do cotejo entre os interesses dos responsáveis pelo tratamento e os direitos individuais dos titulares, houver clara prevalência dos benefícios aos titulares dos dados, como na espécie, em que se busca apurar o cumprimento de cláusulas coletivas e promover a análise estatística e de mobilidade da categoria profissional, bem como realizar as homologações de contratos rescindidos perante o sindicato.

A previsão em sentença normativa de envio de informações de empregados aos sindicatos, com finalidade e adequação específica, como visto, encontra amparo na lei, não importando qualquer violação ou risco de lesão aos direitos dos empregadores. Assim, como já referido no despacho agravado, não há falar em interesse processual do Requerente.

Ante o exposto, nego provimento ao Agravo Interno.

Interessante notar dois aspectos neste acórdão: a SDC entende que o sindicato não pode atuar como substituto processual em temas ligados à LGPD, à luz do artigo 5º, I e V da referida lei, dispositivos estes que transcrevemos abaixo:

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Interessante o posicionamento da SDC do Tribunal Superior do Trabalho à luz deste dispositivo, e que certamente gerará impactos em outras decisões em processos que envolvam sindicatos atuando como substituto processual: a LGPD deve ser invocada de forma individual, não tendo legitimidade o respectivo sindicato profissional.

Outro aspecto bastante interessante do acórdão em questão é a aceitação de que informações dos trabalhadores sejam divulgadas como forma de apurar o cumprimento de determinações previstas em normas coletivas, de forma a garantir que os direitos ali tutelados serão bem observados pelos empregadores, em conformidade com o artigo 7º da LGPD supramencionado. A celeuma discutida nesta ação, em suma, era de cláusula aprovada em dissídio coletivo, a qual previa que os empregadores deveriam, impreterivelmente, a cada 30 (trinta) dias, enviar ao sindicato profissional a relação dos empregados admitidos, afastados e demitidos no período. Assim como deveriam enviar cópia da RAIS - Relação Anual de Informações Sociais dentro do prazo de 15 (quinze) dias contados após a entrega ao sistema do Ministério do Trabalho e Emprego, a fim de que se pudesse apurar o cumprimento das cláusulas coletivas e promover à análise estatística e de mobilidade da categoria profissional, bem como, realizar as homologações de contratos rescindidos no sindicato.

A SDC, desta forma, entendeu justificável, à luz do artigo 7º da LGPD, que informações dos empregados fossem transferidas ao sindicato, tendo em vista que a prestação destas informações têm o condão de otimizar as efetivações de direitos previstas em norma coletiva. Tem-se, desta forma, duas importantes tendências de entendimento do TST acerca da LGPD:

- O sindicato profissional não tem legitimidade para atuar como substituto processual em causas que versem sobre previsões da LGPD;
- Prestação de informações privadas dos empregados pelos empregadores ao sindicato, desde que visando à otimização da efetivação de direitos previstos em norma coletiva, não configura violação à liberdade e privacidade de dados, à luz do artigo 7º da LGPD.

3. O Tribunal Regional da 4ª Região e a LGPD

No âmbito do Tribunal Regional do Trabalho da 4ª Região, há sentença de 1º grau bastante interessante proferida pela Exma. Juíza Ivanisa Marilene Uhlig de Barros, juíza substituta na Vara do Trabalho de Montenegro/RS.

Nos autos do processo n.º 0020043-80.2021.5.04.0261¹⁰¹, movido pelo Sindicato dos Trabalhadores nas Indústrias de Alimentação de Montenegro em face da Cooperativa dos Citricultores Ecológicos do Vale do Caí: nesta ação, o sindicato-autor alega descumprimento sistemático relativo à proteção de dados por parte da empresa reclamada. Afirma que, além da posse de dados, a empresa os compartilha com diversos outros controladores e operadores, sem as cautelas necessárias. Refere não haver indicação do encarregado pelos dados pessoais. Argumenta também que o tratamento de dados é compartilhado por intermédio da Internet, em desatenção ao Marco Civil da Lei 12.965/14, arts. 10 e 11, pois não se observa o respeito à intimidade, privacidade e imagem. Entende haver presunção de dano moral e requer a condenação da cooperativa ao pagamento de indenização por danos morais consubstanciado no artigo 52 da LGPD. Na sentença exarada, a MMª. Juíza tece sua argumentação:

101 <https://trt-4.jusbrasil.com.br/jurisprudencia/1247214376/acc-200438020215040261-trt04/inteiro-teor-1247214378>

Em linhas gerais, a Lei 13.709/2018 passou a ter vigência escalonada a partir de 28/12/2018, trazendo previsões sobre o tratamento de dados no intuito de proteção dos direitos fundamentais de liberdade e privacidade (art. 1º).

Diante da omissão legislativa até então existente, buscou-se assegurar que os titulares dos direitos envolvidos estejam resguardados em sua dignidade/privacidade e protegidos também em face da automação, na forma do art. 7º, XXVII, da Constituição Federal. A este exemplo, o art. 20 da LGPD assegura o direito à reversão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais.

Também está assentada a função social da propriedade, art. 170, III, da CRFB. É consabido que atualmente os dados pessoais constituem um novo insumo da economia globalizada e tecnológica; e tal proteção revela importância pela necessidade em se erigir ao mercado igualdade de concorrência e função antidumping.

Dando efetividade a isso, dentre as bases principiológicas previstas no art. 6º da LGPD, destaco a finalidade, o livre acesso, transparência, segurança, prevenção, não discriminação e prestação de contas.

[...]

Sobre a alegada competência exclusiva da ANPD, igualmente não procede o argumento, pois a disposição do art. 55-J da LGPD não exclui o direito dos próprios titulares, ou, no caso, seu substituto processual, segundo art. 9º da LGPD.

Além do mais, a reclamada está subsumida à legislação vigente, por se tratar de pessoa jurídica de direito privado que opera tratamento de dados para fornecimento de serviços (art. 3º, II).

[...]

Ante o exposto, nos termos da fundamentação, rejeito a preliminar lançada pelas reclamadas e, no mérito **JULGO PROCEDENTE EM PARTE** a ação movida por **SIND TRAB NAS INDS DE ALIMENTACAO DE MONTENEGRO** contra **COOPERATIVA DOS CITRICULTORES ECOLOGICOS DO VALE DO CAI LTDA**, para reconhecer parcialmente a inadequação à Lei Geral de Proteção de Dados e condenar a reclamada nas seguintes obrigações, conforme os termos da fundamentação supra e observada a liquidação pelo procedimento comum, conforme art. 509, II, do CPC:

1. determinar que a empresa indique e nomine encarregado;

2. que a reclamada implemente e comprove nos autos as práticas relacionadas à segurança e sigilo de dados; sob pena de multa a ser fixada;

3. comprovar nos autos o cumprimento das obrigações impostas, no prazo de 90 (noventa) dias, sob pena de multa diária de R\$ 1.000,00.

Interessante notar, sobre esta sentença, os seguintes fatos:

- Ao contrário da SDC do TST, o sindicato profissional foi considerado legítimo a atuar como substituto processual;
- A MM. Juíza prolatora da sentença considerou que a empresa ré descumpriu preceitos da LGPD, exigindo que a ré comprove a adoção de práticas visando à segurança e sigilo de dados de empregados;
- Entendimento de que, à luz do artigo 65, II, da LGPD, a adoção das medidas independe de regulamentação específica, tendo as obrigações previstas na lei aplicabilidade imediata;
- Entendimento que apenas as sanções administrativas terão entrada em vigor posteriormente à prolação da sentença, por isso não foram aplicadas, o que não impede a condenação à obrigação de fazer consistente em adequar os procedimentos da ré à LGPD.

4. A LGPD e o segredo de justiça na Justiça do Trabalho

Fato corriqueiro está sendo o pedido de segredo de justiça com base na LGPD, fundamentado em seu artigo 18, inciso IV.¹⁰²

Interessante observar alguns posicionamentos da Justiça do Trabalho quanto a estes pedidos, principalmente quando confrontados com os requisitos legais já admitidos como base ao segredo de justiça.

No processo n.º MSCiv 1001177-68.2021.5.02.0000 SP¹⁰³, julgado pela Seção de Dissídios Individuais do Tribunal Regional do Trabalho da 2ª Região em 06/04/2021, assim decidiu a seção:

Na hipótese dos autos, entretanto, a simples alegação da impetrante de que haveria risco de ser inserida nas intituladas *black lists* de empresas, em razão do trâmite público dos autos principais, não se enquadra em qualquer das hipóteses estabelecidas pela legislação.

Entendimento diverso implicaria reconhecer a necessidade de atribuição de sigilo a todos os processos ajuizados por trabalhadores nesta Justiça Especial, em nítida violação ao princípio da publicidade (CF, artigo 93, IX) e aos dispositivos suso mencionados.

102 Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...) IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

103 <https://trt-2.jusbrasil.com.br/jurisprudencia/1263044832/mandado-de-seguranca-civel-msciv-10011776820215020000-sp/inteiro-teor-1263044849>

Registre-se, ademais, que o artigo 7º, VI, da Lei nº 13.709/2018 (Lei de Proteção de Dados Pessoais - LGPD) estabelece, expressamente, a possibilidade de tratamento de dados pessoais “*para o exercício regular de direitos em processo judicial*”, de modo que a previsão contida no artigo 18, IV, do referido diploma, quanto à “*anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei*”, não acarreta os efeitos pretendidos pela impetrante, tampouco lhe confere o direito à tramitação do feito em segredo de justiça.

Deveras, o tratamento das informações da trabalhadora, nos autos em epígrafe, é realizado com o único objetivo de prestar a tutela jurisdicional por ela vindicada, à luz dos princípios da finalidade, da adequação, da necessidade, da transparência e da boa-fé (artigos 6º, I, II, III e VI e 7º, § 3º, da LGPD).

Neste processo, a impetrante do mandado de segurança, pessoa física, alegava que a publicidade de seu nome em reclamação trabalhista a estava prejudicando na busca por um novo emprego, razão pela qual impetrou a medida à luz da LGPD. O Tribunal, entretanto, negou a segurança, alegando que, fosse o caso de se atribuir sigilo por conta de risco de “black list”, todas as reclamações trabalhistas do país deveriam tramitar sob sigilo, bem como ressaltou o artigo 7º, VI da LGPD, o qual assegura possibilidade de tratamento de dados pessoais “para o exercício regular de direitos em processo judicial”. Mesmo entendimento teve o Tribunal Superior do Trabalho em processo análogo (Processo nº AIRR 2248-02.2013.5.02.0066)¹⁰⁴

5 Considerações Finais

A LGPD começa, paulatinamente, a permear as decisões da Justiça do Trabalho. Há que se firmar os entendimentos, principalmente, acerca da legitimidade para pleitear direitos à luz da LGPD, bem como a parametrização das sanções disciplinares que entraram em vigor em agosto de 2021.

As disciplinas da LGPD, entretanto, não parecem ser a salvaguarda de empregados que movem reclamações trabalhistas contra empregadores e ex-empregadores, mas desejam sigilo de justiça por temor de dificuldades de contratação por empresas concorrentes.

Às empresas que não cumprem o quanto determinado pela LGPD, ainda, nota-se predisposição da Justiça do Trabalho em condenar tais empresas às obrigações de fazer consistentes em adequar políticas de proteção de dados aos ditames da lei. Ainda, a partir de agosto de 2021, as sanções disciplinares previstas na LGPD já são passíveis de aplicação plena pelo Poder Judiciário.

Não restam dúvidas, entretanto, acerca do aumento da proteção dos direitos individuais de liberdade e privacidade dos empregados em decorrência da entrada em vigor da LGPD. É de suma importância, desta forma, que os operadores do

¹⁰⁴ <https://tst.jusbrasil.com.br/jurisprudencia/679306102/agravo-de-instrumento-em-recurso-de-revista-airr-22480220135020066/inteiro-teor-679306139>.

direito do trabalho mantenham vigilância sobre a jurisprudência acerca do tema, que servirá de norte a sindicatos, Ministério Público do Trabalho e, principalmente, aos empregadores, aos quais se recomenda a imediata adoção de políticas em conformidade com a LGPD.

REFERÊNCIAS

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Organiza a Justiça do Trabalho. Diário Oficial da União de 15/08/2018.

BRASIL. **Lei nº 13.853, de 08 de julho de 2019.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Diário Oficial da União, 20/12/2019.

BRASIL. **Lei nº 14.010, de 10 de junho de 2020.** Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (covid-19). Diário Oficial da União, 08/09/2020.

CALCINI, Ricardo; ARAÚJO, Christiane Carvalho Andrade. **O impacto da LGPD nas relações de trabalho.** Disponível em: <https://www.conjur.com.br/2020-set-17/lgpd-impactos-trabalhistas>.

GIUNTINI, Adriana (et al.) **LGPD nas relações de trabalho.** E-book 1 ed. Salvador (BA): Motres, 2021. Disponível em: https://oabdf.org.br/wp-content/uploads/2021/08/eBook_LGPD-nas-Relacoes-de-Trabalho-1-1.pdf.

PESSOA, André; MOLLICONE, Bianca Medalha; MIZIARA, Raphael. **Reflexos da LGPD no Direito do Trabalho e no Processo do Trabalho.** 1. ed. São Paulo: Editora Revista dos Tribunais, 2020.

SEGUNDA PARTE

A PROTEÇÃO DOS DADOS SOB O PRISMA JURISDICIONAL

STF. ACÓRDÃO. PROTEÇÃO DOS DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO.

MINISTRA ROSA WEBER

EMENTA: MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO.

1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais.

2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais não de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados.

3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam “adequados, relevantes e não excessivos em relação a esse propósito” e “conservados apenas pelo tempo necessário.” (artigo 45, § 2º, alíneas “b” e “d”).

4. Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia.

5. Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades.

6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros.

7. Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada.

8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020.

9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição.

10. *Fumus boni juris* e *periculum in mora* demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel.

11. Medida cautelar referendada.

ACÓRDÃO Vistos, relatados e discutidos estes autos, acordam os Ministros do Supremo Tribunal Federal em, por maioria, referendar a medida cautelar deferida para suspender a eficácia da Medida Provisória nº 954/2020, nos termos dos votos proferidos, vencido o Ministro Marco Aurélio, em sessão Plenária (realizada inteiramente por videoconferência - Resolução 672/2020/STF), presidida pelo Ministro Dias Toffoli, na conformidade da ata do julgamento. [STF. Plenário. REFERENDO NA MEDIDA CAUTELAR NA AÇÃO DIRETA DE INCONSTITUCIONALIDADE 6.387/DF. Relatora: Ministra Rosa Weber. Data: 7-5-2020. A: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629>]

ACÓRDÃO. TRT 4. Art. 18 LGPD.

DESEMBARGADOR WILSON CARVALHO DIAS

PROCESSO nº 0020101-72.2021.5.04.0006 (AIRO)

AGRAVANTE: RODRIGO SERRANO DOS SANTOS

AGRAVADO: CENTRO CLINICO GAUCHO LTDA

RELATOR: WILSON CARVALHO DIAS

AGRAVO DE INSTRUMENTO EM RECURSO ORDINÁRIO DO AUTOR

ACORDAM os Magistrados integrantes da 7ª Turma do Tribunal Regional do Trabalho da 4ª Região: por unanimidade, DAR PROVIMENTO AO AGRAVO DE INSTRUMENTO DO AUTOR (RODRIGO) para receber o seu recurso ordinário. Por unanimidade, DAR PROVIMENTO PARCIAL AO RECURSO para condenar o réu ao pagamento de honorários sucumbenciais de 5% sobre o valor atribuído à causa, devidos à procuradora do autor. [...]

Examino.

Trata-se a presente de "ação de produção antecipada de provas", ajuizada em 11.02.2021, tendo o autor alegado, na peça inicial, que notificou o réu, extrajudicialmente, para que fornecesse documentos a fim de subsidiar a futura ação trabalhista, sem ser atendido na sua solicitação. Foram juntadas cópias da correspondência eletrônica enviada pela procuradora do autor para os endereços "jucileia.farias@ccgrs.com.br" e "vanda.moura@ccgrs.com.br" (ID. 8541a6e) e do comprovante de leitura da correspondência por "vanda.moura@ccgrs.com.br" no "sábado, 23 de janeiro de 2021 08:34:20" (ID. 6fc50ab - Pág. 1).

Notificado, o réu apresentou defesa e juntou aos autos os documentos requeridos (ID. 6d7b0b7 a ID. 803072c). Inicialmente, o réu negou a pretensão resistida. Disse não ter recebido o requerimento extrajudicial. Sucessivamente, afirmou que a procuração juntada não confere aos procuradores do autor os poderes especiais para requisitar documentos sensíveis. Citou a LGPD. Argumentou que o autor poderia ter comparecido pessoalmente ao local de trabalho para requerer a documentação.

No caso, considerando que o réu não apresentou argumentos capazes de infirmar o comprovante de leitura da notificação extrajudicial pela via eletrônica (e-mail), juntado aos autos no ID. 6fc50ab - Pág. 1, presumo que o réu recebeu o requerimento.

O § 3º do art. 18 da LGPD dispõe que "Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento."

Há evidências de que a correspondência eletrônica enviada para fins de notificação extrajudicial estava acompanhada de instrumento de procuração. Nesse contexto, pelo dever de cooperação, que decorre do princípio da boa-fé objetiva, entendo que cabia ao réu, caso entendesse que a documentação não atendia às exi-

gências legais ou que era insuficiente, informar tal circunstância ao requerente no prazo especificado, sob pena de, no seu silêncio, ter-se por configurada a pretensão resistida que legitima o ajuizamento da ação de produção antecipada de provas e que dá ensejo à condenação em honorários sucumbenciais.

Quanto aos honorários sucumbenciais, aplica-se ao caso o art. 791-A da CLT ("Ao advogado, ainda que atue em causa própria, serão devidos honorários de sucumbência, fixados entre o mínimo de 5% (cinco por cento) e o máximo de 15% (quinze por cento) sobre o valor que resultar da liquidação da sentença, do proveito econômico obtido ou, não sendo possível mensurá-lo, sobre o valor atualizado da causa."), considerando que a presente ação trabalhista foi ajuizada na vigência da Lei 13.467/2017.

A exibição dos documentos pela reclamada ocorreu apenas em juízo, tendo sido julgada procedente a ação (ID. c2174e2). Logo, comprovada a existência de pretensão resistida e sendo o réu sucumbente na presente demanda, são devidos honorários sucumbenciais em favor da procuradora do autor.

Como não houve condenação em pecúnia, conforme art. 791-A da CLT, cumpre arbitrar os honorários com base no valor da causa atribuído na peça inicial (R\$ 20.000,00), que entendo ser razoável.

Com relação ao percentual dos honorários, devem ser fixados considerando os critérios legais previstos no 791-A, § 2º, da CLT - grau de zelo do profissional, lugar da prestação de serviço, natureza e importância da causa, o trabalho realizado pelo advogado e o tempo exigido para o seu serviço. Assim, tendo em vista tais critérios, fixo os honorários sucumbenciais em 5% sobre o valor atribuído à causa.

Dou parcial provimento ao recurso para condenar o réu ao pagamento de honorários sucumbenciais de 5% sobre o valor atribuído à causa, devidos à procuradora do autor.

https://www.trt4.jus.br/pesquisas/rest/cache/acordao/pje/nptRk9A2eqeiIG_D660u2g

ACÓRDÃO. TRT4. CUMPRIMENTO DE OBRIGAÇÃO LEGAL PELO CONTROLADOR.

DESEMBARGADOR FABIANO HOLZ BESERRA

PROCESSO nº 0020727-86.2020.5.04.0601 (ROT)
RECORRENTE: PORTALSUL SERVICOS LTDA - ME
RECORRIDO: FED TRABAL EMPR ASSEIO CONSER LIMP URBA AMBIEN A VERDES, ZELADORIA, SERV TERCEIRIZADOS NO RGS
RELATOR: FABIANO HOLZ BESERRA
EMENTA

AÇÃO DE CUMPRIMENTO. Comprovado pela Federação autora a existência de previsão normativa que contemplando o recolhimento de contribuição social para efetivar a viabilidade do Plano de Benefício Social Familiar, incumbe à reclamada a produção de prova acerca do seu adimplemento, não havendo afronta ao ônus da prova no aspecto.

ACÓRDÃO

Vistos, relatados e discutidos os autos.

ACORDAM os Magistrados integrantes da 1ª Turma do Tribunal Regional do Trabalho da 4ª Região: preliminarmente, por unanimidade, NÃO CONHECER DO RECURSO ORDINÁRIO DA RECLAMADA no que se refere aos honorários advocatícios e justiça gratuita, por ausência de ataque aos fundamentos da sentença. No mérito, por unanimidade, NEGAR PROVIMENTO AO RECURSO ORDINÁRIO DA RECLAMADA, PORTALSUL SERVICOS LTDA - ME.

Intime-se.

Porto Alegre, 10 de agosto de 2021 (terça-feira).

RELATÓRIO

A reclamada recorre da sentença de ID. 2a85c20, que julgou parcialmente procedentes os pedidos, buscando a sua reforma quanto a ilegitimidade ativa, benefício social familiar, assistência judiciária gratuita e honorários advocatícios (ID. 4da45d1).

Com contrarrazões da Federação reclamante (ID. 328b6dc), os autos vêm ao Tribunal para julgamento e são distribuídos a este Relator, na forma regimental.

É o relatório.

FUNDAMENTAÇÃO

I – PRELIMINARMENTE

1. Não conhecimento do recurso ordinário da reclamada em relação aos honorários

Ao final de sua peça recursal, a parte autora apresenta requerimentos não ligados aos fundamentos do recurso, dentre os quais um em relação aos honorários (ID. 4da45d1 - Pág. 7):

Reformada a sentença de primeiro grau, sendo julgado improcedente o pedido de condenação da Recorrente ao pagamento dos honorários assistenciais no percentual de 15% sobre o valor da causa.

Neste sentido, assim constou na sentença (ID. 2a85c20 - Pág. 10):

Por outro lado, vencida integralmente a reclamada, nos termos do art. 791-A da CLT, são devidos honorários de sucumbência ao procurador da autora, que, observadas as moduladoras dos incisos do § 2º do referido dispositivo consolidado, estipulo em 10% do valor da condenação.

Como se vê, o pedido realizado não tem relação com a fundamentação apresentada na sentença, não merecendo conhecimento.

Conforme artigo 1.010 do CPC, de aplicação subsidiária ao processo do trabalho em razão do permissivo do art. 769 da CLT, é pressuposto extrínseco do recurso ordinário o ataque aos fundamentos da sentença nas razões recursais de

sorte a evidenciar o equívoco do julgamento a quo.

Ainda que o princípio da dialeticidade seja mitigado pelo efeito devolutivo à profundidade inerente ao recurso ordinário, não se conhece do apelo cujas razões sejam inteiramente dissociadas dos fundamentos da sentença. Nesse sentido o item III da Súmula n.º 422 do TST:

RECURSO. FUNDAMENTO AUSENTE OU DEFICIENTE. NÃO CONHECIMENTO.

I - Não se conhece de recurso para o Tribunal Superior do Trabalho se as razões do recorrente não impugnem os fundamentos da decisão recorrida, nos termos em que proferida. [...]

III - Inaplicável a exigência do item I relativamente ao recurso ordinário da competência de Tribunal Regional do Trabalho, exceto em caso de recurso cuja motivação é inteiramente dissociada dos fundamentos da sentença. (grifei)

Diante do exposto, não conheço do recurso ordinário da reclamada em relação aos honorários advocatícios, por ausência de ataque aos fundamentos da sentença.

2. Não conhecimento do recurso ordinário da reclamada em relação à justiça gratuita.

Ao final de sua peça recursal, a parte autora apresenta diversos requerimentos não ligados aos fundamentos do recurso, dentre os quais um em relação à justiça gratuita (ID. 4da45d1 - Pág. 6):

Reformada a sentença de primeiro grau, sendo negado o benefício da Assistência Judiciária Gratuita à Federação, eis que inexistem provas comprobatórias da carência financeira da entidade.

Neste sentido, assim constou na sentença (ID. 2a85c20 - Págs. 9/10):

O caso em exame não envolve empregado e empregador, mas sim discussão entre ente sindical e empregador. Tem-se que, com a promulgação da Emenda Constitucional n.º 45 de 2004, a inexistência de honorários de sucumbência na Justiça do Trabalho foi repensada na esfera trabalhista. Com a competência da Justiça Obreira sensivelmente ampliada, nos termos do artigo 114 da CF/88, e não mais restrita às relações de emprego, os motivos que embasam o antigo posicionamento deixam de existir, pois ausente a figura do hipossuficiente nas demais relações que podem ser levadas a litígio.

De acordo com a atual redação do art. 790, § 4º, da CLT, é facultado o deferimento do benefício da justiça gratuita àquele que comprovar a insuficiência de recursos, hipótese que, de início, não se presume em relação a uma entidade sindical. Entretanto, considerando o teor do disposto no § 2º do art. 606 consolidado, aplicável analogicamente à cobrança das contribuições negociadas, defiro à federação reclamante o benefício da isenção do pagamento de custas. Como se vê, o pedido realizado não tem relação com a fundamentação apresentada na sentença, não merecendo conhecimento.

Conforme artigo 1.010 do CPC, de aplicação subsidiária ao processo do trabalho em razão do permissivo do art. 769 da CLT, é pressuposto extrínseco do recurso ordinário o ataque aos fundamentos da sentença nas razões recursais de

sorte a evidenciar o equívoco do julgamento a quo.

Ainda que o princípio da dialeticidade seja mitigado pelo efeito devolutivo à profundidade inerente ao recurso ordinário, não se conhece do apelo cujas razões sejam inteiramente dissociadas dos fundamentos da sentença. Nesse sentido o item III da Súmula n.º 422 do TST:

RECURSO. FUNDAMENTO AUSENTE OU DEFICIENTE. NÃO CONHECIMENTO.

I - Não se conhece de recurso para o Tribunal Superior do Trabalho se as razões do recorrente não impugnem os fundamentos da decisão recorrida, nos termos em que proferida. [...]

III - Inaplicável a exigência do item I relativamente ao recurso ordinário da competência de Tribunal Regional do Trabalho, exceto em caso de recurso cuja motivação é inteiramente dissociada dos fundamentos da sentença. (grifei)

Diante do exposto, não conheço do recurso ordinário da reclamada em relação à justiça gratuita, por ausência de ataque aos fundamentos da sentença.

II - RECURSO ORDINÁRIO DA RECLAMADA

1. Ilegitimidade da Federação autora

O Magistrado a quo assim decidiu (ID. 2a85c20 - Págs. 2/4):

A parte ré defende que a Federação autora não é parte legítima para promover a presente demanda, visto que existem 7 sindicatos em sua base territorial de representação, de modo que, mesmo que as convenções coletivas atribuam à entidade a administração do fundo, a prerrogativa deve observar o disposto no art. 513, a, segundo o qual a legitimidade ativa é do sindicato.

Argumenta que os direitos pleiteados na demanda são individuais, uma vez que o recebimento de benefícios instituído importa individualmente à pessoa, excluindo a legitimidade do próprio sindicato.

O antigo Código de Processo Civil Brasileiro, de 1973, filiando-se à teoria ecletica, desenvolvida por Enrico Tulio Liebman, subordinava o exame do mérito da "ação" ao implemento de determinadas condições prévias, quais sejam: possibilidade jurídica do pedido, interesse de agir e legitimatio ad causam. A arguição de carência da ação indicava a ausência de uma das condições da ação, constituindo defesa direta contra o processo. Diz-se defesa direta por se dirigir, direta e imediatamente, contra o processo e não contra o mérito da causa.

Já o NCPC não mais enuncia, expressamente, as condições de ação, tampouco utiliza a expressão carência de ação.

Ao revés, o inciso VI do art. 485 autoriza a extinção do processo sem resolução do mérito pela ausência de legitimidade ou interesse processual, que mantêm a qualidade de pressupostos processuais, excluindo a possibilidade jurídica, que passa a ser vinculada a vedações legais específicas.

Nesta senda, o interesse de agir consiste na necessidade e utilidade de obter o provimento jurisdicional. Já a legitimidade para a causa está vinculada à titularidade do direito substancial deduzido em juízo, verificando-se tanto em relação ao polo ativo como passivo.

Obtempero que constitui entendimento do Juízo que o inc. III do art. 8º da Constituição Federal confere ao sindicato a defesa dos direitos e interesses coletivos ou individuais da categoria, inclusive em questões judiciais ou administrativas, independentemente da expressa autorização de seus membros para representá-los em juízo. No particular, portanto, o sindicato recebeu tratamento distinto do conferido às entidades associativas em geral, pelo art. 5º, XXI, da Constituição, que a elas atribui legitimidade para representar seus filiados judicial e extrajudicialmente, quando expressamente autorizadas. Tenha-se presente, ainda, que a Lei n.º 8.984/95, nada obstante se trate de norma relativa a competência, permite que o sindicato postule o cumprimento de acordo e convenção coletiva, atuando tanto em favor de sua pessoa jurídica quanto em prol de direitos individuais da categoria, exercendo, nessa última hipótese, a substituição processual dos trabalhadores.

No caso dos autos, a pretensão formulada objetiva o cumprimento de normas coletivas, considerando a criação, nas convenções coletivas, de um Plano de Benefício Social Familiar, direcionado a auxiliar os empregados pertencentes à categoria obreira diante de distintas contingências. Nas sucessivas cláusulas negociadas restou ajustado que caberia aos empregadores o custeio desse plano, a partir do pagamento dos valores fixados, por trabalhador que pertença ao seu quadro funcional. Ainda, restou pactuado que o plano seria administrado pela Federação autora.

Logo, o pleito de adimplemento dessa contribuição social, de gênese normativa, não envolve direito individual, singular de cada empregado, mas sim um direito coletivo, já que o custeio do plano tem por escopo a manutenção de um amplo rol de benefícios para a categoria como um todo. Nesta esteira, ainda que as federações, de início, detenham legitimidade subsidiária aos sindicatos, com atuação autorizada apenas diante da omissão dos entes representativos de primeiro grau, tem-se que as cláusulas coletivas, assinadas pelos sindicatos que integram a Federação reclamante, a estabelecem como a administradora do referido plano e, conseqüentemente, destinatária das contribuições, circunstância que configura sua legitimidade ativa concorrente.

Esse é o entendimento majoritário que vem se consolidando nas cortes trabalhistas:

""FEDERAÇÃO. LEGITIMIDADE ATIVA. Hipótese em que a Federação é parte legítima para ajuizar ação buscando o cumprimento de norma coletiva firmada por sindicato que a integra, pois é administradora e destinatária da contribuição instituída com a finalidade de implementar o "Plano de Benefício Social Familiar". (TRT da 4ª Região, 7ª Turma, 0020811-97.2017.5.04.0761 ROT, em 23/08 /2019, Desembargador Emilio Papaleo Zin)

""AÇÃO DE CUMPRIMENTO DE CLÁUSULAS NORMATIVAS. LEGITIMIDADE ATIVA DA FEDERAÇÃO. Sendo a Federação a administradora e destinatária da contribuição instituída em convenção coletiva por Sindicato que a integra, inegável a sua legitimidade para postular o cumprimento de cláusulas normativas em Juízo. Recurso da parte autora provido, no ponto."" (TRT da 4ª Re-

gião, 4ª Turma, 0021333-80.2016.5.04.0302 ROT, em 08/03/2018, Desembargador Andre Reverbel Fernandes) "

"FEDERAÇÃO - AÇÃO DE CUMPRIMENTO – LEGITIMIDADE ATIVA – Considerando que a Federação é a administradora do produto da contribuição social estabelecida nas normas coletivas, inarredável é a conclusão de que esta detém legitimidade para postulá-lo." (TRT da 4ª Região, 3ª Turma, 0020625-85.2015.5.04.0101ROT, em 06/04/2017, Desembargador Claudio Antonio Cassou Barbosa)

Destarte, rejeito a preliminar suscitada na tese defensiva.

A empresa reclamada afirma que: 1) não se pode falar em legitimidade da recorrida para propor ação de cumprimento de convenção coletiva, relativa às mensalidades do Plano Benefício Social Familiar, eis se tratar de pretensão de natureza individual e não coletiva; 2) o direito em questão é de ordem individual dos trabalhadores, sendo que a legitimidade ativa é conferida aos Sindicatos e, apenas, subsidiariamente da Federação, o que apenas poderia ocorrer em caso de inexistência de Sindicato na cidade ou região da empregadora, o que não é o caso da primeira demanda; 3) se há sindicato da categoria registrado na região, caberia a tais demandar com esta pretensão, visando efetivar o direito daqueles trabalhadores que se sentiram lesados de alguma forma, o que sequer fizeram; 4) a Constituição da República outorgou aos sindicatos a atribuição de defender os direitos e interesses da categoria, quer na seara judicial, quer na seara administrativa (art. 8º, inciso III). Requer seja reformada a sentença de primeiro grau, no sentido de ser reconhecida a ilegitimidade ativa da Federação, e conseqüentemente julgada improcedente a presente demanda.

Examino.

Trata-se de Ação de Cumprimento apresentada Federação de Trabalhadores em Empresas de Asseio Conservação Limpeza Urbana e em Geral, Ambiental, Áreas Verdes, Zeladoria e Serviços Terceirizados no Estado do Rio Grande do Sul - FEEAC para cobrar da reclamada o adimplemento de parcelas relativas ao plano de benefício social familiar.

Neste sentido, as normas coletivas preveem que a administração de tal plano ficará a cargo da FEEAC, consoante instituído na Convenção Coletiva da Categoria, na cláusula 25ª (ID. 0ee1fe5 - Págs. 9/11), sendo descabida a alegação de ilegitimidade da Federação autora, pois a cláusula normativa é clara ao estabelecer que tal entidade administrará o referido Plano, custeado com contribuições das empresas e em um primeiro momento dos empregados.

No intuito de evitar discussões desnecessárias, transcrevo a seguir fundamentos de acórdão desta Turma, no qual participei e acompanhei o voto da Relatora, adotando-o como razões de decidir:

Entendo que a Federação em questão tem legitimidade para propor ação de cumprimento na qualidade de substituta processual dos sindicatos convenientes conforme o art. 8º, inciso III, da Constituição Federal que confere ampla legitimação às entidades sindicais, incluindo nesse conceito as Federações, à defesa dos

direitos e interesses coletivos ou individuais da categoria.

Outrossim, a Federação, nos termos das Convenções Coletivas de Trabalho carreadas ao feito, ID. a204823 pág.9-11, por exemplo, é a responsável pela implementação e gestão do Plano de Benefício Social Familiar, de forma que a parte autora é legítima para figurar no polo ativo da presente demanda.

No mesmo sentido, as seguintes decisões:

AÇÃO DE CUMPRIMENTO DE CLÁUSULAS NORMATIVAS. LEGITIMIDADE ATIVA DA FEDERAÇÃO. Sendo a Federação a administradora e destinatária da contribuição instituída em convenção coletiva por Sindicato que a integra, inegável a sua legitimidade para postular o cumprimento de cláusulas normativas em Juízo. Recurso da parte autora provido, no ponto. (TRT da 4ª Região, 4ª Turma, 0021333-80.2016.5.04.0302 (RO), em 08.03.2018, Desembargador André Reverbél Fernandes)

FEDERAÇÃO - AÇÃO DE CUMPRIMENTO - LEGITIMIDADE ATIVA - Considerando que a Federação é a administradora do produto da contribuição social estabelecida nas normas coletivas, inarredável é a conclusão de que esta detém legitimidade para postulá-lo. (TRT da 4ª Região, 3ª Turma, 0020972-78.2015.5.04.0761 RO, em 10.08.2017, Desembargadora Maria Madalena Telesca)

Pelo exposto, nego provimento. (TRT da 4ª Região, 1ª Turma, 0021336-16.2017.5.04.0006 ROT, em 29/05/2020, Desembargadora Rosane Serafini Casa Nova)

Portanto, nego provimento ao recurso ordinário no tópico.

2. Ausência de provas de descumprimento de convenção coletiva de trabalho
Em sentença assim constou (ID. 2a85c20 - Págs. 6/9):

Inicialmente, cumpre esclarecer que as contribuições postuladas não equivalem às contribuições sindicais, outrora instituídas pelo art. 578 e seguintes da CLT, que correspondiam a uma modalidade de imposto sindical de natureza inequivocamente tributária, assim como não se trata de uma contribuição assistencial criada como mera fonte de custeio para a estrutura sindical propriamente dita, condicionada à autorização prévia e expressa dos participantes das respectivas categorias econômica ou profissional. Trata-se de uma contribuição social, de gênese normativa, negociada pelos entes sindicais como forma de custeio para o plano de benefício social familiar, deliberadamente administrado pela federação autora e destinado a garantir uma série de benefícios, auxílios e direitos expressamente delineados para os membros da categoria profissional, em consonância com o princípio da melhoria da condição social, consubstanciado no caput do art. 7º da carta constitucional, bem como com o princípio da autodeterminação normativa, consagrado no inciso XXVI da mesma Carta Magna.

Neste diapasão, atento que os argumentos de defesa são bastante evasivos, já que a empresa alega que a parte autora não comprovou o fato constitutivo do direito e, por sua vez, não poderia apresentar documentos identificando os empregados. Com efeito, cabe ao demandante comprovar o fato constitutivo do seu direito, conforme art. 818, I, consolidado, mas a federação trouxe ao feito a totalidade das

convenções coletivas que invoca como fundamento jurídico para a pretensão.

Nos termos do inciso II do mesmo art. 818 da CLT, cabe à parte reclamada produzir prova do fato impeditivo, modificativo ou extintivo do direito, mas a ré, em momento algum, defende que teria pago qualquer das mensalidades pleiteadas com fulcro nas cláusulas coletivas. Ao revés, alega que parte dos seus empregados presta serviços de portaria e vigia, vinculando-se ao sindicato dos vigilantes, assim como que não estaria obrigada a cumprir as normas coletivas invocadas.

Cumpra destacar que, de acordo com o estatuído nos arts. 511 e 570, caput, da CLT, o enquadramento sindical é determinado pela atividade econômica predominante da empresa e pelo local da prestação de serviços (Princípio da Territorialidade), exceto no tocante aos trabalhadores integrantes de categoria profissional diferenciada. Diga-se, ainda, que é sabido que para a definição da atividade preponderante vale-se do disposto no art. 581, § 2º, da CLT, que refere:

""Entende-se por atividade preponderante a que caracterizar a unidade de produto, operação ou objetivo final, para cuja obtenção todas as demais atividades convirjam, exclusivamente, em regime de conexão funcional.""

Despiciendo registrar que os dispositivos em questão foram recepcionados pela Constituição Federal de 1988 e constituem normas de ordem pública, portanto de aplicação compulsória, inafastável pela vontade das partes diante do caráter de imperatividade emanado do comando estatal. Deste modo, ocioso mencionar que não é dado à empregadora ""escolher"" o seu enquadramento sindical e, por consequência, o de seus empregados.

Assim dispõe o conceito legal de categoria profissional diferenciada:

""Categoria profissional diferenciada é a que se forma dos empregados que exerçam profissões ou funções diferenciadas por força de estatuto profissional especial ou em consequência de condições de vida singulares".

Ocorre que, entre as atividades descritas no objeto da sociedade, em seu contrato social, a maior parte delas encontra-se inserida na órbita da categoria econômica representada pelo sindicato patronal que firma as convenções coletivas anexadas ao feito, do que se depreende que constituem, efetivamente, a atividade preponderante. Neste diapasão, considerando o argumento de que parte dos empregados estaria inserido na categoria profissional diferenciada dos vigilantes, destaco que o vigia ou auxiliar de segurança privada não se enquadra na hipótese legal da Lei nº 7.102/83, que define e regula a atividade dos vigilantes, que por sua vez não figura entre as atividades descritas no objeto social. Assim, resta inequívoco que a empresa ré é representada pelo sindicato patronal signatário dos regramentos.

Por fim, não prosperam os argumentos da contestante acerca da impossibilidade de trazer ao feito a relação de empregados, imperativa para a apuração do número de obreiros em atividade e, conseqüentemente, da mensalidade devida em face do plano de benefício social familiar. Os documentos em questão destinam-se a comprovar o efetivo cumprimento, pelo empregador, de obrigações trabalhistas, fiscais e previdenciárias, não se inserindo, ao menos perante os órgãos de fisca-

lização, dentre os quais se incluem as entidades sindicais representativas dos interesses dos próprios trabalhadores, inclusive por prerrogativa constitucional, na hipótese do inciso I do art. 7º da Lei nº 13.709 /18. Incide, na verdade, a hipótese do inciso II do mesmo dispositivo legal, qual seja, o cumprimento de obrigação legal ou regulatória.

Não se olvide que, a teor do estatuído no art. 399 do NCPC, a parte não pode escusar-se de exhibir documentos quando a eles referiu, no processo, com o intuito de constituir prova ou se estes, pelo seu conteúdo, forem comuns às partes e pertinentes à solução do litígio. Não exibidos, preceitua o art. 400 do mesmo diploma que serão considerados verdadeiros os fatos que, por intermédio dos mesmos, a outra parte pretendia provar. Em consequência, deixando a ré de anexar as provas documentais expressamente requeridas na petição inicial, inclusive após admitir a existência dos documentos, incide a presunção relativa de veracidade dos fatos descritos na causa de pedir.

Em que pese o inc. XXVI do art. 611-B da CLT, inserido pela Lei nº 13.467/17, assegure tanto a liberdade de associação profissional ou sindical do trabalhador quanto o direito de o mesmo não sofrer, sem sua expressa e prévia anuência, qualquer cobrança ou desconto salarial estabelecidos em convenção coletiva ou acordo coletivo de trabalho, a contribuição social em questão não incide sobre as folhas de pagamento dos empregados, ou seja, o custeio é integralmente atribuído às empresas empregadoras.

Dessarte, acolho as pretensões formuladas e condeno a reclamada ao cumprimento das normas coletivas que regulamentam o Plano Benefício Social Familiar, nos termos das convenções firmadas entre 2015 e 2020 (anexadas nos autos), atentando-se aos respectivos períodos de vigência, devendo recolher os valores referentes às mensalidades do Plano Benefício Social Familiar que estejam pendentes, a serem apuradas em liquidação de sentença a partir do rol de empregados em atividade a cada mês, de dezembro de 2015 ao final da vigência da convenção firmada em 2020.

Para tanto, a empresa deverá trazer ao feito os recibos de CAGED ou SEFIP do período, sob pena de que se presumam verdadeiras as informações prestadas pela Federação acerca do número de vínculos ativos por mês.

A reclamada alega que: 1) a redação do artigo 818, da Consolidação das Leis do Trabalho, em conjunto com a inteligência do artigo 373, do Código Civil, revela que o ônus probatório quanto ao fato constitutivo de seu direito incumbirá à reclamante; 2) o juízo de primeiro grau incorreu em erro ao considerar que caberia à recorrente apresentar documentos que evidenciam a regularidade da contribuição sindical, eis que claramente o ônus da prova é responsabilidade da reclamante e não da reclamada; 3) eventual cumprimento da decisão, que considerou necessária a apresentação das SEFIP e dos CAGE's, está em desconformidade com o artigo 7º, inciso I, da Lei 13.709/2018, reconhecida Lei Geral de Proteção de Dados, pois não há nos autos documento comprobatório da autorização expressa dos trabalhadores, permitindo o compartilhamento de seus dados particulares.

Requer seja reformada a sentença de primeiro grau, no sentido de ser julgado improcedente o pedido de condenação ao pagamento de 60 meses de Benefício Familiar Social.

Analiso.

Trata-se de ação de cumprimento de cláusulas de normas coletivas proposta em 26.11.2020 pela Federação dos Trabalhadores em Empresas de Asseio e Conservação, Limpeza Urbana e em Geral, Ambiental, Áreas Verdes, Zeladoria e Serviços Terceirizados no Estado do Rio Grande do Sul – FEEAC /RS (ID. b30fe69), por meio da qual pretende o cumprimento das Convenções Coletivas de Trabalho da categoria firmadas entre o SEEAC RS e o Sindicato das Empresas de Asseio e Conservação do Rio Grande do Sul nos anos de 2014 (cláusula 25ª), 2015 (cláusula 25ª), 2016 (cláusulas 24ª e 25ª), 2017 (cláusulas 24ª e 25ª), 2018 (cláusulas 22ª e 23ª), 2019 (cláusulas 22ª e 23ª) e 2020 (cláusula 23ª).

No caso, e tal qual decidido na origem, entendo que a instituição das cláusulas em questão não constitui ilegalidade, tampouco afronta a questão do ônus da prova suscitada pela ré como fundamento principal de seu recurso:

A questão acerca do pagamento de tal parcela já foi abordada em julgamentos desta 1ª Turma Julgadora, destacando-se o processo nº 0020497-37.2017.5.04.0702 (RO), do qual participei, e cujos fundamentos peço vênias para transcrever:

Trata-se de ação de cumprimento ajuizada pela Federação dos Trabalhadores em Empresas de Asseio e Conservação, Limpeza Urbana e em Geral, Ambiental, Áreas Verdes, Zeladoria e Serviços Terceirizados no Estado do Rio Grande do Sul - FEEAC/RS, cujo objetivo é a observância da cláusula normativa que prevê o recolhimento da contribuição social instituída para efetivar a viabilidade do "Plano de Benefício Social Familiar", prevista nas CCTs dos anos de 2014, 2015, 2016 e 2017.

A cláusula vigésima quinta da norma coletiva, CCT 2015, assim prevê (Id 3ac-d8dc - Págs. 7-9):

As entidades sindicais convenientes renovam, neste ato, o "PLANO DE BENEFÍCIO SOCIAL FAMILIAR" em favor de todos os empregados abrangidos pela presente convenção coletiva de trabalho, associados ou não do Sindicato Profissional, com intuito de proporcionar atendimento aos trabalhadores nos casos de falecimento ou incapacitação permanente para o trabalho do empregado, ou quando do nascimento de filho de empregado.

O plano continuará sendo administrado pela FEEAC/RS - Federação dos Empregados em Empresas de Asseio e Conservação do Estado do Rio Grande do Sul, sendo gerido por empresas especializadas que garantam o fiel cumprimento dos auxílios abaixo estabelecidos e que sejam previamente autorizadas em conjunto pela FEEAC/RS e o Sindicato das Empresas de Asseio e Conservação do Estado do Rio Grande do Sul. [...] 10) Para a efetiva viabilidade financeira deste "Plano de Benefício Social Familiar", e com o expresse consentimento das entidades convenientes, as empresas recolherão a título de contribuição social, até o dia 10 (dez) de cada mês, o valor de R\$ 8,46 (oito reais e quarenta e seis centavos) por trabalhador que possua, exclusivamente por meio de boleto disponibilizado pela gestora ou

sindicato profissional. [...] 11) Caso a empresa opte por uma prestação de serviço não gerida por entidade contratada pelos sindicatos, deverá, antes da contratação, encaminhar à FEEAC/RS minuta do contrato discriminando a forma de prestação dos serviços, cuja contratação deverá ser autorizada por escrito pela FEEAC/RS. [...]

Como visto, a contribuição refere-se à parcela a ser recolhida por todas as empresas da categoria econômica para o custeio de plano de benefícios em favor dos empregados em caso de morte ou incapacidade permanente para o trabalho, ou quando do nascimento de filho, sendo que o direito em questão é instrumentalizado pela Federação, que é a administradora do Plano de Benefício Social Familiar.

Pois bem. A própria norma coletiva prevê a possibilidade de que a empresa opte pela prestação do serviço por outra empresa que não seja contratada pelo sindicato, não obstante exija que seja encaminhada à Federação a minuta do contrato discriminando a forma de prestação do serviço, bem como seja obtida a autorização por escrito deste para contratação.

No caso dos autos, entretanto, a reclamada alega o fornecimento dos benefícios a seus empregados, conforme o seu entendimento, mas não comprova o cumprimento do disposto no item 11 da cláusula supra citada.

Assim, tendo em vista que a reclamada não demonstrou o efetivo cumprimento da norma coletiva em questão, merece ser mantida a condenação.

Na mesma linha, colaciono o recente julgado proferido pela 8ª Turma deste Tribunal, cujo excerto reproduzo e adoto como razões de decidir: [...] 2. PLANO DE BENEFÍCIO SOCIAL FAMILIAR. RECOLHIMENTO DA CONTRIBUIÇÃO PATRONAL. [...] Como já referido, trata-se de contribuição a ser paga por todas as empresas da categoria econômica para o custeio de plano de benefícios em favor dos empregados em caso de morte ou incapacidade permanente para o trabalho, ou quando do nascimento de filho, nos termos de cláusula normativa vertida nos seguintes termos: [...]

A matéria foi muito bem analisada em parecer do Ministério Público do Trabalho, da lavra do Exmo. Procurador do Trabalho Gilson Luiz Laydner de Azevedo, em processo envolvendo a mesma matéria, com cópia no ID. cc475da, cujos fundamentos adoto, in verbis: "Plano assistencial previsto em norma coletiva.

Alega a ré, em síntese, que o plano assistencial disponível a seus empregados é mais benéfico que aquele previsto em convenção coletiva de trabalho firmada entre os sindicatos das categorias profissional e econômica (objeto da presente ação de cumprimento). Contudo, a ré não demonstra este maior benefício.

Ao contrário, a convenção coletiva apresenta normas claras, objetivas, de fácil interpretação, com indicação dos valores a serem concedidos em cada hipótese de incidência. Ainda, a convenção não traz cláusulas condicionais, com limites de idade para adesão ou tipo de acidente segurado. Já o contrato de seguro de vida em grupo firmado pela reclamada, embora com valor de benefício aparentemente superior (ao indicar, como "capital segurado individual da Garantia Básica", a quantia de R\$ 6.000,00), não será sempre aplicado integralmente: há tabelas com

percentuais que incidirão conforme o tipo de invalidez sofrida. Ademais, tal contrato não prevê auxílio no caso de nascimento de filhos do empregado ou concessão de cestas básicas, como o faz a norma convencional.

Cumprido ressaltar que a cláusula da norma coletiva em discussão já foi objeto de inquérito civil, no âmbito do Ministério Público do Trabalho, tendo a Procuradora Regional do Trabalho Beatriz de Holleben Junqueira Fialho concluído:

A nova disposição normativa não prevê desconto salarial para custeio do Plano de Benefícios instituído pela CCT e, por outro lado, a negociação entre as partes não extrapola os limites da autonomia coletiva no que se refere ao percentual de participação do empregado no auxílio-alimentação, que, nos termos do art. 2º, § 1º, do Decreto nº 05 /1991, é limitada a 20%. (Promoção de Arquivamento exarada no Inquérito Civil nº IC 000955.2014.04.000/5).

Dessarte, as razões apresentadas pela federação autora, em especial, quanto à continuidade do plano ainda que a empregadora não aporte os recursos previstos para tanto, permitem concluir inexistir ao final e no geral, prejuízo aos trabalhadores, devendo, no mínimo, ser garantidos os mesmos benefícios previstos na norma coletiva, o que não se verifica na hipótese dos autos.

No que tange à liberdade de adesão do trabalhador à contribuição social e à inconstitucionalidade da cobrança compulsória, não há como concordar com a requerida, haja vista a inexistência de desconto dos salários dos trabalhadores. A elevação do limite do percentual de desconto do auxílio-alimentação, como contrapartida ao não desconto pela adesão ao plano ajustado, encontra-se nos limites legais de negociação entre as partes convenientes.

Não se olvide que a norma coletiva deve ser analisada na sua integralidade, já que se trata de negociação entre categorias com interesses imediatos distintos, havendo, como resultado do processo de negociação, naturais avanços e retrocessos.

Deve, pois, ser julgado procedente o pedido formulado na presente ação de cumprimento, a fim de que reste condenada a empresa ré (...) a cumprir a norma coletiva, nos termos em que firmada."

Com efeito, trata-se de norma coletiva em que os integrantes da categoria econômica concordaram, por meio de seu sindicato, a contribuir para o Plano de Benefício Social Familiar, em favor de seus empregados. A cláusula normativa em questão passou pelo crivo do Ministério Público do Trabalho, em inquérito civil, que concluiu pela sua validade.

De outro lado, não se trata, no presente processo, de contribuição a ser descontada dos trabalhadores, mas da contribuição das empresas vinculadas ao sindicato patronal, caso da recorrente, para o custeio do benefício. Não se aplicam, portanto, a orientação jurisprudencial 17 da SDI1 do TST e tampouco a súmula 666 do STF.

Ainda, de acordo com o item 11 da cláusula 25ª da convenção coletiva, transcrito acima, a empresa que optar por contratar benefício semelhante a ser prestado por outra entidade deverá submeter a minuta do contrato à Federação autora, que deverá autorizar por escrito a contratação. No caso presente, tal autorização não foi comprovada.

Por fim, a corroborar o entendimento ora adotado, merece transcrição o seguinte excerto do parecer lançado nos presentes autos (ID. 79a90e6), da lavra do Procurador Regional do Trabalho Leandro Araujo, in verbis: "Cumprimento de cláusula prevista em Convenção Coletiva. Plano Benefício Social Familiar.

No mérito, igualmente coaduna-se com o entendimento exposto pelo juízo singular, no sentido de que, uma vez inexistente controvérsia acerca da validade da Convenção Coletiva, já que o demandado se encontrava legitimamente representado pelo Sindicato patronal, signatário da convenção, que anuiu com o conteúdo da norma coletiva em toda sua extensão, inclusive em relação à Cláusula 25ª, objeto da presente ação, que prevê benefício social de caráter permanente, inexistente qualquer indício de ilegalidade que justifique a pretensão de nulidade suscitada pelo ora recorrente.

Note-se que as regras estabelecidas nas convenções coletivas de trabalho são de incidência obrigatória aos integrantes das categorias profissional e econômica representadas pelos sindicatos que formalizaram o acordo, independentemente de filiação a essas entidades.

Quanto ao argumento de que o reclamado fornecia o mesmo benefício assistencial, inclusive mais vantajoso, a seus empregados, sem qualquer custo, através de seguradora contratada, verifica-se, primeiro, que essa possibilidade dependeria de prévia aprovação pela Federação autora, como consta no Parágrafo Terceiro da citada Cláusula 25ª (ID 12ab8f3 - Pág. 11), requisito esse não atendido; segundo, não se identifica a suposta identidade de benefícios entre aquele previsto na norma coletiva e aquele contratado pela empresa. [...]

Por fim, quanto ao fato de a Convenção Coletiva de 2014 estipular que a empresa deveria recolher a contribuição social no valor de R\$ 7,77 por trabalhador, podendo descontar até R\$ 2,77 de cada um deles, e de a Convenção Coletiva de 2015 aumentar essa contribuição para R\$ 8,46, vedando, no entanto, o desconto dos empregados, mas aumentando a porcentagem do auxílio-alimentação descontado destes (de 15% para 17,5%), identifica-se que a matéria já foi analisada por este Órgão (tanto que acatada, na Convenção de 2015, a proposta de não mais persistir desconto dos trabalhadores), no Inquérito Civil nº 000955.2014.04.000/5, que decidiu pelo arquivamento do procedimento nos seguintes termos:

A nova disposição normativa não prevê desconto salarial para custeio do Plano de Benefícios instituído pela CCT e, por outro lado, a negociação entre as partes não extrapola os limites da autonomia coletiva no que se refere ao percentual de participação do empregado no auxílio-alimentação, que, nos termos do art. 2º, § 1º, do Decreto nº 05 /1991, é limitada a 20%.

Nos termos das razões expostas, não se identifica prejuízo aos trabalhadores com a implantação do Benefício Social Familiar, tampouco violação a norma legal, razão pela qual opinamos pelo não provimento ao recurso."

Nego provimento. (TRT da 4ª Região, 8ª Turma, 0020256-28.2015.5.04.0025 RO, em 22/06/2017, Desembargador João Paulo Lucena) - sublinhei

Por fim, não há falar em dedução dos valores já pagos, porquanto os emprega-

dos não podem ser penalizados pelo descumprimento da norma coletiva por parte da empregadora, relativamente ao período da condenação.

Diante do exposto, nego provimento ao recurso. (TRT da 4ª Região, 1ª Turma, 0020497-37.2017.5.04.0702 RO, em 13/07/2018, Desembargadora Lais Helena Jaeger Nicotti -Relator. Participaram do julgamento: Desembargadora Rosane Serafini Casa Nova; Desembargador Fabiano Holz Beserra)

A alegação que envolve o ônus da prova no presente não socorre a reclamada, pois existindo a obrigação normativa da reclamada contribuir para o custeio do plano assistencial previsto em sua norma coletiva, incumbia a esta a demonstração do cumprimento da obrigação ou a justificação em relação ao seu inadimplemento.

Embora a reclamada alegue a inexistência de prova de inadimplemento, não cumpriu seu ônus de comprovar o cumprimento das cláusulas coletivas objeto da presente ação de cumprimento, restando irreparável a sentença que a condenou ao recolhimento do valor total do plano Benefício Social Familiar que estiver em aberto desde a sua implementação, inclusive aqueles que venceram durante o trâmite processual e na vigência das normas.

Em relação ao fornecimento dos documentos necessários em relação aos empregados abrangidos pelo benefício, assim determina a norma coletiva (ID. ff4d380 - Pág. 10):

Convenção de 2016 - Cláusula Vigésima Quarta

(...)

2 (...) O empregador, sempre que solicitado pelo Sindicato Profissional ou pela gestora do Plano de Benefício Social Familiar, deverá apresentar outros documentos sob sua responsabilidade, como: cópia da ficha de registro e recibo do CAGED (Cadastro Geral de Empregados e Desempregados), informado ao Ministério do Trabalho e Emprego, necessários à continuidade da prestação dos benefícios, além dos documentos relativos ao arrimo/representante legal do trabalhador.

Como se vê, descabida a aplicação do disposto no art. 7º, inc. I, da Lei 13.709/2018, no que se refere ao fornecimento dos documentos necessários para a apuração das contribuições devidas no presente, já que como bem sublinhado pelo Magistrado da origem, o caso é de aplicação do disposto no art. 7º, inciso II, da referida lei, que prevê o fornecimento de dados pessoais no caso de "cumprimento de obrigação legal ou regulatória pelo controlador".

Assim, quanto ao pedido sucessivo de não fornecimento de documentos, referente à suposta vedação legal, indefiro, consoante fundamentos acima referidos e também pelo fato de que estes objetivam à apuração do quantum devido, o que visa concretizar o cumprimento da prestação jurisdicional e dentre outras coisas, visa a evitar o enriquecimento sem causa da parte autora.

Nada a prover.

III – PREQUESTIONAMENTO

Consideram-se prequestionados todos os dispositivos constitucionais e infra-constitucionais invocados pelo recorrente, ainda que não expressamente mencio-

nados na decisão, à luz da OJ nº 118 da SDI-1 do TST.

FABIANO HOLZ BESERRA

Relator

VOTOS

PARTICIPARAM DO JULGAMENTO:

DESEMBARGADOR FABIANO HOLZ BESERRA (RELATOR)

DESEMBARGADORA ROSANE SERAFINI CASA NOVA

DESEMBARGADORA LAÍS HELENA JAEGER NICOTTI

Assinado eletronicamente por: FABIANO HOLZ BESERRA - 10/08/2021
17:12:32 - 934a0e8

<https://pje.trt4.jus.br/segundograu/Processo/ConsultaDocumento/listView.seam?nd=21071521490483400000056838621>

ACÓRDÃO. TRT4. SINDICATO E LGPD.

DESEMBARGADORA BRÍGIDA JOAQUINA CHARÃO BARCELOS

Polo Ativo: SIND DOS TRABS NAS INDS DA CONSTR E DO MOB DE B GONCAL - Adv. Francisco Zimmermann de Almeida, Adv. PAULO SERGIO ALVES DE SOUZA

Polo Passivo: CAMPUS EMPREENDIMENTOS IMOBILIARIOS LTDA - Adv. Caroline Crescente Rubattino

E M E N T A

EMBARGOS DE DECLARAÇÃO. OMISSÃO. PREQUESTIONAMENTO. Caso em que não se verifica a ocorrência de nenhuma das hipóteses previstas no artigo 897-A da Consolidação das Leis do Trabalho, tampouco a anunciada necessidade de manifestação deste colegiado para fins de prequestionamento, tendo a Turma Julgadora adotado tese expressa acerca da matéria, objeto da presente ação.

A C Ó R D Ã O

Vistos, relatados e discutidos os autos. ACORDAM os Magistrados integrantes da 8ª Turma do Tribunal Regional do Trabalho da 4ª Região: à unanimidade, **NEGAR PROVIMENTO AOS EMBARGOS DECLARATÓRIOS DA RECLAMADA, EMBARGOS DE DECLARAÇÃO DA RECLAMADA. HONORÁRIOS DE ADVOGADO. OMISSÃO. PREQUESTIONAMENTO,** porém, tem-se por prequestionada a matéria.

Intime-se.

Porto Alegre, 26 de maio de 2021 (quarta-feira).

R E L A T Ó R I O

A reclamada opõe, tempestivamente, embargos de declaração (Id. 637ddf3), alegando a existência de vícios no julgado.

Regularmente processados, vêm os autos a julgamento.

É o relatório.

V O T O

DESEMBARGADORA BRÍGIDA JOAQUINA CHARÃO BARCELOS

(RELATORA):

EMBARGOS DE DECLARAÇÃO DA RECLAMADA

HONORÁRIOS DE ADVOGADO. OMISSÃO. PREQUESTIONAMENTO

Não se conforma a reclamada com a condenação ao pagamento de honorários de advogado, apontando omissão no acórdão. Alega que em contrarrazões requereu expressa manifestação quanto à aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n.º 13.709/18, bem como que reiterou que não houve pretensão resistida não justificada. Ainda, alega que os documentos que não envolviam dados sensíveis de seus empregados foram apresentados ao sindicato quando solicitado (Id. e9d6da6), bem como que os documentos resguardados pela LGPD, de fato, não foram disponibilizados em atendimento ao que dispõe a legislação específica. Por fim, alega que não pretende alteração do julgado, somente a manifestação sobre as questões trazidas em contrarrazões, ressaltando que se faz necessário o prequestionamento nos termos da Súmula n. 297 do TST.

Análise.

É cabível a interposição de embargos de declaração para atacar sentença ou acórdão em que seja necessário esclarecer obscuridade ou eliminar contradição, suprimir omissão de ponto ou questão sobre o qual deveria se pronunciar o Juiz de ofício ou a requerimento e, ainda, corrigir erro material (na forma dos incisos I, II e III do art. 1.022 do CPC), considerando omissa a decisão que "deixe de se manifestar sobre tese firmada em julgamento de casos repetitivos ou em incidente de assunção de competência aplicável ao caso sob julgamento", ou que incorra em uma das condutas descritas no art. 489, § 1º do CPC.

Nesta ótica, a importância deste recurso está no fato que seu único objetivo é o de postular esclarecimentos, complementação e correção de eventuais defeitos nas decisões judiciais, que comprometem sua utilidade. Não se verifica omissão ou contradição no julgamento recorrido, na forma prevista como hipótese ensejadora de oposição de embargos de declaração como descrito acima.

Ao contrário do que sugerido, o que se constata é o objetivo da embargante de obter a reforma do acórdão, à luz dos argumentos expendidos no seu recurso, pretendendo rediscutir a matéria, o que não se afigura cabível por meio do remédio processual escolhido. Portanto, não há omissão a ser sanada.

Independentemente do entendimento que se tenha sobre o acerto ou não da decisão proferida neste grau de jurisdição em face do recurso interposto, é certo que o acórdão enfrentou toda a matéria controvertida, nos termos da fundamentação lançada.

Ressalta-se, também, a ausência de omissão quando adotada tese explícita a respeito da matéria debatida. Como se sabe, por decisão fundamentada não se entende a necessidade de manifestação do Juízo sobre todos os argumentos e raciocínios lógicos jurídicos adotados pelas partes.

Dessa forma, em que pese a necessidade de oposição para efeitos de preques-

tionamento, conforme reza a Súmula nº 297 do TST, os embargos de declaração não constituem remédio processual com características recursais. Ressalta-se que o prequestionamento não se confunde com interpretação literal de dispositivo de lei, não estando o Julgador obrigado a manifestar-se sobre todos os argumentos e artigos de lei utilizados pela parte, mas a aplicar as normas do ordenamento jurídico incidente no caso, fundamentando o julgado no sentido de conferir plena prestação jurisdicional, sendo de ressaltar que esta Turma Julgadora adotou tese explícita a respeito da matéria.

Nesse sentido, a Orientação Jurisprudencial 118 da SDI-1 do Tribunal Superior do Trabalho: "Pquestionamento. Havendo tese explícita sobre a matéria, na decisão recorrida, desnecessário contenha nela referência expressa do dispositivo legal para ter-se como prequestionado este. Inteligência do Enunciado 297."

Ainda, como se sabe, por decisão fundamentada não se entende a necessidade de manifestação do Juízo sobre todos os argumentos e raciocínios lógico-jurídicos adotados pelas partes. Basta que ele torne clara a razão de decidir, explicitando a tese adotada, tal como, "data venia", se fez neste caso. Repita-se, não é obrigação do Juiz responder a simples perguntas sobre ter ou não a decisão violado a lei ou se esta deve prevalecer sobre os entendimentos jurisprudenciais. A função dos Juízos e dos Tribunais, nos embargos de declaração, não é responder aos questionários ou quesitos esclarecedores: a dúvida deixou de ser matéria de embargos de declaração. Acresça-se, a título de esclarecimento, que os embargos de declaração não se prestam para prequestionamento. Como já dito, servem apenas para provocar a complementação ou aperfeiçoamento formal de uma decisão jurisdicional sob algum aspecto obrigatório, trazido à baila no curso do processo, no momento e pela forma adequada, e que não tenha sido objeto de deliberação explícita do Juízo (omissão ou contradição).

É fato que a Súmula nº 297 do TST, que teve a sua redação revisada pela Resolução nº 121/2003 daquela mesma Corte, diz que se considera "prequestionada a matéria ou questão quando na decisão impugnada haja sido adotada, explicitamente, tese a respeito", incumbindo "à parte interessada, desde que a matéria haja sido invocada no recurso principal, opor embargos declaratórios objetivando o pronunciamento sobre o tema, sob pena de preclusão", bem como que se considera "prequestionada a questão jurídica invocada no recurso principal sobre a qual se omite o Tribunal de pronunciar tese, não obstante opostos embargos de declaração". Entretanto, é de se interpretar que o TST diz que o prequestionamento é essencial e desafia embargos de declaração quando houver omissão de questão que o Juiz era obrigado a se manifestar e não o fez. Não se pode entender que, jurisprudencialmente, tenha sido criada uma nova situação de adequabilidade para os embargos de declaração, o que, evidentemente, extrapolaria a competência do Poder Judiciário.

Além do mais, os embargos de declaração não são remédio processual destinado à nova decisão de questões abordadas e decididas. Insatisfeita a parte, resta-lhe outro caminho processual a seguir.

Pelo exposto, nego provimento aos embargos de declaração da reclamada, porém tenho por prequestionada a matéria.

**SENTENÇA. NEGATIVA DE ACESSO A DADOS PESSOAIS
TRATADOS (ART. 9º DA LGPD).**

JUIZ PAULO ROBERTO DORNELLES JUNIOR

Juiz do Trabalho do TRT da 4ª Região. Mestre em Direito pela Universitat Pompeu Fabra. Mestrando em Relações Internacionais pela Universidade Federal de Santa Maria.

ATOrd 0020023-18.2021.5.04.0802

RECLAMANTE: MARCIO DO AMARAL SANTOS

RECLAMADA: OPEN TECH SISTEMAS DE GERENCIAMENTO DE RISCOS S/A

S E N T E N Ç A

I - RELATÓRIO

Postula a parte reclamante, em suma, provimento jurisdicional para impedir que a reclamada restrinja seu direito ao trabalho.

A reclamada é revel e confessa quanto à matéria fática.

Produzida prova documental, é encerrada a instrução.

Razões finais remissivas.

Propostas de conciliação prejudicadas.

Instado, o reclamante informa ter interesse na manutenção da presente demanda em face da demanda coletiva.

É o breve relatório.

II - FUNDAMENTAÇÃO

DIREITO INTERTEMPORAL

A aplicação da Lei 13.467/17 é imediata, sem atingir, no entanto, situações pretéritas iniciadas ou consolidadas sob a égide da lei revogada (art. 1º da IN TST 41/2018).

As disposições relativas à justiça gratuita (art. 790, §§ 3º e 4º da CLT), honorários advocatícios sucumbenciais (art. 791-A da CLT) e periciais (art. 790-B da CLT), com as alterações dadas pela Lei 13.467/17, são constitucionais e não ofendem ao art. 5º, incisos XXXV e LXXXIV da CF/88. Cabe ao legislador infraconstitucional delimitar o alcance da garantia constitucional do acesso à justiça e assistência jurídica. Não há incompatibilidade com as normas constitucionais.

As normas relativas aos honorários advocatícios (art. 6º da IN TST nº 41/2018) e periciais (art. 10 da IN TST 41/2018) são inteiramente aplicáveis aos processos propostos após a data de 11/11/2017.

As disposições de direito material, com as alterações da Lei 13.467/17, são aplicáveis, após 11/11/2017, integralmente aos contratos de trabalho em curso, respei-

tadas as situações já consolidadas conforme a lei anterior (art. 5º, XXXVI da CF).

PRELIMINARES

COMPETÊNCIA MATERIAL

A parte reclamante refere que haveria competência material da Justiça do Trabalho porque “a presente demanda versa acerca de cessação de restrição ao exercício de trabalho pelo reclamante, com ameaça concreta de perda do emprego em virtude da conduta ilícita da reclamada, bem como indenização por danos morais, tendo como causa de pedir a clara violação ao direito ao trabalho (art. 5º, inciso XIII c/c art. 6º, ambos da Constituição Federal), pelo que configurada a competência material da Justiça do Trabalho ex vi do art. 114, incisos I, VI, e IX, da Carta Magna de 1988”.

Complementando que: “atividade desenvolvida pela reclamada de “varredura” da vida pessoal dos motoristas profissionais, com pesquisa de dados protegidos pelo direito fundamental à intimidade (art. 5º, X, da Constituição Federal), com a negativa liberação do autor para realizar o carregamento de carga, acaso não cessada, acarretará a perda do emprego.

Portanto não se trata de mera atividade econômica que atinge de forma eventual e indireta a relação de emprego, mas de atos ilícitos que afetam de forma direta o contrato de trabalho, razão pela qual os danos decorrentes de tais atos praticados inserem-se na competência material da Justiça do Trabalho ex vi do art. 114, I, VI e IX, da Constituição Federal”.

A parte reclamada é revel.

Analisando.

Competência é o pressuposto processual de validade que atua como limitação legal ao exercício da jurisdição. Deve ser definida pela natureza da relação jurídica, indicada pela causa de pedir e pedidos.

No caso, há competência material da Justiça do Trabalho, nos termos do art. 114, I da CLT. Embora não exista relação de trabalho direta entre o reclamante e a reclamada, a conduta desta afeta diretamente o contrato de emprego ao impedir acesso ao mercado de trabalho. Presente, portanto, a competência material desta Justiça especializada para a causa.

Apenas ponto que negar a competência trabalhista no presente contexto colocaria o reclamante em situação de obstrução de acesso à justiça. Não poderia ajuizar ação em face de sua empregadora para dispensar as exigências discriminatórias, pois não é ela quem as pratica. Não poderia discutir na Justiça Comum as condições do contrato de seguro celebrado entre sua empregadora e a seguradora, por lhe faltar legitimidade e não ser parte no acordo (art. 17 do CPC). Esta situação atentaria contra a garantia constitucional de livre acesso à justiça (art. 5º, XXXV).

Os reflexos do contrato entre empregadora e seguradora na relação de emprego devem, portanto, ser discutidos na Justiça do Trabalho conforme art. 114, I da CF. Cito a título meramente ilustrativo julgados recentes do C. TST:

"RECURSO DE REVISTA INTERPOSTO NA VIGÊNCIA DA LEI Nº

13.015/2014. COMPETÊNCIA DA JUSTIÇA DO TRABALHO. FASE PRÉ-PROCESSUAL. MOTORISTA QUE TEVE O NOME INCLUÍDO EM "LISTA DE RISCO" POR SEGURADORAS. INFORMAÇÕES DESABONADORAS A POSSÍVEIS EMPREGADORAS. ACESSO AO MERCADO DE TRABALHO RESTRINGIDO. INDENIZAÇÃO POR DANOS MORAIS. Cinge-se a controvérsia a decidir se a Justiça do Trabalho é competente para examinar pretensão de pagamento de indenização por dano moral em face de empresas seguradoras que incluíram o nome do trabalhador, motorista profissional, em "lista de risco", emitindo informações desabonadoras para as empresas transportadoras, dificultando, assim, sua inserção no mercado de trabalho. No caso, o Regional, acolhendo preliminar arguida pela primeira reclamada, declarou a incompetência absoluta desta Justiça especializada para examinar a matéria, pois concluiu que, "ainda que não haja qualquer condicionamento a essa competência, uma vez que podem subsistir demandas em que não seja o empregador integrante do polo passivo da demanda judicial trabalhista, sendo a hipótese prevista no inciso IX, do art. 114, entendo que tal abrangência não se adequa ao presente caso. A ação indenizatória proposta em face das seguradoras/corretoras das transportadoras de carga que o autor sequer foi empregado é de competência da Justiça Comum, por se tratar de demanda de natureza exclusivamente civil". A competência da Justiça do Trabalho, ampliada pela EC nº 45/2004, abrange as relações de emprego e também as de trabalho, com suas lides conexas, nos termos do artigo 114, incisos I a IX, da Constituição Federal. Não atinge, porém, relações de natureza jurídico-administrativo, tampouco as relações de consumo. Constata-se que o caso em exame assemelha-se ao de dano ocorrido na fase pré-contratual, tendo em vista a causa de pedir, qual seja a existência de conduta discriminatória por parte das reclamadas, que, ao fornecer informações desabonadoras sobre o reclamante, acabam por restringir seu acesso ao mercado de trabalho. E, em razão dessa prática, foi formulado pedido de indenização por dano moral. Com efeito, as consequências que essas informações desabonadoras têm, prestadas para empregadores em potencial (relações de trabalho), inserem, indiscutivelmente, o caso dos autos na competência da Justiça do Trabalho. Observa-se que a conduta das reclamadas está consubstanciada na forma discriminatória com que procederam, pois visa à inibição da prestação de serviços dos motoristas que figurem em suas listas cadastrais. A prática da conduta discriminatória em apreço importa ofensa a princípios de ordem constitucional, tais como o da dignidade da pessoa humana, do valor social do trabalho, da isonomia e da não discriminação. Nesse contexto, conclui-se que a inclusão do nome do trabalhador em "lista de risco", confeccionada pelas seguradoras ré e entregue a possíveis empregadores, não afasta a competência desta Justiça especializada, pois o ato ilícito guarda relação direta com relações de trabalho. Precedentes. Recurso de revista conhecido e provido" (RR-83-60.2015.5.17.0141, 2ª Turma, Relator Ministro Jose Roberto Freire Pimenta, DEJT 27/09/2019)".

MÉRITO

REVELIA E CONFISSÃO FICTA

Decretada a revelia e a confissão sobre a matéria fática (art. 844, CLT), prevalece a versão dos fatos declinada na petição inicial.

A confissão ficta não se aplica, no entanto, nas hipóteses do art. 844, §1º da CLT: I - havendo pluralidade de reclamados, algum deles contestar a ação; II - o litígio versar sobre direitos indisponíveis; III - a petição inicial não estiver acompanhada de instrumento que a lei considere indispensável à prova do ato; IV - as alegações de fato formuladas pelo reclamante forem inverossímeis ou estiverem em contradição com prova constante dos autos.

RESTRIÇÃO DO DIREITO AO TRABALHO

O reclamante refere ser “motorista, laborando com o transporte internacional de cargas, sendo que atualmente exerce a sua função na empresa Veiga & Santos Importação, Exportação de Hortifrutigranjeiros, Cereais e Transportes Ltda – doc. Anexo”.

Acrescenta que “referida empresa realiza o transporte internacional de produtos da empresa SEARA, sendo que o contrato de seguro de cargas exige a avaliação dos riscos pela empresa Open Tech Sistemas de Gerenciamento de Riscos S/A. Nesta atividade de gerenciamento de riscos, a reclamada realiza a avaliação do perfil do motorista e o autoriza ou não a realizar o transporte da carga. Sabidamente a demandada se utiliza de critérios ilegais e que violam o direito fundamental ao trabalho do reclamante (art. 6º da Constituição Federal), como a utilização de dados sigilosos de banco de cadastro de restrição ao crédito (SPC, SERASA), da Receita Federal, de processos cíveis e criminais sem sentença transitada em julgado e até de inquéritos policiais sem qualquer indiciamento”.

A situação teria sido reconhecida na ação civil pública ajuizada pelo SINDI-MERCOSUL (processo nº 0000241-06.2013.5.04.0802), segundo a inicial com decisão favorável pela 2ª Turma do TRT4.

A reclamada não teria autorizado o reclamante a transportar cargas na operação SEARA, o que acarretará a perda do emprego do reclamante caso não seja revertido.

O empregado não possuiria antecedentes criminais e a empresa se negaria a fornecer as razões pelas quais não foi liberado o seu perfil.

A reclamada é revel e confessa quanto à matéria fática.

Análise.

A jurisprudência desta Corte e do C. Tribunal Superior do Trabalho consolidou-se favoravelmente à tese do reclamante. A restrição imposta pela seguradora ao desautorizar o transporte da carga pelo reclamante, sem informar as razões para tal, abre margem para toda sorte de discriminação no trabalho, o que viola os arts. 5º, V e X da CF, a Convenção 111 da OIT e o art. 1º da Lei 9029/95.

Ademais, a negativa da empresa em fornecer acesso da parte reclamante aos dados pessoais tratados viola os arts. 5º, X; 6º, IV e art. 9º da LGPD. Ao empregado é negado direito a ter conhecimento das razões pelas quais é negado o direito ao trabalho, em ofensa ao art. 6º da CF.

Nesse sentido, a jurisprudência em formação no TST:

"RECURSO DE REVISTA INTERPOSTO SOB A ÉGIDE DO CPC/2015 E DA IN Nº 40/2016 DO TST. MOTORISTA DE CARGAS. EMPRESA QUE REPASSA INFORMAÇÕES ORIUNDAS DE BANCO DE DADOS DE DOMÍNIO PÚBLICO. INDENIZAÇÃO POR DANO MORAL. ATO ILÍCITO CONFIGURADO. Trata-se de ação de indenização por danos morais decorrentes do impedimento do demandante de realizar o trabalho de carregamento de mercadorias, em razão de informações prestadas e compartilhadas pelas rés advindas de cadastros informativos sobre a idoneidade de motoristas a serem contratados para transporte de cargas. O Regional consignou que o fato de as ora agravadas prestarem e compartilharem informações de domínio público às empresas que contratavam motoristas não seria suficiente para a condenação em danos morais, notadamente pela ausência da prática de ato ilícito. Ao contrário do decidido pela Corte de origem, observa-se que a conduta das reclamadas está consubstanciada na forma discriminatória com que procederam, pois visa à inibição da prestação de serviços dos motoristas que figurem em suas listas cadastrais. A prática da conduta discriminatória em apreço importa em ofensa a princípios de ordem constitucional, tais como o da dignidade da pessoa humana, do valor social do trabalho, da isonomia e da não discriminação. Esclarece-se que o dano moral de ordem íntima prescinde de prova da sua ocorrência em virtude de ele consistir em ofensa a valores humanos, bastando a demonstração do ato ilícito ou antijurídico, em função do qual a parte afirma tê-lo sofrido, por ser *in re ipsa*, ou seja, decorre do próprio evento danoso, não havendo falar em demonstração do dano, pois, nesse caso, ele se situa no psicológico do lesado, em que é impossível se extrair uma prova material (precedentes). Recurso de revista conhecido e provido " (RR-83-60.2015.5.17.0141, 2ª Turma, Relator Ministro Jose Roberto Freire Pimenta, DEJT 13/11/2020).

"RECURSO DE REVISTA INTERPOSTO NA VIGÊNCIA DA LEI Nº 13.015/2014. COMPETÊNCIA DA JUSTIÇA DO TRABALHO. FASE PRÉ-PROCESSUAL. MOTORISTA QUE TEVE O NOME INCLUÍDO EM "LISTA DE RISCO" POR SEGURADORAS. INFORMAÇÕES DESABONADORAS A POSSÍVEIS EMPREGADORAS. ACESSO AO MERCADO DE TRABALHO RESTRINGIDO. INDENIZAÇÃO POR DANOS MORAIS. Cinge-se a controvérsia a decidir se a Justiça do Trabalho é competente para examinar pretensão de pagamento de indenização por dano moral em face de empresas seguradoras que incluíram o nome do trabalhador, motorista profissional, em "lista de risco", emitindo informações desabonadoras para as empresas transportadoras, dificultando, assim, sua inserção no mercado de trabalho. No caso, o Regional, acolhendo preliminar arguida pela primeira reclamada, declarou a incompetência absoluta desta Justiça especializada para examinar a matéria, pois concluiu que, " ainda que não haja qualquer condicionamento a essa competência, uma vez que podem subsistir demandas em que não seja o empregador integrante do polo passivo da demanda judicial trabalhista, sendo a hipótese prevista no inciso IX, do art. 114, entendo que tal abrangência não se adequa ao presente caso. A ação indenizatória proposta em face das seguradoras/corretoras das transportadoras de carga que o autor

sequer foi empregado é de competência da Justiça Comum, por se tratar de demanda de natureza exclusivamente civil". A competência da Justiça do Trabalho, ampliada pela EC nº 45/2004, abrange as relações de emprego e também as de trabalho, com suas lides conexas, nos termos do artigo 114, incisos I a IX, da Constituição Federal. Não atinge, porém, relações de natureza jurídico-administrativo, tampouco as relações de consumo. Consta-se que o caso em exame assemelha-se ao de dano ocorrido na fase pré-contratual, tendo em vista a causa de pedir, qual seja a existência de conduta discriminatória por parte das reclamadas, que, ao fornecer informações desabonadoras sobre o reclamante, acabam por restringir seu acesso ao mercado de trabalho. E, em razão dessa prática, foi formulado pedido de indenização por dano moral. Com efeito, as consequências que essas informações desabonadoras, prestadas para empregadores em potencial (relações de trabalho), inserem, indiscutivelmente, o caso dos autos na competência da Justiça do Trabalho. Observa-se que a conduta das reclamadas está consubstanciada na forma discriminatória com que procederam, pois visa à inibição da prestação de serviços dos motoristas que figurem em suas listas cadastrais. A prática da conduta discriminatória em apreço importa ofensa a princípios de ordem constitucional, tais como o da dignidade da pessoa humana, do valor social do trabalho, da isonomia e da não discriminação. Nesse contexto, conclui-se que a inclusão do nome do trabalhador em "lista de risco", confeccionada pelas seguradoras e entregue a possíveis empregadores, não afasta a competência desta Justiça especializada, pois o ato ilícito guarda relação direta com relações de trabalho. Precedentes. Recurso de revista conhecido e provido" (RR-83-60.2015.5.17.0141, 2ª Turma, Relator Ministro Jose Roberto Freire Pimenta, DEJT 27/09/2019).

No mesmo sentido é a jurisprudência desta E. Corte:

“COMPETÊNCIA DA JUSTIÇA DO TRABALHO. EMPRESA SEGURADORA DE CARGAS. MOTORISTA. INSCRIÇÃO EM CADASTRO DE DEVEDORES. ANTECEDENTES JUDICIAIS. RESTRIÇÃO DE TRANSPORTE. OFENSA AO DIREITO DE ACESSO AO TRABALHO. ARTIGO 114, VI, DA CF. O art. 114 da CF, alterado pela Emenda Constitucional 45/2004, ampliou a competência da Justiça Trabalhista, em razão da matéria, para julgar ações referentes às relações de trabalho e não apenas as relações que envolvam vínculo de emprego, previstas na CLT. Ainda, o inciso VI deste artigo expressamente fixou a competência da Justiça do Trabalho para julgar ações de indenização por dano moral ou patrimonial oriundas da relação de trabalho. No caso, em que pese não exista relação de emprego entre o autor e a ré, a alegação de que a reclamada estaria interferindo, de forma ilegal e inconstitucional na relação de trabalho do autor, em face de exigências de caráter discriminatório para a atuação dos motoristas no transporte de cargas, de modo a impedir seu direito ao trabalho pleno, atrai a competência desta Especializada.

(TRT da 4ª Região, 5ª Turma, 0020107-95.2020.5.04.0012 ROT, em 10/03/2021, Desembargador Manuel Cid Jardim)”

Há precedente, inclusive, específico em desfavor da reclamada, em sede de

ação civil pública:

“EMENTA AÇÃO CIVIL PÚBLICA. EMPRESAS GERENCIADORAS DE RISCO E EMPRESAS SEGURADORAS. BANCO DE DADOS. MOTORISTAS TRANSPORTE CARGA INTERNACIONAL. INFORMAÇÕES CADASTRAIS SOBRE RESTRIÇÕES CREDITÍCIAS, INQUÉRITOS POLICIAIS E PROCESSOS COM DECISÕES NÃO TRANSITADAS EM JULGADO. DISCRIMINAÇÃO. Prova indicativa de que a criação e manutenção do banco de dados pelas demandadas voltadas para a área de gerenciamento e avaliação de riscos com atuação no transporte rodoviário de cargas, em atenção às exigências das empresas seguradoras, considerada a sua amplitude, provocam atitude discriminatória na seleção e manutenção no trabalho de motoristas para atuar no transporte da carga, pela existência de resultados positivos quanto à restrição creditícia ou dívidas, antecedentes criminais e processos judiciais não transitados em julgado”.

(TRT da 4ª Região, 2ª Turma, 0000241-06.2013.5.04.0802 ROT, em 23/09/2020, Juiz Convocado Carlos Henrique Selbach).

Em respeito à jurisprudência sólida a respeito da matéria, julgo procedente o pedido para determinar que a reclamada abstenha-se de repassar, utilizar ou restringir o direito fundamental ao trabalho do reclamante com base em dados constantes de cadastros de restrição ao crédito (SPC e SERASA), situação fiscal perante a Receita Federal, boletins de ocorrência e inquéritos policiais, processos criminais e cíveis sem sentença transitada em julgado.

Em relação à tutela inibitória, inadequada a fixação de multa diária, conforme pedido na inicial, visto que o fornecimento da informação é ato ilícito que possui efeitos continuados. Ou seja, com sua prática, mesmo que em ato único, os efeitos lesivos prolongam-se no tempo por prazo indeterminado, visto que a empregadora, de posse das informações, pode dispensar sem justa causa, nunca mais admitir ou compartilhar informações sobre a parte reclamante com terceiros.

Dessa forma, em observância ao art. 497, parágrafo único do CPC, fixo multa de R\$ 10.000,00 (dez mil reais) para cada descumprimento da tutela específica deferida, sem prejuízo do conhecimento de novo pedido de dano moral em ação própria.

DANO MORAL

O reclamante refere que a conduta da reclamada teria restringido de forma ilegal seu direito ao trabalho, violado sua intimidade e privacidade, o que causaria dano moral *in re ipsa*. Postula a “condenação ao pagamento de indenização equivalente a R\$ 45.368,80 (quarenta e cinco mil trezentos e sessenta e oito reais e oitenta centavos)”.

Analiso.

Dano moral é aquele que atinge a honra, intimidade, imagem e dignidade do ofendido, atentando contra seu direito de personalidade (art. 5º, incisos V e X da CF). Provoca dor, sofrimento e angústia, sentimentos que são presumidos (“*in re ipsa*”).

No caso, o reclamante comprovou o fornecimento de informações desabona-

doras pela parte reclamada (ID. c8d7f7f - Pág. 1), que, além de lhe constranger perante a empregadora, colocaram em risco sua permanência no emprego.

Desse modo, considerando os parâmetros do art. 223-G da CLT, fixo indenização no montante de R\$ 5.000,00 (cinco mil reais) pelos danos morais causados.

TUTELA PROVISÓRIA DE URGÊNCIA

O reclamante postula “a concessão de medida liminar de tutela de urgência de natureza antecipada, em caráter inaudita altera parte, consistente em determinar que a reclamada se abstenha de repassar, utilizar ou restringir o direito fundamental ao trabalho do reclamante com base em dados constantes de cadastros de restrição ao crédito (SPC e SERASA), situação fiscal perante a Receita Federal, boletins de ocorrência e inquéritos policiais, processos criminais e cíveis sem sentença transitada em julgado, sob pena de aplicação de multa-diária consistente em R\$ 500,00, com fulcro no art. 300, caput c/c art. 297, caput, ambos do CPC”;

Analiso.

O art. 300 do CPC dispõe que “a tutela de urgência será concedida quando houver elementos que evidenciem a probabilidade do direito e o perigo de dano ou o risco ao resultado útil do processo”.

No caso, a probabilidade do direito está no e-mail juntado pelo reclamante à ID. c8d7f7f - Pág. 1, além de a reclamada ser revel e confessa quanto à matéria fática.

O perigo de dano está na possibilidade de dispensa iminente do reclamante caso a reclamada continue se negando a segurar as cargas que ele transporte sem apresentar qualquer justificativa plausível para tal.

Dessa forma, concedo, nos termos do art. 300 do CPC, tutela provisória de urgência antecipada para determinar que a reclamada se abstenha de repassar, utilizar ou restringir o direito fundamental ao trabalho do reclamante com base em dados constantes de cadastros de restrição ao crédito (SPC e SERASA), situação fiscal perante a Receita Federal, boletins de ocorrência e inquéritos policiais, processos criminais e cíveis sem sentença transitada em julgado.

Fixo multa de R\$ 10.000,00 (dez mil reais) para cada descumprimento comprovado em Juízo.

JUSTIÇA GRATUITA

Defiro à parte reclamante o benefício da justiça gratuita, considerando que declarou a percepção de salário inferior ao limite do art. 790, §3º da CLT (R\$ 2.440,42) e a CTPS juntada à ID. c8d7f7f - Pág. 3.

HONORÁRIOS ADVOCATÍCIOS

Considerando que não houve sucumbência integral da parte reclamante em nenhum pedido (art. 86, parágrafo único do CPC c/c Súmula 326 do STJ), arbitro os honorários advocatícios dos procuradores da parte reclamante em R\$ 2.250,00 (dois mil, duzentos e cinquenta reais).

Foram considerados no montante os parâmetros do art. 791-A da CLT, a natureza da tutela inibitória deferida (astreintes de R\$ 10.000,00), o dano moral fixado (R\$ 5.000,00) e o percentual legal (5-15%).

DESCONTOS PREVIDENCIÁRIOS E FISCAIS

Dispensados os descontos fiscais e previdenciários em razão da natureza da condenação.

CORREÇÃO MONETÁRIA E JUROS

Juros e correção monetária na forma da lei, sendo a fixação de critérios relegada à fase de liquidação de sentença.

PRAZO E CONDIÇÕES DE CUMPRIMENTO

Cumpra-se após o trânsito em julgado.

REQUISITOS DA SENTENÇA

Embargos de declaração opostos pelas partes sem fundamento legal e com objetivo de alterar o julgado possuem caráter protelatório, atraindo as penalidades cabíveis.

III - DISPOSITIVO

Ante o exposto, nos termos da fundamentação, que integra o presente dispositivo, decido:

1) Determino que a reclamada se abstenha de repassar, utilizar ou restringir o direito fundamental ao trabalho do reclamante com base em dados constantes de cadastros de restrição ao crédito (SPC e SERASA), situação fiscal perante a Receita Federal, boletins de ocorrência e inquéritos policiais, processos criminais e cíveis sem sentença transitada em julgado. Fixo multa de R\$ 10.000,00 (dez mil reais) para cada descumprimento da tutela específica deferida, sem prejuízo do conhecimento de novo pedido de dano moral em ação própria;

2) Condene a parte reclamada a pagar à parte reclamante indenização no montante de R\$ 5.000,00 (cinco mil reais) pelos danos morais causados;

3) Concedo, nos termos do art. 300 do CPC, tutela provisória de urgência antecipada para determinar que a reclamada se abstenha de repassar, utilizar ou restringir o direito fundamental ao trabalho do reclamante com base em dados constantes de cadastros de restrição ao crédito (SPC e SERASA), situação fiscal perante a Receita Federal, boletins de ocorrência e inquéritos policiais, processos criminais e cíveis sem sentença transitada em julgado. Fixo multa de R\$ 10.000,00 (dez mil reais) para cada descumprimento comprovado em Juízo;

4) Arbitro os honorários advocatícios dos procuradores da parte reclamante em R\$ 2.250,00 (dois mil, duzentos e cinquenta reais);

Defiro à parte reclamante os benefícios da justiça gratuita.

Custas pela parte reclamada no valor de R\$ 300,00, calculadas sobre o valor provisório da condenação (R\$ 15.000,00).

Cumpra-se após o trânsito em julgado, à exceção da medida liminar, cujo cumprimento é imediato.

Notifiquem-se as partes.

Nada mais.

SENTENÇA. DADOS PESSOAIS E PROCESSO JUDICIAL ELETRÔNICO.

JUIZ MAX CARRION BRUECKNER

Juiz do Trabalho Substituto, TRT da 4ª Região

Vistos.

A reclamante aduz, no item 3 dos requerimentos, que “firma declaração anexa com o escopo que o cadastro do presente dissídio seja feito exclusivamente com as iniciais da autora e da parte ré, assim requer a esse MM. Juízo com base na Constituição Federal de 1988 e pelo artigo 7º da Lei 13.709, de 14 de agosto de 2019, o cadastro da parte autora no sistema na forma supra requerida”.

De acordo com o art. 5º, LX, da Constituição, “a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem”. A regra, portanto, é a publicidade dos atos processuais.

Todavia, a fim de evitar a consulta de processos pelo nome dos reclamantes e a formação de listas identificando aqueles que buscaram a tutela do Poder Judiciário, a Resolução CNJ nº 121/2010 dispõe que a consulta pública, na Justiça do Trabalho, será restrita ao número do processo, nome dos advogados e número do registro na OAB (art. 4º, § 1º) – o que é observado no âmbito do TRT da 4ª Região. Portanto, os dados da parte autora já estão devidamente protegidos.

O art. 7º da LGPD em nada altera essa sistemática, uma vez que o consentimento do titular não é exigido no caso de processo judicial (art. 11, II, “d”, da LGPD).

Todavia, no documento de ID f110354, a autora manifesta o desejo inequívoco de litigar sem ser identificada, afirmando que não autoriza “a publicação, veiculação ou distribuição” de seus dados pessoais, em especial o nome, “junto à rede mundial de computadores (INTERNET), em qualquer site”. Assim, levando em consideração que os processos na Justiça do Trabalho são eletrônicos, impõe-se a extinção do processo, sem resolução do mérito, nos termos do art. 485, IV, do CPC.

Ante o exposto, extingo o processo sem resolução do mérito. Custas de R\$ 1.239,91, pela parte autora, dispensadas, uma vez que sequer houve a citação da parte adversa. Arquite-se após o trânsito em julgado.

Intime-se.

PORTO ALEGRE/RS, 05 de abril de 2021.

SENTENÇA. LGPD E EXIBIÇÃO DE DOCUMENTOS.

JUIZ MAURICIO DE MOURA PEÇANHA

Juiz do Trabalho do TRT da 4ª Região

Sentença: 0020746-18.2020.5.04.0561

Vara: Vara Do Trabalho De Carazinho

JOSE IGNACIO DA SILVA ajuíza, em 27/10/2020, ação de produção antecipada de provas contra E. ORLANDO ROOS COMERCIO DE CEREAIS LTDA, postulando a exibição de documentos, com pedido de tutela de urgência, com fixação de multa por descumprimento, além do pagamento de honorários de sucumbência. Atribui à causa o valor de R\$20.000,00.

Os autos vêm conclusos para julgamento.

É o relatório.

ISTO POSTO

O autor postula a exibição de documentos que comprovem o valor dos salários dos trabalhadores da função Operador de Máquinas – Carregadeira e Empilhadeira, aduzindo que o reclamante recebia salário inferior ao dos colegas que ocupavam o mesmo cargo. Refere, também, que tais documentos são necessários para verificação de seu direito.

Com relação aos trabalhadores da mesma função, que sequer foram identificados, seja pelo nome ou local de trabalho, a postulação encontra óbice no direito à privacidade, tutelado pela Constituição e pela Lei 13.709/18, não sendo possível a divulgação de tais dados, principalmente na forma generalizada pretendida. Determinar a entrega de documentos nesse caso implica em expor dados de terceiros estranhos à relação havida entre o autor e a demandada.

Com relação à assertiva que os documentos postulados se destinam à verificação do direito, registro que não se admite ação para investigação de direito ou postulação em tese, ainda mais por considerar que o próprio autor já afirma que seu salário era inferior ao dos demais.

Ante o exposto, extingo o processo sem resolução do mérito, nos termos do art. 485, VI, do CPC.

Custas de R\$400,00, calculadas sobre o valor dado à causa, atribuídas ao autor das quais fica dispensado do recolhimento em face do benefício da justiça gratuita que ora lhe defiro.

Não há honorários advocatícios a serem deferidos, eis que a ação resta extinta, não havendo sucumbência.

Intime-se a parte autora.

Arquive-se os autos após o trânsito em julgado.

CARAZINHO/RS, 29 de outubro de 2020.

MAURICIO DE MOURA PEÇANHA

Juiz do Trabalho Titular

SENTENÇA. PROTEÇÃO DE DADOS DE PESSOA JURÍDICA. INAPLICABILIDADE.

JUÍZA LINA GORCZEWSKI

Juíza do Trabalho do TRT da 4ª Região

Sentença: 0020058-49.2021.5.04.0261

Vara: Vara Do Trabalho De Montenegro

Autora: SIMONE GABRIELA RITTER

Ré: SOLAR COMERCIO E AGROINDUSTRIA LTDA.

Dispensado o relatório nos termos do art. 852-I da CLT. Decido.

PRELIMINARMENTE

Aplicação da Lei 13.467/17

Dada a grande controvérsia criada com a vigência da Lei 13.467/2017, a partir de 11-11-17, que alterou, cancelou e introduziu diversos dispositivos à CLT, cumpro esclarecer algumas questões:

Em relação às regras de direito material, aplica-se o disposto no art. 6º da Lei de Introdução ao Código Civil, que diz que “A Lei em vigor terá efeito imediato e geral, respeitados o ato jurídico perfeito, o direito adquirido e a coisa julgada”. Portanto, as normas de direito material alteradas pela Lei 13.467/17 aplicam-se imediatamente aos contratos de trabalho em curso à data de sua vigência, de forma não retroativa, respeitados os atos jurídicos já consumados segundo a lei vigente ao tempo em que se efetuaram (parágrafo 1º do mesmo artigo).

Em relação às regras de direito processual, aplica-se o disposto no art. 14 do CPC, que diz que “A norma processual não retroagirá e será aplicável imediatamente aos processos em curso, respeitados os atos processuais praticados e as situações jurídicas consolidadas sob a vigência da norma revogada.” Portanto, aplicam-se as normas de direito processual previstas na Lei 13.467/17 aos processos em curso quando da entrada em vigor da referida lei, bem como às ações ajuizadas a partir de 11-11-17.

No presente caso, em que tanto o ajuizamento da ação quanto o início do contrato de trabalho ocorreram após 11-11-17, aplicam-se as regras de direito material e processual da Lei 13.467/2017.

PREJUDICIAL DE MÉRITO

Prescrição

Considerando a data do ajuizamento da reclamatória trabalhista, em 01-02-21, e o período de duração do pacto laboral (09-11-18 a 21-08-20), não há prescrição a ser declarada, com fundamento no inc. XXIX do art. 7º da Constituição Federal.

MÉRITO

Acúmulo de funções

A autora alega que, após um período, passou a realizar diversas atividades que não eram inerentes à sua função de auxiliar de produção, mas sim à função de auxiliar de expedição. Refere que também era responsável pelo “monitoramento de saúde de visitantes”, controlando o acesso de pessoas no local de trabalho, bem como da “higienização operacional” da área produtiva. Diz que ainda era responsável pelo controle de fluxo de uniformes dos colaboradores. Assevera que, em janeiro de 2020, aproximadamente, foi criado, efetivamente, o cargo de auxiliar de expedição, no organograma de funções da ré; contudo, não foi alterada sua CTPS, tendo exercido as atividades de auxiliar de produção e auxiliar de expedição cumulativamente. Requer o pagamento de “plus” salarial, a ser arbitrado,

decorrente do acúmulo de função, com integrações em férias com 1/3, 13º salários, horas extras pagas e postuladas, FGTS, repousos e feriados.

A reclamada se opõe ao pedido, argumentando que a autora sempre exerceu as mesmas tarefas desde o início de seu contrato, as quais eram intrínsecas à função de auxiliar de produção I, não havendo o cargo de auxiliar de expedição na filial onde ela trabalhava.

Analiso.

Consoante o ordenamento jurídico brasileiro, salvo na hipótese de a empresa possuir plano de cargos no qual especificadas as respectivas atribuições, não há previsão para pagamento de salário por funções, de sorte que se presumem contratadas com o empregado todas as atividades ordinariamente exercidas, observando-se os limites impostos pelo parágrafo único do art. 456 da CLT.

É faculdade do empregador atribuir ao empregado, no curso do contrato de trabalho, outras tarefas além daquelas inicialmente desempenhadas, de modo a adequar a prestação laborativa às necessidades do empreendimento. Ao assim proceder, não está promovendo alteração contratual lesiva ao empregado, vedada pelo art. 468 da CLT, mas sim exercitando legitimamente o jus variandi que lhe é inerente, a teor do disposto no caput do art. 2º da CLT. Não haverá irregularidades se as novas tarefas forem compatíveis com a função ajustada e executadas dentro da jornada de trabalho.

Da análise da ficha de empregado da autora (ID. 17ff9d4), vejo que ela foi admitida em 09-11-18 para exercer a função de AUXILIAR DE PRODUÇÃO INDUSTRIAL I, não havendo anotações formais de alteração do cargo durante o contrato de trabalho.

Em seu depoimento, a autora afirma que “quando começou a trabalhar na ré, era auxiliar de produção e nessa função envasava sacos de albumina e encaixotava, e também ajudava na limpeza do local de trabalho; que depois de uns 2 meses passou a trabalhar na expedição, carregando e descarregando, monitoramento da portaria para autorizar entrada e saída, separação de pedidos com a nota, conferência de produtos e uniformes; que ajudava no envasamento de sacos de albumina quando sobrava tempo na expedição, por meia hora ou 1h por dia; que todas essas atividades eram executadas dentro da jornada; (...) que na expedição não havia empregado com a função de auxiliar de expedição; que sua líder era líder geral, da produção e da expedição; que a líder era a responsável pelo controle dos produtos mas na prática era a depoente que fazia isso; que passou a manusear efetivamente a transpaleteira a partir de fevereiro de 2019 quando fez curso para tal.”

A preposta da reclamada diz que “a autora trabalhava como auxiliar de produção industrial, fazendo carregamento de insumos de albumina e whey, registros, documentações, serviços de rotina como receber pessoas, atender a portaria, separação de pedidos, entrega de notas fiscais nos caminhões etc; que no setor da autora não tem auxiliar de expedição e a autora fazia atividades de produção e as atividades de expedição faziam parte de seu trabalho na produção; que na época da autora havia 4 auxiliares de produção, Marilei, Luane e Eunize e todos faziam as

mesmas atividades da autora; que os relatórios de atividades podem ser assinados por todos os auxiliares de produção.”

A testemunha Marilei refere que “trabalha na reclamada desde mai/2015; que sempre trabalhou como auxiliar de produção; que suas atividades eram serviços gerais de ajudar na produção, higienização de superfície; que se precisa ajuda na expedição, ajudando a embalar caixas; que a autora trabalhava junto fazendo trabalho na produção; que ela ia trabalhar na expedição quando tinha carregamento, para carregar; que na expedição só precisa alguém quando tem carregamento, o que ocorre 1x de manhã, quando chega caminhão, e às vezes 1x de tarde; que fora isso, não tem trabalho na expedição; que a autora sempre fez as mesmas atividades; que os controles de acesso da expedição eram feitos pela autora mas qualquer auxiliar de produção poderia fazer; que a higienização do setor era feita por todos os auxiliares de produção; que não dirigia transpaleteira; que a autora dirigia, quando havia carregamento; que o monitoramento de saúde de entrada dos visitantes (controle de temperatura) podia ser feito por qualquer auxiliar e todos faziam; que não assinava documentos de higienização e de controle de fluxo de uniformes; que não assinava documentos de monitoramento de saúde de visitantes.”

Do depoimento da testemunha, extraio que todas as tarefas narradas pela autora estão inseridas no corolário de atividades da função de auxiliar de produção, e foram realizadas desde a contratação, sendo que todos os auxiliares de produção fazem as mesmas atividades, atuando tanto na produção quanto na expedição. Inclusive, a autora afirma que somente um empregado atua como líder geral, da produção e da expedição, evidenciando que se trata de um único setor, apenas subdividido.

O fato de a autora ter operado transpaleteira, por si só, não caracteriza qualquer acúmulo, depreendendo-se da prova oral produzida que se trata de instrumento de trabalho para exercício das atividades do cargo para o qual foi contratada. Ademais, era atividade exercida de forma eventual, quando a obreira atuava no descarregamento na expedição, sem implicar em aumento de responsabilidades.

Por fim, refiro que a totalidade das atividades desenvolvidas foi prestada em proveito do mesmo empregador e dentro da mesma jornada de trabalho, não tendo havido acúmulo de funções.

Pelo exposto, rejeito o pedido da alínea “b” da petição inicial.

Nulidade do regime compensatório. Horas extras

A autora alega que sua atividade era insalubre, dizendo estão ausentes os requisitos autorizadores da prorrogação da jornada constantes no artigo 60 da CLT. Refere que, no verão, teve de laborar aos sábados para realizar a limpeza da empresa. Postula a declaração de nulidade do regime compensatório e o pagamento das horas extras consideradas como tal as excedentes à 8ª diária, bem como a revisão e o consequente pagamento correto das horas extras, com adicional de 50% para as horas laboradas excedentes à 8ª diária e de 100% para as horas laboradas além da 44ª hora, calculado minuto a minuto, com integrações em aviso prévio, férias com 1/3, natalinas, repouso semanal remunerado e FGTS.

A reclamada se opõe ao pedido, argumentando que todo o labor extraordinário foi devidamente anotado, computado e corretamente pago.

Análise.

A autora foi contratada para laborar de segundas a sextas-feiras, das 7h30min às 12h e das 13h12min às 17h30min (contrato de ID. 5f262b5).

A reclamada apresentou cartões ponto no ID. 5e5593f e ss, os quais são documentos fidedignos para comprovar todo o horário de trabalho da autora durante todo o período contratual, pois não há nenhuma prova nos autos que os invalide, inclusive, tais documentos sequer foram impugnados pela obreira.

Analisando os documentos em comento, verifico que a autora laborou das 7h30min às 12h e das 13h12min às 17h30min e das 7h12min às 12h e das 13h às 17h, sempre de segundas a sextas-feiras, tendo as partes adotado a compensação horária semanal, autorizada individualmente na contratação.

Vejo, ainda, que houve a prática de outra espécie de compensação de jornada, que se refere ao banco de horas, pois o limite para compensação das horas extras praticadas em um dia é mensal, conforme evidenciam os recibos de pagamento anexados no ID. 8af237a e ss (em cada mês, foi pago o saldo existente no banco de horas). Destaco que tal espécie de compensação, a partir da vigência da Lei 13.467/2017, pode ser ajustada inclusive de forma tácita com o trabalhador (§6º do art. 59 da CLT).

Os registros de horário revelam que em inúmeras oportunidades durante o contrato de trabalho a obreira prestou horas extras, o que configura a habitualidade. Consigno, porém, que a partir da entrada em vigor da Lei 13.467/2017, a prestação habitual de horas extras não descaracteriza o acordo de compensação semanal de jornada e o banco de horas (art. 59-B, parágrafo único, da CLT), pelo que não há falar em irregularidade sob este argumento.

Ainda, os recibos de pagamentos da autora (ID. 8af237a e ss) revelam que o seu labor era insalubre, pois percebeu o pagamento do adicional de insalubridade durante toda a contratualidade.

Assim, em que pese o regime de compensação de jornada seja autorizado pela Constituição da República (art. 7º, inciso XIII), há requisitos mínimos que devem ser observados, dentre eles o que dispõe o art. 60 da CLT, in verbis:

"Nas atividades insalubres, assim consideradas as constantes dos quadros mencionados no capítulo "Da Segurança e da Medicina do Trabalho", ou que neles venham a ser incluídas por ato do Ministro do Trabalho, Indústria e Comércio, quaisquer prorrogações só poderão ser acordadas mediante licença prévia das autoridades competentes em matéria de higiene do trabalho, as quais, para esse efeito, procederão aos necessários exames locais e à verificação dos métodos e processos de trabalho, quer diretamente, quer por intermédio de autoridades sanitárias federais, estaduais e municipais, com quem entrarão em entendimento para tal fim".

Nos termos do dispositivo consolidado em comento, a validade dos regimes compensatórios instituídos pela reclamada depende de licença prévia das autori-

dades competentes em matéria de higiene do trabalho.

Destaco que, com o cancelamento da Súmula 349 do E. TST pela Resolução 174/2011 da Superior Corte trabalhista, a previsão normativa acerca da possibilidade de instituição do regime de compensação em atividade insalubre, independentemente de licença prévia das autoridades competentes em matéria de higiene do trabalho, não era admitida até a entrada em vigor da Lei 13.467/2017. Assim, ainda que houvesse previsão na norma coletiva de compensação de horários sem autorização da autoridade administrativa, o fato é que tal matéria era considerada infensa à negociação coletiva, por tratar da saúde do trabalhador e da segurança do trabalho, representando patamar civilizatório mínimo que deve ser respeitado pelos entes coletivos. Ocorre que não há nos autos comprovação de que a reclamada tenha recebido esta licença, ônus que lhe incumbia (art. 818 da CLT c/c art. 333, II, do CPC).

Há precedentes do E. TST, neste sentido, cujo entendimento compartilho:

“ACORDO DE COMPENSAÇÃO BANCO DE HORAS. O Tribunal Regional considerou inválido o regime de compensação adotado pela reclamada, em face das seguintes premissas: tratar-se de trabalho insalubre e sem autorização do órgão competente, como exige o art. 60 da CLT, e não estar demonstrado, nos autos, o cumprimento das exigências para a regular adoção do banco de horas. Citou como exemplo, o fato de inexistir planilha individual de acompanhamento da jornada de trabalho, conforme os critérios estabelecidos na norma coletiva, fato que também contribuiu para se entender pela invalidade do banco de horas. O art. 7º, inciso XIII, da Constituição Federal não foi violado na sua literalidade. Esse dispositivo faculta a compensação de horários mediante acordo ou convenção coletiva de trabalho, mas não trata da questão peculiar dos autos, de prorrogação e compensação de jornada em atividade insalubre bem como a invalidade do banco de horas porque inobservados os critérios previstos na norma coletiva. Os arestos trazidos a cotejo não abordam todos os fundamentos da decisão recorrida. Incide na espécie, a afastar o conhecimento do recurso de revista, óbice das Súmulas nos 23 e 296, item I, do TST. Acrescenta-se que o cancelamento da Súmula nº 349 do TST pelo Tribunal Pleno (DEJT 30/05/2011) vem consolidar o entendimento desta Corte quanto à impossibilidade de negociação coletiva de jornada de trabalho em atividade insalubre. Recurso de revista não conhecido.” (RR-146900-83.2006.5.04.0331, Rel. Min. José Roberto Freire Pimenta, 2ª Turma, DEJT de 5-8-2011). (grifei).

Em que pese a convenção coletiva de trabalho aplicável às partes (ID. 1b10469), dispense a licença da autoridade administrativa para prorrogação de jornada em atividade insalubre (cláusula vigésima oitava), na forma do disposto no artigo 611-A, XIII, da CLT, esta norma tem vigência no período de 01-06-19 a 31-05-21. Portanto, até 31-05-19, os regimes compensatórios adotados pela reclamada restam descaracterizados, sendo devido o pagamento do adicional de horas extras em relação às horas destinadas à compensação semanal, nos termos da Súmula 85, itens III e IV, do TST. No entanto, em relação ao banco de horas, por não se aplicar

o disposto na referida Súmula, conforme seu item V, a descaracterização acarreta a nulidade do regime, pelo que são devidas horas extras mais o adicional.

Por outro lado, os registros de ponto também mostram que comumente havia trabalho em sábados. Por exemplo, a autora laborou 2 sábados em janeiro, 2 em junho, 1 em outubro, 2 em novembro e 1 em dezembro do ano de 2019, e, no ano de 2020, laborou 1 sábado em janeiro, 1 em março e 4 em maio. Tal circunstância caracteriza o regime de compensação semanal durante todo o período contratual, já que frustra a sua própria finalidade, sendo devido à empregada o pagamento do adicional de horas extras em relação às horas destinadas à compensação semanal, nos termos da Súmula 85, item III, do TST.

Por fim, não cabe a aplicação do adicional de 100% para as horas laboradas além da 44ª hora, como pretendido pela autora, por ausência de previsão, contratual ou normativa.

Por todo o exposto, acolho em parte o pedido elencado na alínea “a” da petição inicial e condeno a reclamada ao pagamento de (I) adicional de horas extras, durante todo o período contratual, para as horas destinadas à compensação semanal, legal, normativo (considerado o período de validade das normas coletivas) ou o praticado pela ré, o que for mais favorável à autora, e (II) horas extras, até 31-05-19, assim consideradas as prestadas além do regime compensatório semanal, com adicional legal, normativo (considerado o período de validade das normas coletivas) ou o praticado pela ré, o que for mais favorável à autora, tudo com reflexos em férias com 1/3, 13º salários, e repouso semanal remunerado e feriados, na forma da OJ 394 da SDI-I do TST. Não cabem reflexos em aviso prévio, pois a autora pediu demissão e não trabalhou neste período. O pedido de reflexos em FGTS será analisado em tópico próprio. Base de cálculo das horas extras: Súmula 264 do TST, observando-se o adicional de insalubridade. Divisor: 220h. Observem-se as disposições do parágrafo 1º do art. 58 da CLT, e da Súmula 366 do TST.

A fim de evitar o enriquecimento ilícito, autorizo a dedução de todas as parcelas pagas sob idênticos títulos ora deferidos, na forma da Orientação Jurisprudencial 415 da SDI-I do TST.

Descontem-se todos os períodos de afastamento da parte autora.

FGTS

Condeno a reclamada a depositar na conta vinculada da autora o FGTS incidente sobre as parcelas salariais nesta decisão deferidas. É indevido o acréscimo de 40% ao FGTS, tendo em vista o pedido de demissão.

RECONVENÇÃO

Indenização por danos morais

A reclamada, juntamente com a defesa, apresentou reconvenção, buscando a reparação de dano que alega lhe ter sido causado pela autora-reconvinda, em razão de violação de termo de sigilo e confidencialidade firmado entre as partes, pois ela utiliza, como prova na presente ação, documentos internos e privativos da empresa. Diz que os documentos sob IDs 2a5b8fd, 8388504, ff2bee8, 032e0e6, 3b29a47, d2d2718, 5b5de4e, 26cc577 são exclusivos da empresa, internos e não

disponíveis ao público, ou seja, protegidos pela LGPD. Requer a condenação da reconvinada ao pagamento de indenização por danos morais, em valor mínimo de R\$ 5.000,00.

A reconvinada apresenta defesa (ID. bdf5131 - Pág. 3), contestando articuladamente os pedidos, requerendo a improcedência da reconvenção.

Ao início, refiro que as disposições da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) destinam-se tão somente à pessoa natural, razão pela qual, em relação à pessoa jurídica da reconvinde, não há falar em proteção de dados sensíveis e operacionais por força desta Lei.

No mais, em que pese a reconvinada tenha violado o termo de compromisso, sigilo e confidencialidade que firmou na admissão na empresa, para que a pessoa jurídica faça jus a indenização por dano moral é necessária a comprovação de que sua credibilidade e seu nome foram atingidos pela conduta ilícita, ou seja, é necessária a comprovação inequívoca do prejuízo extrapatrimonial. Inclusive, são nesse sentido os termos da cláusula oitava do aludido termo.

Cito jurisprudência do Tribunal Regional do Trabalho da 4ª Região acerca do tema:

DANO MORAL A PESSOA JURÍDICA. O dano moral a pessoa jurídica se dá quando são comprovadamente atingidos direitos inerentes à honra objetiva da empresa: sua imagem pública, nome ou reputação. Todavia, não é presumível, sendo necessária a prova da ação do ofensor, da existência do dano e do nexo causal entre ambos. (TRT da 4ª Região, 10ª Turma, 0020648-94.2015.5.04.0662 RO, em 11/03/2016, Desembargadora Cleusa Regina Halfen).

No presente caso, não há qualquer prova de que a imagem da reconvinde perante seus clientes ou no meio em que atua tenha sido abalada.

Ademais, não se pode comparar a juntada de documentos internos da empresa em processo judicial para prova do direito que a reconvinada alega, com a divulgação a terceiros de informações sigilosas.

Dessa feita, rejeito o pedido.

Compensação/Dedução

Não há valores a serem compensados. A dedução já foi analisada e deferida, quando cabível.

Limites da condenação

Nas ações submetidas ao rito sumaríssimo, por força do disposto no art. 852-B, I, da CLT, a jurisprudência consolidou-se no sentido de que a condenação está limitada aos valores atribuídos aos pedidos na petição inicial, na forma do art. 492 do CPC, o qual entendo aplicável ao processo do trabalho. Cito precedente da Seção Especializada em Execução do Tribunal Regional do Trabalho da 4ª Região:

AGRAVO DE PETIÇÃO. RITO SUMARÍSSIMO. CÁLCULOS DE LIQUIDAÇÃO. OBSERVÂNCIA DOS VALORES INDICADOS NA PETIÇÃO INICIAL. Os valores apurados em liquidação de sentença não podem superar aqueles indicados a cada verba na petição inicial, sob pena de violação aos artigos 852-B, inciso I, da CLT e 460 do CPC. (TRT da 4ª Região, Seção Especializada Em Execu-

ção, 0000589-67.2012.5.04.0411 AP, em 02/06/2015, Desembargador João Alfredo Borges Antunes de Miranda - Relator).

Portanto, limito a condenação aos valores informados pela autora na petição inicial.

Justiça gratuita

A Lei 13.467/17 alterou a redação do §3º do art. 790 da CLT, bem como incluiu no mesmo artigo o §4º, passando o dispositivo celetista a ter a seguinte redação:

Art. 790. Nas Varas do Trabalho, nos Juízos de Direito, nos Tribunais e no Tribunal Superior do Trabalho, a forma de pagamento das custas e emolumentos obedecerá às instruções que serão expedidas pelo Tribunal Superior do Trabalho.

(...)

§3º É facultado aos juízes, órgãos julgadores e presidentes dos tribunais do trabalho de qualquer instância conceder, a requerimento ou de ofício, o benefício da justiça gratuita, inclusive quanto a traslados e instrumentos, àqueles que perceberem salário igual ou inferior a 40% (quarenta por cento) do limite máximo dos benefícios do Regime Geral de Previdência Social.

§4º O benefício da justiça gratuita será concedido à parte que comprovar insuficiência de recursos para o pagamento das custas do processo. (grifei)

A partir da vigência da referida lei, em 11 de novembro de 2017, é necessária a comprovação da insuficiência de recursos pela parte autora para a viabilização da concessão do benefício, não bastando a mera declaração, conforme a redação revogada do art. 790 da CLT.

A autora, ao longo do contrato de trabalho, percebeu salário inferior ao valor correspondente a 40% do limite máximo dos benefícios do Regime Geral de Previdência Social (R\$ 6.433,57 na data da propositura da ação).

Ademais, a declaração de hipossuficiência econômica apresentada no ID. b495eb3 constitui presunção favorável quanto à alegada impossibilidade de arcar com os custos do processo, razão pela qual concedo à autora o benefício da justiça gratuita.

Honorários sucumbenciais

Na Justiça do Trabalho, as regras atinentes aos honorários de sucumbência estão disciplinadas no art. 791-A da CLT, inserido pela Lei 13.467/17, que assim dispõe:

Art. 791-A. Ao advogado, ainda que atue em causa própria, serão devidos honorários de sucumbência, fixados entre o mínimo de 5% (cinco por cento) e o máximo de 15% (quinze por cento) sobre o valor que resultar da liquidação da sentença, do proveito econômico obtido ou, não sendo possível mensurá-lo, sobre o valor atualizado da causa.

§1º Os honorários são devidos também nas ações contra a Fazenda Pública e nas ações em que a parte estiver assistida ou substituída pelo sindicato de sua categoria.

§2º Ao fixar os honorários, o juízo observará:

I - o grau de zelo do profissional;

II - o lugar de prestação do serviço;

III - a natureza e a importância da causa;

IV - o trabalho realizado pelo advogado e o tempo exigido para o seu serviço.

§3º Na hipótese de procedência parcial, o juízo arbitrará honorários de sucumbência recíproca, vedada a compensação entre os honorários.

§4º Vencido o beneficiário da justiça gratuita, desde que não tenha obtido em juízo, ainda que em outro processo, créditos capazes de suportar a despesa, as obrigações decorrentes de sua sucumbência ficarão sob condição suspensiva de exigibilidade e somente poderão ser executadas se, nos dois anos subsequentes ao trânsito em julgado da decisão que as certificou, o credor demonstrar que deixou de existir a situação de insuficiência de recursos que justificou a concessão de gratuidade, extinguindo-se, passado esse prazo, tais obrigações do beneficiário.

§5º São devidos honorários de sucumbência na reconvenção. (grifei)

No presente caso, a autora obteve êxito parcial em relação a alguns pleitos formulados na petição inicial, pelo que condeno a reclamada a pagar ao seu advogado honorários sucumbenciais, que, observados os critérios previstos no §2º do art. 791-A da CLT, fixo em 10% do valor bruto que resultar da liquidação da sentença, não se computando o valor da contribuição previdenciária patronal, nos termos da Súmula 37 e da OJ nº 18 da Seção Especializada em Execução, ambas do TRT da 4ª Região.

Ressalto, na mesma linha do entendimento firmado na PROPOSTA 2 da Comissão 05 da I Jornada sobre a Reforma Trabalhista realizada pelo TRT da 4ª Região, inexistente sucumbência da parte autora nos pedidos formulados nos autos em que houve deferimento parcial das respectivas parcelas, pois nos termos da referida tese, a sucumbência ocorre somente "em caso de indeferimento total do pedido específico. O acolhimento do pedido, com quantificação inferior ao postulado, não caracteriza sucumbência parcial, pois a verba postulada restou acolhida. Quando o legislador mencionou "sucumbência parcial", referiu-se ao acolhimento de parte dos pedidos formulados na petição inicial. (grifei)

Com base, também, no art. 791-A da CLT, condeno a autora ao pagamento de honorários advocatícios de sucumbência em favor dos procuradores da ré, que, observados os critérios previstos no §2º do art. 791-A da CLT, fixo em 5% sobre o valor dos itens da petição inicial integralmente rejeitados – alínea "b".

Sinalo que a fixação dos honorários sucumbenciais nestes percentuais decorre da consideração da distinta situação econômica das partes envolvidas, sendo o autor, inclusive, beneficiário da gratuidade judiciária.

Os honorários advocatícios devidos pela parte autora aos procuradores da ré deverão ser abatidos dos créditos apurados em favor do reclamante. Se estes forem inferiores àqueles, a respectiva exigibilidade (da parte remanescente) ficará suspensa, conforme o disposto no § 4º do art. 791-A da CLT.

Outrossim, com base no § 5º do mesmo artigo, condeno a reclamada-reconvincente ao pagamento de honorários advocatícios de sucumbência em favor do procurador da autora-reconvinda, no valor de R\$ 500,00, equivalente a 10% sobre o

valor atribuído ao pedido formulado em reconvenção, de R\$ 5.000,00.

Contribuições previdenciárias e recolhimentos fiscais

Os descontos previdenciários e recolhimentos fiscais são devidos na forma da lei vigente ao tempo da liquidação de sentença, autorizado o desconto da cota da empregada.

Juros e correção monetária

Incidem por imposição legal na forma da lei vigente ao tempo da liquidação de sentença.

ANTE O EXPOSTO, REJEITO a reconvenção formulada por SOLAR COMERCIO E AGROINDUSTRIA LTDA. em face de SIMONE GABRIELA RITTER, na forma da fundamentação, e ACOLHO EM PARTE os pedidos formulados por SIMONE GABRIELA RITTER em face de SOLAR COMERCIO E AGROINDUSTRIA LTDA., para condenar a reclamada a pagar à autora, observados os descontos previdenciários e fiscais cabíveis, as seguintes parcelas, deferidas na forma da fundamentação, que passa a fazer parte deste dispositivo para todos os efeitos legais:

a) adicional de horas extras, durante todo o período contratual, para as horas destinadas à compensação semanal, legal, normativo (considerado o período de validade das normas coletivas) ou o praticado pela ré, o que for mais favorável à autora, e (II) horas extras, até 31-05-19, assim consideradas as prestadas além do regime compensatório semanal, com adicional legal, normativo (considerado o período de validade das normas coletivas) ou o praticado pela ré, o que for mais favorável à autora, tudo com reflexos em férias com 1/3, 13º salários, e repouso semanal remunerado e feriados, na forma da OJ 394 da SDI-I do TST. Base de cálculo das horas extras: Súmula 264 do TST, observando-se o adicional de insalubridade. Divisor: 220h. Observem-se as disposições do parágrafo 1º do art. 58 da CLT, e da Súmula 366 do TST. A fim de evitar o enriquecimento ilícito, autorizo a dedução de todas as parcelas pagas sob idênticos títulos ora deferidos, na forma da Orientação Jurisprudencial 415 da SDI-I do TST. Descontem-se todos os períodos de afastamento da parte autora;

Deve a reclamada depositar na conta vinculada da autora o FGTS incidente sobre as parcelas salariais nesta decisão deferidas.

Determino a liberação à autora do valor depositado conforme guia de ID. df-03cd9, mediante alvará judicial, independentemente do trânsito em julgado desta decisão, na forma requerida na manifestação de ID. bdf5131 - Pág. 5.

Concedo à autora o benefício da justiça gratuita.

Custas da ação principal no valor de R\$ 100,00, calculadas sobre o valor atribuído à condenação, de R\$ 5.000,00, pela reclamada.

Custas da reconvenção de R\$ 100,00, calculadas sobre o valor atribuído à causa, de R\$ 5.000,00, pela reclamada-reconvinte.

Deve a reclamada pagar honorários sucumbenciais de 10% do valor bruto que resultar da liquidação da sentença, não se computando o valor da contribuição previdenciária patronal, nos termos da Súmula 37 e da OJ nº 18 da Seção Especia-

lizada em Execução, ambas do TRT da 4ª Região. Deve, ainda, a reclamada-reconvinte pagar honorários advocatícios de sucumbência em favor do procurador da autora-reconvinda, no valor de R\$ 500,00, equivalente a 10% sobre o valor atribuído ao pedido formulado em reconvenção, de R\$ 5.000,00.

Deve a autora pagar honorários de sucumbência em favor dos procuradores da ré, fixados em 5% sobre o valor dos itens da petição inicial integralmente rejeitados (alínea “b”), que deverão ser abatidos dos créditos apurados em seu favor. Se estes forem inferiores àqueles, a respectiva exigibilidade (da parte remanescente) ficará suspensa, conforme o disposto no § 4º do art. 791-A da CLT.

Cumpra-se após o trânsito em julgado e liquidação.

Intimem-se as partes. Nada mais.

Montenegro, 02 de junho de 2021.

LINA GORCZEWSKI

Juíza do Trabalho

TERCEIRA PARTE

GLOSSÁRIO PRINCIPAIS TERMOS CORRELATOS À LGPD

A

AGENTES DE TRATAMENTO (art. 5º, IX e art. 37).

FERNANDA JULIANE BRUM CORRÊA¹

Conforme definição expressa da lei, são o controlador e o operador. A eles cabe a documentação das operações realizadas durante o processo de tratamento de dados, fundamental ao controle e transparência sobre o cumprimento dos propósitos do referido tratamento. Enquanto o primeiro é o responsável pelas decisões acerca do tratamento, o segundo realiza o tratamento. Ambos têm responsabilidade jurídica pela segurança e privacidade dos dados.

O controlador é definido pela legislação (art. 5º, VI) como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Trata-se, assim, daquele que detém o domínio dos fatos acerca das operações de tratamento e, por essa razão, no regulamento europeu (GDPR) é designado como “responsável pelo tratamento” (art. 4º, item 7). No âmbito das relações de trabalho subordinado, é ainda mais relevante a identificação e conceituação do controlador para que os titulares de dados possam exercer seus direitos. Neste caso, como regra, o controlador será o empregador, visto que é quem obtém os dados e indica o tratamento a ser conferido. O controlador detém o consentimento do titular e o operador deve seguir as instruções daquele (art. 39), motivado por contrato ou obrigação legal. Eventual dispensa do consentimento não desobriga os agentes de tratamento das demais obrigações previstas em lei (art. 7º, §6º).

O operador, por sua vez, é descrito pela LGPD (art. 5º, VII) como a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Ainda que sem essa denominação na lei, na prática também tem sido chamado de processador de dados. No regulamento europeu (GDPR), é designado como uma pessoa com atribuição de realizar o tratamento segundo instruções fornecidas pelo controlador, o qual verificará a observância das próprias instruções e das normas sobre a matéria (art. 4º, item 8, e art. 39). O operador, a partir de decisão tomada pelo controlador, pode ser alguém interno à organização ou empresa (empregado), ou terceiro a quem se confiem as atividades de tratamento. Não há consenso doutrinário acerca da classificação a depender da internalização ou não do papel de operador. Miziara destaca o dissenso entre autores que entendem que o empregado designado a essa função não é, juridicamente, um operador, mas apenas *longa*

¹ Analista Judiciário do TRT da 4ª Região. Graduada em Direito pela Universidade Federal de Santa Maria. Especialista em Direito do Trabalho e Processo do Trabalho pela Faculdade Damásio. fernanda.brum@trt4.jus.br

manus do empregador, e outros que concluem efetivamente configurada a figura do operador.²

ANONIMIZAÇÃO (art. 5.º, XI).

FERNANDA JULIANE BRUM CORRÊA³

É uma prática de segurança de dados, definida pela lei como a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, pelos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Com a anonimização, assim, procede-se à ruptura entre o dado e o respectivo titular, eliminando-se a vinculação com identificadores em uma base de dados.

Na prática, o processo de anonimização pode ser efetuado por *supressão*, como a eliminação de dado identificador capaz de diferenciar até mesmo pessoas homônimas, como o número do CPF. Ainda, o vínculo entre o dado e o titular pode ser rompido pela *generalização*, pela qual passa a constar somente um dado que não permite atribuição específica a um titular, como, exemplificativamente, a faixa etária. Bruno Bioni também menciona as técnicas de *randomização* e *pseudonimização* (verbetes específicos neste glossário).

Segundo o art. 12 da LGPD, dados submetidos ao procedimento de anonimização (dados anonimizados) não são considerados dados pessoais, previsão similar à contida na GDPR, conforme preâmbulo, que afasta a proteção de dados das informações anônimas, assim entendidas como as que não se relacionem a pessoa identificada ou identificável.

A previsão, contudo, não considera a possibilidade de identificação de pessoas a partir de algoritmos, o que ocorre, por exemplo, na identificação de hábitos de compra. A falibilidade da anonimização tem sido frequentemente apontada pela doutrina, baseada em estudos que revelam a possibilidade de reidentificação, tornando o anonimato definitivo inalcançável.

Diante desse risco, considerando a possibilidade de que os métodos de anonimização ainda sejam “considerados corruptíveis e passíveis de falhas”, seria aconselhável adotar o conceito expansionista de dado pessoal, mencionado por Bruno Bioni, que classifica como dado pessoal o equivalente a informação que, direta ou indiretamente, identifica alguém, ou seja, quaisquer informações com potencial para a identificação, mesmo que remota.⁴

2 Referências: MIZIARA, Raphael. Reflexos da LGPD no Direito e no processo do trabalho (livro eletrônico). Raphael Miziara, André Pessoa, Bianca Mollicone – 1. ed. - São Paulo: Thomson Reuters Brasil, 2020. PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. – São Paulo: Saraiva Educação, 2020.

3 Analista Judiciário do TRT da 4ª Região. Graduada em Direito pela Universidade Federal de Santa Maria. Especialista em Direito do Trabalho e Processo do Trabalho pela Faculdade Damásio. fernanda.brum@trt4.jus.br

4 Referências: BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3 ed. – Rio de Janeiro: Forense, 2021. PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. – São Paulo: Saraiva Educação, 2020.

APLICAÇÃO DA LGPD

GILBERTO DESTRO⁵

A LGPD aplica-se: i) a toda operação de tratamento com dados pessoais, seja para produzir, coletar, receber, acessar, extrair, armazenar, arquivar, utilizar, classificar, processar, avaliar ou controlar a informação, modificar, reproduzir, transferir, distribuir, transmitir, comunicar, difundir ou eliminar dados; ii) em operação de tratamento realizada por qualquer pessoa, natural ou jurídica, de direito público ou privado; iii) em tratamento por qualquer meio (eletrônico, em papel, outros); iv) nos seguintes casos: a) os dados pessoais tenham sido coletados no Brasil (isto é, o titular se encontre no Brasil no momento da coleta); b) ou os dados sejam de pessoas localizadas no Brasil; c) ou o tratamento objetive a oferta ou o fornecimento de bens ou serviços a pessoas no Brasil; d) ou os dados sejam tratados no Brasil; e) ou os dados provenham do exterior e sejam objeto de comunicação ou uso compartilhado com agente de tratamento brasileiro ou sejam objeto de transferência internacional com país diferente sem que estejam protegidos no país de proveniência em grau adequado ao previsto na LGPD.

A LGPD não se aplica ao tratamento: i) realizado por pessoa natural apenas para fins particulares e não econômicos; ii) realizado para fins exclusivamente jornalísticos e artísticos; iii) realizado apenas para fins acadêmicos, observando-se os requisitos legais de tratamento (art. 7º e 11 da LGPD); iv) realizado para fins exclusivos de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais, observadas as restrições estabelecidas na LGPD. Também não se aplica a LGPD aos dados que chegam no Brasil provenientes do exterior e não sejam objeto de comunicação ou uso compartilhado com agente de tratamento brasileiro ou objeto de transferência internacional com país diferente, quando os dados estejam protegidos no país de proveniência em grau adequado ao previsto na LGPD.

Possui a LGPD, portanto, abrangência extraterritorial, buscando a proteção internacional ao tratamento, tanto à coleta de dados no Brasil ou à oferta de bens ou serviços a pessoas que estejam no Brasil, mesmo que o tratamento dos dados seja realizado no exterior, quanto aos dados que venham do exterior e tenha algum tratamento no Brasil.⁶

APLICAÇÃO DA LGPD NO ÂMBITO LABORAL

GILBERTO DESTRO⁷

A proteção conferida pela LGPD, irradiando a tutela constitucional à intimidade e privacidade, alcança as relações laborais, âmbito repleto de tratamento de dados pessoais. Desse modo, devem se adequar os procedimentos em todos os momentos:

5 Juiz Titular de Vara do Trabalho no TRT da 4ª Região. Especialista em Direito Processual Civil e graduado em Direito pela Universidade do Sul de Santa Catarina.

6 Referências: PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à Lei n 13.709/2018 (LGPD). 2 ed. São Paulo: Saraiva educação, 2020. 152p. SANDIM, Bruna Carolina Martins. A proteção de dados pessoais à luz da transnacionalidade da tecnosfera: soberania versus segurança jurídica mundial para uma adequada cooperação jurídica internacional. TCC. UniCEUB, 2020. Disponível em: <https://repositorio.uniceub.br/jspui/handle/prefix/14820>. Acesso em: 15 nov. 2021.

7 Juiz Titular de Vara do Trabalho no TRT da 4ª Região. Especialista em Direito Processual Civil e graduado em Direito pela Universidade do Sul de Santa Catarina.

Na fase pré-contratual: reduzir a coleta de informações ao necessário na seleção de candidatos à vaga de trabalho, afastando-se os dados sensíveis geradores de discriminação, cuidando de informar sobre a eliminação dos dados ou de obter o consentimento para armazená-los em vista de seleções futuras.

Na fase contratual: na formalização do contrato de trabalho e durante o contrato, proteger os dados de identificação do trabalhador e de sua família coletados, que podem incluir: nomes e número de documentos, endereços, situação familiar, formação escolar, veículos e patrimônio; dados de saúde, exames periódicos, atestados médicos, doenças, acidentes, incapacidade laboral; reconhecimento facial e biometrias, registros de jornada e ausências, registros disciplinares; filiação associativa e sindical; registros financeiros (salário, descontos, associações, pensões, consignações); compartilhamento de dados com empresas do mesmo grupo ou com prestadoras de serviços (nas áreas de contabilidade, consultoria, auditoria, informática, convênios e financeira), com seguradoras, planos de saúde, previdência complementar, entidades sindicais, associativas e conveniadas; dados de monitoramento interno e externo do ambiente laboral; monitoramento de uso da Internet e meios de comunicação eletrônica funcionais (e-mail e outros). Cuidar, ainda, no caso de teletrabalho, com a vulnerabilidade à invasão dos dados e à desconformidade em ser usado equipamento pessoal para o trabalho.

Na fase pós-contratual: observar que, finda a relação de trabalho e terminado o tratamento dos dados pessoais, segue-se a eliminação dos dados, permitida a conservação em cumprimento de obrigação legal, a transferência a terceiros e a anonimização para uso exclusivo do controlador ou para estudo. Sobre o prazo para a conservação dos dados para cumprimento de obrigação legal, lembre-se que o prazo prescricional de cinco anos, até o limite de dois anos após a extinção do contrato de trabalho (art. 7º, XXIX, da CRFB/1988), pode ser influenciado por causas de impedimento, interrupção ou suspensão de sua contagem, como nos casos de: existência de legitimado com menos de 18 anos de idade; ocorrência de doenças relacionadas ao trabalho que venham a se manifestar, consolidar ou serem conhecidas posteriormente; surgimento de pretensão meramente declaratória (imprescritível) para fins previdenciários, mesmo após décadas (inclusive em revisão de benefícios antigos com exigência de correção ou complementação de dados).

Portanto, impõe-se implantar a proteção de dados pessoais no âmbito laboral de acordo com os regramentos da LGPD.⁸

ARMAZENAMENTO (art. 5º, X)

ALINE DAL BÓ CORREA⁹

Conforme o art. 5º, X, da LGPD, o tratamento também envolve a atividade de

8 Referências: PAMPLONA FILHO, Rodolfo; CONI JUNIOR, Vicente Vasconcelos. A lei geral de proteção de dados pessoais e seus impactos no direito do trabalho. Disponível em: <https://revistas.unifacs.br/index.php/redu/article/view/7108>. Acesso em: 13 nov. 2021. PINHEIRO, Iuri; BOMFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. Disponível em: <http://trabalhoemdebate.com.br/artigo/detalhe/a-lei-geral-de-protECAo-de-dados-e-seus-impactos-nas-relacoes-de-trabalho>. Acesso em: 13 nov. 2021.

9 Graduanda na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedalbo04@gmail.com

armazenamento de dados pessoais. O armazenamento somente ocorrerá quando for necessário para que seja concretizada a finalidade da coleta.¹⁰

AUTODETERMINAÇÃO INFORMATIVA

DANIELA FALCADI COELHO¹¹

Com o advento de tantos dados pessoais disponíveis em redes, fez-se necessário a criação de uma Lei Geral de Proteção de Dados. Esta lei ganhou grande repercussão nos últimos meses, trazendo uma série de novos termos ao ordenamento jurídico pátrio. Na disciplina de proteção de dados pessoais, a autodeterminação informativa é um dos seus fundamentos.

Conceitualmente falando, a autodeterminação informativa se constitui na faculdade de exercer, de algum modo, controle sobre seus dados pessoais, garantindo, em determinadas circunstâncias, decidir se a informação pode ser objeto de tratamento por outrem, bem como acessar bancos de dados para exigir correção ou retirada de informações.

O direito à autodeterminação informativa se baseia em três fundamentos: (i) o indivíduo possui poder de decisão sobre o uso de seus dados pessoais; (ii) o direito não abrange um cunho de proteção pré-determinado, não se restringindo a um âmbito fixo de proteção; e (iii) todos os dados pessoais são passíveis de proteção, diante disso, a personalidade do dado é decisiva para a análise protetiva.

Bem como outros direitos, o direito à autodeterminação informativa não é absoluto; desta feita, pode, em confronto com o interesse público ou outros valores constitucionais, sofrer restrições pelo legislador e intérprete. Um exemplo desta situação foi destacado pela decisão proferida pela Suprema Corte alemã no julgamento em 1983, bem como, recentemente, pelo Supremo Tribunal Federal no julgamento do pedido cautelar proferido na ADI 6.387. Na ocasião, a Corte analisou a constitucionalidade da MP 954/2020, a qual previu o compartilhamento de dados de usuários de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE) para a produção de estatística oficial durante a pandemia da covid-19.

Ao pleno exercício do direito à autodeterminação informativa, apresentam-se os institutos do direito de ação e do direito de petição, aquele através dos instrumentos oferecidos pela legislação processual, tais como o Habeas Data, o Mandado de Segurança, as Ações Ordinárias e Cautelares, e este através dos requerimentos e recursos administrativos que, protocolizados perante os órgãos e autoridades competentes, no âmbito de suas atribuições de coleta e gestão de dados pessoais permitem, gratuitamente, a expressão do direito de acesso e de retificação, de apagamento, de oposição, de limitação do tratamento e de portabilidade para a tomada das medidas cabíveis, em prazo razoável.

O direito à autodeterminação informativa também se apresenta sob uma vertente de deveres de *facere* e *non facere* a serem observados pelos organismos de captação e de tratamento de dados pessoais para a prevenção de lesões.

10 Referências: MALDONADO, Viviane Nóbrega, BLUM, Renato Opice. *LGPD: Lei Geral de Proteção de Dados Pessoais comentada* - 3. ed - São Paulo: Thomson Reuters Brasil, 2021.

11 Pós graduanda em Direito Civil - USP. danielafalcadidf@gmail.com

A autodeterminação informativa surge como decorrência da consolidação do direito geral da personalidade. Isso porque a relevância do referido direito possibilitou a aplicação de novas vertentes, visando assegurar a proteção necessária e suficiente aos indivíduos.¹²

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (art 5º, XIX)

CAMILA DOZZA ZANDONAI¹³

A Lei 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), em seu artigo 5º, inciso XIX, define a Autoridade Nacional de Proteção de Dados como órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei em todo o território nacional.

A Autoridade Nacional de Proteção de Dados (ANPD) foi criada pela Lei 13.853, de 08 de julho de 2019, que incluiu disposições na LGPD e passou a regular a matéria. A ANPD foi instituída como órgão da administração pública federal, integrante da Presidência da República, com jurisdição no território nacional e cuja natureza jurídica é transitória e poderá ser transformada, pelo Poder Executivo, em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República, conforme artigo 55-A da Lei 13.709/2018. A possível revalidação da natureza jurídica da ANPD deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da sua estrutura regimental.

A ANPD é órgão central de interpretação e regulação da Lei Geral de Proteção de Dados, com autonomia técnica e decisória no âmbito de suas amplas competências dispostas na LGPD. É nesse sentido que o Decreto 10.474, de 26 de agosto de 2020, o qual aprovou a estrutura regimental e organizacional da ANPD, estabelece ser objetivo desta autoridade proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural. Implementar a aplicação da legislação de proteção de dados, uniformizar a interpretação da lei, traduzir conceitos, educar a população sobre o tema, certificar cláusulas padrão a fim de viabilizar operações econômicas, regular o fluxo informacional transnacional, fiscalizar e sancionar os agentes de tratamento são algumas das finalidades da ANPD.

Além disso, sob a perspectiva internacional do tema, a existência de um órgão de controle independente para regular a aplicação da legislação de proteção de dados é premissa fundamental na análise, pela Comissão Europeia, do nível de proteção aos dados que um país assegura aos cidadãos. Não basta a existência de uma lei que regule a matéria, mas a atuação de um órgão técnico autônomo e independente que garanta a sua implementação.

No âmbito da União Europeia, o Regulamento Geral sobre Proteção de Dados Europeu 2016/679 (*General Data Protection Regulation*), marco normativo essen-

12 Referências: BESSA, Leonardo Roscoe. *A LGPD e o direito à autodeterminação informativa*. GenJurídico, 2020. Disponível em: <http://genjuridico.com.br/2020/10/26/lgpd-direito-autodeterminacao-informativa/>. Acesso em: 23 out. 2021. HESSE, Konrad. *Temas Fundamentais do Direito Constitucional*. São Paulo: Saraiva, 2009.

13 Analista Judiciário do TRT da 4ª Região. Graduada em Direito pela PUCRS. Especialista em Direito e Processo do Trabalho pela Uniderp. Mestranda do Curso de Direito da UFRGS. camila.zandonai@trt4.jus.br

cial ao estudo do tema e inspirador da LGPD, disciplina a organização e a competência das autoridades de controle dos Estados-membros em seus artigos 51 a 59. Prevê que as autoridades de controle são responsáveis pela aplicação do Regulamento, a fim de proteger os direitos e liberdades fundamentais das pessoas em relação ao tratamento e de facilitar a livre circulação de dados pessoais na União, atuando com total independência no desempenho de suas funções. A independência destas autoridades também é ressaltada no Regulamento no ponto em que explicita a isenção às influências externas, diretas ou indiretas, de seus membros.

No Brasil, a LGPD disciplina a organização e a competência da Autoridade Nacional de Proteção de Dados nos artigos 55-A a 55-L, dispondo sobre as competências também ao longo de outros dispositivos da lei. A ANPD é composta pelo Conselho Diretor, Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, Corregedoria, Ouvidoria, órgão de assessoramento jurídico próprio e unidades administrativas e unidades especializadas necessárias à aplicação do disposto na LGPD. O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente, e seus membros serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, dentre brasileiros que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados.

As competências da autoridade nacional de proteção de dados estão previstas no artigo 55-J da LGPD, mas também espalhadas ao longo da lei, dividindo-se sua natureza em competências de implementação da lei de proteção de dados, bem como competências normativas, fiscalizatórias e sancionatórias. Como exemplo da primeira, podemos indicar a competência para a elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, promoção na população do conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança, promoção e elaboração de estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade, promoção de ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional. Exemplo de competência normativa é a edição de regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei.

Também compete à ANPD fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso, realizar auditorias ou determinar sua realização, no âmbito da atividade de fiscalização, comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal.

Tal como no Regulamento Geral de Proteção de Dados Europeu, a LGPD fortalece o aspecto do diálogo social e do dever de cooperação com outras entidades, públicas e privadas, e setores da sociedade civil, ao dispor que os regulamentos

e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório, assim como que a ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental.

A transparência e a publicidade são princípios efetivados por meio da determinação para que a ANPD elabore relatórios de gestão anuais acerca de suas atividades, a fim de que a comunidade tenha conhecimento sobre sua efetiva atuação.

Ainda, embora outros órgãos e instituições trabalhem de forma coordenada na proteção de dados pessoais, a LGPD é expressa quanto à competência prevaiente e exclusiva da ANPD para a aplicação de sanções previstas nessa Lei, o que reforça a autonomia decisória desse órgão técnico.

Quanto ao fluxo informacional em territórios internacionais, a LGPD atribui papel primordial à ANPD que, junto com as partes envolvidas na operação, deve assegurar a máxima segurança aos titulares que terão seus dados transferidos para o exterior. Será a ANPD que avaliará o nível de proteção de dados do país estrangeiro ou do organismo internacional, verificando se as garantias fundamentais são observadas, o que, em nível europeu, é denominado decisão de adequação. Também será atribuição da autoridade nacional de proteção certificar os selos, códigos de conduta e certificados e definir conteúdo de cláusulas-padrão contratuais e cláusulas específicas para transferências internacionais.

A especialidade dos trabalhadores envolvidos nas atividades da ANPD é de fundamental importância para o desenvolvimento das diversas e diversificadas atribuições da autoridade de proteção. A realização de cursos profissionalizantes e capacitatórios é urgente, pois a implementação dos propósitos da ANPD é complexa e exige trabalhadores qualificados. A independência e a autonomia decisória da autoridade de proteção de dados são essenciais para a execução de um nível de proteção de dados no país adequado, o que requer profissionais especializados.

São desafios da Autoridade Nacional de Proteção de Dados promover a efetiva garantia dos direitos fundamentais previstos na LGPD, entre eles a autodeterminação informativa, o livre desenvolvimento, a privacidade e a liberdade e, ao mesmo tempo, permitir o fluxo de dados para a realização de atividades sociais, econômicas e a inovação tecnológica. O equilíbrio entre essas duas premissas – respeito aos direitos fundamentais e desenvolvimento tecnológico – norteia todos os institutos do novo marco regulatório da proteção de dados pessoais brasileiro.¹⁴

14 Referências: BEZERRA, Maria Ruth Borges. *Autoridade Nacional de Proteção de Dados Pessoais: a importância do modelo institucional independente para a efetividade da Lei*. 2019. p. 17. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3828/1660> Acesso em: 20 out. 2021. BRASIL. Lei 13.709, de 14 de agosto de 2018. Brasília: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 19 out. 2021. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA. Regulamento Geral de Proteção de Dados. REGULAMENTO (UE) 2016/679. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679> Acesso em: 20 out. 2021.

B

BANCO DE DADOS (art 5.º, IV)

ALINE DAL BÓ CORREA¹⁵

Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.¹⁶

BLOQUEIO (art. 5º, XIII)

ALINE DAL BÓ CORREA¹⁷

De acordo com a LGPD, o bloqueio é a suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados. Este bloqueio pode ser solicitado pelo próprio titular ou ser uma penalidade por infração à LGPD.¹⁸

BOA-FÉ (art. 6º)

ALINE DAL BÓ CORREA¹⁹

Está previsto no artigo 6º da LGPD que as atividades de tratamento de dados pessoais deverão observar a boa-fé e uma série de princípios listados. A boa-fé consiste na adoção da conduta correta e adequada no agir em sociedade, portanto, torna-se premissa básica no tratamento de dados pessoais. É preciso refletir sobre questões como “Qual o objetivo deste tratamento?”, “É preciso mesmo utilizar essa quantidade de dados?”, “O cidadão com quem me relaciono deu o consentimento?”, “O uso dos dados pode gerar alguma discriminação?”²⁰

BOAS PRÁTICAS (art. 50)

ALINE DAL BÓ CORREA²¹

Está previsto na LGPD que os controladores e operadores, no âmbito de suas competências, responsáveis pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de

15 Graduada na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedalbo04@gmail.com

16 Referências: DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei Geral de Proteção de Dados - 2. ed. - São Paulo: Thomson Reuters Brasil, 2019.

17 Graduada na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedalbo04@gmail.com

18 Referências: DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei Geral de Proteção de Dados - 2. ed. - São Paulo: Thomson Reuters Brasil, 2019.

19 Graduada na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedalbo04@gmail.com

20 Referências: MIZIARA, Raphael; PESSOA, André; MOLLICONE, Bianca. *Reflexos da LGPD no Direito do Trabalho e no Processo do Trabalho* - 1. ed - São Paulo: Thomson Reuters Brasil, 2020.

21 Graduada na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedalbo04@gmail.com

riscos e outros aspectos relacionados ao tratamento de dados pessoais.²²

BONA FIDE OCCUPATIONS

RAPHAEL MIZIARA²³

Em regra, a exigência de dados sensíveis (artigo 5º, inciso II, da LGPD) no contexto empregatício viola a Lei Geral de Proteção de Dados, especialmente o princípio da necessidade ou da minimização. Contudo, em situações excepcionais, será lícito ao empregador a exigência de dados sensíveis do candidato ao emprego. É o que se dá, por exemplo, nas chamadas qualificações ocupacionais de boa-fé.

Em português, as chamadas “bona fide occupations” significam qualificações ocupacionais de boa-fé. De acordo com o item 2 da Convenção nº 111 da OIT, concernente à discriminação em matéria de emprego e profissão, as distinções, exclusões ou preferências fundadas em qualificações exigidas para um determinado emprego não são consideradas como discriminação. São as chamadas qualificações ocupacionais de boa-fé.

Com efeito, a BFOQ – Bona Fide Occupational Qualification se trata de uma exceção expressa à previsão de discriminação positivada no art. 703, “e”, (1) do Civil Rights Act, a qual menciona que não será ilegal uma prática de contratar diretamente empregados, ou por meio de agências de empregos, com base nos motivos proibidos, em certas situações em que a religião, sexo ou origem nacional é uma qualificação vocacional de boa-fé, necessária para a operação normal de determinado negócio ou empreendimento.

Firmino Alves Lima enumera exemplos de BFOQ citados pela doutrina norte-americana e que foram aceitos com sucesso pela jurisprudência estrangeira. Podem ser citados: a) o caso de uma garçonete de origem chinesa para laborar em um restaurante chinês autêntico; b) alguns casos em que a privacidade dos clientes de determinada atividade exige pessoas de determinado sexo, como enfermeiras em determinados tipos de hospitais²⁴.

Logo, não será ilegal uma prática de exigir certos dados sensíveis visando a contratação de tais empregados, com base nos motivos em regra proibidos. Em certas situações em que a religião, sexo ou origem nacional são uma qualificação vocacional de boa-fé, necessária para a operação normal de determinado negócio ou empreendimento

Assim, há um direito para discriminar, mas mediante uma razão que seria a qualificação ocupacional de boa-fé, necessária ao normal desenvolvimento e operação de um particular negócio, sendo que o ônus da prova é do empregador para articular e demonstrar motivos que justifiquem o trato diferenciado.

22 Referências: LIMBERGER, Têmis, SZINVELSKI, Mártin, SALDANHA, Jânia. *Transnacionalização e selos de qualidade em proteção de dados: um novo campo de estudo na era digital*. Revista dos Tribunais, vol. 1020, p.143-162, out, 2020. DONEDA, Danilo (org) et al. *Boas práticas e governança na LGPD*. Rio de Janeiro: Forense, 2021.

23 Doutorando em Direito do Trabalho pela Faculdade de Direito da Universidade de São Paulo (USP). Mestre em Direito do Trabalho e das Relações Sociais pela UDF. Especialista em Direito do Trabalho pela Universidad Castilla-La Mancha (UCLM – Espanha). Advogado. Professor em cursos de graduação e pós-graduação em Direito. rmiziara@usp.br

24 LIMA, Firmino Alves. *Teoria da discriminação nas relações de trabalho*. Rio de Janeiro: Elsevier, 2011. p. 142-143.

CONSENTIMENTO (art 8º)

FERNANDA JULIANE BRUM CORRÊA²⁵

O consentimento, expressamente definido pela Lei Geral de Proteção de Dados como a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5.º, XII), foi previsto como uma das hipóteses autorizadoras do tratamento de dados (art. 8º).

A preocupação com o consentimento acerca de dados já foi revelada em textos legais anteriores, a exemplo do Código de Defesa do Consumidor (Lei 8.078/90, art. 43), que conferiu ao consumidor o direito de controlar as informações. Também esteve presente na Lei do Cadastro Positivo (Lei 12.414/2011, com redação anterior a 2019) e no Marco Civil da Internet (Lei 12.965/2014), conforme pontua Bruno Bioni.

Na LGPD, por outro lado, o consentimento ganhou novas dimensões e, na linha do que expõe Raphael Miziara, entre os diversos elementos da cadeia de proteção conferida por esta lei, pode ter aptidão a garantir a autodeterminação informativa, um dos fundamentos da referida lei, compreendida como o poder de o titular dos dados de comandar a gestão destes, o que inclui o acesso, a retificação, a transposição a outro controlador e a eliminação de informações. Nesse panorama, a lei prevê situações excepcionais em que o tratamento de dados pode ser realizado sem o consentimento (art. 7º, II-X; art.11, II; e art. 14, §3º), todavia este afigura-se uma das mais importantes causas legitimadoras.

A adoção do consentimento como hipótese legitimadora pressupõe a observância de forma escrita ou de outro meio que demonstre a manifestação de vontade, de modo que não é admitido o consentimento tácito. Além disso, depende de expressa referência a finalidades determinadas, havendo vedação a autorizações genéricas. Proíbe-se, assim, o consentimento generalista, sem destinação a fins ou pessoas específicas, ou mesmo sua extensão a outras etapas não previstas, característica que a doutrina vem denominando de granularidade. Além desses requisitos, a lei explicita a possibilidade de revogação do consentimento, a qual deve ser informada ao titular.

Nesse contexto, o consentimento informado – na acepção de consentimento verdadeiramente esclarecido – dependeria do fornecimento de todas as informações para que o titular dos dados compreenda o que está fornecendo ou autorizando, bem como a finalidade e o alcance das informações. Sobre o ponto, Bruno Bioni destaca que a complexidade do fluxo informacional - composto por pedaços de informações e um miríade de sujeitos -, somada às limitações cognitivas do ser humano, torna difícil o real entendimento sobre o desenrolar efetivo dos seus dados. Com argumentos que perpassam desde a tendência humana a focar nos bene-

25 Analista Judiciário do TRT da 4ª Região. Graduada em Direito pela Universidade Federal de Santa Maria. Especialista em Direito do Trabalho e Processo do Trabalho pela Faculdade Damásio. fernanda.brum@trt4.jus.br

fícios imediatos, discorrem sobre a lógica de escolha baseada nas perdas maiores que ganhos (produto gratuito, por exemplo) e culminam na questão do paradoxo da privacidade, questiona a amplitude real do consentimento, ou sua contaminação por fatores sobre os quais conscientemente o titular nem mesmo pondera.

No âmbito das relações de trabalho, em que há evidente assimetria entre as partes contratantes, sua adoção como hipótese legitimadora do tratamento de dados carrega inúmeros riscos. O desequilíbrio de poder e a dependência econômica (como regra) podem conduzir a presunções de que o empregado não teve legítima escolha, mas foi compelido a consentir como condição, ainda que tácita, de manutenção do vínculo. Diante da inexistência ou escassez de poder de barganha do empregado titular dos dados, a liberdade do consentimento (como manifestação *livre*, conforme já citado art. 5º, XII) restaria prejudicada.

A manifesta influência do desequilíbrio de poder (*imbalance of power*) na regularidade do consentimento foi, inclusive, prevista na General Data Protection Regulation (GDPR), vigente na União Europeia, como situação que invalida seu uso como fundamento jurídico para o tratamento de dados. Transcreve-se o considerando 43, referente ao art. 7º da GDPR:

A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução.

Sobre a presunção de vício no consentimento na relação laboral, discute-se acerca do menor risco de adoção ao empregado *hiperssuficiente* - figura criada com a Lei 13.467/2017, no art. 444 da CLT-, uma vez que este teria maiores possibilidades de renúncia e transação de direitos e, assim, maior liberdade, tornando o consentimento um pouco mais próximo do real. De qualquer modo, somente a aplicação reiterada da lei aos casos em concreto poderá mostrar os rumos jurisprudenciais.

Por ora, diante de uma lei tão nova e cuja aplicação ainda suscita muitos questionamentos, no contexto das relações laborais sugere-se que o consentimento não seja utilizado prioritariamente como base para o tratamento de dados, exceto para

situações excepcionais e alheias ao objeto central do contrato, como, por exemplo, para autorização de fotografias no ambiente de trabalho.²⁶

CONTROLADOR (art. 5.º, VI)

FERNANDA JULIANE BRUM CORRÊA²⁷

É um dos agentes de tratamento de dados, definido pela legislação como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Trata-se, assim, daquele que detém o domínio dos fatos acerca das operações de tratamento e, por essa razão, no regulamento europeu (GDPR) é designado como “responsável pelo tratamento” (art. 4º, item 7).

Quando o tratamento de dados for baseado no consentimento, cabe ao controlador o ônus da prova de que o consentimento foi dado em conformidade com a lei (art. 8º, §2º). Por outro lado, quando o tratamento de dados sensíveis ocorrer por previsão legal, mediante dispensa de consentimento, é obrigação do controlador publicizar essa situação (art. 11, §2º).

No âmbito das relações de trabalho subordinado, a relevância da identificação e conceituação do controlador é ainda mais premente, para que os titulares de dados possam exercer seus direitos. Neste caso, como regra, o controlador será o empregador, visto que é quem obtém os dados e indica o tratamento a ser conferido.²⁸

CRIANÇA E ADOLESCENTE (art. 14)

BÁRBARA FAGUNDES²⁹

A Lei Geral de Proteção de Dados, Lei n.º 13.709/2018, apresenta um dispositivo específico quanto aos dados de crianças e de adolescentes, qual seja, o artigo 14. No entanto, mesmo antes do surgimento da mencionada legislação, a intimidade, a vida privada e mesmo dados de crianças e de adolescentes já eram tutelados tanto por normas internacionais quanto por normas internas. No plano internacional, pode-se citar o art. 40, item 7, da Convenção sobre os Direitos da Criança da ONU que, em síntese, estabelece que *todas as crianças que, alegadamente, teriam infringido a legislação penal tenham plenamente respeitada sua vida privada durante todas as fases do processo*.

Seguindo essa diretriz, o Estatuto da Criança e do Adolescente, em seu art.

26 Referências: BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 3 ed. – Rio de Janeiro: Forense, 2021. MIZIARA, Raphael. *Reflexos da LGPD no Direito e no processo do trabalho* (livro eletrônico). Raphael Miziara, André Pessoa, Bianca Mollicone – 1. ed. - São Paulo: Thomson Reuters Brasil, 2020. PINHEIRO, Iuri. *Manual do compliance trabalhista: teoria e prática*. Fabrício Silva Lima, Iuri Pinheiro, Vólia Bomfim. 2 ed. – Salvador: Juspodivm, 2021.

27 Analista Judiciário do TRT da 4ª Região. Graduada em Direito pela Universidade Federal de Santa Maria. Especialista em Direito do Trabalho e Processo do Trabalho pela Faculdade Damásio. fernanda.brum@trt4.jus.br

28 Referências: MIZIARA, Raphael. *Reflexos da LGPD no Direito e no processo do trabalho* (livro eletrônico). Raphael Miziara, André Pessoa, Bianca Mollicone – 1. ed. - São Paulo: Thomson Reuters Brasil, 2020. PINHEIRO, Patricia Peck. *Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)*. 2. ed. – São Paulo: Saraiva Educação, 2020.

29 Juíza do Trabalho Substituta do TRT da 4ª Região, Mestre em Direito pela Universidade Federal do Rio Grande do Sul (UFRGS) barbara.fagundes@trt4.jus.br

143, proíbe a identificação de criança ou adolescente acusado de cometer ato infracional, vedando-se fotografia, referência a nome, apelido, filiação, parentesco, residência. Com a Lei n.º 10.764/2003, mesmo iniciais do nome e do sobrenome de crianças e de adolescentes não podem ser veiculadas à notícia do ato infracional. Assim, a preocupação quanto aos dados de crianças e de adolescentes precede a LGPD.

Segundo o artigo 14, *o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse*. A citada expressão é utilizada diversas vezes na Convenção sobre Direitos da Criança da ONU. Logo, no aspecto, o artigo da LGPD é compatível com a normativa internacional quanto à tutela da criança.

Para que os dados pessoais da criança sejam tratados, é necessário o consentimento específico e destacado de ao menos um dos pais ou de um responsável legal. Note-se que a expressão *adolescente* não é citada no art. 14, §1º da LGPD. No entanto, mesmo com a citada lacuna legislativa, pressupõe-se, com base no *caput* do dispositivo, no art. 227 da Constituição Federal, nas normas internacionais que integram o *corpus iuris* internacional de proteção da criança, como a Convenção sobre Direitos da Criança da ONU e a Convenção 182 da OIT que trata das piores formas de trabalho infantil, que estabelecem que criança é o indivíduo de até 18 anos, que mesmo quanto aos dados dos adolescentes, é necessário o consentimento parental para o seu tratamento. É oportuno lembrar que, no âmbito da União Europeia, a General Data Protection Regulation (GDPR) estabelece que o tratamento de dados de pessoas com até 16 anos necessita de consentimento parental ou de responsável legal, podendo os Estados reduzirem o critério etário desde que não seja inferior a 13 anos.

Outra fonte que reforça a interpretação de que os adolescentes também dependem do consentimento parental para ter seus dados tratados é o art. 439 da CLT, dispositivo que permite ao jovem trabalhador firmar recibos de recebimento de salário, mas veda que o indivíduo com menos de 18 anos dê quitação ao empregador quanto à indenização devida no caso de extinção contratual sem a assistência dos responsáveis legais. Disso se pode concluir que para o tratamento de dados de adolescentes trabalhadores, ou seja, indivíduos de 14 a 18 anos, faixa etária em que se permite o trabalho do adolescente, conforme art. 7º, XXXIII, da Constituição Federal, no âmbito de uma relação de trabalho, é necessário o consentimento de um dos pais ou de um responsável legal.

É necessário também que o adolescente trabalhador, o que inclui aprendizes e estagiários, consiga entender o tratamento que será dado pelo empregador ou contratante quanto aos seus dados pessoais. A linguagem a ser utilizada quanto à informação sobre o tratamento de dados do adolescente trabalhador deve ser compatível com suas características físico-motoras, perceptivas, sensoriais, intelectuais e mentais. Mesmo quanto à criança, entendida esta como o indivíduo de até 12 anos, conforme o direito interno, a LGPD exige que seja concretizado o direito à informação ao estabelecer no §6º do art. 14 que deve ser observado seu adequado entendimento. Há na LGPD a promoção da educação sobre o tratamento de dados desde a infância, razão pela qual o adolescente trabalhador também

tem direito à adequada informação, ainda que seja necessário o consentimento parental para a consecução do tratamento de dados.

Deve-se também conferir proteção aos dados de crianças e adolescentes que, embora não mantenham relação de emprego ou trabalho, tenham seus dados tratados em razão do contrato de trabalho mantido por um de seus pais ou responsáveis, como no caso de percepção pelo empregado de salário família quando este tem filhos de até 14 anos ou com algum tipo de deficiência, nos termos dos arts. 65 a 70 da Lei n.º 8.213/1991.

Nesses casos, o pai ou o responsável empregado deve fornecer a certidão de nascimento do dependente, caderneta de vacinação ou equivalente para menores de seis anos (dado pessoal sensível da criança, conforme art. 5º, II, da LGPD) ou comprovante de frequência escolar dos dependentes de sete a 14 anos. Presume-se que o fornecimento desses dados ao empregador atende ao melhor interesse da criança e do adolescente quando tem por finalidade aumentar a renda da família, conceder algum benefício ao genitor ou ao dependente titular do dado.

Não haveria, assim, necessidade do consentimento da criança e do adolescente para o tratamento desses dados, mas apenas o consentimento parental. A LGPD não demanda que o tratamento de dados do adolescente maior de 16 anos tenha de ser feito com consentimento conjunto do titular impúbere, determinando apenas que seja observado o melhor interesse do adolescente.

Manter dados dos dependentes do empregado atende ao melhor interesse da criança e do adolescente e também ao legítimo interesse do controlador/empregador, pois, em caso de falecimento do empregado genitor ou responsável, o empregador terá ciência de quem são os dependentes previdenciários, podendo entrar em contato com estes ou mesmo ajuizar ação de consignação em pagamento para a quitação de valores decorrentes da extinção contratual na forma do art. 1º, *caput*, da Lei n.º 6.858/1980.³⁰

D

DADO ANONIMIZADO (art. 5º, III)

FERNANDA JULIANE BRUM CORRÊA³¹

A lei define dado anonimizado como aquele relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Assim, é o dado que perdeu a possibilidade de as-

30 Referências: BOTELHO, Marcos César. A LGPD E A PROTEÇÃO AO TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES. Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE), v. 8, n. 2, 2020. Disponível em: [www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/Rev-Dir-Soc-Pol-Publicas_v.8_n.2.08.pdf]. Acesso em: 27 set. 2021. FOLLONE, Renata Aparecida. Cassiane de Mello Fernandes. PROTEÇÃO DE DADOS PESSOAIS DA CRIANÇA E DO ADOLESCENTE. In: Direito em Movimento: Saberes Transformadores da Sociedade Contemporânea 2. E-book. Disponível em: [https://www.atenaeditora.com.br/post-artigo/36952]. Acesso em: 27.09.2021. TEFFÉ, Chiara Spadaccini de. PROTEÇÃO DE DADOS DE CRIANÇAS E ADOLESCENTES. Revista do Advogado, São Paulo, AASP, n. 144, p. 54-9 nov. 2019.

31 Analista Judiciário do TRT da 4ª Região. Graduada em Direito pela Universidade Federal de Santa Maria. Especialista em Direito do Trabalho e Processo do Trabalho pela Faculdade Damásio. fernanda.brum@trt4.jus.br

sociação, direta ou indireta, a um indivíduo, porque se rompeu a vinculação com caracteres identificadores do titular.

Na prática, são dados que foram submetidos a procedimentos como a supressão ou generalização, de modo que não é mais possível sua atribuição específica a um titular. Um exemplo de dado anonimizado por supressão é a eliminação de dado identificado bem específico, como o número do CPF, o qual seria capaz de destacar e identificar até mesmo pessoas homônimas. Outro exemplo, mas de anonimização por generalização, é a utilização de faixa etária como dado de clientes, porquanto não permite a distinção dos titulares específicos. Com isso, diante de um espectro de informações presente em um banco de dados, não seria possível a identificação ou associação do titular destes, direta ou indiretamente.

Para o art. 12, tais dados não são considerados pessoais, o que os excluiria da proteção da norma, previsão similar à contida na GDPR, conforme preâmbulo, que afasta a proteção de dados das informações anônimas, assim entendidas como as que não se relacionem a pessoa identificada ou identificável. Contudo, tal artigo não considera as possibilidades de reversão - com identificação de pessoas a partir de algoritmos, o que ocorre, por exemplo, na identificação de hábitos de compra - e a circunstância de que os métodos de anonimização ainda “são considerados corruptíveis e passíveis de falhas”.³²

DADO BIOMÉTRICO

MARCELO LUCCA³³

Dado biométrico é toda aquela propriedade física, fisiológica, comportamental ou de traço de personalidade, atribuível a uma única pessoa e que seja mensurável, a partir da qual o dano por furto ou uso indevido é potencialmente irreversível, uma vez que os dados biométricos de um indivíduo não podem ser alterados a não ser de forma permanente, e uma vez alterado, perde-se a segurança no seu uso.³⁴

Conforme Mayer³⁵, Biometria é a ciência e tecnologia dedicada a medir e analisar dados biológicos. No campo dos dados inseridos em sistemas digitais, a biometria refere-se ao conjunto de tecnologias que medem e analisam as características do corpo humano, como DNA, impressões digitais, a retina e a íris dos olhos, padrões faciais ou a voz, entre outros, a fim de identificar pessoas.

Os dados biométricos são, portanto, aqueles que permitem identificar uma pessoa física por meio de processos técnicos, que coletam informações relacionadas ao aspecto físico, corporal ou comportamental. Como sua imagem facial,

32 Referências: PINHEIRO, Patricia Peck. *Proteção de dados pessoais: comentários à Lei n.º 13.709/2018 (LGPD)*. 2. ed. – São Paulo: Saraiva Educação, 2020.

33 Doutorando em Direito (UFRGS); Mestre e Bacharel em Direito; Mestre em Prevenção de Riscos; Eng. Civil e de Segurança do Trabalho. Servidor e chefe da unidade de Perícias Judiciais do TRT da 4ª Região.

34 L.P.V. Lombardi; M.C.C.L. Santos. Proteção de dados genéticos e o direito à intimidade como direito fundamental na dignidade humana. In: M.C.C.L.(org.). *Declaração Universal dos Direitos Humanos 70 anos depois*. Porto: Editorial Juruá, 2018.

35 MAYER, Virginia. *Protección de datos biométricos en Argentina: Análisis del marco legal vigente y de las tecnologías incorporadas a su almacenamiento*. Disponível em http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1593_MayerVI.pdf. Acesso em: 19 out. 2021.

impressão digital ou algo semelhante.³⁶

A principal novidade estabelecida pela LGPD, que torna importante analisar o impacto causado por esse tratamento, é a modificação da qualificação dos dados biométricos como dados sensíveis.

De acordo com sua natureza, os dados biométricos são divididos em três categorias principais:

Universal: são os dados que existem em todas as pessoas, sem distinção;

Único: dados distinguíveis em cada indivíduo;

Permanente: dados mantidos continuamente.

Por outro lado, de acordo com as características individuais que coletam, dois grupos se diferenciam:

Características físicas e fisiológicas	Características comportamentais e de personalidade
Impressão digital	Reconhecimento de assinatura
Reconhecimento facial	Reconhecimento de caligrafia
Reconhecimento de íris	Reconhecimento de voz
Geometria da mão	Reconhecimento de escrita manual do teclado
Reconhecimento de retina	Reconhecimento de marcha
Reconhecimento vascular	

Breves comentários sobre cada um deles:

Impressão digital. A impressão digital é um dos dados biométricos mais usados. Apresenta vantagens importantes como baixo custo de implantação e fácil adaptação. Também possui um índice de alta precisão³⁷. Há dois métodos principais para coletar impressões digitais:

“Com base em minúcias”: através dela, são identificadas as formas da impressão digital e sua localização dentro dela.

“Com base em correlação” examina a impressão digital de forma abrangente.

Reconhecimento facial. Os sistemas de reconhecimento facial permitem identificar uma pessoa por meio da análise das características biométricas de seu rosto.

O rosto será analisado por determinados programas de cálculo que o comparam
36 SANTOS, M.C.C.L. Limites éticos e jurídicos do Projeto Genoma Humano. In: SANTOS, M.C. C.L. (org.). Biodireito: ciência da vida, os novos desafios. São Paulo: Revista dos Tribunais, 2001.

37 UNAM - Facultad de Ingeniería Biometría Informática -Clasificación de Sistemas: Reconocimiento de Huellas - <http://redyseguridad.fip.unam.mx/proyectos/biometria/clasificacionsistemas/recohuella.html>

com a fotografia ou imagem obtida anteriormente. Uma das vantagens desse sistema é que ele é muito discreto e quase não é necessária a participação do usuário. Os sistemas de reconhecimento facial existentes são:

Geométricas: levam em consideração as características faciais do indivíduo: olhos, nariz, boca etc. Eles também usam avaliações dos ângulos da face e cálculos de distâncias entre os diferentes recursos.

Fotométrica, fornece informações de forma global, de toda a face.

Misturados, eles adicionam elementos dos dois anteriores.

É importante levar em consideração as consequências que a idade tem nos rostos. E as mudanças que as pessoas podem sofrer com o uso de óculos, pelos faciais etc.

Reconhecimento de íris. O reconhecimento da íris é a técnica de identificação mais confiável, pois a íris das pessoas não muda com o tempo. Para esse reconhecimento, é utilizada uma câmera infravermelha, que tira uma fotografia do olho, e por meio dela são obtidos os detalhes da íris.

Reconhecimento da geometria da mão. Esse reconhecimento é baseado na captura de uma imagem 3D da mão da pessoa. Por meio dele, todos os detalhes possíveis serão obtidos. Por exemplo, as medidas da mão, sua estrutura óssea ou o comprimento e a espessura dos dedos. Esta técnica pode não ser muito confiável no caso de a pessoa sofrer uma lesão nas mãos.

Reconhecimento de retina. O reconhecimento retinal é um bom sistema de identificação biométrica, uma vez que a retina, assim como a impressão digital, é única para cada pessoa. Por meio de uma câmera infravermelha, a retina é digitalizada. Essa técnica torna a falsificação difícil, mas é considerada mais invasiva do que o reconhecimento da íris.

Reconhecimento vascular. Esta técnica biométrica consiste no estudo da geometria da árvore das veias do dedo ou dos punhos. O formato da veia é capturado por meio de um processo diferencial de absorção dos feixes de luz do espectro infravermelho. Semelhante ao usado por câmeras de circuito fechado de televisão para visualização em ambientes sem luz visível.

Reconhecimento de assinatura. O reconhecimento de assinaturas é o sistema mais amplamente utilizado no mundo como método de autenticação. Por meio desse sistema, a assinatura é examinada. Os seguintes métodos podem ser usados para isso:

Comparação simples (semelhança entre duas assinaturas).

Teste dinâmico (forma e velocidade são estudadas).

Reconhecimento de caligrafia. Existem dois tipos de reconhecimentos: está-

ticos e dinâmicos. São analisadas as características personalíssimas, decorrentes da assimilação idiogenética (nível de pressão, inclinação, ataque e arremate do grafismo).

Reconhecimento de voz. Para reconhecimento de voz são utilizados aplicativos com algoritmos que medem as amostras e retornam o resultado com a identificação daquela pessoa.

Reconhecimento de escrita manual do teclado. Este tipo de reconhecimento analisará os seguintes elementos: a) a energia com a qual a pessoa digita; b) o tempo de pulsação; c) o tempo decorrido entre duas teclas.

Reconhecimento de marcha. Este sistema consiste em examinar a marcha da pessoa por meio de almofadas especiais no chão e uma câmera de alta resolução. Essa câmera de alta definição medirá a distribuição de peso, velocidade do passo e marcha.

Outros tipos de exames biométricos. Existem também outros reconhecimentos para identificar pessoas, como o estudo da palma da mão, o formato das orelhas, o DNA ou a pele.

DADO PESSOAL (art. 5º, I)

MAX CARRION BRUECKNER³⁸

Conforme art. 5º, I, da LGPD, considera-se dado pessoal toda informação relacionada a pessoa natural identificada ou identificável. Esse conceito é idêntico ao existente no art. 4º, 1, do Regulamento Geral de Proteção de Dados (GDPR) europeu.

Os dados pessoais são aqueles que dizem respeito a uma pessoa natural. Incluem-se aí os dados biométricos, que podem ser definidos como “aqueles relacionados às características físicas, fisiológicas e comportamentais de uma pessoa natural que permitem ou confirmam de maneira inequívoca a sua identidade, tais como imagens faciais ou impressões digitais”. Não se consideram dados pessoais, portanto, os dados relativos a pessoas jurídicas.

Embora a LGPD não explique o que é “pessoa natural identificada ou identificável”, o GDPR esclarece que identificável é a pessoa natural “que possa ser identificada, direta ou indiretamente”, em especial por referência a um identificador (p. ex., nome, CPF, dados de localização, identificadores eletrônicos ou outros elementos específicos relacionados a essa pessoa natural), sendo razoável que o mesmo conceito seja adotado no Brasil.

Nesse contexto, dados anonimizados (isto é, aqueles que não podem ser relacionados a uma determinada pessoa) não são considerados dados pessoais, conforme art. 12 da LGPD.³⁹

³⁸ Juiz do Trabalho Substituto do TRT da 4ª Região.

³⁹ Referências: BARZOTTO, Luciane Cardoso. *LGPD e Desafios Recentes da Negociação Coletiva no Brasil*. In: Revista LTr, vol. 85, nº 6, junho de 2021, p. 733-742. BUCHAIN, Luiz Carlos. A Lei Geral de Proteção de Dados: Noções Gerais. In Revista Eletrônica do TRT do Paraná, ano X, nº 96, 2021, p. 51-66. LEONARDI, Marcel. *Legítimo Interesse*. In: Revista do Advogado, ano XXXIX, nº 144, novembro de 2019, p. 67-73.

DADO PESSOAL SENSÍVEL - I (art. 5º, II)

MAX CARRION BRUECKNER⁴⁰

Conforme art. 5º, II, da LGPD, considera-se dado pessoal sensível o dado pessoal “sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”. Trata-se, portanto, de um conjunto de dados cujo tratamento pode implicar riscos significativos para os direitos e liberdades fundamentais.

Diante da natureza desses dados, o consentimento para o seu tratamento deve ser qualificado pela finalidade, isto é, deve ser limitado pelo propósito pelo qual os dados foram coletados. Por exemplo, a coleta de dados por uma seguradora a respeito de doenças preexistentes não pode ser utilizada para obter informações a respeito de outras questões envolvendo o indivíduo. Em outras palavras, dada a autorização para o tratamento dos dados com relação ao objeto “doenças preexistentes”, o acesso a esses dados não pode envolver outras questões. Veja-se, a propósito, o item 42 da exposição de motivos do GDPR europeu.

Por implicar restrição ao tratamento dos dados, considera-se que o rol previsto na LGPD é taxativo. Nesse sentido: LEONARDI, 2019. Em sentido contrário: MULHOLLAND, 2019.⁴¹

DADO PESSOAL SENSÍVEL - II

MARCO AURÉLIO SERAU JUNIOR⁴²

Dentro de uma perspectiva geral conferida pelo ordenamento jurídico a determinados dados pessoais, ampliando, especificando e aprimorando a proteção ao campo da privacidade e da intimidade, observou-se recentemente, sobretudo diante do impacto causado na sociedade pelas novas tecnologias de comunicação e informação (conhecidas pela sigla TIC), a edição da Lei Geral de Proteção de Dados – LGPD, Lei nº 13.709/2018.

Essa norma bastante relevante apresenta uma série de repercussões no campo do Direito do Trabalho, dos quais merece destaque o tema dos dados pessoais sensíveis, categoria criada pela LGPD em seu art. 5º, inciso II:

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

40 Juiz do Trabalho Substituto do TRT da 4ª Região.

41 Referências: BARZOTTO, Luciane Cardoso. LGPD e Desafios Recentes da Negociação Coletiva no Brasil. In: Revista LTr, vol. 85, nº 6, junho de 2021, pp. 733-742. LEONARDI, Marcel. *Legítimo Interesse*. In: Revista do Advogado, ano XXXIX, nº 144, novembro de 2019, pp. 67-73. MULHOLLAND, Caitlin. *Dados Pessoais Sensíveis e Consentimento na Lei Geral de Proteção de Dados*. In: Revista do Advogado, ano XXXIX, nº 144, novembro de 2019, pp. 46-52.

42 Doutor e Mestre em Direitos Humanos pela USP. Professor da UFPR – Universidade Federal do Paraná. Advogado. maseraunior@hotmail.com

Dado pessoal é toda “informação relacionada a pessoa natural identificada ou identificável” (art. 5º, I, da Lei 13.709/2018). O dado pessoal sensível, por sua vez, é um tipo de dado pessoal considerado pela LGPD como um segmento mais relevante de informações sobre a pessoa natural e, assim, merecedor de proteção jurídica mais significativa, prevista no art. 11, da Lei 13.709/2018:

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

Tratamento é, em linhas gerais, o manuseio das informações da pessoa natural e, conforme o art. 5º, X, da LGPD, abrange uma vasta gama de possibilidades:

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamen-

to, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

O tratamento de dados pessoais sensíveis poderá ocorrer de forma consentida ou, mesmo sem o consentimento pessoal, para algumas finalidades de interesse público listadas no art. 11 da LGPD.

As hipóteses previstas no art. 11, II, da LGPD, são taxativas, isto é, não poderão ser ampliadas por interpretação extensiva ou analogia, visto que a hermenêutica de qualquer norma de tutela de direitos fundamentais impede sua restrição para além do que expressamente previsto em lei.

Dos temas indicados pela LGPD como dados pessoais sensíveis, é bastante evidente a repercussão trabalhista da menção à “filiação a sindicato”.

A Constituição Federal, na esteira do que estabelece a OIT – Organização Internacional do Trabalho, assegura a livre associação sindical (art. 8º, caput). A formação de bancos de dados sobre quais empregados sejam ou não filiados a sindicatos (“listas negras”) pode configurar alguma forma de intervenção ou restrição a esse direito fundamental, motivando perseguições ou discriminações no ambiente de trabalho.

Todavia, a formação de cadastros dos sindicalizados poderá ocorrer, licitamente, quando se tratar do cumprimento de decisões judiciais que promovam direitos destes empregados ou mesmo para cobrança das contribuições sindicais, bem como para alcance de direitos tratados em convenções coletivas ou acordos coletivos de trabalho.

Nesse sentido, o banco de dados sobre aqueles e aquelas filiados ao sindicato terá como objetivo o exercício regular de direitos (art. 11, II, d, da LGPD), e será limitado pelos princípios da finalidade, adequação e necessidade estabelecidos na própria LGPD:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

Os outros pontos mencionados como dados pessoais sensíveis, embora não configurem diretamente matéria trabalhista, podem apresentar reflexos igualmente

te marcantes no Direito do Trabalho.

O acesso e utilização de dados referentes à “saúde ou à vida sexual, dado genético ou biométrico”, porventura obtidos em cadastros/bancos de dados do convênio médico patrocinado pela empresa ou em fichas/formulários a serem preenchidos pelos empregados e empregadas, ou mesmo durante a realização dos exames médicos periódicos, pode motivar ou acarretar a despedida de certas pessoas, que usufruam ou possam a vir a usufruir de afastamentos por motivos de saúde (auxílio-doença ou outras hipóteses de suspensão do contrato de trabalho).

Esse cenário, todavia, pode configurar despedida discriminatória. Conforme a Súmula 443 do TST – Tribunal Superior do Trabalho, é considerada discriminatória a despedida do empregado portador do vírus HIV, e esse entendimento muitas vezes é ampliado para outros tipos de doença, a exemplo do câncer ou do alcoolismo.

O tema do acesso aos dados referentes à saúde perpassa a discussão sobre a possibilidade de a empresa exigir exames toxicológicos e antecedentes criminais de seus funcionários, bem como testes de gravidez ou atestados de esterilidade, temas controversos na jurisprudência.

O conceito de dados pessoais sensíveis ainda contempla outros tópicos, referentes a “origem racial ou étnica, convicção religiosa, opinião política”, bem como filiação a “organização de caráter religioso, filosófico ou político”.

Esses pontos já registram, mesmo antes da vigência da LGPD, algumas vivências problemáticas no ambiente laboral, encontrando-se na jurisprudência diversos casos de assédio moral e dano moral trabalhista de cunho racial, étnico, religioso e político. Atualmente, esses bens jurídicos foram tutelados de modo mais robusto na Convenção 190 da OIT.

Compreendemos que a proteção aos dados pessoais sensíveis também se espalha no que concerne aos elementos pré-contratuais da relação de emprego, a exemplo de determinadas condutas ou perguntas realizadas durante o processo de contratação do empregado e da empregada (a exemplo da já mencionada requisição de atestados de gravidez ou informações sobre a condição de maternidade e idade dos filhos).⁴³

DIREITO DOS TITULARES

GILBERTO DESTRO⁴⁴

O titular dos dados tem os seguintes direitos específicos: i) consentir ou não com o uso de seus dados pessoais para a finalidade que agente de tratamento lhe informar, podendo revogar o consentimento anteriormente fornecido; ii) saber sobre a possibilidade de negar o consentimento e as consequências da negativa; iii) confirmar a existência de tratamento dos dados; iv) acessar os dados; v) pe-

⁴³ Referências: MIZIARA, Raphael. *Reflexos da LGPD no Direito e no processo do trabalho* (livro eletrônico). Raphael Miziara, André Pessoa, Bianca Mollicone – 1. ed. - São Paulo: Thomson Reuters Brasil, 2020. ROMITA, Arion Sayão. *Direitos Fundamentais nas relações de trabalho* – 3 ed. – S. Paulo: LTr, 2009. SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais* – 4 ed. – Porto Alegre: Livraria do Advogado, 2004.

⁴⁴ Juiz Titular de Vara do Trabalho no TRT da 4ª Região. Especialista em Direito Processual Civil e graduado em Direito pela Universidade do Sul de Santa Catarina.

dir a atualização dos dados ou a correção de dados incompletos ou inexatos; vi) pedir que sejam anonimizados, bloqueados ou eliminados os dados desnecessários, os que excedem à finalidade do tratamento e os que estejam sendo tratados em desconformidade com a lei; vii) pedir a eliminação dos dados mesmo quando fornecido anteriormente o consentimento ao tratamento deles; viii) obter a portabilidade dos dados para tratamento por outro fornecedor de serviço ou produtos; ix) saber com quem o controlador compartilhou o uso dos dados; x) peticionar, em relação aos seus dados, contra o controlador perante a autoridade nacional de proteção de dados ou organismos de defesa do consumidor; xi) opor-se a tratamento indevidamente justificado em hipótese de dispensa de consentimento; xii) apresentar, sem custos, requerimento a agente de tratamento e obter dele resposta de atendimento do direito pretendido ou de esclarecimento sobre quem é o agente de tratamento ou sobre as razões que impedem a adoção imediata de providências (art. 18 da LGPD).

A proteção de dados pessoais na LGPD tem como fundamentos: i) o respeito à privacidade; ii) a autodeterminação informativa; iii) a liberdade de expressão, de informação, de comunicação e de opinião; iv) a inviolabilidade da intimidade, da honra e da imagem; v) o desenvolvimento econômico e tecnológico e a inovação; vi) a livre iniciativa, a livre concorrência e a defesa do consumidor; e vii) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (art. 2º da LGPD).⁴⁵

E

ELIMINAÇÃO (art 5º, XIV)

SUELEN HENTGES⁴⁶

Eliminação é a exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado – consoante definição da própria LGPD. A eliminação pode ser realizada “mediante requisição do titular ou quando cessado o tratamento, ou seja, quando eles deixam de ser necessários”⁴⁷, inclusive mediante revogação de eventual consentimento anteriormente fornecido.

Conforme previsto nos arts. 16 e 18, VI da LGPD, é autorizada a conservação dos dados, mesmo diante do pedido de eliminação realizado pelo titular, para as seguintes finalidades: I - cumprimento de obrigação legal ou regulatória pelo con-

45 Referências: PAMPLONA FILHO, Rodolfo; CONI JUNIOR, Vicente Vasconcelos. *A lei geral de proteção de dados pessoais e seus impactos no direito do trabalho*. Disponível em: <https://revistas.unifacs.br/index.php/redu/article/view/7108>. Acesso em: 13 nov. 2021. PINHEIRO, Iuri; BOMFIM, Vólia. *A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho*. Disponível em: <http://trabalhoemdebate.com.br/artigo/detalhe/a-lei-geral-de-protecao-de-dados-e-seus-impactos-nas-relacoes-de-trabalho>. Acesso em: 13 nov. 2021.

46 Mestranda em Direito pela Universidade Federal do Rio Grande do Sul; graduada em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul; advogada. suelenh@gmail.com

47 OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: FRAZÃO, Ana; TE-PEDINO, Gustavo; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. [e-book]

trolador; II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados (vide verbete anonimização). Tendo em vista que essas hipóteses são exceções, a interpretação deve ser realizada de maneira restritiva, não se admitindo outras situações, ainda que análogas⁴⁸.

O titular pode requerer a eliminação de dados por considerar que estes são desnecessários ou excessivos para a finalidade declaradas quando da coleta, cabendo ao controlador provar que adotou as medidas solicitadas pelo titular⁴⁹. Conforme referido por Doneda⁵⁰, também é possível se valer de habeas data “exclusivo” a fim de eliminar informações.

ENCARREGADO DE DADOS - I

RODRIGO THOMAZINHO COMAR⁵¹

A Lei Geral de Proteção de Dados (LGPD) é a norma que regula a forma de tratamento de dados pessoais de titulares pessoas físicas, seja pelo meio virtual ou físico, com intuito de atender a proteção de direitos fundamentais de privacidade, liberdade, livre desenvolvimento da personalidade dos indivíduos e também, conforme consta na exposição de motivos do regramento, atender a finalidade econômica das organizações.

A regra em questão, influenciada pela diretiva nº 46/1995 do Conselho da Europa e, posteriormente, pelo Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, inaugurou, no país, um “microsistema” voltado a disciplinar a forma com que os dados pessoais de titulares eram manuseados, seja por pessoas físicas ou jurídicas.

De início, importa esclarecer que, de acordo com a disposição normativa nacional, considera-se tratamento de dados o que consta no inciso X do art. 5º: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Neste diapasão, a legislação atribuiu a determinados sujeitos a responsabilidade pela realização do tratamento dos dados, sua segurança e observância dos

48 GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. Término do Tratamento de Dados. In: FRAZÃO, Ana; TEPEDINO; Gustavo; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. [e-book]

49 CONI JUNIOR, Vicente Vasconcelos; PAMPLONA FILHO, Rodolfo. A Lei Geral de Proteção de Dados e seus reflexos nas relações jurídicas trabalhistas. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. (org.). *Reflexos da LGPD no Direito e no Processo do Trabalho*. Editora Revista dos Tribunais: São Paulo, 2020. [e-book]

50 DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020 [e-book]

51 Professor de Direito (Unicesumar). Mestre em Direito Empresarial e Cidadania (Unicuritiba). Especialista em Direito Digital e Compliance (IBMEC/Damásio). Especialista em Direito e Processo Civil (PUCPR). Email:rodrigoadvoc@hotmail.com

princípios elencados em suas disposições, previstos nos incisos IV, VII e VIII do já referido artigo 5º, os quais são denominados de controlador, operador, encarregado de dados.

Desta forma, entende-se como controlador “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”; e, como operador, a “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”.

Na referida relação, denota-se, pela leitura dos incisos VI e VII do artigo 5º, que o controlador é o responsável pelas decisões quanto ao tratamento, enquanto o operador é o que atende e obedece às ordens em nome e sob determinação do controlador, ou seja, o primeiro é o responsável pelas decisões a respeito do tratamento de dados e o último, o executor destas.

Acerca da figura do encarregado de dados, importa ressaltar que a inspiração para sua criação decorre do artigo 37 da GDPR, sendo denominado com Data Protection Officer – DPO e tem suas atividades descritas no artigo 39 do referido documento.

Em que pese a sua semelhança, é de se notar que o encarregado de dados difere do Data Protection Officer na medida em que este último possui papel preponderante nas hipóteses da legislação europeia, enquanto o seu congêneres brasileiro desempenha função de assessoramento ao controlador de dados.

Cabe ressaltar que o encarregado de dados, em razão do que consta na norma brasileira, não será pessoalmente responsável por eventuais falhas ou incidentes com dados, salvo se agir com dolo, diversamente do que ocorre com o Data Protection Officer – DPO.

De outro bordo, ainda em relação à figura do encarregado de dados, a norma o conceitua como sendo o “[...] canal de comunicação entre o controlador, titulares e a Autoridade Nacional de Proteção de Dados” (artigo 5º, VIII), ou seja, o “elo de ligação” entre controlador, titulares e órgão regulatório, do qual deve-se realizar a sua indicação, podendo ser pessoa física ou jurídica, tendo em vista a inexistência de vedação legal para tanto, admitindo-se, inclusive, que tal função seja desempenhada de forma terceirizada ou por empregado, podendo, inclusive, que um mesmo encarregado atue para diferentes organizações.

Não é demais ressaltar, de acordo com o art. 23, III da LGPD, a figura do encarregado tem aplicação tanto para pessoas jurídicas de direito privado como para as de direito público, devendo os dados e a forma de contato deste sujeito de tratamento ser divulgadas publicamente e de maneira clara e objetiva, respeitando, assim, as determinações constantes do art. 41, §1º da LGPD.

A respeito da obrigatoriedade de indicação, convém citar o artigo 41, §3º da referida norma, que permite à ANPD editar normas complementares, sendo certo que o referido Órgão Regulatório poderá dispensar a nomeação para determinadas empresas, a depender do volume de demanda no tratamento de dados, o que, de fato, até o presente momento, não ocorreu.

Outrossim, ainda que em função da natureza eminentemente técnica do cargo, não se vislumbra a necessidade de concessão de gratificação ao empregado, bastando, para tanto, que se faça um aditivo contratual com data de sua nomeação,

que a nomeação seja feita por controlador com poderes para tanto, além da descrição das atividades e responsabilidades do encarregado.

Acerca de suas atribuições, o artigo 41, §2º, da LGPD assim dispôs:

aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; receber comunicações da autoridade nacional e adotar providências; orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Pelo mesmo artigo, ainda é possível destacar que o rol de atividades constantes da norma é exemplificativo, tendo em vista que admite a possibilidade de o controlador ou mesmo a ANPD proceder a um incremento de responsabilidades a serem desenvolvidas pelo encarregado de dados.

Desta feita, em que pese a LGPD não ter sido editada para fins exclusivamente trabalhistas, a estes ela também se aplica, tendo em vista a sua nítida abrangência em relação aos contratos de trabalho e de terceiros que se relacionam com as empresas, além de sua nítida relação da norma em questão com práticas de *compliance*, boas práticas e governança.

Assim, é de se notar que o encarregado de dados também pode atuar, posto que sua atuação também diz respeito a treinamentos, orientações, recebimento de reclamações e também zelar pelo cuidado em relação aos dados de prestadores de serviços, clientes e empregados, cabendo proceder a certificação de regularidade dos sistemas e meios adotados pela organização nesta seara.⁵²

ENCARREGADO - II (art. 5º, VIII)

FERNANDA JULIANE BRUM CORRÊA⁵³

É definido pela lei como a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Não foi previsto como um dos agentes de tratamento (controlador e operador, conforme art. 5º, IX), embora no Capítulo VI, Seção II, conste “do encarregado pelo tratamento de dados pessoais”. Ainda assim, é importante que controlador e operador permitam o acesso aos dados e às operações, para que o encarregado possa bem desempenhar as funções.

52 Referências: BRASIL. Lei 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 15 out. 2021. CARLOTO, Selma. *Lei Geral de Proteção de dados: enfoque nas relações de trabalho*. São Paulo: LTr, 2020. PINHEIRO, Iuri. *Manual do compliance trabalhista: teoria e prática*. Fabrício Silva Lima, Iuri Pinheiro, Vólia Bomfim. 2 ed. Salvador: Juspodivm, 2021. MALDONADO, Viviane Nóbrega (coord.). *Manual do DPO: data protection officer* [livro eletrônico]. 1. ed. São Paulo: Thomson Reuters Brasil, 2021.

53 Analista Judiciário do TRT da 4ª Região. Graduada em Direito pela Universidade Federal de Santa Maria. Especialista em Direito do Trabalho e Processo do Trabalho pela Faculdade Damásio. fernanda.brum@trt4.jus.br

Deve ser indicado pelo controlador (art. 41), mas a ANPD pode estabelecer normas complementares sobre sua definição e atribuições. As atribuições, elencadas em rol exemplificativo (art. 41, §2º), incluem o recebimento de reclamações, prestação de esclarecimento, orientação de empregados sobre práticas acerca da proteção de dados, bem como a execução de outras atribuições determinadas pelo controlador ou por normas complementares.

No regulamento europeu (GDPR), o agente com função similar foi denominado de *Data Protection Officer* (DPO). Cotejando-se a GDPR com a LGPD, constatam-se pontos omissos desta, não havendo esclarecimentos sobre a obrigatoriedade de o encarregado ser detentor de conhecimento jurídico regulatório, sobre a possibilidade de terceirização, sobre a possibilidade de desempenho de outras funções na empresa ou sobre a existência de autonomia. Raphael Miziara recomenda que o encarregado detenha conhecimento jurídico-regulatório, argumenta que a terceirização traz a vantagem da especialização mas aumenta o risco de exposição, e reflete sobre o acréscimo salarial devido ao empregado que passa a acumular a função de “DPO”.⁵⁴

F

FINALIDADE ESPECÍFICA (art. 9º, I)

ALINE DAL BÓ CORREA⁵⁵

Com a LGPD, os dados devem ser tratados com fins específicos e determinados. Todo dado coletado deverá ter, no momento de seu colhimento, a indicação clara e completa que justifique sua coleta.⁵⁶

FINS EXCLUÍDOS DA LEI (art. 4º)

ALINE DAL BÓ CORREA⁵⁷

A LGPD não se aplica ao tratamento de dados pessoais: 1) realizado por pessoa natural para fins exclusivamente particulares e não econômicos; 2) realizado para fins exclusivamente jornalísticos, artísticos e acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 da Lei; 3) realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais; ou 4) provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.⁵⁸

54 Referências: MIZIARA, Raphael. *Reflexos da LGPD no Direito e no processo do trabalho* (livro eletrônico). Raphael Miziara, André Pessoa, Bianca Mollicone – 1. ed. - São Paulo: Thomson Reuters Brasil, 2020.

55 Graduada na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedalbo04@gmail.com

56 Referências: MALDONADO, Viviane Nóbrega, BLUM, Renato Opice. *LGPD: Lei Geral de Proteção de Dados Pessoais comentada* - 3. ed - São Paulo: Thomson Reuters Brasil, 2021.

57 Graduada na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedalbo04@gmail.com

58 Referências: MALDONADO, Viviane Nóbrega, BLUM, Renato Opice. *LGPD: Lei Geral de Proteção*

FISCALIZAÇÃO (art. 52)

ALINE DAL BÓ CORREA⁵⁹

Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: a) advertência; b) multa simples; c) multa diária; d) publicização da infração após devidamente apurada e confirmada a sua ocorrência; e) bloqueio dos dados pessoais a que se refere a infração até a sua regularização; f) eliminação dos dados pessoais a que se refere a infração; g) suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; h) suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; i) proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.⁶⁰

G

GOVERNANÇA (art. 50)

ALINE DAL BÓ CORREA⁶¹

A Lei prevê que os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.⁶²

GRANULARIDADE

FERNANDA JULIANE BRUM CORRÊA⁶³

Ainda que sem essa denominação expressa na LGPD, a granularidade é um atributo aplicável nas situações de coleta de vários dados com finalidades distintas, e é capaz de garantir a efetiva liberdade do consentimento (art. 5º, XII).

A granularidade do consentimento pressupõe a indicação pontual, tanto dos dados aos quais se consente o tratamento, quanto ao fim específico deste trata-

de Dados Pessoais comentada - 3. ed - São Paulo: Thomson Reuters Brasil, 2021.

59 Graduada na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedalbo04@gmail.com

60 Referências: DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei Geral de Proteção de Dados - 2. ed. - São Paulo: Thomson Reuters Brasil, 2019.

61 Graduada na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedalbo04@gmail.com

62 Referências: TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. *Lei Geral de proteção de dados pessoais*: Comentada artigo por artigo - 2. ed - Salvador: Editora JusPodivm, 2020.

63 Analista Judiciário do TRT da 4ª Região. Graduada em Direito pela Universidade Federal de Santa Maria. Especialista em Direito do Trabalho e Processo do Trabalho pela Faculdade Damásio. fernanda.brum@trt4.jus.br

mento, o que se opõe ao consentimento generalista (art. 8º, 4º). Com isso, inibem-se práticas “tudo ou nada”, que conduzem o titular dos dados a permissões além das quais seriam necessárias e ferem, inclusive, o Princípio da Necessidade (art. 6º, III).⁶⁴

H

HONRA (art 2º da LGPD e art. 5º, X, da CRFB)

ALINE DAL BÓ CORREA⁶⁵

A disciplina da proteção de dados pessoais tem como um de seus fundamentos a inviolabilidade da intimidade, da honra e da imagem, bem como está garantido em nossa Constituição Federal que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.⁶⁶

HABEAS DATA⁶⁷

DENISE FINCATO⁶⁸

O habeas data é uma ação constitucional que permite o acesso às informações da própria pessoa que as solicita conhecer, retificar ou excluir. Helly Lopes Meirelles⁶⁹ leciona que “o habeas data é [...] o meio constitucional posto à disposição de pessoa física ou jurídica para lhe assegurar o conhecimento de registros concernentes ao postulante e constantes de repartições públicas ou particulares acessíveis ao público, para retificação de seus dados pessoais”.

Sua função não se restringe a atender ao direito de informação da própria pessoa ou a retificar seus dados. Presta-se também à exclusão de bancos públicos de dados daquilo que diga respeito à esfera íntima do indivíduo. Dados como posição política, religiosa e saúde da pessoa, dentre outros dessa natureza, não devem ser registrados, pois extrapolam as categorias necessárias à qualificação civil do indivíduo ou, no particular deste verbete, ao necessário para o estabelecimento, manutenção e término de uma relação de trabalho. Caso já estejam registradas essas informações, o habeas data é o instrumento adequado para sua exclusão⁷⁰.

64 Referências: MIZIARA, Raphael. *Reflexos da LGPD no Direito e no processo do trabalho* (livro eletrônico). Raphael Miziera, André Pessoa, Bianca Mollicone – 1. ed. - São Paulo: Thomson Reuters Brasil, 2020.

65 Graduanda na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedalbo04@gmail.com

66 Referências: BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento* - Rio de Janeiro: Forense, 2019.

67 Este trabalho revisita material publicado anteriormente: FINCATO, D.P; KRIEGER, M.A. Habeas Data na Justiça do Trabalho. *Justiça do Trabalho*, Porto Alegre, ano 32, n. 377, p. 38-53, maio 2015.

68 Pós-Doutora em Direito do Trabalho pela Universidad Complutense de Madrid (Espana). Doutora em Direito pela Universidad de Burgos (Espana). Professora Pesquisadora do PPGD da PUCRS. Titular da Cadeira nº 34 da Academia Sul-Riograndense de Direito do Trabalho. Advogada e Consultora Trabalhista no Brasil e em Portugal. CEO do Instituto Workab.

69 MEIRELLES, Hely Lopes. *Mandado de segurança*. 28.ed. atualizada por Arnaldo Wald e Gilmar Ferreira Mendes com a colaboração de Rodrigo Garcia da Fonseca. São Paulo: Malheiros, 2005, p.283.

70 GARCIA, Maria. Habeas data. O direito à informação. O direito fundamental à intimidade, à vida privada, à honra e à imagem das pessoas. Um perfil constitucional. *In*: WAMBIER, Teresa Arruda

De acordo com a Constituição Federal de 1988, em seu art. 5.º, LXXII: “conceder-se-á habeas data (a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; (b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo”. Seu rito processual está definido na Lei nº 9.507/97 e, para manejo na esfera trabalhista, deve-se observar o contido na Instrução Normativa nº 27, de 16 de fevereiro de 2005, do Tribunal Superior do Trabalho⁷¹, não se admitindo sua interposição via *jus postulandi*⁷².

É uma ação personalíssima: o pedido não poderá ser requerido por terceiros ou até mesmo por herdeiros, muito embora existam decisões em sentido contrário⁷³. Assim, o entendimento é que órgãos como o Ministério Público e a Defensoria Pública também não poderiam agir em nome próprio para a defesa de interesses alheios. Quanto à legitimação passiva, poderá figurar no polo passivo da relação processual tanto a entidade governamental como a entidade particular, desde que esta possua banco de dados sobre a pessoa, podendo ser citado como o Serviço de Proteção do Crédito (SPC)⁷⁴.

O habeas data pode ser impetrado na Justiça do Trabalho⁷⁵, desde que o direito material esteja relacionado com a relação de trabalho (art. 114, IV da CF/88) e será distribuído junto às Varas do Trabalho ou Tribunais Trabalhistas, a depender da qualidade do coator. Deverá partir de uma petição inicial que, mesmo na justiça

Alvim. (coord). *Habeas Data*. São Paulo: Editora Revista dos Tribunais, 1998, p. 227.

71 Art. 1º As ações ajuizadas na Justiça do Trabalho tramitarão pelo rito ordinário ou sumaríssimo, conforme previsto na Consolidação das Leis do Trabalho, excepcionando-se, apenas, as que, por disciplina legal expressa, estejam sujeitas a rito especial, tais como o Mandado de Segurança, Habeas Corpus, Habeas Data, Ação Rescisória, Ação Cautelar e Ação de Consignação em Pagamento. Art. 2º A sistemática recursal a ser observada é a prevista na Consolidação das Leis do Trabalho, inclusive no tocante à nomenclatura, à alçada, aos prazos e às competências.

72 O habeas data tem inquestionável ligação com o habeas corpus e com o mandado de segurança, pois viabiliza a prestação de tutela jurisdicional que afeta a coisa julgada, o ato jurídico perfeito e/ou o estado da ordem constitucional e está subordinada à produção de prova pré-constituída. Inteligência da Súmula 425 do TST: “O *jus postulandi das partes, estabelecido no art. 791 da CLT, limita-se às Varas do Trabalho e aos Tribunais Regionais do Trabalho, não alcançando a ação rescisória, a ação cautelar, o mandado de segurança e os recursos de competência do Tribunal Superior do Trabalho*”.

73 CHIMENTI, Ricardo Cunha; CAPEZ, Fernando; ROSA, Márcio F. Elias; SANTOS, Marisa F. *Curso de direito constitucional*. São Paulo: Saraiva, 2004. p.96.

74 SLAIBI FILHO, Nagib. *Direito constitucional*. Rio de Janeiro: Forense, 2004. p.503.

75 HABEAS DATA – Via Eleita - “O Habeas data é o remédio constitucional para obtenção ou correção de dados pessoais, oponível não apenas contra os entes governamentais, mas também entidades de caráter público, como no caso em tela, e contra entidades privadas que possam divulgar dados a terceiros, o que leva a entender que o instrumento pode ser utilizado inclusive contra o empregador privado, quando se recuse a fornecer dados pessoais de seu empregado ou informações sobre sua vida profissional”. (...) Também o empregador privado dispõe de assentamentos, cadastros e bancos de dados, acerca de seus empregados ou ex-empregados, e quando solicitados por terceiros divulgam tais informações. São comuns as cartas de referência, que são posteriormente investigadas para que se constate a veracidade de suas declarações. Portanto, se tais informações estão disponíveis a terceiros, que podem averiguar a vida profissional de postulante a emprego ou cargo público, parece claro que o instrumento adequado para obtenção de tais registros ou sua retificação haverá de ser o habeas data” (TRT 2ª R. 00730008020065020086 (00730200608602000) RO. Ac. 1ªT 20110450838. Rel. Maria Inês Moura Santos Alves da Cunha. DOE 25/04/2011).

obreira, observará os requisitos dos artigos 319 e 320 do Código de Processo Civil e, ainda, será instruída com provas “(i) - da recusa ao acesso às informações ou do decurso de mais de dez dias sem decisão; (ii) - da recusa em fazer-se a retificação ou do decurso de mais de quinze dias, sem decisão; ou (iii) - da recusa em fazer-se a anotação a que se refere o § 2º do art. 4º ou do decurso de mais de quinze dias sem decisão.” Nos termos do art. 5.º, LXXVII da CF/88, “são gratuitas as ações de *habeas corpus* e *habeas data*, e, na forma da lei, os atos necessários ao exercício da cidadania”. O coator será notificado do conteúdo da ação e terá prazo para prestar informações. Logo após, será ouvido o Ministério Público e os autos serão conclusos para decisão.

O conteúdo do *writ* pode ser tanto de natureza mandamental quanto constitutiva, ou seja, quando seu objetivo for assegurar o conhecimento de informações será mandamental, pois se trata de uma ordem judicial aos órgãos governamentais ou de caráter público, cujo desrespeito gera pena de desobediência. Por outro lado, será considerado constitutivo quando o fim pretendido, para além do acesso, for a retificação de dados, sendo criada a partir daí e, portanto, um novo status de informação, fruto do provimento jurisdicional⁷⁶.

Podem-se trazer como exemplos de cabimento do *habeas data* situações em que servidor não estatutário (celetista) o move em face do Estado, para obtenção de informação de seu tempo de serviço; empregador o impetra em face de Procurador ou Auditor Fiscal do trabalho, para ter acesso a conteúdo de processo administrativo ou “listas sujas” etc. Não serve, no entanto, para acesso, pelo empregado, dos resultados financeiros de seu empregador (para fins de conferência da regularidade de seu pagamento de parcela de participação em lucros e resultados), tampouco para acessar dados da contratualidade para o fito de atribuir valor a pedidos da petição inicial de sua demanda (para estes casos, cabíveis ações exorbitárias, inclusive com pedidos liminares).

O remédio constitucional vem perdendo objeto em razão de sua complexidade e formalismo. Na prática, comumente prefere-se ajuizar uma ação de produção antecipada de provas (art. 381, II do CPC) ou uma ação autônoma de exibição de documentos para acessar os dados da contratualidade (com o fito de elaborar cálculos para o pedido inicial, por exemplo).

A contribuir, a recente promulgação da Lei nº 13.709/18 (Lei Geral de Proteção de Dados) trouxe ainda mais informalidade aos pedidos de informações sobre dados pessoais, a partir da previsão de sua requisição pelo titular do dado pessoal (arts. 18 e 19 LGPD), o que lhe permitirá solicitar correções, anonimizações, bloqueios, eliminações, portabilidade etc. O controlador dos dados pessoais poderá confirmar imediatamente e de forma simplificada a existência dos dados ou, fornecendo mais detalhes como origem, critérios e finalidade de tratamento das informações, em até 15 dias.

Como remédio constitucional que é, no entanto, poderá seguir sendo instrumento importante, notoriamente diante do exaurimento e/ou ineficácia das vias administrativas nas quais se solicite acesso a informações pessoais. O *habeas data*,

76 CHIMENTI, Ricardo Cunha; CAPEZ, Fernando; ROSA, Márcio F. Elias; SANTOS, Marisa F. *Curso de direito constitucional*. São Paulo: Saraiva, 2004. p.96.

nessa nova quadra da proteção de dados no Brasil, ganha relevo por garantir a autodeterminação informativa e, em última *ratio*, por seguir servindo a seu objetivo-gênese: proteger a dignidade da pessoa humana.⁷⁷

I

INFORMAÇÃO, DIREITO À

LUCIELI BREDA⁷⁸

A Lei nº 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados – LGPD, faz referência expressa em 13 (treze) momentos à informação. Logo, não se pode olvidar da relevância do Direito à Informação no contexto da LGPD.

Tanto é verdade que a informação está identificada expressamente como um dos fundamentos da disciplina da proteção de dados pessoais, no artigo 2º, inciso III da LGPD.

Além disso, a informação integra o próprio conceito de dado pessoal definido pela lei, como se verifica do inciso I do artigo 5º da LGPD: “I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;” e, ainda, é apontada como uma das principais operações realizadas no tratamento de dados pessoais, como se extrai do inciso X do mesmo artigo: “X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”.

O Direito à Informação também está expresso no rol dos direitos do titular de dados, descritos no artigo 18 da LGPD, notoriamente nos incisos VII e VIII. Não bastasse isso, a segurança da informação é um dos principais objetivos da referida legislação, consoante artigo 47: “Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.”

Esse Direito tem ganhado mais espaço e relevância no ordenamento jurídico brasileiro, na medida em que várias legislações, notoriamente após o ano de 2010, estão fundamentadas, mesmo que implicitamente, na sua garantia. Como exemplo, pode-se destacar a Lei nº 12.527/2011 (Lei da Transparência no Setor Público), a Lei nº 12.965/2014 (Marco Civil da Internet) e, na esfera trabalhista, destaque para a Lei nº 13.467/2017 (Reforma Trabalhista).

⁷⁷ Referências: CHIMENTI, Ricardo Cunha; CAPEZ, Fernando; ROSA, Márcio F. Elias; SANTOS, Marisa F. *Curso de direito constitucional*. São Paulo: Saraiva, 2004. FINCATO, D.P.; KRIEGER, M.A. Habeas Data na Justiça do Trabalho. *Justiça do Trabalho*, Porto Alegre, ano 32, n. 377, p. 38-53, maio 2015. GARCIA, Maria. Habeas data. O direito à informação. O direito fundamental à intimidade, à vida privada, à honra e à imagem das pessoas. Um perfil constitucional. WAMBIER, Teresa Arruda Alvim. (coord). *Habeas Data*. São Paulo: Editora Revista dos Tribunais, 1998. MEIRELLES, Hely Lopes. *Mandado de segurança*. 28.ed. atualizada por Arnaldo Wald e Gilmar Ferreira Mendes com a colaboração de Rodrigo Garcia da Fonseca. São Paulo: Malheiros, 2005. SLAIBI FILHO, Nagib. *Direito constitucional*. Rio de Janeiro: Forense, 2004

⁷⁸ Advogada. Mestre em Direito (UFRGS). Currículo Lattes: <http://lattes.cnpq.br/8459365035563332>. lucielibreda@hotmail.com

Embora a LGPD não aborde especificamente as relações trabalhistas e as informações decorrentes deste tipo de relação, seu artigo 1º define como objetivo principal proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. E, por sua vez, no artigo 2º verifica-se que o legislador se preocupou com a questão da liberdade de informação, bem como em correlacionar a proteção de dados pessoas com os direitos humanos e a dignidade humana. Assim, em que pese não se trate de uma legislação específica de Direito do Trabalho, denota-se a relevância e seus reflexos também para as relações trabalhistas, estando implícitas as relações de trabalho nos primeiros artigos da referida lei.

Deste modo, o Direito à Informação vem se confirmando como um dos protagonistas das relações de trabalho neste momento de incertezas, despontando como uma alternativa válida e eficaz para tornar as relações trabalhistas mais transparentes e seguras, corroborado pela previsão expressa na LGPD, seja como fundamento, como direito e/ou como objetivo da referida legislação protetiva de dados.⁷⁹

INTIMIDADE (art. 2º LGPD e CRFB)

ALINE DAL BÓ CORREA⁸⁰

A disciplina da proteção de dados pessoais tem como um de seus fundamentos a inviolabilidade da intimidade, da honra e da imagem, bem como está garantido em nossa Constituição Federal que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.⁸¹

IMAGEM (art. 2º LGPD e CRFB)

ALINE DAL BÓ CORREA⁸²

A disciplina da proteção de dados pessoais tem como um de seus fundamentos a inviolabilidade da intimidade, da honra e da imagem bem como está garantido em nossa Constituição Federal que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.⁸³

J

79 Referências: BREDA, Lucieli. *O direito à informação aplicado às relações de trabalho*. Orientadora: Luciane Cardoso Barzotto. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2019. CASTELLS, Manuel. *A sociedade em rede: a era da informação: economia, sociedade e cultura*, 2 ed, v 1.

80 Graduanda na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedalbo04@gmail.com

81 Referências: BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento* - Rio de Janeiro: Forense, 2019.

82 Graduanda na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedalbo04@gmail.com

83 Referências: BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento* - Rio de Janeiro: Forense, 2019.

JUDICIÁRIO E TRATAMENTO DE DADOS (art. 25 e art. 26)

ALINE DAL BÓ CORREA⁸⁴

A respeito da atuação do poder público, os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral. Ainda, o uso compartilhado de dados pessoais pelo poder público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.⁸⁵

L

LEGÍTIMO INTERESSE (art. 10)

ALINE DAL BÓ CORREA⁸⁶

O legítimo interesse da empresa só poderá embasar o tratamento de dados pessoais para objetivos específicos e legítimos, considerados a partir de situações concretas, que incluem, mas não se limitam a: apoio e promoção de atividades do controlador; e proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.⁸⁷

LIVRE ACESSO (art. 6º, IV)

ALINE DAL BÓ CORREA⁸⁸

Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.⁸⁹

M

MICROEMPRESAS, STARTUPS E EMPRESAS DE INOVAÇÃO PERANTE A LGPD

GERALDA MAGELLA DE FARIA ROSSETTO⁹⁰

84 Graduanda na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedalbo04@gmail.com

85 Referências: DONEDA, Danilo (org) *et al. O regime jurídico do tratamento de dados pessoais pelo Poder Público*. Rio de Janeiro: Forense, 2021.

86 Graduanda na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedalbo04@gmail.com

87 Referências: DONEDA, Danilo (org) *et al. O regime jurídico do tratamento de dados pessoais pelo Poder Público*. Rio de Janeiro: Forense, 2021.

88 Graduanda na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedalbo04@gmail.com

89 Referências: MALDONADO, Viviane Nóbrega, BLUM, Renato Opice. *LGPD: Lei Geral de Proteção de Dados Pessoais comentada - 3. ed - São Paulo: Thomson Reuters Brasil, 2021.*

90 Doutorado em Direito pela UFSC. Mestre em Direito pela UNISINOS. Advogada. Procuradora Federal aposentada. Pesquisadora do Direito e Fraternidade; do DataLab e do NEJUSCA. Email:

A LGPD, em seu art. 55-J, XVIII (2021a), confere competência à Autoridade Nacional de Proteção de Dados para prescrever a edição de normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem *startups* ou empresas de inovação, possam adequar-se às disposições da LGPD. O que significa que terão de moldar seu modo operandi segundo uma lógica de adequação, simetria e conformidade em face do tratamento de dados pessoais e, conseqüentemente, inculir proteção de direitos, em específico, a proteção de direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, segundo a “cartilha” da proteção de dados pessoais.

A concepção desse propósito tem o condão de educar e formatar a microempresa, as *startups* ou empresas de inovação em prol de iniciativas empresariais, sabendo que as mesmas devem estar frente a um novo comportamento: por mais que pedagógico, firmá-lo segundo uma prática de nova realidade, cuja tônica roga compromisso com a privacidade e uma dinâmica de segurança da informação. É que o empresário, à frente de seu negócio, precisa levar em consideração novas perspectivas quanto à proteção de dados pessoais sob seu encargo, visando o atendimento de um modelo de fidelidade, confidencialidade e de confiança, sobretudo de respeitosa relação entre o usuário e o prestador de serviço; entre o titular do dado e quem recebe esses dados em tratamento.

De outro modo, é de especial significado traduzir quem são cada uma dessas qualificadoras microempresas, empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem *startups* ou empresas de inovação. Senão, veja-se:

Diz respeito à sociedade empresária, à sociedade simples, empresa individual de responsabilidade limitada e o empresário a que se refere o art. 966 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), incluído o microempreendedor individual, com faturamento máximo nos termos do art. 3º da Lei Complementar nº 123 de 14 de dezembro de 2006. (BRASIL, 2021c).

Corroborando, a resolução com esse fim pode incluir no conceito de agentes de pequeno porte outras categorias de organizações, além das anteriormente mencionadas, porém deverá elucidar quem são, de forma objetiva e clara, a menos que a lei passe a criar com o usuário perspectivas de enfrentamentos e desafios.

Seja como for, há um ponto de especial promoção pertinente ao próprio conceito dessas específicas empresas, o que inclusive foi alvo de recepção junto à Autoridade Nacional de Proteção de Dados, que, recentemente, apresentou a Consulta Pública pertinente a minuta de resolução que regulamenta a aplicação da LGPD para microempresas, empresas de pequeno porte e iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem *startups* ou empresas de inovação.

geraldamagella@gmail.com

O objetivo dessa tarefa refere-se à possibilidade de adoção de procedimentos simplificados e diferenciados, facilitando a conformidade desse grupo à LGPD e contribuindo para a disseminação da cultura de proteção de dados pessoais (ANPD, 2021).

A despeito desse atributo, convém entender e delimitar o conceito de *startups*, conforme consta na disciplina da Lei Complementar nº 182, de 1º de junho de 2021, especificamente, § 1º do art. 4º (BRASIL, 2021b):

Art. 4º São enquadradas como *startups* as organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados.

§ 1º Para fins de aplicação desta Lei Complementar, são elegíveis para o enquadramento na modalidade de tratamento especial destinada ao fomento de *startup* o empresário individual, a empresa individual de responsabilidade limitada, as sociedades empresárias, as sociedades cooperativas e as sociedades simples [...] (BRASIL, 2021b).

Contudo, a ANPD, no artigo 2º, II do regulamento que esteve sob consulta pública, apresentou o seguinte dispositivo:

Art. 2º Para efeitos desta resolução são adotadas as seguintes definições:

I -

II - *startups*: organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados, que atendam aos critérios previstos no § 1º do art. 4º da Lei Complementar nº 182, de 1º de junho de 2021. (ANPD, 2021).

Cabem quanto a estes pontos algumas considerações, a título de esclarecer e reafirmar referido conceito, na medida em que, para alcançar seus objetivos, a LGPD precisa dar conta de cumprir seu papel fundante em relação à proteção de dados pessoais, e, para tanto, a ANPD que tem sob seu encargo uma série de compromissos com a atuação da proteção de dados pessoais. E, em tal razão, deve ser participe no processo de tornar explícito, conferir clareza e previsibilidade ao normativo regulamentador.

Com efeito, o conceito de *startups* que contempla em sua agenda o pertencimento de organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados, deve também confirmar esses requisitos para

os seguintes padrões conceituais e normativos, tais como os de natureza incremental, que buscam inovar em serviços, produtos ou processos já existentes, e os de natureza disruptiva, que se envolvem no processo de criação de algo novo ou de especial interesse, como os relacionados a questões urgentes, tais como as de natureza ambiental, climática, educacionais (especialmente em favor da infância) e relativas à saúde e afins.

Entre as razões motivadoras para que assim sejam, estão as questões de ordem de fundo, de cunho procedimentais, relativas à própria temática (matéria), como, também, as questões instrumentais, de ordem processual, assim compreendidas: i) as agendas urgentes desencadeadas, cujas demandas as questões de saúde pública trazidas pela própria pandemia estão a nos apresentar; ii) em específico, o próprio conceito traduzido pela ANPD, que refere-se a “iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem *startups* ou empresas de inovação”, justificando a presença de, no mínimo, dois tipos de *startups* (incremental e disruptiva); iii) o fato de que a Lei Complementar 182 poderá vir a ser substituída por outra lei, ainda que de igual peso, requer atualizações de demandas à frente do que está posto, procurando abarcar as tutelas urgentes que estão sempre se apresentando no ambiente digital e nas esferas tecnológicas; iv) sobretudo, é importante pensar em demandas que abarquem direitos fundamentais e direitos humanos, conforme encontra-se dirimido pela Agência dos Direitos Fundamentais da União Europeia, no sentido de conferir presença a medidas equilibradas que se baseiem na lei, sejam necessárias, temporárias e proporcionais. Exige também uma resposta ao impacto socioeconômico, protegendo os vulneráveis (FRA, 2021) e combatendo os escapes que a violação da lei sempre oportuniza.⁹¹

MONITORAMENTO DE EMPREGADOS E LGPD SUELEN HENTGES⁹²

Não há definição expressa na LGPD sobre o termo monitoramento. No entanto, todo monitoramento acarreta tratamento de dados (art. 5º, X da LGPD). A nomenclatura é utilizada para definir as formas de observar ou mesmo controlar as atividades de outrem — como o empregado. Assim, nas relações de trabalho, te-

91 Referências ANPD – Autoridade Nacional de Proteção de Dados. ANPD abre consulta pública e inscrições para audiência pública sobre norma de aplicação da LGPD para microempresas e empresas de pequeno porte. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-consulta-publica-e-inscricoes-para-audiencia-publica-sobre-norma-de-aplicacao-da-lgpd-para-microempresas-e-empresas-de-pequeno-porte>. Acesso em: 25 out. 2021. BRASIL. Lei 13709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 out. 2021a. BRASIL. Lei Complementar nº 182, de 1º de junho de 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp182.htm. Acesso em: 25 out. 2021b. BRASIL. Lei complementar nº 123, de 14 de dezembro de 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp123.htm. Acesso em: 25 out. 2021c. FRA – European Union Agency for Fundamental Rights. Relatório sobre os Direitos Fundamentais – 2021. Agência dos Direitos Fundamentais da União Europeia, 2021. Disponível em: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-fundamental-rights-report-2021-opinions_pt.pdf. Acesso em: 24 out. 2021.

92 Mestranda em Direito pela Universidade Federal do Rio Grande do Sul; graduada em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul; advogada. suelenh@gmail.com

mos como exemplos o monitoramento de correspondências eletrônicas, a captura de imagens dos trabalhadores no local de trabalho, as chamadas em sistemas de teleconferência, o registro biométrico da jornada de trabalho, ou mesmo a hipótese de se controlar por meio de geolocalização um empregado que preste serviços a distância.

A evolução da tecnologia tem aumentado exponencialmente as maneiras de se realizar o monitoramento de empregados. Neste sentido, Tereza Coelho Moreira refere que:

Anteriormente à introdução da informática, a vigilância laboral implicava sempre uma certa intromissão física: um superior hierárquico ou, ainda, revistas aos trabalhadores e aos seus bens. Por outro lado, para interceptar as comunicações dos trabalhadores era também necessária a sua realização física e, por vezes, tornava-se fácil detectar quando um correio tinha sido aberto. Actualmente, porém, com o auxílio das novas tecnologias informáticas, os empregadores podem aceder a todos os dados armazenados num computador ou num sistema distribuído em rede sem que os trabalhadores estejam conscientes disso.

Assim sendo, conforme definido por Alain Supiot, estamos diante da “ciber-vigilância dos assalariados”. Por esses motivos, destaca-se a importância cada vez maior de que se reforce a importância do controle humano da tecnologia, a favor do trabalho digno, conforme consta no relatório *Trabalhar para um Futuro Melhor* da Comissão Mundial para o Futuro do Trabalho, da OIT.⁹³

N

93 Referências: BARZOTTO, Luciane Cardoso; MISKULIN, Ana Paula Silva Campos; BREDA; Lucieli. Condições transparente de trabalho, informação e subordinação algorítmica nas relações de trabalho. In: CARELLI; Rodrigo de Lacerda; CAVALCANTI, Tiago Muniz; FONSECA; Vanessa Patriota da. *Futuro do trabalho: os efeitos da revolução digital na sociedade*. Brasília: ESMMPU, 2020. MAIA, Daniel Azevedo de Oliveira. As hipóteses autorizativas de tratamento de dados pessoais nas relações de trabalho sob a ótica da LGPD e do GDPR. In: MIZIARA, Raphael; PESSOA, André; MOLLICONE, Bianca (org). *Reflexos da LGPD no direito e no processo do trabalho*. 1. ed. São Paulo: Thomson Reuters Brasil, 2020. E-book. MOREIRA, Tereza Coelho. *A privacidade dos trabalhadores e as novas tecnologias de informação e comunicação*: contributo para um estudo dos limites ao poder de controle eletrônico do empregador. Coimbra: Almedina, 2010, p. 422. ORGANIZAÇÃO INTERNACIONAL DO TRABALHO. Relatório: *Trabalhar para um Futuro Melhor*. 2019. Disponível em: https://www.ilo.org/wcmsp5/groups/public/---europe/---ro-geneva/---ilo-lisbon/documents/publication/wcms_677383.pdf. Acesso em: 24 out. 2021. PINHEIRO, Iuri; BOMFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. Disponível em: <http://trabalhoemdebate.com.br/artigo/detalhe/a-lei-geral-de-protecao-de-dados-e-seus-impactos-nas-relacoes-de-trabalho> Acesso em: 23 out. 2021. SUPIOT, A. *Homo juridicus*: ensaio sobre a função a função antropológica do Direito. Lisboa: Instituto Piaget, 2006. p. 162.

NÃO DISCRIMINAÇÃO (art. 6º, IX)**LUCIANE CARDOSO BARZOTTO⁹⁴ E VIVIAN MARIA CAXAMBU GRAMINHO⁹⁵**

A Lei n.º 13.709/2018 visa tutelar não só a privacidade e os direitos fundamentais, mas também busca proteger a pessoa contra discriminações. Assim, dentre os princípios enumerados no artigo 6º, está o princípio da não discriminação, constante no inciso IX, o qual especifica a “impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos”.

A discriminação é um aspecto que faz parte do cotidiano da sociedade e dos sistemas legais, de forma que nem sempre será considerada prejudicial às pessoas⁹⁶. Ou seja, apesar da carga negativa da palavra discriminação, ela também é uma forma de generalizar pessoas, ações ou coisas positivamente⁹⁷. No sentido laboral, no entanto, a discriminação possui conotação negativa. A Convenção n.º 111, da Organização Internacional do Trabalho (OIT), em seu artigo 1º, prevê que o termo discriminação compreende a distinção, exclusão ou preferência fundamentada na raça, cor, sexo, religião, opinião política, ascendência nacional ou origem racial, que tenha como resultado a destruição ou alteração da igualdade de oportunidade ou de tratamento em matéria de emprego ou profissão. São aspectos que distinguem os indivíduos em outras áreas da vida, e que não deveriam importar para o exercício das atividades laborais, ou seja, a discriminação na esfera laboral pode ser entendida como a aplicação de critérios não relevantes para o desempenho de certa ocupação⁹⁸. Note-se, ainda, que se trata, em sua maioria, de aspectos relacionados a dados pessoais sensíveis (artigo 5º, inciso II, da LGPD), e que possuem potencial discriminatório.

O princípio da não discriminação constante na LGPD veda as práticas discriminatórias ilícitas ou abusivas⁹⁹, considerando-se permitidas as práticas discriminatórias que não tenham tais finalidades, como, por exemplo, o perfilização (*profiling*), ou ainda a criação de bancos de dados com o histórico de crédito dos consumidores (*credit scoring*). Dessa maneira, a discriminação positiva – também denominada de reversa –, considerada aquela que se dá em benefício de grupos que sofrem discriminações, não violará o referido princípio¹⁰⁰.

94 Mestre em Direito pela Universidade do Vale do Rio dos Sinos (UNISINOS). Doutora em Direito pela Universidade Federal do Paraná (UFPR). Professora adjunta da Universidade Federal do Rio Grande do Sul e Professora do PPGDir Mestrado e Doutorado (UFRGS). Desembargadora do TRT da 4ª Região.

95 Mestre em Direito pela Universidade do Extremo Sul Catarinense – UNESC. Doutoranda em Direito pela Universidade Federal do Rio Grande do Sul – UFRGS. Advogada.

96 MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. Discriminação algorítmica à luz da Lei Geral de Proteção de Dados. In: DONEDA, Danilo *et al.* (coords). *Tratado de proteção de dados pessoais* [livro eletrônico]. Rio de Janeiro: Forense, 2021.

97 MATTIUZZO, Marcela. *Discriminação algorítmica: reflexões no contexto da Lei Geral de Proteção de Dados Pessoais*. In: CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel (coord.). *Lei geral de proteção de dados (Lei nº 13.709/2018): a caminho da efetividade: contribuições para implementação da LGPD* [livro eletrônico]. São Paulo: Thomson Reuters Brasil, 2020

98 BARZOTTO, Luciane Cardoso. Igualdade e discriminação no ambiente de trabalho. In: BARZOTTO, Luciane Cardoso (Coord.). *Trabalho e igualdade: tipos de discriminação no ambiente de trabalho*. Porto Alegre: Livraria do Advogado, 2012.

99 MATTIUZZO, *op. cit.*

100 CARLOTO, Selma. *A Lei geral de proteção de dados: com enfoque nas relações de trabalho* [livro

A ideia de ilicitude referenciada na lei refere-se àquilo que é proibido pelo ordenamento jurídico, lembrando que os grupos que historicamente foram alvos de preconceito e, portanto, considerados mais vulneráveis a tratamentos discriminatórios são expressamente protegidos pelo ordenamento jurídico, como, por exemplo, a previsão dos princípios constitucionais da igualdade (art. 3º, IV, da CF) e da proibição de discriminação que viole direitos e liberdades fundamentais (art. 5º, XLI, da CF)¹⁰¹. Pode-se afirmar que a utilização de um dado colhido sem observância das bases autorizativas constantes na lei pode gerar uma discriminação ilícita.¹⁰²

No âmbito das relações laborais, por exemplo, são passíveis de discriminação ilícita as práticas relacionadas à seleção de trabalhadores que excluem determinados grupos considerados minoritários, bem como aquelas que determinam diferenças salariais em razão do gênero, raça, entre outros. Assim, entende-se que a utilização de dados colhidos sem observância às bases autorizativas da lei gera uma discriminação ilícita¹⁰³. Já o critério para definir o que se entende por abusividade deve ter como fundamento os princípios constantes na LGPD, na Constituição Federal¹⁰⁴ e nos tratados e convenções internacionais, como por exemplo, a Convenção Interamericana contra o Racismo, a Discriminação Racial e Formas correlatas de Intolerância, promulgada em 10 de janeiro de 2022, por intermédio do Decreto n. 10.932¹⁰⁵, sendo que as categorias a seguir podem servir como base para a análise acerca do abuso: a) discriminação por erro estatístico, que é considerada aquela decorrente de erros cometidos pelos profissionais responsáveis pelo desenho do algoritmo; b) discriminação pelo uso de dados sensíveis: que podem gerar perfilamento discriminatório em face de grupos historicamente discriminados; c) discriminação por generalização injusta: nesse caso, embora as informações e o algoritmo estejam corretos, a generalização resultante da decisão automatizada será considerada injusta, pois permitirá que determinadas pessoas sejam classificadas de forma equivocada em certos grupos; d) discriminação limitadora do exercício de direitos: o problema relaciona-se à informação utilizada pelo algoritmo e à realização de um direito, podendo levar à exclusão de determinados grupos¹⁰⁶.

Além da previsão expressa constante no artigo 6º, inciso IX, da LGPD, pode-se observar o princípio da não discriminação em diversas passagens da lei, como, por exemplo, no artigo 21 que determina a impossibilidade de utilização dos dados pessoais relativos ao exercício regular de direito pelo titular em seu prejuízo, bem como no artigo 11, § 5º, que veda às operadoras de planos privados de assistência à saúde o tratamento de dados referentes à saúde para a prática de seleção de riscos na con-

eletrônico]. 2. ed. São Paulo: LTr, 2021.

101 MENDES, *op. cit.*

102 JUNQUEIRA, Thiago. *Tratamento de dados pessoais e discriminação algorítmica nos seguros* [livro eletrônico]. São Paulo: Thomson Reuters Brasil, 2020.

103 *Ibid.*

104 MENDES, *op. cit.*

105 BRASIL. Decreto n.º 10.932, de 10 de janeiro de 2022. Promulga a Convenção Interamericana contra o Racismo, a Discriminação Racial e Formas Correlatas de Intolerância, firmado pela República Federativa do Brasil, na Guatemala, em 5 de junho de 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D10932.htm. Acesso em: 13 jan. 2022.

106 *Ibid.*

tratação de qualquer modalidade ou na contratação e exclusão de beneficiários¹⁰⁷.

A LGPD, portanto, serve como instrumento para impedir a discriminação direta e indireta, envolvendo além dos impactos negativos relacionados à finalidade do tratamento de dados em si, como também aqueles efeitos que resultam, mesmo que de maneira não intencional, desse processo de tratamento.¹⁰⁸



OPERADOR (art. 5.º, VII)

FERNANDA JULIANE BRUM CORRÊA¹⁰⁹

A lei o define como a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. É também denominado de processador de dados.

No regulamento europeu (GDPR), é designado como uma pessoa com atribuição de realizar o tratamento segundo instruções fornecidas pelo controlador, o qual verificará a observância das próprias instruções e das normas sobre a matéria (art. 4.º, item 8, e art. 39).

O operador, a partir de decisão tomada pelo controlador, pode ser alguém interno à organização ou empresa (empregado), ou terceiro a quem se confie as atividades de tratamento. Não há consenso doutrinário acerca da classificação a depender da internalização ou não do papel de operador. Miziara destaca o dissenso entre autores que consideram que o empregado designado a essa função não ser, juridicamente, um operador, e entre outros que concluem configurado o operador, mas apenas *longa manus* do empregador, e outros que concluem configurada a figura do operador.¹¹⁰

ÓRGÃO DE PESQUISA (art. 5.º XVIII)

ALINE DAL BÓ CORREA¹¹¹

No texto da LGPD, consta que é Órgão de Pesquisa aquele órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no país, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.¹¹²

107 JUNQUEIRA, *op. cit.*

108 LINDOSO, Maria Cristine Branco. *Discriminação de gênero no tratamento automatizados de dados pessoais*: como a automatização incorpora vieses de gênero e perpetua a discriminação de mulheres. Rio de Janeiro: Processo, 2021.

109 Analista Judiciário do TRT da 4ª Região. Graduada em Direito pela Universidade Federal de Santa Maria. Especialista em Direito do Trabalho e Processo do Trabalho pela Faculdade Damásio. fernanda.brum@trt4.jus.br

110 Referências: MIZIARA, Raphael. *Reflexos da LGPD no Direito e no processo do trabalho* (livro eletrônico). Raphael Miziara, André Pessoa, Bianca Mollicone – 1. ed. - São Paulo: Thomson Reuters Brasil, 2020. PINHEIRO, Patricia Peck. *Proteção de dados pessoais*: comentários à Lei n.º 13.709/2018 (LGPD). 2. ed. - São Paulo: Saraiva Educação, 2020.

111 Graduanda na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedalbo04@gmail.com

112 Referências: CARLOTO, Selma: *Lei geral da proteção de dados*: enfoque nas relações de trabalho

PRINCÍPIOS

GILBERTO DESTRO¹¹³

O tratamento de dados pessoais deve observar: i) a boa-fé: respeitar com fidelidade o que se compromete a fazer, sem abusar da confiança; ii) o princípio da finalidade: usar os dados pessoais para o fim específico informado ao titular. A finalidade deve ser legítima e explícita. Não pode haver tratamento incompatível com esses propósitos; iii) o princípio da adequação: o uso dos dados deve ser compatível com as finalidades informadas ao titular; iv) o princípio da necessidade: será tratado o mínimo de dados, só os necessários, para o fim pretendido; v) o princípio do livre acesso: garantia ao titular de consulta facilitada e gratuita sobre a forma e a duração do tratamento e sobre a integralidade de seus dados pessoais; vi) o princípio da qualidade dos dados: garantia ao titular de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade; vii) o princípio da transparência: garantia ao titular de informações claras, precisas e facilmente acessíveis sobre o uso dos dados e os respectivos agentes de tratamento, observados os segredos comercial e industrial; viii) o princípio da segurança: os dados pessoais devem estar protegidos de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; ix) o princípio da prevenção: prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; x) o princípio da não discriminação: impossibilidade do uso dos dados para fins discriminatórios ilícitos ou abusivos; xi) o princípio da responsabilização e prestação de contas: o agente deve demonstrar que adota medidas que comprovam o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (art. 6º da LGPD).

PRIVACY BY DEFAULT

PÂMELA ADRIELLE PERTILE DOS PASSOS¹¹⁴ E SÂMARA KENYA DE OLIVEIRA¹¹⁵

A metodologia *Privacy by Default* (privacidade por padrão) decorre da metodologia *Privacy by Design* (privacidade desde a concepção), especialmente na produção dos mais variados aplicativos e de outros serviços digitais. Esses conceitos foram instituídos em 1990 pela Comissária de Informação e Privacidade de Ontário, do Canadá, a Dra. Ann Cavoukian, e são atualmente utilizados no sistema europeu de tratamento de dados.

A *Privacy by Default* consiste em pensar a privacidade e a proteção de dados como padrão a ser seguido. E para que isso ocorra, é necessário ter as configura-

- São Paulo: LTr, 2020.

113 Juiz Titular de Vara do Trabalho no TRT da 4ª Região. Especialista em Direito Processual Civil e Graduado em Direito pela Universidade do Sul de Santa Catarina.

114 Mestranda em Direito Empresarial e Cidadania, integrante do grupo “Impacto do regramento da proteção de dados nas relações do trabalho” da UNICURITIBA. pamelapertile@hotmail.com

115 Advogada, especialista em Gestão de Projetos pela FAR, integrante do grupo “Impacto do regramento da proteção de dados nas relações do trabalho” do PPGD da UNICURITIBA. samarakenya@hotmail.com

ções que garantam esta proteção já predefinida, integradas ao sistema, produto ou serviço, por isso, não há necessidade de ter a interação do usuário para que a proteção e a segurança sejam garantidas.

E por ter adotado medidas que resguardem a privacidade durante o desenvolvimento do projeto, caso, haja necessidade de requerer mais dados dos usuários para novas funcionalidades, estes irão poder decidir se vão permitir o acesso ou não. Destaca-se que, independentemente da escolha o usuário, os critérios de proteção e segurança serão resguardados.

Trata-se da ideia de que o produto ou serviço seja lançado e recebido pelo usuário com todas as salvaguardas que foram concebidas durante o seu desenvolvimento. Ou seja, todas as medidas para proteger a privacidade que foram idealizadas desde o início do desenvolvimento do projeto, atendendo ao princípio do *Privacy by Design*. E para isto, faz-se necessário que o serviço oferecido ao usuário seja construído de forma simples, garantindo acessibilidade ao usuário.

Para garantir a privacidade como padrão, é necessário deixar claros os propósitos do tratamento, trazendo assim a transparência de quais dados que serão coletados. Deve-se obedecer aos princípios de minimização de coletas de dados e da necessidade, restringindo o uso dos dados somente às finalidades definidas anteriormente. Bem como a limitação de uso, divulgação a terceiros, retenção e exclusão devem ser feito observando os mais altos níveis de segurança.

Por fim, a proteção de dados por padrão (*Privacy by Default*) e a privacidade desde a concepção (*Privacy by Design*) são conceitos que se complementam e se reforçam mutuamente durante o processo de execução de um projeto.¹¹⁶

PRIVACIDADE BY DESIGN (art. 46)

ROSANA KIM JOBIM¹¹⁷

O conceito de privacidade *by design* é extraído da governança em privacidade e mobiliza toda a princiologia da LGPD.

A privacidade *by design* observa a realidade da empresa, sua estrutura, sua escala, o volume de suas operações, suas políticas etc. Desta forma, “o *Privacy by design* envolve a adoção da privacidade como diretriz do processamento de dados pessoais em todas as etapas (...)”.

Jonas Valente elenca algumas estratégias necessárias para a concretização do *Privacy by design*, quais sejam: minimizar; esconder; separar; agregar; informar; controlar; fiscalizar e aplicar as leis; e demonstrar.

Como se observa, o conceito de privacidade *by design* é amplo, na medida em

116 Referências: BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). CAVOUKIAN, Ann. Information & Privacy: 7 foundational principles. Internet Architecture Board. 2011. Disponível em: https://www.iab.org/wpcontent/IABuploads/2011/03/fred_carter.pdf. Acesso em: 15 out. 2021. HANSEN, Marit. Data Protection by Design and by Default à la European General Data Protection Regulation. 2017. Disponível em: https://link.springer.com/chapter/10.1007/978-3-319-55783-0_3. Acesso em: 15 out. 2021. SALDANHA, Paloma Mendes. O que estão fazendo com os meus dados? A importância da Lei Geral de Proteção de Dados. Coord. Paloma Mendes Saldanha. OAB Pernambuco: Comissão de Direito da Tecnologia da Informação. Recife: SerifaFina, 2019.

117 Advogada Doutoranda na UFRGS, com enfoque na LGPD aplicável às relações de trabalho. Mestre em Direito do Trabalho na Universidade Federal do Rio Grande do Sul.

que abrange a ingerência na arquitetura da rede, e medidas preventivas visando se obter um maior sucesso na proteção da privacidade de terceiros.¹¹⁸

PSEUDONIMIZAÇÃO (art. 13, § 4º)

FERNANDA JULIANE BRUM CORRÊA¹¹⁹

É uma das práticas de segurança de dados, que pode ser adotada como importante medida de *compliance*. Ainda que prevista na LGPD especificamente no artigo que trata sobre estudos em saúde pública - com o fim de preservar a intimidade e privacidade dos participantes e, assim, proteger direitos da personalidade -, tem aplicabilidade a quaisquer dados.

O regulamento europeu (GDPR) contém previsão semelhante, que estabelece a garantia de “pseudoanonimização” quando o tratamento for de interesse público, investigação científica ou histórica, bem como para fins estatísticos.

Conforme a lei, a pseudonimização é o tratamento por meio do qual um dado “perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro”.

Na prática, em vez de os dados serem apagados (supressão ou generalização), são divididos em mais de um banco de dados, cada um contendo identificador diferente que, isoladamente considerados, inibem a associação com o seu titular. Os dados, portanto, são reestruturados e separados, o que permite posterior associação e identificação.¹²⁰

Q

QUALIDADE DOS DADOS (art. 5º, V)

ALINE DAL BÓ CORREA¹²¹

É a garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.¹²²

118 Referências: BRANCO, Sérgio; LEMOS, Ronaldo. Privacy by design: conceito, fundamentos e aplicabilidade na LGPD. In: MENDES, Laura; DONEDA, Danilo; CUEVA, Ricardo Villas Bôas. *Lei Geral de Proteção de Dados (Lei 13.709/2018): a caminho da efetividade*. São Paulo: Revista dos Tribunais, 2020, p. 445-7. SOMBRA, Thiago Luís Santos. *Fundamentos da Regulação da Privacidade e Proteção de Dados Pessoais: pluralismo jurídico e transparência em perspectiva*. São Paulo: Thomson Reuters Brasil, 2019. p. 204. VALENTE, Jonas. *Promovendo a privacidade e a proteção de dados pela tecnologia: privacy by design e privacy enhancing technologies*. Privacidade em perspectivas. Rio de Janeiro: Lumen Juris, 2018. p. 117.

119 Analista Judiciário do TRT da 4ª Região. Graduada em Direito pela Universidade Federal de Santa Maria. Especialista em Direito do Trabalho e Processo do Trabalho pela Faculdade Damásio. fernanda.brum@trt4.jus.br

120 Referências: BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 3 ed. - Rio de Janeiro: Forense, 2021. TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. *Lei Geral de proteção de dados pessoais: Comentada artigo por artigo - 2. ed - Salvador: Editora JusPodivm, 2020.*

121 Graduada na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedalbo04@gmail.com

122 Referências: COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados comentada -*

R

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS**LUCIANE ERBANO ROMEIRO¹²³**

A Lei Geral de Proteção de Dados (LGPD), Lei n.º 13.709/2018, alterada pela Lei n.º 13.853/2019, estabelece o “tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”, de interesse nacional a ser observada pela União, Estados Federados, Distrito Federal e Municípios.

Dentre vários aspectos previstos na Lei Geral de Proteção de Dados quanto aos procedimentos, aplicabilidade, princípios e conceitos, encontra-se o Relatório de Impacto à Proteção de Dados Pessoais, fulcrado no inciso XVII, do artigo 5º, da Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), consistente na “documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco”.

Considerando a tramitação da Proposta de Emenda Constitucional n.º 17/2019, aprovada em 20 de outubro de 2021 pelo Senado Federal para a inclusão de dados pessoais como direitos e garantias fundamentais constitucionais, necessitando somente de promulgação pelo Congresso Nacional, o Relatório de Impacto à Proteção de Dados Pessoais ganha maior relevância e é de fundamental importância e impacto social.

Assim, o Relatório de Impacto à Proteção de Dados Pessoais deverá ser elaborado pelo Controlador – agente a quem compete as decisões sobre o tratamento de dados pessoais -, com definição de obrigações dos agentes antes mesmo de iniciar o tratamento de dados pessoais e conter, no mínimo, a descrição dos tipos e metodologia de dados coletados, garantir a segurança das informações e indicar as medidas e mecanismos de mitigação de riscos.

O Controlador terá legítimo interesse e somente poderá tratar dados pessoais para finalidades específicas, transparentes e estritamente necessárias, consideradas a partir de situações concretas.

À Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional, compete editar regulamentos e procedimentos sobre o Relatório de Impacto à Proteção de Dados Pessoais quando verificar que o tratamento dos dados pessoais representa alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados – LGPD).

Para tanto, a Autoridade Nacional de Proteção de Dados (ANPD) poderá soli-

2.ed - São Paulo: Thomson Reuters Brasil, 2019.

123 Advogada e Cientista da Computação. Mestre em Direito Empresarial e Cidadania (UniCuritiba). Pós Graduada em Direito e Processo do Trabalho (Ematra/PR, UniCuritiba e UniBrasil). Especialista em Compliance em Proteção de Dados e Certificação em CPC-PD (LEC/FGV). luerbano@gmail.com.

citar ao Controlador o Relatório de Impacto à Proteção de Dados Pessoais quando constatado que o tratamento de dados tiver como fundamento o legítimo interesse do Controlador; ou ainda, determinar que o elabore, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, observados, para ambas as situações, os segredos comercial e industrial do Controlador.

Aos agentes do Poder Público, a Autoridade Nacional de Proteção de Dados (ANPD) poderá solicitar a publicação de Relatório de Impacto à Proteção de Dados Pessoais, com sugestão de adoção de padrões e boas práticas para o tratamento de dados pessoais pelo Poder Público.

Destaca-se que o Relatório de Impacto à Proteção de Dados Pessoais poderá ser utilizado pelo Controlador e pela Autoridade Nacional de Proteção de Dados (ANPD) como um documento comprobatório de todos os atos e omissões quanto ao tratamento dos dados pessoais, segurança e metodologias aplicadas, controles operacionais, bem como constatar os meios utilizados para atenuar eventuais riscos que possam atingir a liberdade civil e os direitos fundamentais das pessoas naturais.

Observa-se que o Relatório de Impacto à Proteção de Dados Pessoais tem estreita conexão com Programas de Compliance em Proteção de Dados, principalmente no que tange aos Controles Internos e Mapeamento de Riscos (Risk Assessment) de uma Organização.

Contudo, em que pese o Relatório de Impacto à Proteção de Dados Pessoais seja crucial para o Controlador de Dados Pessoais e para toda a sociedade, a Autoridade Nacional de Proteção de Dados (ANPD) ainda está fazendo reuniões técnicas, consultas e audiências públicas para o processo de regulamentação do Relatório de Impacto à Proteção de Dados Pessoais.

Os aspectos ainda a serem regulamentados pela Autoridade Nacional de Proteção de Dados (ANPD) se referem a Metodologias e Critérios para Elaboração e Análise do Relatório de Impacto; situações e circunstâncias que ensejam a necessidade ou dispensa de elaboração do Relatório de Impacto e Transparência e publicidade dos Relatórios de Impacto para os setores público e privado.¹²⁴

RESPONSABILIDADE (art. 31)

BRUNA CASIMIRO SICILIANI¹²⁵

A LGPD prevê modalidade de responsabilização preventiva em seu artigo 31, que preceitua que “quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá en-

124 Referências: BRASIL. Lei 13.709, de 14 de agosto de 2018. Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 22 out. 2021. ANPD. Autoridade Nacional de Proteção de Dados. Presidência da República. Governo Federal do Brasil. Disponível em: <https://www.gov.br/anpd/pt-br>. Acesso em: 24 out 2021. NEGRÃO, Celia P. Lima; PONTELO, Juliana de Fátima. *Compliance, Controles Internos e Riscos: A importância da área de gestão de pessoas*. Brasília: Editora Senac, 2014. SILVEIRA, Renato de Mello Jorge; SAAD-DINIZ, Eduardo. *Compliance, Direito Penal e Lei Anticorrupção*. São Paulo: Saraiva, 2015. CUNHA, Matheus; EL KALAY, Marcio. *Manual de Compliance: Compliance Mastermind Vol.1*. São Paulo: LEC, 2019.

125 Professora e advogada. Doutoranda em Direito pela UFRGS. Mestre em Direito pela UFRGS. Especialista em Direito do Trabalho e Processo do Trabalho pela PUCRS.

viar informe com medidas cabíveis para fazer cessar a violação”. Além disso, prevê também a reparação de danos no artigo 42, o qual dispõe que “o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo”. Em virtude disso, nesse sentido, entende-se a responsabilidade na LGPD como “o dever de prevenir, mitigar, ou reparar um dano decorrente da violação da legislação de proteção de dados pessoais”.

Segundo Iuri Pinheiro, Fabrício Lima e Vólia Bomfim (2021, p.756), há forte tendência doutrinária em se adotar apenas a responsabilidade subjetiva, com culpa presumida e, via de consequência, em afastar o entendimento de responsabilidade civil objetiva do empregador, por aplicação do artigo 42 e incisos II e III do artigo 43 da LGPD, que expressamente isenta de responsabilidade aquele que não violou a lei, uma vez que a responsabilidade subjetiva é a regra genericamente prevista pelo Código Civil. Não obstante, uma vez que a LGPD, lei especial, não trouxe a culpa como elemento necessário para a configuração de responsabilidade, estes autores defendem que, em tese, é possível a aplicação da responsabilidade objetiva.¹²⁶

REVOGAÇÃO (art 15, III)

ALINE DAL BÓ CORREA¹²⁷

O consentimento pode ser revogado a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do *caput* do art. 18 da Lei.¹²⁸

S

SAÚDE

BÁRBARA FAGUNDES¹²⁹

O termo “saúde” é mencionado diversas vezes na LGPD, quais sejam: definição de dados pessoais sensíveis (art. 5º, II), requisitos para o tratamento de dados (art.

126 Bibliografia: BELMONTE, Alexandre Agra. *Instituições Cíveis no Direito do Trabalho*: Curso completo de Direito Civil com aplicação subsidiária nas relações de trabalho. Salvador: Editora JusPodivm, 2020. FARIAS, Cristiano Chaves de; NETTO, Felipe Peixoto Braga. ROSENVALD, Nelson. *Novo Tratado de Responsabilidade Civil*. São Paulo: Saraiva, 2019. PINHEIRO, Iuri. *Manual do compliance trabalhista: teoria e prática*. Fabrício Silva Lima, Iuri Pinheiro, Vólia Bomfim. 2 ed. – Salvador: Juspodivm, 2021. ROSENVALD, Nelson. *A polissemia da responsabilidade civil na LGPD*. Migalhas. 6 de novembro de 2020. Disponível em: <https://migalhas.uol.com.br/coluna/migalhas-de-protecao-dedados/336002/a-polissemia-da-responsabilidade-civil-na-lgpd>. Acesso em: 9 nov. 2020.

127 Graduanda na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedal-bo04@gmail.com

128 Referências: MALDONADO, Viviane Nóbrega, BLUM, Renato Opice. *LGPD: Lei Geral de Proteção de Dados Pessoais comentada* - 3. ed - São Paulo: Thomson Reuters Brasil, 2021.

129 Juíza do Trabalho Substituta do TRT da 4ª Região, Mestre em Direito pela Universidade Federal do Rio Grande do Sul (UFRGS). barbara.fagundes@trt4.jus.br

7º, VIII), tratamento de dados pessoais sensíveis sem o consentimento do titular (art. 11, II, “f”), vedação de comunicação e compartilhamento de dados pessoais sensíveis de saúde e suas exceções (art. 11, §4º), proibição do uso de dados de saúde para a discriminação na contratação de planos de saúde (art. 11, §5º) e uso de dados pessoais sensíveis para fins de pesquisa de saúde pública (art. 13).

Dados pessoais referentes à saúde são uma das espécies de dados pessoais sensíveis. São, portanto, dados nucleares e essenciais ao livre desenvolvimento da personalidade humana. Quanto a dados de saúde, o consentimento para o tratamento deve ser específico e destacado para finalidades específicas. No entanto, pode haver tratamento de dados de saúde sem consentimento do titular nos seguintes casos: atendimento de alguma obrigação legal ou regulatória; execução de políticas públicas especificadas em leis, regulamentos ou negócios jurídicos; estudos de órgãos de pesquisa; proteção à vida ou à incolumidade física do titular ou de terceiro; tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

No âmbito da relação de emprego, também há tratamento de dados pessoais sensíveis referentes à saúde. Conforme a Norma Regulamentadora n. 07 (NR 07), *os dados obtidos nos exames médicos, incluindo avaliação clínica e exames complementares, as conclusões e as medidas aplicadas deverão ser registrados em prontuário clínico individual, que ficará sob a responsabilidade do médico-coordenador do PCMSO*. Os mencionados registros devem ser mantidos por, no mínimo, vinte anos após o desligamento do trabalhador, na forma do item 7.4.5.1 da NR 07. Além disso, ao se referir a dados digitais radiológicos, a NR 07 determina, em seu item 12.1, que *os serviços que ofertam radiologia digital devem assegurar a confidencialidade dos arquivos eletrônicos e de dados dos trabalhadores submetidos a radiografias de tórax admissionais, periódicas e demissionais, para fins da classificação radiológica da OIT, através da implementação de medidas e procedimentos técnicos e administrativos adequados*.

Pode o empregador tratar dados pessoais sensíveis referentes à saúde do empregado sem o fornecimento de consentimento do obreiro, pois se trata de cumprimento de obrigação legal e de exercício regular do direito em contrato, nos termos do art. 11, II, “a” e “d”, da LGPD. No entanto, não pode haver o uso e o compartilhamento dos dados de saúde para obtenção de vantagem econômica. O compartilhamento de dados de saúde somente é permitido para prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde em benefício dos interesses do trabalhador titular dos dados. Se houver solicitação do trabalhador titular dos dados de saúde, poderá haver a portabilidade desses dados sensíveis.

Para fins de processo judicial, é permitido o tratamento de dados pessoais sensíveis referentes à saúde, nos termos do art. 11, II, “d”, da LGPD. A recusa expressa ao tratamento de dados pessoais de saúde em processo judicial induz à aplicação dos arts. 231 e 232 do Código Civil. Assim, aquele que se recusa ao tratamento de seus dados pessoais sensíveis referentes à saúde em processo judicial não se aproveitará de sua negativa. Ao contrário, a negativa do titular suprirá a prova que se pretendia obter.¹³⁰

¹³⁰ Referências: SANTOS, F. A lei geral de proteção de dados pessoais (LGPD) e a exposição de dados

SEGURANÇA

MARCELA CASANOVA VIANA ARENA¹³¹

O tratamento de dados pessoais deve observar a boa-fé e outros princípios elencados na Lei 13.709/2018, dentre os quais o princípio da segurança, o qual consiste na utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. No âmbito das relações de trabalho, destaca-se que a empresa que faz o tratamento dos dados é a responsável pela segurança desses dados. Desde a fase pré-contratual, na realização de processo seletivo, cumpre à empresa zelar pela segurança dos dados dos candidatos e empregados, sob pena de responsabilização.¹³²

SEGURANÇA EM LGPD

PAULO GUSTAVO MAGELLA DE FARIA QUINAN¹³³

E GERALDA MAGELLA DE FARIA ROSSETTO¹³⁴

As constantes e sequenciais ameaças seguidas por novas tecnologias que invadem o ambiente digital, a vida comum do cidadão e as relações do Estado fizeram desencadear novas regras e significativas reformas legislativas em muitos países, tendo em conta a segurança informacional no que diz respeito aos dados, especialmente os de cunho pessoal. A referência é mesmo a União Europeia, onde têm sido presenciadas diversas alterações normativas junto aos Estados-Membros da UE, a tornar explícito o que antes era implícito, ou, até mesmo, suplantando uma singela suposição por uma recomendação ou determinação.

No Brasil, esse cenário não é diferente, e pode-se dizer que a GDPR (*General Data Protection Regulation*) foi a grande inspiração para a Lei Geral de Proteção de Dados Pessoais. Muitas outras questões, inclusive exigências de mercado, podem ter contribuído com esse acelerado processo que culminou com a Lei n.º 13.709, de 2018. Se por um lado, a chegada do “regulamento brasileiro” de proteção de dados pessoais foi saudada pelos que prezam a privacidade – situação que no Brasil, desde a Lei Carolina Dieckmann¹³⁵, a sociedade e a comunidade de juristas já havia

sensíveis nas relações de trabalho. Revista do TRT da 10ª Região, v. 24, n. 2, p. 145-151, 14 jan. 2021. SOARES, Flaviana Rampazzo. *Consentimento no direito da saúde nos contextos de atendimento médico e de LGPD: diferenças, semelhanças e consequências no âmbito dos defeitos e da responsabilidade*. Revista IBERC, Belo Horizonte, v. 4, n. 2, p. 18-46, maio/ago. 2021.

131 Mestranda em Direitos Sociais no Programa de Pós-Graduação em Direito da Universidade Federal de Pelotas. Juíza do Trabalho no TRT da 4ª Região.

132 Referências: PINHEIRO, Iuri; BOMFIM, Vólia. *A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho*. Disponível em: <http://trabalhoemdebate.com.br/artigo/detalhe/a-lei-geral-de-protacao-de-dados-e-seus-impactos-nas-relacoes-de-trabalho>. Acesso em: 24.out. 2021.

133 Doutorando em Engenharia de Segurança em Redes pela Universidade de Victória, Canadá. Mestrado pela UDESC. Graduação em Ciências da Computação pela UFSC. Email: quinan@uvic.com

134 Doutorado em Direito pela UFSC. Mestre em Direito pela UNISINOS. Advogada. Procuradora Federal aposentada. Pesquisadora do Direito e Fraternidade; do DataLab e do NEJUSCA. Email: geraldamagella@gmail.com

135 O nome decorre de um fato ocorrido com a referida atriz que proporcionou acirradas discussões, tendo culminado com a Lei n.º 12.737, de 2012, a qual dispõe sobre crimes virtuais. O caso: “Em maio de 2011, um hacker (criminoso virtual) invadiu o computador pessoal da atriz, possibilitando que ele tivesse acesso a 36 fotos pessoais de cunho íntimo. De acordo com a denúncia, o invasor exigiu R\$ 10

tomado consciência de que havia algo mais nessas questões –, de outro modo, o processo legislativo, insuflado com a matéria do “acesso à informação” e da “proteção de dados pessoais”, ficou contaminado pela transparência. Paradoxalmente, questões opostas passaram a ocupar a cena diária, e tanto o público e o privado, a via administrativa e a judicial, passaram a um outro nível de agenda.

Senão, veja-se.

Surgiu um novo modelo, verdadeiro “esquema” dos serviços de informação, os quais, se não estão tão nítidos na comunidade brasileira, mas já são reconhecidos mundo afora pela própria exigência e significado das normas internacionais de direitos humanos, carecendo, por isso mesmo, de clareza, previsibilidade e de uma figura bem específica, a acessibilidade, a afastar fontes de incerteza e de não prevenção, o que é esperado também em relação ao próprio ordenamento. Porém, há um específico alerta a esse respeito: é que, segundo a Agência dos Direitos Fundamentais da União Europeia, “a ‘legislação’ não passou em muitos testes em termos de clareza e previsibilidade”. (FRA, 2021).

Seja como for, é bom ser dito que essa constante e persistente falta de clareza é da ordem normativo-processual e, também, de ordem material, que seguem dispostas em um emaranhado sistema de proteção e de segurança, muitos com particularidades que afastam o cidadão¹³⁶, e, assim, cada vez mais se passa a privilegiar o sigilo, a confidencialidade, a intimidade, qual seja, a proteção de dados pessoais e a privacidade, por excelência. Não obstante, “a mera existência de legislação que permite medidas de vigilância constitui uma interferência no direito à vida privada” (FRA, 2021), e, sob tal prisma, “os tribunais europeus também consideram que a recolha de dados pelos serviços de informações constitui uma interferência. Tal interferência deve ser justificada para respeitar os direitos humanos” (FRA, 2021).

Estão aí postas as premissas da complexidade da temática, não sem antes alertar para o fato de que, se a falta de clareza constitui uma fonte de incerteza, ela também concorre para depositar nos pés da democracia uma pedra – com o tempo, o gigante poderá sangrar e ter de substituir seus sapatos por outros. Nesse sentido, é certa a contraposição, a andar juntos, a segurança da informação, o acesso à informação, os dados pessoais e a privacidade.

mil para não publicar as fotos. Como a atriz recusou a exigência, acabou tendo suas fotos divulgadas na Internet. [...] A atriz abraçou a causa e cedeu seu nome à lei. Ressalta-se que, antes do surgimento da lei, o ato de invadir um ambiente virtual e subtrair dados pessoais já era crime, mas não havia nenhuma norma que tratava especificamente sobre o assunto”.

136 Dentre os muitos aspectos que podem explicar o distanciamento do cidadão quanto a questões do ambiente digital, com implicações sobre o seu tráfego na Internet e na sua segurança informacional, estão as relacionadas à *literacia*. Nesse sentido, há o destaque para a lexia “literacy”, que vem recebendo destaque, passando a incorporar novos significados, “digital literacy” e “media and information literacy” – com o sentido de letramento informacional, alfabetização informacional, habilidade informacional e competência informacional e, paulatinamente, na sociedade da informação, a sinonímia tem recebido adjetivos, i.é, *literacia digital* ou *literacia informacional*, exatamente pela proximidade com a informação e a tecnologia, exprimindo habilidades e competências relativas a busca, seleção, análise, avaliação e processo da informação, considerando o meio, o contexto e o ambiente em que se encontra, sendo que a expressão *literacia informacional* tem se firmado com maior destaque, tendo, inclusive, recebido da UNESCO - Organização das Nações Unidas para a Educação, a Ciência e a Cultura, “a condição de direito básico, tão ou mais importante que o acesso à tecnologia” (UNESCO, 2021).

Ocorre que, sem segurança, não há proteção de dados – e isso inclui os dados de cunho pessoal. Essa máxima, retirada do senso comum teórico da comunidade técnico-científica, retrata com fidelidade o propósito áureo da segurança da informação, ainda que, “a garantia da segurança da informação não se confunda com o direito à proteção de dados pessoais, como muitas vezes se acredita, há inequívoca pertinência entre eles”. (CUEVA, 2021, p. 540).

Contudo, a despeito de que a segurança se encontra sustentada por três fortes balizas, a *disponibilidade*, a *integridade* e a *confidencialidade*, há um quarto elemento que dá amálgama a esse tripé. Trata-se da *confiança*, uma qualidade baseada em *privacidade* construída pela dinâmica da consciência, da proteção de direitos e pela arquitetura que se projeta nos sistemas em redes, que deve estar blindada pela *resiliência* – a qual encontra-se acrescida no Regulamento Europeu (RGPD, art. 32, 1, b).

A respeito da resiliência, inclusive pela novidade no direito brasileiro, o tema tem merecido atenção. A seu respeito, convém ser dito que sua tradução tem a ver com a capacidade de restabelecer uma ordem anterior a um choque, de retomada a um estado prévio da alteração que sobreveio, semelhante a um comportamento de recomposição. Menke e Goulart dão conta do preenchimento de seu conteúdo, em que “se inserem características como as de robustez, elasticidade ou aptidão de adaptação, significando dizer, como ponto de partida, que erros ou incidentes sempre poderão ocorrer” (2020, p. 344). É aquela velha lógica, pessoas, processos e tecnologia¹³⁷ devem seguir, ou no caso dos sistemas, devem funcionar, ainda que objetos de correções, adaptações e modificações.

Seja como for, interessa neste a segurança em relação aos dados pessoais e, para tanto, esses quatro elementos, pelo significado decisivo e condição chave ao deslinde da segurança da informação, são ora referidos, a dar conta de erigir um conceito próprio e a compor a engenharia da segurança informacional voltada aos dados pessoais. Senão, veja-se:

i) *segurança da informação*: como consta na ISO/IEC 27002, trata-se da “proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”;

ii) *segurança na LGPD*, encontra-se distribuída em dois importantes dispositivos: art. 46, *caput*. “Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito” (BRASIL, 2021); também, art. 6º, inciso VII, “segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão” (BRASIL, 2021);

iii) outro importante aspecto diz respeito à prevenção, cujo significado na

137 Essa trilogia contempla, em síntese, os seguintes pontos: checar de detectar vulnerabilidades em processos e em tecnologia a dar conta de bandeiras prioritárias; mapear os principais skills, de forma a facilitar a exploração de vulnerabilidades que denotarão maior impacto.

LGPD é a de “adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais”, art. 6º, inciso VIII (BRASIL, 2021). Também, no art. 50, em que está dito, “os controladores e operadores [...] poderão formular regras de boas práticas e de governança [de aspectos] relacionados ao tratamento de dados pessoais” (BRASIL, 2021), tais como, a organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos;

iv) a respeito do tripé confidencialidade (informação a ser protegida em face do acesso ou uso não autorizado), integridade (garantir que a informação não sofreu alteração durante o seu ciclo de vida), e a disponibilidade (garantia de que a informação está e estará disponível), com largo reconhecimento pela doutrina especializada e que, além do campo teórico, também se encontra recepcionada nas medidas de ordem prática, sejam nas esferas públicas, em relação aos comunicantes/denunciante, organizações da sociedade civil, dos meios de comunicação social.

Há ainda outras importantes categorias que, às voltas com a segurança da informação e com o seu esperado manejo, são decisivas à proteção de dados pessoais. A autenticação é a primeira delas, e da mesma seguem outras mais. A esse respeito, notadamente sobre a figura da autenticação importa dizer que é o processo de estabelecer ou confirmar a identidade de um agente usuário de um sistema, cujos procedimentos (tipos e múltiplos fatores) cabem nas seguintes digressões. A respeito dos *tipos*: *i*) baseada no conhecimento: o que você sabe: senhas, códigos etc; *ii*) baseada na propriedade: o que você tem: tokens, cartões de acesso, smartphone etc.; e, *iii*) baseada na característica: o que você é: dados biométricos: impressão digital, facial, andadura, digitação etc. A respeito dos *múltiplos fatores*: utiliza duas ou mais etapas (fatores de autenticação) para autenticar o usuário. Um aspecto significativo refere-se a que pode ser usada esporadicamente para (re) estabelecer a confiança.

Por fim, tendo como pressuposto os quadros jurídicos relativos à segurança das informações, de suas esferas aplicativas, as quais são de adoção no campo teórico-prático, tem-se que a real influência da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), diz respeito à sua configuração: ser um marco regulatório sobre o tratamento de dados pessoais, verdadeira baliza de proteção desses dados. A gramática da LGPD deve dar conta de proteger, promover e defender as atividades relacionadas à segurança da informação, à governança de dados e à gestão de riscos, a garantir a fórmula da proteção dos direitos, sejam direitos fundamentais ou direitos humanos, os quais necessitam seguir na trajetória da humanidade, cercados da devida dose de confiança, de privacidade e de confidencialidade. Saibamos reconhecer o peso que recai sobre essa geração a dar conta de contar uma história de cultura fraterna e de cultura de dados pessoais, em simetria e sintonia.¹³⁸

138 Referências: BRASIL. Lei n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 out. 2021. CUEVA, Ricardo Villas Bôas. Segurança da Informação e Pro-

T

TRATAMENTO DE DADOS**MARCELA CASANOVA VIANA ARENA**¹³⁹

Tratamento de dados consiste em diversas possibilidades de manipulação dos dados, como coleta, transmissão, armazenamento, utilização, acesso, reprodução, acesso. O tratamento dos dados deve observar a finalidade, a boa-fé e o interesse público. Conforme dispõe o artigo 7º da Lei 13.709 (BRASIL, 2018), o tratamento dos dados pode ser realizado mediante o fornecimento do consentimento do titular ou nas seguintes hipóteses: para o cumprimento de obrigação legal ou regulatória pelo controlador; pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres; para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; para o exercício regular de direitos em processo judicial, administrativo ou arbitral; para a proteção da vida ou da incolumidade física do titular ou de terceiro; para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. Para o tratamento de dados pessoais sensíveis, é necessário o consentimento do titular de forma destacada e específica para a finalidade delimitada. Quando não houver o consentimento do titular, os dados pessoais sensíveis somente poderão ser utilizados quando indispensável para: cumprimento de obrigação legal ou regulatória pelo controlador; tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; exercício regular de

teção de Dados Pessoais. In: FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antonio. *A Lei Geral de Proteção de Dados Pessoais - LGPD: aspectos práticos e teóricos relevantes no setor público e privado*. São Paulo: Thomson Reuters, 2021, p. 539-570. Lei Carolina Dieckmann: você sabe o que essa lei representa? Disponível em: <https://fmp.edu.br/lei-carolina-dieckmann-voce-sabe-o-que-essa-lei-representa/>. Acesso em: 24 out. 2021. FRA – *European Union Agency for Fundamental Rights*. Relatório sobre os Direitos Fundamentais – 2021. Agência dos Direitos Fundamentais da União Europeia, 2021. Disponível em: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-fundamental-rights-report-2021-opinions_pt.pdf. Acesso em: 24 out. 2021. MENKE, Fabiano; GOULART, Guilherme Damásio. Segurança da Informação e Vazamento de Dados. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; (coord); BRIONI, Bruno (coord). *Tratado de Proteção de Dados Pessoais*. 2. reimpressão. Rio de Janeiro: Forense, 2021, p. 339-359. UNESCO. Transformações e Inovações Digitais no Brasil. Disponível em: <https://pt.unesco.org/fieldoffice/brasil/expertise/digital-transformation-brazil>. Acesso em: 14 out. 2021.

139 Mestranda em Direitos Sociais no Programa de Pós-Graduação em Direito da Universidade Federal de Pelotas. Juíza do Trabalho no TRT da 4ª Região.

direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da lei; proteção da vida ou da incolumidade física do titular ou de terceiro; tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da Lei 13.709/2018, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.¹⁴⁰

TÉRMINO DO TRATAMENTO (arts. 15 e 16)

BÁRBARA FAGUNDES¹⁴¹

O art. 15 da LGPD estabelece que o término do tratamento de dados ocorrerá nos seguintes casos: a) quando a finalidade foi alcançada ou os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica; b) fim do período de tratamento; c) comunicação do titular quando houver revogação do tratamento, resguardado o interesse público; d) determinação da autoridade nacional. Com o término do tratamento, os dados pessoais serão eliminados. Podem os dados ser conservados, no entanto, nos termos do art. 16, para as seguintes finalidades: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) estudo por órgão de pesquisa, garantida a anonimização dos dados, quando possível; c) transferência a terceiro; d) uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

É necessário lembrar, contudo, que a revogação do tratamento de dados pessoais tem também como limite o legítimo interesse do controlador e de terceiros, conforme art. 7º, IX, da LGPD. Assim, com o término da relação de emprego, o trabalhador não pode revogar eventual consentimento dado para o tratamento de dados nem exigir a eliminação desses dados, pois o empregador tem a obrigação legal de tratar os dados por certo período, além de ter legítimo interesse de tratar os dados. Por exemplo, a obrigação de conservar os dados referentes à saúde por, no mínimo, após vinte anos do desligamento, item 7.4.5.1 da NR 07, impede a eliminação dos dados, ainda que a pedido do titular dos dados. Da mesma forma, com o término da relação de emprego, o empregador terá interesse em tratar os dados do empregado para o caso de eventuais demandas judiciais, enquanto transcorrerem prazos prescricionais.¹⁴²

140 Referências: PINHEIRO, Iuri; BOMFIM, Vólia. *A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho*. Disponível em: <http://trabalhoemdebate.com.br/artigo/detalhe/a-lei-geral-de-protacao-de-dados-e-seus-impactos-nas-relacoes-de-trabalho>. Acesso em: 24.out.2021.

141 Juíza do Trabalho Substituta do TRT da 4ª Região, Mestre em Direito pela Universidade Federal do Rio Grande do Sul (UFRGS) barbara.fagundes@trt4.jus.br

142 Referências: SANTOS, F. A lei geral de proteção de dados pessoais (LGPD) e a exposição de dados sensíveis nas relações de trabalho. *Revista do TRT da 10ª Região*, v. 24, n. 2, p. 145-151, 14 jan. 2021. STÜRMER, Gilberto. Thaís Oliveira Dorfmann. Lei Geral de Proteção de Dados como meio de garantir sustentabilidade nas relações de trabalho. In: *Constitucionalismo e Meio Ambiente*, tomo 5: Sustentabilidade [recurso eletrônico] / Cleide Calgari; Liton Lanes Pilau Sobrinho; Paulo Márcio Cruz (org.) -- Porto Alegre, RS: Editora Fi, 2021, p. 277-297.

TITULAR (art. 5.º, V e art. 17)

FERNANDA JULIANE BRUM CORRÊA¹⁴³

É um dos sujeitos de tratamento de dados, conceituado como a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Para a LGPD, “toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade”. Assim, embora a pessoa jurídica também seja detentora de direitos de personalidade, no que couber (art. 52 do Código Civil), a LGPD protege apenas dados de pessoas naturais e não alcança dados de pessoas jurídicas. Nesse contexto, vale lembrar que o Microempreendedor Individual (LC 128/2008) não se trata de pessoa jurídica, mas de pessoa física a quem a lei faculta o registro no CNPJ, de modo que seus dados são protegidos pela LGPD.¹⁴⁴

TRANSFERÊNCIA INTERNACIONAL - I (art. 5º, XV)

JAQUELINE MARIA MENTA¹⁴⁵

Nos termos do inciso XV do art. 5º da Lei n.º 13.709/2018, a transferência internacional de dados é a “transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro”.

No Capítulo V, intitulado DA TRANSFERÊNCIA INTERNACIONAL DE DADOS, referida Lei trata das permissões para tanto (art. 33), da verificação do nível de proteção de dados exigido no país estrangeiro (art. 34), da definição do conteúdo de cláusulas-padrão contratuais e da verificação de cláusulas contratuais específicas para uma determinada transferência, além de normas corporativas globais ou selos, certificados e códigos de conduta (art. 35), e das “alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular” (art. 36).

Das disposições contidas na LGPD para a transferência internacional de dados pessoais, tem-se que essa somente ocorre nas hipóteses elencadas na referida lei, não havendo espaço para acréscimo de situações não previstas pelo legislador.

Nesse sentido, leciona Luís Fernando Prado Chaves¹⁴⁶, assegurando a pretensão do legislador em restringir as hipóteses permitidas para a transferência internacional de dados pessoais, apontando que essa é exceção à regra, estando restritas as possibilidades para apenas aquelas situações que configurarem as “taxativamente

143 Analista Judiciário do TRT da 4ª Região. Graduada em Direito pela Universidade Federal de Santa Maria. Especialista em Direito do Trabalho e Processo do Trabalho pela Faculdade Damásio. fernanda.brum@trt4.jus.br

144 Referências: MIZIARA, Raphael. *Reflexos da LGPD no Direito e no processo do trabalho* (livro eletrônico). Raphael Mizziara, André Pessoa, Bianca Mollicone – 1. ed. - São Paulo: Thomson Reuters Brasil, 2020.

145 Juíza do Trabalho Substituta do TRT da 4ª Região. Mestranda em Ciências Jurídicas pela Universidade Autónoma de Lisboa (UAL). Especialista em Direito do Trabalho e Previdenciário pela PUC Minas. Especialista em Direito Privado (Civil e Comercial) à luz do novo Código Civil pelo Centro de Ensino Superior dos Campos Gerais Faculdades Integradas dos Campos, IBEJ, Brasil. jaqueline.menta@trt4.jus.br

146 CHAVES, Luis Fernando Prado. Da Transferência Internacional de Dados. In: Viviane Nóbrega Maldonado e Renato Opice Blum (coord.). *LGPD: Lei Geral de Proteção de Dados Pessoais Comentada*. 3ª ed. São Paulo: Thomson Reuters Brasil, 2021. p. 312. ISBN: 978-65-5614-437-5;

te listadas nos incisos do artigo 33”.

Pese embora ditas disposições consintam a transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro, infere-se não conter o aprofundamento necessário, possuindo elevado grau de generalidade, como se observa no *caput* do art. 34, com o uso da expressão “que levará em consideração” e inciso VI, quando permite que a autoridade considere “outras circunstâncias específicas relativas à transferência”.

Não obstante a generalidade permita o preenchimento das lacunas nos casos concretos, facilitando a adequação da legislação à evolução da sociedade, da tecnologia e da própria legislação, dentre outros fatores que podem influenciar, tanto na necessidade da transferência internacional de dados como na forma que possam ser feitos, também é certo não estipular procedimentos e elementos a serem observados, ainda que tenham sido taxativamente elencadas as possibilidades dessa transferência, consoante se infere das permissões consignadas no art. 33.

Analisando-se o GDPR (ou RGPD, como mais comumente é conhecido no Brasil o Regulamento de Proteção de Dados na União Europeia), tem-se que esse previu todos os procedimentos e elementos para a transferências de dados pessoais para países terceiros ou organizações internacionais, conforme se observa da leitura dos artigos 45, n. 2, e 46, n. 4.

Na LGPD, nove são as hipóteses permitidas para transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

Na primeira delas, inciso I do art. 33, avaliza-se a transferência de dados para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na LGPD, inferindo-se basear-se na proteção emanada do país ou organismo internacional destinatário dos dados pessoais, ou seja, parte do gerenciamento dos riscos a que possam ser submetidos os dados pessoais transferidos.

A segunda possibilidade de transferência, inciso II do art. 33, tem lugar em razão da atuação do controlador, ou seja, quando ele oferece e comprova garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD, na forma de: cláusulas contratuais específicas para determinada transferência (alínea “a”); cláusulas-padrão contratuais (alínea “b”); normas corporativas globais (alínea “c”), e selos, certificados e códigos de conduta regularmente emitidos (alínea “d”).

Já a terceira situação, inciso III do art. 33, baseia-se na necessidade de cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional, do que se extrai sua importância, sobretudo ante o aumento de crimes cometidos pela rede mundial de computadores (*Internet*), por meio do qual a criminalidade espalha-se para além das fronteiras nacionais, sendo vital a cooperação entre Estados e organismos internacionais para a persecução dos criminosos, possibilidade que encontra guarida também na disposição de não aplicação da LGPD quando o tratamento de dados for realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, nos exatos termos do artigo 4º, inciso III da LGPD.

Como quarta possibilidade, contida no inciso IV do art. 33, autorizada remanesce a transferência internacional de dados pessoais quando for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro, sendo evidente que essa disposição visa tutelar a pessoa humana, como ocorre, por exemplo, com o repasse de dados para procura e busca de pessoas desaparecidas ou sequestradas, não se podendo mitigar o direito à vida e à integridade física “por questões relativas à limitação do fluxo de dados pessoais”¹⁴⁷.

A quinta hipótese, inciso V do art. 33, ocorre quando a autoridade nacional autorizar a transferência. Para Luís Fernando Prado Chaves¹⁴⁸, aqui reside uma possibilidade genérica de transferência internacional de dados pessoais, já que a ANPD pode autorizar transferências específicas.

A sexta hipótese, inciso VI, tem lugar quando a transferência resultar em compromisso assumido em acordo de cooperação internacional, como, por exemplo, Convenção das Nações Unidas contra o Tráfico Ilícito de Estupefacientes e Substâncias Psicotrópicas, Convenção das Nações Unidas contra o Crime Organizado Transnacional e Convenção das Nações Unidas contra a Corrupção.

Já a sétima hipótese, inciso VII do art. 33, terá lugar quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do *caput* do art. 23 d LGPD. Extrai-se dessa possibilidade de transferência de dados pessoais que objetiva demarcar a atuação do agente público, podendo deliberar pelo imperativo de transferência de dados de acordo com implantação de políticas públicas e o cumprimento de obrigações legais, podendo-se exemplificar com a transferência de dados para a implementação de políticas públicas de saúde, as quais mostraram-se indispensáveis para contenção de pandemia.

A oitava e penúltima permissão, inciso VIII do art. 33, emana do titular dos dados, ou seja, ele fornece consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades, a qual entendemos como a mais frágil, na medida em que o consentimento poderá ser revogado. De qualquer forma, essa hipótese demanda a observância do contido no inciso XII do art. 5º da LGPD, de modo que a manifestação deve ser livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada e, nessa hipótese específica, com destaque para a transferência e com informação prévia sobre o caráter internacional da operação.

A nona e última hipótese, inciso IX do art. 33, vincula-se ao atendimento das hipóteses previstas nos incisos II, V e VI do art. 7º da LGPD, o qual dispõe sobre o tratamento de dados pessoais, sendo cumprimento de obrigação legal ou regulatória pelo controlador (inciso II do art. 7º), exemplificando-se com o cumprimento de obrigação prevista em lei federal, estadual ou municipal, inclusive em legislação internacional (para os casos de empresas multinacionais), não se enquadrando aqui o cumprimento de obrigações contratualmente assumidas. Quanto ao disposto no inciso V do art. 7º, tem-se permitida a transferência internacional

147 Ibidem.

148 Ibidem.

quando necessária para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados, tendo com situação concreta no contexto laboral o envio de *curriculum* para candidatar-se a uma vaga em uma empresa internacional, cuja seleção seja no Brasil, mas a decisão final e a contratação será em país estrangeiro; e para execução de contrato a informação de dados bancários para o pagamento do salário, consignando-se que sem essa transferência de dados, tanto como procedimento preliminar como para execução de contrato torna-se impossível o início do contrato ou a sua execução. Por fim, no inciso VI do art. 7º, tem-se a possibilidade de transferência internacional de dados pessoais para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem), devendo-se nessa situação observar o prazo prescricional, atentando-se, ainda, a possibilidade de estar em causa uma suspensão ou interrupção do prazo prescricional.¹⁴⁹

TRANSFERÊNCIA INTERNACIONAL - II (art. 5º, XV)

ELEONORA COELHO DOZZA¹⁵⁰

Entre as diversas situações que envolvem o tratamento de dados pessoais, o seu compartilhamento internacional é uma das hipóteses mais complexas, pois necessária para o desenvolvimento das operações sociais e econômicas, entre as quais algumas relações de trabalho; mas, ao mesmo tempo, traduz risco acentuado aos direitos fundamentais, que ficam submetidos às regras de um novo território.

A transferência internacional de dados não se caracteriza pelo simples tráfego de informações por meio da rede e de provedores de Internet de um ponto a outro. A transferência, a que se refere à disciplina normativa nacional e internacional de dados, implica o uso compartilhado de informações de pessoas identificadas ou identificáveis para a realização de determinadas finalidades, tais como a concretização de relação de trabalho que envolva o desempenho de atividades em mais de um país. Imaginemos, a título ilustrativo, uma empresa multinacional com escritórios em diversos países que encaminhe e-mail do escritório, de um país a outro, com dados de candidatos a determinadas vagas de emprego. Essa operação se denomina transferência internacional de dados. Ou a situação de um trabalhador, dessa mesma empresa multinacional, com seu contrato de trabalho ativo, que necessite, de tempos em tempos, encaminhar informações suas a escritórios situados em outros países. Essa operação também caracteriza transferência internacional de dados.

Existem hipóteses específicas em que serão legítimas as transferências internacionais de dados. A Lei de Geral Proteção de Dados Pessoais (LGPD), Lei 13.709/2018, vigente desde agosto de 2020, regula a matéria nos artigos 33 a 36, especificando como deve ocorrer a operação. O artigo 33 da LGPD preceitua que a transferência internacional de dados pessoais somente é permitida nas seguintes hipóteses: 1) para países ou organismos internacionais que proporcionem grau de proteção de dados

149 Referências: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). LGPD: *Lei geral de proteção de dados*: comentada. 3ª ed. São Paulo: Thomson Reuters Brasil, 2021. ISBN: 978-65-5614-437-5.

150 Advogada. Especialista em Direito e Processo Civil pela Faculdade IDC e Mestranda em Direito Europeu e Alemão na Universidade Federal do Rio Grande do Sul. eleonoradozza31@gmail.com

personais adequado ao previsto nesta Lei; 2) quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD, na forma de cláusulas contratuais específicas para determinada transferência ou de cláusulas-padrão contratuais, normas corporativas globais ou selos, certificados e códigos de conduta regularmente emitidos; 3) quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional; 4) quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro; 5) quando a autoridade nacional autorizar a transferência; 6) quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; 7) quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade; 8) quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente essa de outras finalidades; 9) quando necessário para o atendimento de obrigação legal ou regulatória pelo controlador, para o exercício regular de direitos em processo judicial, administrativo ou arbitral, ou para a execução de contrato ou de procedimentos preliminares relacionados a contrato.

A LGPD atribui diversas competências à Autoridade Nacional de Proteção de Dados, a quem incumbirá avaliar o nível de proteção de dados do país estrangeiro ou do organismo internacional, bem como definir o conteúdo de cláusulas-padrão contratuais e verificar cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, na forma do que estabelecem os artigos 34 e 35 da Lei, respectivamente.

A base legal do consentimento, categoria em destaque na Lei Geral de Proteção de Dados, é um substrato legal que atribui garantias ao titular, na transferência internacional de dados. Essa base legal deve ser específica e em destaque, conferindo-se informações prévias sobre o caráter internacional da operação de dados, distinguindo-se essa de outras finalidades. No caso de um contrato de trabalho, é necessária a inserção de cláusula expressa acerca da possibilidade da transferência internacional dos dados do trabalhador, especificado o propósito da operação. Ainda que no Direito do Trabalho existam desigualdades fáticas que comprometam a liberdade do consentimento, é necessária a informação sobre a possibilidade da operação, a fim de que o trabalhador controle, ainda que potencialmente, o cumprimento da finalidade da coleta, armazenamento e uso dos seus dados pessoais.

O Regulamento Geral sobre Proteção de Dados Europeu 2016/679 (General Data Protection Regulation) é marco normativo essencial ao estudo da proteção de dados, especialmente por ter inspirado fortemente a LGPD brasileira. Sobre a transferência internacional de dados, sua regulação é similar à brasileira e está prevista nos artigos 46 a 51 do Regulamento. Para o Regulamento Europeu, a transferência para um país terceiro ou organismo internacional fora do Espaço Econômico Europeu somente pode ser realizada quando for garantido um nível de proteção adequado pela Comissão Europeia por meio de uma decisão de adequação. Na falta de uma decisão de adequação, será possível realizar a transferência

internacional quando o controlador ou operador oferecer salvaguardas, tais como cláusulas padrão adotadas pela Comissão Europeia, códigos de conduta ou procedimentos de certificação.

No RGPD há também a possibilidade de transferência internacional em hipóteses similares às previstas na LGPD, tais como mediante consentimento prévio, informado e explícito, quando necessário à execução de contrato, por razões de interesse público ou para proteger interesses vitais no titular de dados, entre outras.

Em nível internacional, decisão emblemática sobre a matéria e que fornece orientação para estudar e interpretar o assunto é o chamado caso Schrems II, em que o Tribunal de Justiça da União Europeia entendeu que, em certos aspectos e consideradas determinadas circunstâncias, os Estados Unidos não fornecem nível de proteção adequado aos dados pessoais dos cidadãos europeus. O advogado e ativista Maximilian Schrems apresentou queixa em face do Facebook da Irlanda sob a alegação, em síntese, de que direito e as práticas em vigor nos EUA não asseguravam uma proteção suficiente dos dados pessoais conservados em seu território contra as atividades de vigilância exercidas pelas suas autoridades públicas, em desrespeito a determinadas normas previstas na Carta de Direitos Fundamentais da União Europeia.

Em 16 de julho de 2020, em sede de recurso ao TJUE, o órgão avaliou que, de fato, os EUA não possuem um tratamento de dados essencialmente equivalente, violando o artigo 45 do RGPD, pois não limita o suficiente os poderes das autoridades americanas e porque, após o envio dos dados, cidadãos europeus não possuem formas de garantir seus direitos em solo americano. Além disso, firmou-se o entendimento de que as Standard Contractual Clauses - SCCs não são balizadoras da legalidade ou ilegalidade das transferências, competindo às autoridades verificarem e exigirem condutas e práticas que cumpram com as regras do RGPD e sejam essencialmente equivalentes.

Observa-se que a matéria é complexa, pois analisar o nível de proteção de dados de outro território internacional envolve o estudo profundo sobre as leis daquele país acerca da matéria, suas decisões administrativas e judiciais, e demanda o trabalho árduo da Autoridade de Proteção de Dados para certificar as condições de outro país. Contudo, acredita-se que as salvaguardas protetivas, tais como cláusulas contratuais tipo certificados e códigos de conduta, além da funcionalidade da base legal do consentimento do titular e a participação responsável do controlador e do operador de dados, permitirão compatibilizar, com segurança, o fluxo internacional de dados com o respeito à LGPD e, como consequência, garantir o amplo exercício do controle de tratamento de dados pelo seu titular, nas relações jurídico-laborais internacionais.¹⁵¹

151 Referências: BRANDÃO, Luíza Couto Chaves. Fluxo Transnacional de dados: estruturas políticas e o Direito nas vertentes da governança. Dissertação Mestrado - Curso de Direito, Universidade Federal de Minas Gerais, Belo Horizonte, 2020. Disponível em: <https://repositorio.ufmg.br/bitstream/1843/33716/1/DissertacaoLuizaB.pdf>. Acesso em: 19 out. 2020. BRASIL. Lei 13.709, de 14 de agosto de 2018. Brasília: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19 out. 2021. PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA. Regulamento Geral de Proteção de Dados. REGULAMENTO (UE) 2016/679. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=cele>

TRANSPARÊNCIA (art. 10 § 2º)

ALINE DAL BÓ CORREA¹⁵²

A Lei prevê que o controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse, que só poderá embasar o tratamento de dados pessoais para objetivos específicos e legítimos, considerados a partir de situações concretas.¹⁵³

U

USO COMPARTILHADO DE DADOS (art. 5.º, XVI)

ALINE DAL BÓ CORREA¹⁵⁴

Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados (Art. 5.º, XVI).¹⁵⁵

V

VÍCIO DE CONSENTIMENTO

FERNANDA JULIANE BRUM CORRÊA¹⁵⁶

O consentimento foi definido como a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5.º, XII), e autoriza o tratamento de dados (art. 8º).

A compreensão sobre o vício de consentimento, por sua vez, encontra raízes do Direito Civil, em que a manifestação de vontade é o elemento basilar e orientador do negócio jurídico, diferenciando-o do fato jurídico, por exemplo. No Código Civil, os vícios de consentimento (defeitos) são classificados em erro, dolo, coação, fraude, lesão e estado de perigo e sua presença torna anuláveis os negócios jurídicos que deles decorrem. A LGPD, a seu turno, expressamente veda o tratamento de dados mediante vício de consentimento (art. 8º, §3º).

A manifestação externada que não corresponde à vontade – seja por equívoco na compreensão dos elementos que a compunham, seja por estar o titular compelido como condição ao exercício de algum direito ou ato, seja por patente indução x%3A32016R0679. Acesso em: 20 out. 2021.

152 Graduada na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedalbo04@gmail.com

153 Referências: DONEDA, Danilo (org) *et al.* Como implementar a LGPD por meio da avaliação de impacto sobre privacidade e ética de dados (AIPED). Rio de Janeiro: Forense, 2021.

154 Graduada na UFRGS. Estagiária no TRT da 4ª Região. Bolsista PIBIC pelo CNPq. alinedalbo04@gmail.com

155 Referências: COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados comentada* - 2.ed - São Paulo: Thomson Reuters Brasil, 2019.

156 Analista Judiciário do TRT da 4ª Região. Graduada em Direito pela Universidade Federal de Santa Maria. Especialista em Direito do Trabalho e Processo do Trabalho pela Faculdade Damásio. fernanda.brum@trt4.jus.br

a interpretação errônea – permeia de defeito o “consentimento” e afasta sua possibilidade de uso, nos termos da LGPD.

Nas relações de trabalho subordinado, o desequilíbrio de poder entre os contratantes (empregador e empregado) pode conduzir a presunções de que o titular dos dados não teve legítima escolha, mas foi compelido a consentir como condição, ainda que tácita, de manutenção do vínculo. A presunção de vício de consentimento em situações similares foi, inclusive, prevista no regulamento europeu, conforme considerando 43 da GDPR, relativo ao art. 7º.¹⁵⁷

157 Referências: MIZIARA, Raphael. *Reflexos da LGPD no Direito e no processo do trabalho* (livro eletrônico). Raphael Miziara, André Pessoa, Bianca Mollicone – 1. ed. - São Paulo: Thomson Reuters Brasil, 2020.



LGPD

DOCTRINA E APLICABILIDADE NO ÂMBITO LABORAL

ISBN: 978-65-995463-8-9
(EBOOK)

