

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

9º volume

Direito Digital em Movimento: Dados, Plataformas e Democracia

COORDENAÇÃO
Sérgio Branco
Chiara de Teffé

PUBLICAÇÃO
junho/2025



**DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL**

9º volume

Direito Digital em Movimento: Dados, Plataformas e Democracia

COORDENAÇÃO
Sérgio Branco
Chiara de Teffé

PUBLICAÇÃO
junho/2025



COORDENAÇÃO:

Sérgio Branco e Chiara de Teffé

PROJETO GRÁFICO, CAPA E DIAGRAMAÇÃO:

Leandro Collares e Stephanie Lima

PRODUÇÃO EDITORIAL:

Instituto de Tecnologia
e Sociedade -ITS

REVISÃO:

Chiara de Teffé e Mariana Bertoluci

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Direito digital em movimento [livro eletrônico] :
dados plataformas e democracia / coordenação
Sérgio Branco , Chiara de Teffé. -- 9. ed. --
Rio de Janeiro : ITS - Instituto de Tecnologia
e Sociedade, 2025. -- (Diálogos da pós-graduação
em direito digital)
PDF

Vários autores.
Bibliografia.
ISBN 978-85-5596-011-6

1. Direito digital 2. Plataforma digital
3. Proteção de dados - Leis e legislação
I. Branco, Sérgio. II. Teffé, Chiara de.
III. Série.

25-277726

CDU-34:004

Índices para catálogo sistemático:

1. Direito digital 34:004

Aline Grazielle Benitez - Bibliotecária - CRB-1/3129

COMO CITAR:

BRANCO, Sérgio; TEFFÉ, Chiara Spadaccini de (Coords.). *Direito Digital em Movimento: Dados, Plataformas e Democracia*. 9. v. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2025. 293 p.

INSTITUTO DE TECNOLOGIA E SOCIEDADE:

itsrio.org | [@itsriodejaneiro](https://twitter.com/itsriodejaneiro) | midias@itsrio.org



A obra *Direito Digital em Movimento: Dados, Plataformas e Democracia* está protegida com a seguinte licença:

Creative Commons Atribuição-NãoComercial-Sem Derivações 4.0 Internacional



Você tem o direito de:

Compartilhar — copiar e redistribuir o material em qualquer suporte ou formato.

O licenciante não pode revogar estes direitos desde que você respeite os termos da licença.



De acordo com os seguintes termos:

Atribuição — Você deve dar o crédito apropriado, prover um link para a licença e indicar se mudanças foram feitas. Você deve fazê-lo em qualquer circunstância razoável, mas de nenhuma maneira que sugira que o licenciante apoia você ou o seu uso.



Não Comercial — Você não pode usar o material para fins comerciais.



Sem Derivações — Se você remixar, transformar ou criar a partir do material, você não pode distribuir o material modificado.

Sem restrições adicionais — Você não pode aplicar termos jurídicos ou medidas de caráter tecnológico que restrinjam legalmente outros de fazerem algo que a licença permita.

https://creativecommons.org/licenses/by-nc-nd/4.0/deed.pt_BR



LISTA DE AUTORES

Ana Carolina Gomes Rosa

Carolina Freitas Gomide de Araujo

Daniele Dimas Ramos Garuti

Desirée Marcelle da Cunha

Elmano Rodrigues Pinheiro Filho

Larissa Almeida Del Lhano

Larissa Boullosa Magnavita de Oliveira

Leandro Alcolumbre

Manuela Pereira Gomes

Maria Emilia Loth Machado

Michel Sachs Feuz

Nicole Julie da Silva Rodrigues

Rainier Garacis

Robson Carlos de Souza

Tessália Mariana Fernandes Pirolla

APRESENTAÇÃO

Em um contexto de transformação tecnológica acelerada, que impacta de maneira decisiva as dinâmicas sociais, políticas e econômicas, a obra “Direito Digital em Movimento: Dados, Plataformas e Democracia” emerge como um esforço coletivo de reflexão crítica e interdisciplinar. A partir da interseção entre direito, tecnologia e democracia, esta coletânea oferece ao leitor uma visão abrangente acerca dos desafios que caracterizam a regulação do ambiente digital e a proteção dos direitos fundamentais na sociedade hiperconectada.

Organizado em cinco eixos temáticos, o livro reúne análises aprofundadas sobre os complexos desafios da regulação digital, desenvolvidas por 15 profissionais, estudantes da pós-graduação em Direito Digital do ITS-UERJ, dedicados à compreensão das dinâmicas contemporâneas envolvendo dados, privacidade, democracia e novas tecnologias.

No primeiro eixo, “Desinformação, Democracia e Regulação de Plataformas”, a obra aborda questões sobre os impactos da desinformação para a democracia e analisa perspectivas de regulação das plataformas digitais no Brasil.

O segundo eixo, intitulado “Privacidade, Consentimento e Dados Sensíveis”, explora temas como o uso da geolocalização como prova digital no âmbito trabalhista, limites do consentimento na LGPD, desafios na transferência internacional de dados pessoais e práticas éticas em *Developer Experience*, reforçando a importância da autodeterminação informativa.

“Neurotecnologia e neurodados”, o terceiro eixo, lança um olhar crítico sobre o emergente campo dos neurodireitos, enfatizando a necessidade de proteger dados sensíveis relacionados à atividade cerebral e refletindo sobre os riscos da vigilância neurotecnológica.

O quarto eixo, “Inteligência Artificial, Trabalho e Discriminação”, apresenta reflexões sobre os riscos regulatórios e discriminatórios trazidos pela governança tecnológica nas relações de trabalho, abordando desde o treinamento de inteligência artificial generativa até o uso de algoritmos em processos seletivos, destacando desafios éticos e legais.

Finalmente, no eixo “Reconhecimento Facial, Segurança e Infância”, os autores examinam criticamente a implementação de tecnologias biométricas, especial-

APRESENTAÇÃO

mente o reconhecimento facial em arenas esportivas e escolas públicas brasileiras, além de analisar iniciativas legislativas voltadas à proteção da segurança patrimonial de crianças e adolescentes influenciadores digitais.

“Direito Digital em Movimento: Dados, Plataformas e Democracia” combina rigor acadêmico com reflexões atuais sobre os impactos das novas tecnologias na sociedade contemporânea. Uma obra indispensável para enfrentarmos os desafios jurídicos e éticos impostos pela inovação tecnológica e pela sociedade conectada.

O ITS Rio acredita na importância da difusão e do acesso ao conhecimento. Por essa razão, esta e as demais publicações da pós-graduação encontram-se disponíveis de forma gratuita, aberta e com a licença *Creative Commons Attribution-Non-Commercial-NoDerivatives 4.0 International* (CC BY-NC-ND 4.0).

Para os próximos anos, esperamos ampliar parcerias e desenvolver mais ações destinadas à educação digital que impactem positivamente a sociedade e promovam o acesso à cultura, inovação e informação.

Observamos que o conteúdo aqui exposto não reflete, necessariamente, a opinião institucional do ITS Rio ou de seus membros, representando reflexão acadêmica de responsabilidade exclusiva de seu autor.

Agradecemos a todos que contribuíram e se interessaram por esse projeto.

Convidamos você a conferir as demais [publicações](#) do ITS Rio.

Ficamos à disposição e sempre abertos ao diálogo.

Rio de Janeiro, 24 de maio de 2025.

OS COORDENADORES

OS COORDENADORES

Sérgio Branco

Doutor e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Autor dos livros “Memória e Esquecimento na Internet”, “Direitos Autorais na Internet e o Uso de Obras Alheias”, “O Domínio Público no Direito Autoral Brasileiro – Uma Obra em Domínio Público” e “O que é Creative Commons – Novos Modelos de Direito Autoral em um Mundo Mais Criativo”. Especialista em propriedade intelectual pela Pontifícia Universidade Católica do Rio de Janeiro – PUC-Rio. Pós-graduado em cinema documentário pela FGV. Graduado em Direito pela Universidade do Estado do Rio de Janeiro (UERJ). Advogado. Cofundador e diretor do ITS Rio.

Chiara de Teffé

Doutora e mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Graduada em Direito pela Universidade Federal do Rio de Janeiro (UFRJ). Atualmente, é coordenadora acadêmica da pós-graduação em Direito Digital do Instituto de Tecnologia e Sociedade do Rio (ITS Rio), em parceria com a UERJ, e professora adjunta de Direito Civil e Direito Digital na faculdade de Direito do IBMEC. Pós-graduada em Direito Civil e em Processo Civil (lato sensu), bem como em Ciências Jurídicas Aplicadas à Advocacia Pública (lato sensu), pelo Gran Centro Universitário. Leciona em cursos específicos de pós-graduação e extensão do CEPE-D-UERJ, da PUC-Rio, da EMERJ e do ITS Rio. Membro da Comissão de Proteção de Dados e Privacidade da OAB/RJ (2022/2027). Membro da Comissão de Direito Civil do Conselho Seccional do Rio de Janeiro da OAB (2022/2027). Membro da comissão de direitos autorais, direitos imateriais e entretenimento (2025/2027). Membro do Fórum Permanente de Liberdade de Expressão, Liberdades Fundamentais e Democracia da EMERJ. Membro do Fórum permanente de inovações tecnológicas no Direito da EMERJ. Foi professora substituta de Direito Civil na UFRJ. Associada ao Instituto Brasileiro de Estudos em Responsabilidade Civil (IBERC). Membro Titular do Conselho Municipal de Proteção de Dados Pessoais e Privacidade do Rio de Janeiro. Autora dos livros “Dados pessoais sensíveis: qualificação, tratamento e boas práticas” e “Proteção do direito à imagem na Internet: da identificação do dano à sua compensação”.

SUMÁRIO

EIXO I

DESINFORMAÇÃO, DEMOCRACIA E REGULAÇÃO DE PLATAFORMAS

13

Desinformação e riscos à democracia: A verdadeira informação deve ser isenta de opiniões, juízos de valor e mentiras

ROBSON CARLOS DE SOUZA

42

Regulação das plataformas digitais no Brasil: desinformação, discurso de ódio e as perspectivas de uma atuação estatal

ELMANO RODRIGUES PINHEIRO FILHO

65

Políticos em rede: desafios constitucionais no tratamento de perfis de interesse público nas redes sociais

CAROLINA FREITAS GOMIDE DE ARAUJO

EIXO II

PRIVACIDADE, CONSENTIMENTO E DADOS SENSÍVEIS

82

A geolocalização como meio de prova digital no processo trabalhista: desafios jurídicos e éticos

TESSÁLIA MARIANA FERNANDES PIROLLA

103

Limites do consentimento na LGPD

MICHEL SACHS FEUZ

119

Desafios práticos de adequação frente a nova resolução de transferência internacional de dados pessoais (Resolução CD/ANPD nº19/2024): Análise dos impactos regulatórios e operacionais

RAINIER GARACIS

SUMÁRIO

134

Práticas éticas em *Developer Experience*: indicadores e a autodeterminação Informativa na LGPD

LEANDRO ALCOLUMBRE

EIXO III

NEUROTECNOLOGIA E NEURODADOS

150

Neurodireitos e dados sensíveis: a proteção da mente na era digital

DESIRÉE MARCELLE DA CUNHA

170

Big Brother na Era da Neurotecnologia: Neurodireitos e a Proteção dos Neurodados no Brasil

NICOLE JULIE DA SILVA RODRIGUES

189

Governança na era das novas tecnologias e as relações de trabalho: riscos de discriminação e desafios regulatórios da IA

LARISSA ALMEIDA DEL LHANO

207

IA Generativa e tratamento de dados pessoais: uso do legítimo interesse para o tratamento de imagens para treinamento de IA generativa – o caso Meta

DANIELE DIMAS RAMOS GARUTI

221

Entre o algoritmo e a decisão humana: a abrangência do art. 20 da LGPD na análise de compatibilidade de perfis através do uso de inteligência artificial em processos de recrutamento e seleção

LARISSA BOULLOSA MAGNAVITA DE OLIVEIRA

SUMÁRIO

EIXO IV

RECONHECIMENTO FACIAL, SEGURANÇA E INFÂNCIA

241

Segurança biométrica: a utilização de reconhecimento facial para identificação biométrica dos espectadores em arenas esportivas e o tratamento de dados pessoais sensíveis à luz da Lei Geral de Proteção de Dados

MANUELA PEREIRA GOMES

258

Reconhecimento facial nas escolas públicas brasileiras: sistema de segurança ou risco à privacidade?

ANA CAROLINA GOMES ROSA

273

Segurança patrimonial da criança e adolescente que executam trabalho de teor artístico: análise do projeto de lei nº 3916/2023 e apensos e a observância ao influenciador digital mirim

MARIA EMILIA LOTH MACHADO

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

EIXO I

Desinformação, Democracia e Regulação de Plataformas

AUTORES

Carolina Freitas Gomide de Araujo

Elmano Rodrigues Pinheiro Filho

Robson Carlos de Souza

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

1

Desinformação e riscos à democracia: A verdadeira informação deve ser isenta de opiniões, juízos de valor e mentiras

ROBSON CARLOS DE SOUZA

Sumário: Introdução. 1. Desinformação: conceito, características e histórico. 2. Como a internet e as novas tecnologias podem potencializar a desinformação. 3. Riscos à Democracia e à Liberdade de Expressão e Direito à Informação Verdadeira. Considerações finais. Anexo: Desinformação ao longo dos séculos XX e XXI. Referências.

Introdução

O trabalho busca demonstrar como o crescimento da desinformação que circula pelos meios digitais, em especial no universo das Redes Sociais, tem potencial para desestabilizar sistemas políticos, até mesmo colocando em risco os modelos conhecidos de democracia, ao minar a confiança da população neles e difundir pseudo-soluções para os problemas da sociedade.

Inicia delimitando um conceito e apontando características da desinformação mais apropriadas para o momento atual, seguidos de um levantamento de ocorrências, em especial nos séculos XX e XXI da história da humanidade, em que o seu uso colocou em risco governos, paz social, saúde pública e, até mesmo, a Democracia.

Em seguida, aponta que o advento da Internet, das novas tecnologias e de uma sociedade hiperconectada aumentou consideravelmente as possibilidades de a desinformação reproduzir-se acelerada e descontroladamente em escala global.

Passa, então, a abordar como a proliferação de versões falsas ou falseadas da realidade pode minar a Democracia e a Liberdade de Expressão e a dificuldade do combate à desinformação. Também demonstra que a Liberdade de Expressão não pode justificar a divulgação de mentiras, que turvam a circulação da Informação Verdadeira, um direito fundamental.

Muitas das mensagens que transitam pelas redes sociais travestidas de informação, notícias estão, na verdade, repletas de opiniões e juízos de valor, quando não totalmente deturpadas por mentiras. Por isso, é necessário buscar resposta para a seguinte questão: a liberdade de expressão engloba o direito de difundir falsidades, mentiras ou opiniões como se notícias fossem?

O trabalho visa servir como subsídio para enfrentar o problema, fomentando discussões e medidas que não redundem em retrocessos aos níveis de Liberdade de Expressão já alcançados em nosso país, mas que tenham efeti-

1. Jornalista e Advogado, pós-graduando em Direito Digital pela UERJ em parceria com o Instituto de Tecnologia e Sociedade (ITS Rio) e o Centro de Estudos e Pesquisas no Ensino do Direito (CEPED) e pós-graduando em Direito do Trabalho e Previdenciário pelo Centro de Estudos e Pesquisas no Ensino do Direito (CEPED), da UERJ.

vidade no combate à desinformação. E baseou-se em revisão bibliográfica² de autores e pesquisadores, artigos em revistas e sites jurídicos e educacionais, relatórios de entidades envolvidas com o tema e consulta a dispositivos que tratam dele direta ou indiretamente ou que sirvam ao propósito almejado. E certamente não esgota o assunto, que é extenso, complexo e demanda abordagens que levem em conta contribuições interdisciplinares.

1. Desinformação: conceito, características e histórico

Informação é fator determinante para criação, estabilidade e aprimoramento das relações em sociedade. Quando distorcida, a ponto de descaracterizar-se e tornar-se desinformação, o papel de indutora de progresso daquela transmuda-se no de potencializadora de riscos desta.

Desinformação é o termo mais adequado à situação que temos vivenciado, pois é abrangente (inclui notícias falsas, meias verdades, descontextualização e outras variantes) e *fake news*, termo popularizado e utilizado com mais frequência, é mais restrito às notícias falsas. No entanto, utiliza-se aqui os dois indistintamente.

Os pesquisadores Claire Wardle e Hossein Derakhshan, no Relatório “Desordem Informacional: para um quadro interdisciplinar de investigação e elaboração de políticas públicas”³, do *Council of Europe*, propuseram a adoção de três categorias de desordem informacional: Desinformação (*dis-information*) – informação falsa deliberadamente criada para causar danos individuais ou coletivos, Informação falsa (*mis-information*) – informação falsa criada sem intenção de causar danos e Informação maliciosa (*mal-information*) – informação baseada na realidade, mas usada para causar danos.

Ainda Wardle, no artigo Notícias Falsas. É complicado⁴, detalha sete tipos de Desinformação e Informação falsa (as que mais interessam a este trabalho): Sátira ou Paródia – sem potencial para causar danos, mas com potencial para enganar; Conteúdo enganoso – uso enganoso de informações para enquadrar um problema ou indivíduo; Conteúdo impostor – fontes genuínas são personifi-

2. “A revisão da literatura, revisão do conhecimento ou revisão bibliográfica se constitui no conjunto de informações sobre o estado atual do objeto de pesquisa – o estado do conhecimento, ou estado da arte, utilizando a expressão clássica. Deve incluir, sinteticamente, os principais – ou todos, dependendo da espécie de revisão e dos seus objetivos – trabalhos produzidos sobre o tema e seus resultados.” RODRIGUES, Horácio Wanderlei; GRUBBA, Leilane Serratine. *Pesquisa Jurídica Aplicada*. p. 177. Florianópolis, Habitus Editora, 2023. *E.book*.

3. WARDLE, Claire; DERAKHSHAN, Hossein. Relatório *Desordem Informacional: para um quadro interdisciplinar de investigação e elaboração de políticas públicas*. p.28. São Paulo, 2023 Disponível em: <https://edoc.coe.int/en/media/11609-desordem-informacional-para-um-quadro-interdisciplinar-de-investigacao-e-elaboracao-de-politicas-publicas.html#>. Acesso em: 22 dez. 2024.

4. WARDLE, Claire. *Notícias Falsas. É complicado*. First Draft. 2017. Disponível em: <https://firstdraftnews.org/articles/noticias-falsas-es-complicado/>. Acesso em: 17 dez. 2024.

cadadas; Conteúdo fabricado – novo conteúdo 100% falso, projetado para enganar e prejudicar; Conexão falsa – títulos, imagens ou legendas não suportam o conteúdo; Contexto falso – conteúdo genuíno compartilhado em contextos falsos, e Conteúdo manipulado – informações ou imagens genuínas manipuladas para enganar.

Interessante observar a relação entre esses tipos de conteúdo e oito possíveis motivações na criação de *fake news*, conforme o artigo da pesquisadora.

FIRST DRAFT	CONTEÚDO						
MOTIVAÇÃO	Sátira/ Paródia	Enganoso	Impostor	Fabricado	Conexão falsa	Contexto falso	Manipulado
Jornalismo Ruim		✓			✓	✓	
Paródia	✓		✓	✓			
Provocação			✓	✓			✓
Paixão						✓	
Partidarismo		✓				✓	
Lucro			✓	✓	✓		
Política/Poder		✓		✓		✓	✓
Propaganda		✓	✓	✓		✓	✓

5

Rais aponta que há um consenso de que desinformação é informação amplamente disseminada e fraudulenta que “pode ter, ou não, o intuito de causar premeditado prejuízo ou danos resultantes de sua inveracidade”⁶.

Binenbojm considera que *fake news* são externalidades negativas que refletem numa falha do mercado digital de livre difusão de informações, ideias e opiniões, gerando lucros abusivos para grupos e um custo externo à Liberdade de Expressão na forma de prejuízos econômicos, políticos e sociais à comunidade. Para ele, não é possível enfrentar o problema sem regular o mercado⁷.

5. Adaptação do autor de quadro divulgado no site da **First Draft**. Disponível em: <https://firstdraftnews.org/articles/noticias-falsas-es-complicado/>. Acesso em: 17 dez. 2024.

6. RAIS, Diogo. *Fake News: a conexão entre a desinformação e o direito/* (Portuguese Edition). p. 368. São Paulo, Thomson Reuters Brasil, 2020. *E-book*.

7. BINENBOJM, Gustavo. *Fake news como externalidades negativas*. JOTA. Disponível em: <https://www.jota.info/opiniao-e-analise/columnas/publicistas/fake-news-como-externalidades-negativas>. Acesso em: 20 dez. 2024.

Helena Martins, do Interviços – Coletivo Brasil de Comunicação Social, valendo-se de levantamento do Índice Global de Desinformação (GDI, na sigla em inglês), é categórica em afirmar que a desinformação é lucrativa para o modelo de negócios das plataformas digitais, gerando por publicidade programática (*softwares* para comprar e vender espaço publicitário na *web*) de 20 mil sites “desinformadores” US\$ 235 milhões por ano^{8 9}.

A desinformação gera, no mínimo, três problemas: (i) a bolha fechada em si, impermeável à realidade; (ii) a deliberação quanto à sua ocorrência, quando acontece, é tardia, ignorada e sucateada pelo grupo, por conta de novas postagens desinformativas, e (iii) os destinatários (vítimas) das mensagens são capturados por elas ou, se representam um obstáculo ao fluxo, não conseguem “reverter o caminho já percorrido pelo conteúdo”¹⁰.

Farah salienta que a Internet propicia destaque da desinformação e lista como instrumentais, técnicas e efeitos as bolhas, as câmaras de eco, os robôs, os algoritmos, a mineração de dados, o impulsionamento, a perfilização, os disparos em massa, a criptografia e o *microtargeting*. Esses fatores “entregam maior velocidade, alcance e profundidade ao conteúdo desinformativo”, além da instrumentalização por “gatilhos emocionais e vieses”, que geram monetização¹¹.

Na avaliação de Bachur, um “efeito paradoxal” compõe a sociabilidade criada pelas novas tecnologias: embora sozinhos, dentro das bolhas digitais, estamos também mais vulneráveis aos efeitos de massa, que suspendem a racionalidade individual por força de um contágio emocional, independentemente de uma multidão concreta¹². Nas bolhas do mundo digital com uma determinada orientação política, a contaminação dos usuários das Redes Sociais decorre de uma intensa emoção que circula com a desinformação, desativando o processamento cognitivo do conteúdo semântico das mensagens, que passam a ser validadas em bases emocionais. “O que circula nas Redes Sociais é emoção, e não informação”¹³.

8. MARTINS, Helena. Muito além das fake news: o problema da desinformação em meio à crise social. In: *Desinformação: crise política e saídas democráticas para as fake news*. Helena Martins (Org.). Prefácio de Sérgio Amadeu da Silveira. São Paulo, Veneta, 2020. 108 p. E-book.

9. Global Disinformation Index Staff. *The quarter billion dollar question: How is Disinformation Gaming Ad Tech?* GDI, 2019. p.4. Disponível em: https://disinformationindex.org/wp-content/uploads/2019/09/GDI_Ad-tech_Report_Screen_AW16.pdf. Acesso em: 20 fev. 2020.

10. FARAH, André. *Desinformação Online, Liberdade de Expressão e Democracia* (Portuguese Edition). p. 136-137. Rio de Janeiro, Editora Lumen Juris, 2024. E-book.

11. *Ibidem*. p. 340.

12. BACHUR, João Paulo. Desinformação Política, Mídias Digitais e Democracia: Como e por que as fake news funcionam. *Revista Direito Público*. p. 453. Brasília. Vol. 18. p. 436-469. 2021. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5939>. Acesso em: 15 dez. 2024.

13. *Ibidem*. p.457.

Citando artigo¹⁴ de Hunt Allcott e Matthew Gentzkow sobre a eleição presidencial dos EUA em 2016, Rais expõe que: (i) *fake news* são mais fáceis de criar do que notícias verdadeiras, (ii) a verificação de sua autenticidade não é simples, (iii) há a preferência de visões polarizadas sobre vários assuntos, (iv) muitas decisões que tomamos descartam a racionalidade e se baseiam no conhecimento coletivo, (v) além de buscarmos alinhamento com nossos pensamentos¹⁵.

A desinformação foi extensa e extremamente utilizada no período da pandemia de Covid-19, de 2020 a 2021, a ponto de a Organização Mundial da Saúde (OMS) tê-la declarado uma infodemia, termo primeiramente utilizado pelo jornalista David Rothkopf em artigo publicado no jornal *Washington Post* em 11 de maio de 2003 sobre a rápida disseminação de informações, precisas e imprecisas, durante um surto de Síndrome Respiratória Aguda Grave (SARS, na sigla em inglês)¹⁶.

Atualmente é preocupante a transição de influenciadores de saúde para outras áreas da ciência, como o negacionismo climático. Estudo da ONG americana *Institute for Strategic Dialogue* indica que eles exploram narrativas que misturam espiritualidade e teorias conspiratórias, a “conspiritualidade”, promovendo, por exemplo, ideias de que mudanças climáticas derivam de forças ocultas ou de “geoengenharia”¹⁷, o que desvia o foco das evidências científicas¹⁸.

Outra preocupação que se tem acentuado é com relação à utilização de recursos de Inteligência Artificial generativa para criação e difusão de conteúdo desinformativo. Com o avanço dessa tecnologia, pode-se produzir desinformação de forma “extremamente sofisticada e praticamente imperceptível em vídeos, áudios e até mesmo nas alterações de voz”, segundo o pesquisador e professor Juliano Maranhão, do Centro de Inteligência Artificial e da Faculdade de Direito, ambos da Universidade do Estado de São Paulo (USP)¹⁹.

14. ALLCOTT, Hunt; GENTZKOW, Matthew. Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives*. Vol. 31. p. 211-236. Disponível em: <https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.31.2.211>. Acesso em: 18 dez. 2024.

15. RAIS, *Op. cit.* p. 205.

16. ROTHKOPF, David. J. *When the Buzz Bits Back*. Washington Post. Washington. May 11, 2003. Outlook (Comentary). B4-B5. Disponível em: https://www.researchgate.net/profile/Zhiwen-Hu-4/publication/339926961_The_earliest_usage_track-down_of_infodemic/links/5e6c6b6fa6fdccf994c66c4c/The-earliest-usage-track-down-of-infodemic.pdf. Acesso em: 09 abr. 2025.

17. Manipulação intencional do clima terrestre para reduzir o aquecimento global. Geoengenharia. Disponível em: <https://pt.wikipedia.org/wiki/Geoengenharia>. Acesso em: 12 abr. 2025.

18. Redação MediaTalks. *Cinco anos de ‘infodemia’: como a desinformação sobre vacinas continua a afetar a saúde pública*. MediaTalks By J&Cia. 11 mar. 2025. Disponível em: <https://mediatalks.uol.com.br/2025/03/11/covid-cinco-anos-e-infodemia-o-legado-da-desinformacao-online/>. Acesso em: 09 abr. 2025.

19. PACHECO, Denis. *Inteligências artificiais entram em campo contra e a favor da desinformação*. Jornal da USP. 17 nov. 2023. Disponível em: <https://jornal.usp.br/atualidades/inteligencias-artificiais-entram-em-campo-contra-e-a-favor-da-desinformacao/>. Acesso em: 09 abr. 2025.

Para Fabio Cozman, professor da Escola Politécnica da USP e diretor do Centro de Inteligência Artificial USP/IBM/Fapesp, conhecido como C4AI, a tendência de se substituir o Google por plataformas de IA generativa como fonte de informação e essas plataformas passarem a produzir fatos e argumentos falsos é preocupante. Na sua avaliação, a sociedade precisa se preparar “para entender e ter as ferramentas necessárias, dentro do possível, para analisar o que está recebendo”²⁰.

Em vários momentos da história, mentiras ameaçaram ou eliminaram a paz social, mas em alguns os efeitos da desinformação foram mais críticos, levando à derrubada de governos, ao aumento de tensões entre países, ao início de conflitos armados, a genocídios, entre outros acontecimentos. Merecem destaque: Genocídio do povo armênio (1915–1923), Terceiro Reich (1933–1945), Crise dos Mísseis (1962), Guerra do Vietnã (1964), Genocídio dos tutsis (1994), Invasão do Iraque (2003), Genocídio dos rohingyas (2017), Pandemia de Covid-19 (2022–2022). Ao final deste trabalho, em Anexo, está disponível um quadro mais completo sobre o assunto²¹.

2. Como a internet e as novas tecnologias podem potencializar a desinformação

Com o incremento do uso de Redes Sociais e aplicativos de mensageria, a velocidade de transmissão das (des)informações aumentou exponencialmente. Há alguns anos, o Brasil figura nos primeiros lugares das listas dos países que mais utilizam a Internet e suas ferramentas. Por exemplo, era o 3º no uso de Redes Sociais, segundo o estudo Tendências Digitais 2023²², da ComScore Brasil, e o 2º mercado do WhatsApp (197 milhões de usuários), conforme dados da proprietária do aplicativo, Meta Platforms, divulgados no WhatsApp Business Summit Brasil 2023²³.

Essa conjuntura, aliada ao fato de que as instituições têm enfrentado crescente perda de credibilidade, cria um ambiente ideal para surgimento

20. *Ibidem*.

21. Elaborado com utilização dos Chat GPT Português e Gemini e consulta ao *A short guide to the history of 'fake news' and disinformation*. O foco da seleção foram as situações que colocaram em risco governos, saúde pública ou levaram ao início de guerras. Salienta-se que muitas das ocorrências se deram em período em que a Internet e as Redes Sociais não existiam ou ainda não tinham o destaque e a penetração de hoje e se valeram dos meios tradicionais de divulgação de notícias e não notícias. POSETTI, Julie; MATTHEWS, Alice. *A short guide to the history of 'fake news' and disinformation*. International Center for Journalists. 2018. Disponível em: https://www.icfj.org/sites/default/files/2018-07/A%20Short%20Guide%20to%20History%20of%20Fake%20News%20and%20Disinformation_ICFJ%20Final.pdf. Acesso em: 16 dez. 2024.

22. COMSCORE. *Tendências Digitais 2023*, ComScore Brasil. Jan. 2023. Brasil. Disponível em: <https://www.comscore.com/por/Insights/Apresentacoes-e-documentos/2023/Tendencias-Digitais-2023>. Acesso em: 27 dez. 2024.

23. VIEIRA, Marcelo Gimenes. *Brasil é prioridade da Meta para ampliar uso comercial do WhatsApp no mundo*. itforum. 23 ago. 2023. Disponível em: <https://itforum.com.br/noticias/brasil-meta-whatsapp-uso-comercial/>. Acesso em: 06 dez. 2024.

e circulação de desinformação, gerando, inclusive, um círculo vicioso de retroalimentação.

Um fator que potencializa o crescimento da desinformação é o alto consumo de notícias no Brasil por meio das Redes Sociais e dos aplicativos de mensagens. Dados de 2023, da *Reuters* e Universidade de Oxford, apontam que 51% da população brasileira se informava por meio de Redes Sociais²⁴. Apesar de uma tendência de queda desde 2016, quando atingiu um pico pouco acima de 70%, o contingente da população que se informa por Redes Sociais ainda é bastante alto.

Contrariando um senso comum presente entre muitos pesquisadores do tema, a pesquisa *The spread of true and false news online*, de Soroush Vosoughi, Deb Roy e Sinan Aral, pelo Instituto de Tecnologia de Massachusetts (MIT), publicada na revista *Science* em março de 2018, demonstra que a utilização de *bots* acelera a propagação de notícias verdadeiras e falsas em intensidade aproximadamente igual, mas as notícias falsas “se espalham mais longe, mais rápido, mais profundamente e mais amplamente por humanos e não por robôs”²⁵.

Na corrente difusora das *fake news*, o papel das pessoas que, de boa-fé, acreditam nas postagens que recebem e as consideram verdadeiras notícias é muito importante para a concretização da engrenagem da desinformação. Portanto, “boa parte de toda essa produção se escoia com o apoio das próprias vítimas”²⁶.

Citando o pesquisador e professor de jornalismo Alfred Hermida, Fernanda Bruno e Tatiana Roque salientam que a capacidade de persuasão das emoções fortes, como o asco, o medo e a raiva, é grande, o que confirma que o “engajamento no repasse da mensagem pode estar menos vinculado à veracidade de seu conteúdo do que à sua pertinência a um conjunto de convicções coletivas”²⁷.

A preocupação com a evidência da desinformação em nossa sociedade é geral e o Judiciário há tempos tem se debruçado sobre o tema. Destaca-se,

24. NEWMAN, Nic; FLETCHER, Richard; ROBERTSON, Craig T.; ARGUEDA, Amy Ross; NIELSEN, Rasmus Kleis. *Digital News Report 2024*. Reuters Institute. Reuters Institute for the Study of Journalism. Disponível em: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2024-06/RISJ_DNR_2024_Digital_v10%20lr.pdf. Acesso em: 17 dez. 2024.

25. “Although the inclusion of bots, [...] accelerated the spread of both true and false news, it affected their spread roughly equally. This suggests that false news spreads farther, faster, deeper, and more broadly than the truth because humans, not robots, are more likely to spread it.” Embora a inclusão de bots tenha acelerado a propagação de notícias verdadeiras e falsas, ela afetou sua propagação de forma aproximadamente igual. Isso sugere que as notícias falsas se espalham mais longe, mais rápido, mais profundamente e mais amplamente do que a verdade porque os humanos, não os robôs, são mais propensos a espalhar notícias falsas. (tradução nossa). VOSOUGH, Soroush; ROY, Deb; ARAL, Sinan. *The spread of true and false news online*. Science. 9 mar. 2018. Disponível em: <https://www.science.org/doi/10.1126/science.aap9559>. Acesso em: 17 dez. 2024.

26. RAIS, Op. cit.

27. BRUNO, Fernanda; ROQUE, Tatiana. A ponta de um iceberg de desconfiança. In: *Pós-Verdade e fake news. Reflexões sobre a guerra de narrativas*. Cobogó Editora. Org Mariana Barbosa. 2019. Rio de Janeiro. E-book.

a seguir, trechos de alguns julgados do Supremo Tribunal Federal (STF) e do Tribunal Superior Eleitoral (TSE) em que essa preocupação fica patente²⁸:

(i) AIJE 0601771-28.2018.6.00.0000-BRASÍLIA-DF/ACÓRDÃO/VOTO DO RELATOR MINISTRO LUIS FELIPE SALOMÃO (TSE)²⁹.

[...]

O conjunto probatório das AIJEs 0601968-80 e 0601771-28 não deixa margem para dúvidas de que a campanha dos vencedores das eleições presidenciais de 2018 assumiu caráter preponderante nos meios digitais, mediante utilização indevida, dentre outros, do aplicativo de mensagens *WhatsApp* para promover disparos em massa em benefício de suas candidaturas, valendo-se de estrutura organizada e capilarizada composta por apoiadores e pessoas próximas ao primeiro representado.

[...]

Como consectário lógico, penso não haver margem para dúvida de que constitui ato abusivo, a atrair em tese as sanções eleitorais cabíveis, a promoção de disparos em massa em aplicativos de mensagens instantâneas, fazendo chegar ao eleitorado informações inverídicas e enviesadas a respeito de adversários políticos e em contexto no qual determinado candidato sobrevenha como beneficiário dessa prática.

[...]

5.5. Em resumo, diante de temática tão relevante e inédita, penso que o caso convida a Corte a fixar a tese jurídica no sentido de que a exacerbação do uso de aplicativos de mensagens instantâneas para realizar disparos em massa, promovendo desinformação, diretamente por candidato ou em seu benefício e em prejuízo de adversários políticos, pode configurar abuso do poder econômico e uso indevido dos meios de comunicação social, nos termos do art. 22 da LC 64/90, a depender da gravidade da conduta, que será examinada em cada caso concreto.

Como se pretende demonstrar a seguir, a gravidade deve ser aferida com base nos seguintes parâmetros que entendo preponderantes: (a) teor das mensagens e, nesse contexto, se continham propaganda negativa ou informações efetivamente inverídicas; (b) de que forma o conteúdo repercutiu perante o eleitorado; (c) alcance do ilícito em termos de mensagens veiculadas; (d) grau de partici-

28. Outros julgados sobre os mesmos temas podem ser pesquisados nos sites das duas Cortes: No TST, AgR-REspEI 060016608 e ED-Rec-Rp 060125906; no STF, ARE 1483399 AgR, ARE 660861 RG e ARE 1448234 AgR.

29. BRASIL. Tribunal Superior Eleitoral. Acórdão AIJE 0601771-28.2018.6.00.0000. Relator Ministro Luis Felipe Salomão. Sessão de 28/10/2021. Brasília, TSE, 2021. p. 6, 102, 106. Disponível em: <https://jurisprudencia.tse.jus.br/#/jurisprudencia/pesquisa?expressaoLivre=0601771-28.2018.6.00.0000&tipoDecisao=Ac%25C3%25B3rd%25C3%25A3o%252CResolu%25C3%25A7%25C3%25A3o%252CDecis%25C3%25A3o%2520sem%2520resolu%25C3%25A7%25C3%25A3o¶ms=s>. Acesso em: 10 abr. 2025.

pação dos candidatos nos fatos; (e) se a campanha foi financiada por empresas com essa finalidade.
[...]

(ii) ADPF 572-DF/ACÓRDÃO/VOTO DO RELATOR MINISTRO EDSON FACHIN (STF)³⁰.

[...]

Esse julgado evidencia que este Supremo Tribunal Federal reconhece que liberdade de expressão compreende o direito de informar, de buscar a informação, de opinar, de criticar.

Os limites à liberdade de expressão estão em constante conformação e, penso, demandarão ainda reflexão do Poder Legislativo e do Poder Judiciário e, especialmente, dessa Corte, no tocante ao que se denomina atualmente de “fake news”. Como observou o Justice Kennedy, no caso *Packingham v. North Carolina*, as mídias sociais são as “novas praças públicas”.

Nesse contexto de confusão informacional em que a manifestação se automatiza, não há mais propriamente sujeitos de direito, mas algoritmos ecoando inadvertidamente uma informação sem respaldo na lógica do hipertexto:

[...]

(iii) ADI 7261-DF/ACÓRDÃO/VOTO DO RELATOR MINISTRO EDSON FACHIN³¹ (STF).

[...]

Em suma, a normalidade das eleições está em questão quando a liberdade se converte em ausência de liberdade, porquanto desconectada da realidade, da verdade e dos fatos. Esse exercício abusivo coloca em risco a própria sociedade livre e o Estado de Direito democrático.

Não há Estado de Direito nem sociedade livre numa democracia representativa que não preserve, mesmo com remédios amargos e limítrofes, a própria normalidade das eleições.

A liberdade de expressão não pode ser a expressão do fim da liberdade. Não se trata de proteger interesses de um estado, organização ou indivíduos, e sim de resguardar o pacto fundante da sociedade brasileira: a democracia por meio de eleições livres,

30. BRASIL. Supremo Tribunal Federal. Acórdão ADPF 572. Relator Ministro Edson Fachin. Sessão de 18/06/2020. Brasília, STF, 2020. p. 16. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=755791517>. Acesso em: 10 abr. 2025.

31. BRASIL. Supremo Tribunal Federal. Acórdão ADI 7.261. Relator Ministro Edson Fachin. Sessão de 19/12/2023. Brasília, STF, 2023. p. 6. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=774895965>. Acesso em: 10 abr. 2025.

verdadeiramente livres. Não se trata de juízo de conveniência em critérios morais ou políticos, e sim do dever de agir para obstar a aniquilação existencial da verdade e dos fatos, sob pena da democracia e da verdade decaírem “em poeira de informação levada pelo vento digital” (Ob. cit., p. 107)³².
[...]

3. Riscos à Democracia e à Liberdade de Expressão e Direito à Informação Verdadeira

Os ambientes virtuais são um convite para que grupos mal-intencionados busquem desestabilizar as instituições. Um fator que auxilia nessa ação é a rapidez de propagação das desinformações: se espalham 70% mais rápido do que notícias verdadeiras, segundo o estudo de Vosoughi, Roy e Aral anteriormente citado³³.

Nesse sentido, podemos lembrar do ataque às sedes dos Poderes da República em 8 de janeiro de 2023, que certamente mirava um golpe de Estado e foi articulado por meio da divulgação de mensagens com o codinome “Festa da Selma”, cuja motivação foi uma *fake news* sobre fraude nas urnas que teria ocorrido na eleição presidencial de 2022³⁴.

O Direito, nesse cenário, é um dos meios propícios para contribuir com a restauração da estabilidade, assegurando equilíbrio entre liberdades individuais e bem-estar da sociedade, mas existem algumas dificuldades para o enfrentamento do problema da desinformação. Dentre elas, destacam-se: os limites tênues entre as medidas de proteção da sociedade e a manutenção da Liberdade de Expressão e as complexidades técnicas de se determinar a autoria das desinformações.

No entanto, esses percalços não impedem o exercício do Direito, a partir da legislação existente, mesmo considerando-se que a falta de um regramento específico sobre desinformação é um complicador.

Na falta de norma própria, alguns dispositivos, a depender do caso concreto e da área em que a desinformação ocorre, servem como um primeiro enfrentamento ao problema. Entre eles, merecem menção aqueles relacionados à Justiça Eleitoral, onde o combate à desinformação tem-se mostrado mais

32. Citação do Ministro ao livro *Infocracia: digitalização e a crise da democracia*, de Byung-Chul Han.

33. VOSOUGHI, *Op.cit.*

34. FONSECA, Bruno; SCOFIELD, Laura. *Bolsonaristas usam código “Festa da Selma” para coordenar invasão em Brasília*. Pública. 2023. Disponível em: <https://apublica.org/sentinela/2023/01/bolsonaristas-usam-codigo-festa-da-selma-para-coordenar-invasao-em-brasilia/>. Acesso em: 17 dez. 2024.

efetivo. São exemplos os artigos 323 e 326-A do Código Eleitoral³⁵ e os artigos 2º, § 1º e 3º da Resolução 23.714/2022³⁶, do Tribunal Superior Eleitoral (TSE). Outro dispositivo está presente no Marco Civil da Internet: o art. 19³⁷, cuja constitucionalidade ainda está pendente de decisão do Supremo Tribunal Federal (STF) e que tem sido alvo de muitas polêmicas.

Considerando-se que ocorrem eleições no Brasil de dois em dois anos (alternadamente entre municipais e gerais) e que as convicções políticas, muitas delas embasadas em desinformação, vão se formando paulatinamente, mesmo antes das campanhas dos pleitos eleitorais, por que não tornar permanentes as incidências dos dispositivos contra a desinformação da legislação eleitoral? Perde-se um tempo precioso para rechaçar a desinformação, o que contribui para a dificuldade posterior de alterar a percepção da realidade pelos eleitores.

O peso conferido à Liberdade de Expressão na Constituição da República Federativa do Brasil tem relevância e não poderia ser diferente, face à neces-

35. **Art. 323.** Divulgar, na propaganda eleitoral ou durante período de campanha eleitoral, fatos que sabe inverídicos em relação a partidos ou a candidatos e capazes de exercer influência perante o eleitorado: Pena – detenção de dois meses a um ano, ou pagamento de 120 a 150 dias-multa. § 1º Nas mesmas penas incorre quem produz, oferece ou vende vídeo com conteúdo inverídico acerca de partidos ou candidatos. § 2º Aumenta-se a pena de 1/3 (um terço) até metade se o crime: I – é cometido por meio da imprensa, rádio ou televisão, ou por meio da internet ou de rede social, ou é transmitido em tempo real; II – envolve menosprezo ou discriminação à condição de mulher ou à sua cor, raça ou etnia. **Art. 326-A.** Dar causa à instauração de investigação policial, de processo judicial, de investigação administrativa, de inquérito civil ou ação de improbidade administrativa, atribuindo a alguém a prática de crime ou ato infracional de que o sabe inocente, com finalidade eleitoral: Pena – reclusão, de 2 (dois) a 8 (oito) anos, e multa. § 1º A pena é aumentada de sexta parte, se o agente se serve do anonimato ou de nome suposto. § 2º A pena é diminuída de metade, se a imputação é de prática de contravenção. § 3º Incorrerá nas mesmas penas deste artigo quem, comprovadamente ciente da inocência do denunciado e com finalidade eleitoral, divulga ou propala, por qualquer meio ou forma, o ato ou fato que lhe foi falsamente atribuído. BRASIL. Tribunal Superior Eleitoral. *Código Eleitoral. Lei nº 4.737, de 15 de julho de 1965*. Brasília: TSE, 1965. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l4737compilado.htm. Consulta em: 21 dez. 2024.

36. **Art. 2º** É vedada, nos termos do Código Eleitoral, a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos. § 1º Verificada a hipótese prevista no caput, o Tribunal Superior Eleitoral, em decisão fundamentada, determinará às plataformas a imediata remoção da URL, URI ou URN, sob pena de multa de R\$ 100.000,00 (cem mil reais) a R\$ 150.000,00 (cem e cinquenta mil reais) por hora de descumprimento, a contar do término da segunda hora após o recebimento da notificação. **Art. 3º** A Presidência do Tribunal Superior Eleitoral poderá determinar a extensão de decisão colegiada proferida pelo Plenário do Tribunal sobre desinformação, para outras situações com idênticos conteúdos, sob pena de aplicação da multa prevista no art. 2º, inclusive nos casos de sucessivas replicações pelo provedor de conteúdo ou de aplicações. BRASIL. Tribunal Superior Eleitoral. *Resolução nº 23.714, de 20 de outubro de 2022. Dispõe sobre o combate à desinformação nas eleições*. Brasília: TSE, 2022. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-714-de-20-de-outubro-de-2022>. Acesso em: 21 dez. 2024..

37. **Art. 19.** Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. § 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material. § 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal. § 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais. § 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação. BRASIL. *Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Dispõe sobre os direitos e deveres dos usuários da internet, e sobre os provedores de aplicação, de conexão e de infraestrutura*. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 17 dez. 2024.

sidade de se proteger o cidadão de uma atuação exorbitante do Estado, mas consignado no próprio artigo 5º, inciso IV³⁸, que confere liberdade de pensamento, está o limitador: a proibição do anonimato. E uma característica central de considerável quantidade de desinformação é justamente o anonimato do seu criador. A dificuldade aqui é chegar à verdadeira identidade dele.

Nesses casos, o anonimato não guarda nenhum aspecto positivo: não é artifício para a busca da privacidade nem para a proteção à retaliação do Estado ou à livre expressão do pensamento. Em outra direção, os criadores e divulgadores de desinformação abusam do direito à Liberdade de Expressão, manipulando a opinião pública e impedindo o acesso à Informação Verdadeira.

Destaque-se que a utilização de *bots* (robôs) como artifício para a criação de contas automatizadas, anônimas, é frequente pelos disseminadores de desinformação. Essas contas conseguem driblar os algoritmos que padronizam grupos de usuários e, com isso, ganham visibilidade e adesão de perfis humanos, gerando viralização das notícias fraudadas. Mas pergunta-se: robôs têm direito à Liberdade de Expressão?

A Liberdade de Expressão reflete-se igualmente no Direito à Informação Verdadeira, sem a qual subtraem-se à sociedade as condições de estabelecer um debate público de qualidade na busca de uma “convicção informada”³⁹. Grandinetti destaca dois pontos importantes que distinguem a expressão da informação: nesta devem estar presentes incondicionalmente a veracidade e a imparcialidade. “E é, justamente, em razão dessa distinção fundamental que se deve pensar em um direito de informação que seja distinto em sua natureza da liberdade de expressão”⁴⁰.

Conforme destaca Goltzman⁴¹, citando obra de O’Rourke, essa distinção foi percebida até mesmo por um dos expoentes do pensamento liberal, John Stuart Mill.

[...] o reino da verdade, no entanto, é muito diferente da opinião, e distorcer ou ocultar factos ou mentir não é algo que Mill tolera. Ele considera os interesses da verdade e justiça necessários para

38. **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: (...) IV – é livre a manifestação do pensamento, sendo vedado o anonimato; (...) BRASIL. *Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 13 dez. 2024.

39. RAIS, *Op. cit.*

40. CARVALHO, Luis Gustavo Grandinetti Castanho de. *Direito de Informação e Liberdade de Expressão*. Rio de Janeiro: Renovar, 1999. p. 24.

41. MAIA GOLTZMAN, Elder. *Liberdade de Expressão e Desinformação em Contextos Eleitorais*. Belo Horizonte, Fórum, 2022. E-book.

o bem-estar geral da discussão, enquanto a fraude, traição e força são contrárias ao interesse geral⁴² (tradução nossa).

No entanto, ele considera inadequada a censura legal à mentira, pois representa um cunho paternalista do Estado, que deve capacitar o sujeito para que ele possa ter ferramentas necessárias para raciocinar e escapar, por si, dessa armadilha⁴³.

Para alguns autores, como os professores Robert Post (*Yale Law School*) e Cass Sunstein (Universidade de Harvard) a Liberdade de Expressão deve ser abordada com uma certa instrumentalidade, visando proteger o sistema democrático. Para o primeiro, por exemplo,

Quando um discurso que não está presente no discurso público transmite informações ou conhecimento valioso para a formação da opinião pública, sua comunicação pode se enquadrar no escopo da Primeira Emenda. Mas as formas de proteção constitucional estendidas em tais circunstâncias têm um caráter muito particular: protegem o direito das pessoas de receber informações, não o direito autônomo dos oradores de transmitir essas informações. Assim, permitem a discriminação de conteúdo, a censura estatal com base na verdade ou falsidade e a compulsão de expressão para garantir que a comunicação não seja enganosa⁴⁴. (tradução nossa)

E para o segundo,

Um sistema de livre mercado de expressão frequentemente falha nos aspectos relevantes; reformas regulatórias poderiam melhorar as coisas. Não afirmo que os direitos de expressão devam ser livremente sujeitos à determinação política, como o são as questões atuais de segurança e saúde ocupacional, por exemplo. Insisto, no entanto, que, em algumas circunstâncias, políticas que parecem envolver a regulamentação governamental da expressão podem,

42. “[...] the realm of fact, however, is quite different from that of opinion, and to distort or withhold facts or to lie is not something which Mill condones. He regards the interests of truth and justice as necessary to the overall well-being of discussion, while fraud, treachery and force are ‘contrary to the general interest to permit’. The one exception which Mill allows to his argument is where the circumstances in which an opinion is expressed are such as to constitute an instigation to a mischievous act.” O’ROURKE, K. C. *John Stuart Mill and Freedom of Expressions – The genesis of a theory*. Taylor & Francis e-Library, 2003. p. 124. Disponível em: <https://epdf.pub/john-stuart-mill-and-freedom-of-expression-the-genesis-of-a-theory-routledge-stu.html>. Acesso em: 13 dez. 2024.

43. MAIA GOLTZMAN, *Op. cit.*, p.40.

44. “Speech outside public discourse may also on occasion be invested with First Amendment value. Where speech which is not otherwise in public discourse conveys information or knowledge that is valuable for the formation of public opinion, its communication may come within the scope of the First Amendment. But the forms of constitutional protection extended in such circumstances have a very particular character: they protect the right of persons to receive information, not the autonomous right of speakers to convey that information. They thus allow content discrimination, state censorship on the basis of truth or falsity, and the compulsion of expression in order to ensure that communication is not misleading.” POST, Robert. Participatory Democracy and Free Speech *In: Virginia Law Review*, Volume.97, May 2011, Number 3, p. 486. Disponível em: <https://virginialawreview.org/wp-content/uploads/2020/12/477.pdf>. Acesso em 10 abr. 2025.

na verdade, promover a profundidade e a diversidade que são essenciais para um sistema de liberdade de expressão e não devem ser tratados como restrições⁴⁵. (tradução nossa)

A desinformação viola o livre mercado de ideias e a busca pela verdade. Isso caracteriza uma afronta ao fundamento da Liberdade de Expressão, o que gera uma desconformidade entre o fenômeno (desinformação) e esse fundamento⁴⁶.

Segundo o LupaMundi – Mapa das Legislações sobre Desinformação, apenas 35 países têm leis específicas sobre o tema. Assim como o Brasil, 114 países tratam do assunto por meio de outras leis mais genéricas. E 38 não dispõem de qualquer tipo de regulamentação⁴⁷.

O problema do vácuo legislativo no Brasil sobre criação e compartilhamento de desinformação persiste, apesar da urgência de um regramento específico para enfrentar essa realidade. O Projeto de Lei 2.630/2020 (PL das *Fake News*)⁴⁸, um dos mais abrangentes e com significativas similaridades à Lei de Serviços Digitais (*Digital Services Act*–DSA, na sigla em inglês), conjunto de regras da União Europeia, recebeu no Senado diversas modificações ao texto original apresentado pelo senador Alessandro Vieira (Cidadania-SE) em 13 de maio de 2020, mas foi aprovado com rapidez em 30 de junho do mesmo ano e encaminhado à Câmara dos Deputados. Nesta, porém, o projeto se arrasta, mesmo tendo recebido em maio de 2023 a condição de urgência na tramitação. Atualmente, encontra-se pronto para votação no Plenário, mas os meandros políticos têm retardado a sua colocação em pauta e o então presidente da Câmara, deputado Arthur Lira, criou Grupo de Trabalho para redigir novo texto, alegando que o projeto que tramita está fadado a ir a lugar nenhum⁴⁹.

Alguns pontos positivos do projeto são, por exemplo, a limitação do disparo de mensagens pelas plataformas e a proibição de que contas automatizadas

45. “A system of free markets in speech often fails on the relevant counts; regulatory reforms could make things better. I do not claim that speech rights should be freely subject to political determination, as are current issues of occupational safety and health, for instance. I do, however, insist that in some circumstances, policies that seem to involve government regulation of speech actually might promote the depth and diversity that are central to a system of free speech, and should not be treated as abridgements at all.” SUNSTEIN, Cass. *Is Free Speech the Enemy of Democracy?* p. 5-6. Disponível em: <https://www.bostonreview.net/articles/cass-sunstein-free-speech-enemy-democracy/>. Acesso em: 09 abr. 2025.

46. FARAH. *Op. cit.*, p.127-128.

47. DINIZ, Iara. *Só 35 países têm leis específicas contra desinformação, aponta LupaMundi*. LUPA. 6 nov. 2023. Disponível em: <https://lupa.uol.com.br/jornalismo/2023/11/06/so-35-paises-tem-leis-especificas-contra-desinformacao-aponta-lupamundi>. Acesso em: 16 dez. 2024.

48. BRASIL. Senado Federal. *Projeto de Lei nº 2.630, de 3 de setembro de 2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet*. Brasília: Senado Federal, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1909983&filename=PL%202630/2020. Acesso em: 20 dez. 2024.

49. LOBO, Ana Paula. *CGI.br sai em defesa do PL 2630 e diz que zerar discussão é um erro*. *nic.br*. 15 abr. 2024. Disponível em: <https://www.nic.br/noticia/na-midia/cgi-br-sai-em-defesa-do-pl-2630-e-diz-que-zerar-discussao-e-um-erro/>. Acesso em: 23 dez. 2024.

divulguem *fake news*, o que pode auxiliar a atuação da justiça. Em contrapartida, a sociedade civil fez críticas a outros pontos do projeto, como os riscos à privacidade, o perigo da censura, a dificuldade de rastreabilidade, a ausência de um órgão regulador claro, a imunidade parlamentar e as remunerações de conteúdo jornalístico e dos direitos autorais.

Caso seja incorporada ao PL (e ele siga seu trâmite) a criação do Sistema Brasileiro de Regulação de Plataformas, sugerida pela Ordem dos Advogados do Brasil/Nacional, abre-se a possibilidade de o quadro alterar-se em benefício da sociedade. Afinal de contas, regular não significa reduzir direitos, antes, é um passo para agir na sua preservação.

A discussão sobre a regulamentação das plataformas é polêmica e envolve muitos atores e posições ora convergentes, ora discordantes. Destacam-se abaixo algumas delas:

No prefácio do documento *Diretrizes para a Governança das Plataformas Digitais*, da Organização das Nações Unidas para a Educação, Ciência e Cultura (Unesco), a Diretora-geral, Audrey Azoulay, destacou que elas “tornaram-se palco para os defensores da igualdade e da liberdade”, mas, ao mesmo tempo, muitas vezes desvirtuam-se em “bolhas de isolamento”, “casulos de desinformação”, que “fomentam teorias da conspiração e violência extrema”⁵⁰.

Uma das conclusões dos debates no fórum intersessional Rede de Políticas sobre Acesso Significativo (PNMA, na sigla em inglês) que ocorreram na edição 2024 do *Internet Governance Forum* (IGF) foi a de que ainda são necessárias “ferramentas de mensuração confiáveis”, depois de muitos anos de discussão, pois problemas persistem, destacando que “soluções alternativas, para tais medidas, além da regulamentação direta, podem ser exploradas a fim de evitar ônus desnecessários”⁵¹⁵².

No documento *Padrões de Direitos Humanos como Linhas de Base para a Regulação de Prestação de Contas das Plataformas: uma contribuição para o debate brasileiro*, a Fundação Fronteira Eletrônica (EFF, na sigla em inglês) e a ONG *Access Now* defendem uma estrutura de supervisão independente e participativa, destacando as propostas da Coalizão Direitos na Rede e da Comissão Especial de Direito Digital da OAB, que “refletem a necessidade de freios

50. UNESCO. *Diretrizes para a Governança das Plataformas Digitais*. UNESCO. 2023. p.6. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000387560>. Acesso em: 10 abr. 2025.

51. IGF-Internet Governance Forum. *IGF 2024-Annual Meeting Summary Report*. IGF-Internet Governance Forum. 2024. p.45. Disponível em: https://intgovforum.org/en/filedepot_download/305/28529. Acesso em: 11 abr. 2025.

52. Traduções nossas.

e contrapesos robustos, incluindo uma participação significativa da sociedade civil, no projeto de supervisão do PL 2.630”⁵³.

Uma visão bastante crítica do multissetorialismo adotado na governança da internet é a de James Görgen, do Ministério do Desenvolvimento, Indústria e Comércio (MDIC). Para ele, esse modelo facilitou o “predomínio do setor privado sobre os demais atores e de uma comunidade técnica que funciona com pouca transparência e ensimesmada”. Destacando que muitos dos elementos que fazem parte da internet não são virtuais (cabos, antenas e seres humanos) e têm “os pés fincados em uma determinada jurisdição”, onde há códigos legais, salienta que as atividades desses elementos são passíveis de regulação no país em que estão localizados⁵⁴.

A título de contribuição para o debate e comparação com o PL das *Fake News*, apresentam-se a seguir pequenos levantamentos de algumas legislações vigentes e projetos de lei de quatro países:

A NetzDG (Lei para Melhoria da Aplicação da Lei nas Redes Sociais) vigora na Alemanha desde o início de 2018. Seu foco é o combate mais eficaz aos crimes de ódio, às notícias criminosas falsas e outros conteúdos criminosos. Regulamenta plataformas com mais de 2 milhões de usuários, que devem, em prazo de até sete dias após o recebimento da reclamação, deletar, remover ou bloquear conteúdo claramente ilegal. Outra obrigação é a de apresentarem relatórios a cada seis meses, dando conta das medidas adotadas com relação às reclamações de crimes de ódio e conteúdos ilegais. O descumprimento à lei pode gerar multas que podem chegar a 50 milhões de euros. Além da NetzDG, as disposições do DSA também vigoram na Alemanha⁵⁵.

Desde dezembro de 2018, a França conta com a Lei n. 2018/1202 (Lei da Luta contra a Manipulação da Informação). Ela determina que “as plataformas devem combater as contas que divulgam massivamente conteúdos falsos e implementar medidas de educação midiática”. Também definem que, em período eleitoral, alegações inexatas ou enganosas sobre candidato ou às próprias eleições precisam ser apresentadas a um juiz, que terá 48 horas para decidir sobre as medidas visando impedir que a desinformação se propague⁵⁶.

53. EFF-Eletronic Frontier Foundation e Access Now. *Padrões de Direitos Humanos como Linhas de Base para a Regulação de Prestação de Contas das Plataformas – Uma contribuição para o debate brasileiro*. EFF-Eletronic Frontier Foundation e AccessNow. p. 14. Disponível em: https://www.eff.org/files/2023/07/07/padroes_de_direitos_humanos_como_linhas_de_base_para_a_regulacao_e_prestacao_de_contas_das_plataformas_pt-br.pdf. Acesso em: 10 abr. 2025.

54. GÖRGEN, James. *A internet e a armadilha do consenso*. OUTRASPALAVRAS. 2024. Disponível em: <https://outraspalavras.net/tecnologiaemdisputa/a-internet-e-a-armadilha-do-consenso/#sdfootnote15anc>. Acesso em: 11 abr. 2025.

55. LUPA e ICFJ. *Lupamundi-Mapa das Legislações sobre Desinformação*. LUPAMUNDI. Disponível em: <https://lupa.uol.com.br/lupa-mapa-leis-desinformacao/>. Acesso em 13 abr. 2025.

56. *Ibidem*.

Quatro projetos de lei que abordam a divulgação de informações falsas tramitam no legislativo das Filipinas. Três deles visam incluir na Lei de Crimes Cibernéticos dispositivo que criminalize a divulgação de informações falsas. O outro cria uma legislação específica que criminaliza a desinformação⁵⁷. Durante a pandemia de Covid-19, utilizou-se o Código Penal e o *Bayanihan Act* para criminalizar notícias falsas que causassem pânico, caos ou prejudicassem o interesse público, valendo-se de tipos penais já existentes⁵⁸.

Desde 2019, Cingapura conta com a Lei de Proteção contra Falsidades e Manipulação Online. O seu 7º artigo determina que é proibido comunicar qualquer declaração suspeita ou sabidamente falsa que possa prejudicar a segurança, a saúde pública, a ordem ou finanças públicas, bem como as relações com outros países. O dispositivo vale também no caso de a declaração poder influenciar nos resultados de eleições e referendos, incitar hostilidade entre grupos ou diminuir a confiança pública em órgãos do Estado. “As penas podem chegar a até 10 anos de prisão e multa de 100 mil dólares cingapurianos”. A utilização de robôs na disseminação de informações falsas também é proibida e as penas alcançam quem financia ou oferece serviços para espalhar desinformação. Ao receberem ordens do governo, provedores, plataformas e veículos de imprensa devem informar aos usuários finais sobre a falsidade e bloquear esses conteúdos⁵⁹.

Nosso sistema judiciário, não obstante alguns problemas de conhecimento público, como a morosidade, já deu mostras de que dispõe de meios para enfrentar situações de conflito entre as normas, valendo-se de um juízo de ponderação e proporcionalidade, mantendo o equilíbrio entre direitos e liberdades. Também aqui, no caso da desinformação, esse é um caminho a trilhar. Auxilia nessa direção, o respeito ao princípio sensível da democracia, presente no *caput* do artigo 1º da CRFB⁶⁰.

Outra frente de atuação do Direito é a da participação dos seus operadores em iniciativas que visem à educação da sociedade, para auxiliar na busca de um estado de resiliência capaz de blindá-la contra as investidas da desinformação. Para isso, o profissional do direito deve se manter sempre informado.

57. *Ibidem*.

58. COALIZÃO DIREITOS NA REDE. *Referências Internacionais em Regulação de Plataformas Digitais*. COALIZÃO DIREITOS NA REDE. 2024. p. 66. Disponível em: https://direitosnarede.org.br/wp-content/uploads/2024/04/WEB_V3-Relatorio-sobre-ref-internacionais-em-regulacao-de-plataformas_19-04.pdf. Acesso em: 10 abr. 2025.

59. LUPA e ICFJ. *Op cit*.

60. **Art. 1º** A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito (...). BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm. Acesso em: 13 dez. 2024.

Para além da contribuição desses profissionais, o investimento em educação digital pode ser um caminho eficaz na direção da preparação da sociedade para esses novos tempos. Exemplos nesse sentido já nos deram outras nações, como a Finlândia, que liderou pela quinta vez consecutiva levantamento do *Open Society Institute* de 2022⁶¹ sobre resiliência à desinformação na Europa⁶².

Para Amaral e Prando, a instrução é um dos fatores indispensáveis para atenuar os efeitos das *fake news*. Consideram fundamental a inclusão nas grades curriculares, desde o ensino fundamental, de matérias que ensinem o bom uso das Redes Sociais. E para os que já deixaram os bancos escolares, sugerem campanhas de alerta quanto aos perigos que elas representam⁶³.

Nessa linha de atuação, o Conselho Nacional de Justiça (CNJ) publica desde abril de 2019, no seu site, o Painel de Checagem de *Fake News*. A iniciativa tem parceria de associações da magistratura, de tribunais superiores e da imprensa.

Deve-se, também, lançar um olhar sobre o papel de uma educação inclusiva e integradora para as novas gerações com relação ao tema da digitalização no mundo. O modelo educacional baseado unicamente no aprendizado mecânico não é capaz de fazer frente às mudanças, que tendem a se acelerar, e aos riscos a elas atrelados. Nesse sentido, adotar uma formação que considere primordial o letramento⁶⁴ digital das futuras gerações parece ser um caminho promissor.

Nessa direção, em janeiro de 2023, foi promulgada a Lei nº 14.533/2023⁶⁵ – Política Nacional de Educação Digital (PNED), que contém dispositivos propícios a dar efetividade a uma educação que capacite as gerações a usufruírem das novidades tecnológicas com visão crítica.

61. LESSENSKI, Marin. *How it Started, How it is Going: Media Literacy Index 2022*. OPEN SOCIETY INSTITUTE-SOFIA. 2022. Disponível em: https://osis.bg/wp-content/uploads/2022/10/HowItStarted_MediaLiteracyIndex2022_ENG_.pdf. Acesso em: 19 dez. 2024.

62. FIRPO, Mafê. *Como a Finlândia está ensinando os jovens a não caírem em fake news*. VEJA. 12 jan. 2023. Mundo. Disponível em: <https://veja.abril.com.br/mundo/como-a-finlandia-esta-ensinando-os-jovens-a-nao-cairem-em-fake-news>. Acesso em: 17 dez. 2024.

63. AMARAL, Luiz Fernando Prudente do; PRANDO, Rodrigo Augusto. *Fake news: riscos à democracia* (Portuguese Edition). Posição 2099. São Paulo, Editora IASP, 2021. *E-book*.

64. “É esse, pois, o sentido que tem letramento, palavra que criamos traduzindo ‘ao pé da letra’ do inglês literacy: letra-, do latim littera, e o sufixo -mento, que denota o resultado de uma ação (como, por exemplo, em fermento, resultado da ação de ferir). Letramento é, pois, o resultado da ação de ensinar ou de aprender a ler e escrever: o estado ou a condição que adquire um grupo social ou um indivíduo como consequência de ter-se apropriado da escrita.” SOARES, Magda. *Letramento: um tema em três gêneros*. p. 18. 3ª ed. Belo Horizonte: Autêntica Editora, 2009.

65. Posteriormente, em dezembro de 2023, promulgaram-se alguns dispositivos que foram objeto de veto do presidente da República, mas depois derrubados pelo Congresso. BRASIL. Lei nº 14.533, de 11 de janeiro de 2023. Institui a Política Nacional de Educação Digital. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14533.htm#:~:text=LEI%20N%C2%BA%2014.533%2C%20DE%2011%20DE%20JANEIRO%20DE%202023&text=Institui%20a%20Pol%C3%ADtica%20Nacional%20de,30%20de%20outubro%20de%202003. Acesso em: 20 dez. 2024.

Importante ressaltar também a promulgação posterior do § 11, do art. 26, que estabelece que a educação digital será componente curricular do ensino fundamental e do ensino médio. É essencial ressignificar o currículo com “atratividade e vivências”. Daí a importância da PNED. Os estudantes não podem ser apenas usuários, precisam produzir tecnologia, com visão de mundo⁶⁶.

Uma comparação entre as características do letramento digital e da alfabetização digital é elucidativa quanto às vantagens daquele para uma educação inclusiva, propiciadora de uma formação capaz de criar cidadãos mais conscientes, necessária ao enfrentamento de um mundo cada vez mais tecnologizado. O letramento digital vai além da simples alfabetização digital. Esta restringe-se ao uso básico de ferramentas digitais e Internet, já aquele potencializa a capacidade de usar, entender, integrar e avaliar informações digitais em suas várias formas, desenvolvendo habilidades crítico-analíticas dos usuários⁶⁷.

Considerações finais

A Meta começou a testar nos Estados Unidos, em 18 de março de 2025, o recurso Notas da Comunidade no Instagram, no Facebook e no Threads, o que permite que usuários adicionem notas explicativas a postagens públicas. A medida veio em substituição a um programa de verificação de fatos realizado por agências independentes especializadas para checagem de conteúdos suspeitos e, dependendo dos resultados, poderá se estender para outros países.

Plataformas concorrentes já fizeram testes com esse tipo de moderação e os resultados demonstraram que postagens de teor político ou científico escapam com frequência da checagem coletiva. Outra preocupação é que o recurso não se aplicará a anúncios pagos, o que abre uma brecha para a desinformação patrocinada⁶⁸.

Pela visão da professora Letícia Cesarino, da Universidade Federal de Santa Catarina (UFSC), divulgada no Jornal da USP, plataformas dominadas por grupos com visão política específica tendem a reproduzir vieses e falsear

66. GAROFALO, Débora. *O que você precisa saber sobre a Política Nacional de Educação Digital*. Revista Educação. 2023. Disponível em: <https://revistaeducacao.com.br/2023/02/17/politica-nacional-de-educacao-digital/>. Acesso em: 2 dez. 2024.

67. *Ibidem*.

68. MORAES, Lígia. *Meta começa a testar ‘notas da comunidade’ no Instagram e Facebook nos EUA*. VEJA. 7 mar. 2025. Tecnologia. Disponível em: <https://veja.abril.com.br/tecnologia/meta-comeca-a-testar-notas-da-comunidade-no-instagram-e-facebook-nos-eua/>. Acesso em: 06 abr. 2025.

a realidade, o que reforça notícias falsas em um cenário carente de uma regulação efetiva⁶⁹.

Alterações nas circunstâncias de estruturação do debate público podem justificar mudanças no valor atribuído à Liberdade de Expressão. “Momentos históricos e circunstâncias sociais distintas exigem modulações distintas das prerrogativas de expressão”, visando incentivar o debate público qualificado. Daí o valor instrumental da Liberdade de Expressão implicar na proteção ou não das falsidades⁷⁰.

Pelo exposto, fica patente a necessidade de regulação dos ambientes digitais. Salientando que não há perfeição nessa área, que a autorregulação não se tem mostrado efetiva e que a regulação estatal pode se tornar perigosa para a Liberdade de Expressão, Farah sugere a adoção de um modelo híbrido, que observe transparência, prestação de contas, devido processo, proporcionalidade, não discriminação e direito de defesa. Também considera que os maiores provedores devem arcar com maiores exigências e que um eventual colegiado deve contemplar vários segmentos da sociedade, inclusive com espaços para jornalistas profissionais e membros da sociedade civil⁷¹.

O provérbio “O direito não socorre aos que dormem” se ajusta como luva à realidade brasileira e serve como alerta para que tenhamos mais cuidados com a nossa Democracia. Não podemos nos esquecer das lições da história.

Atenuar os efeitos das *fake news* demanda das plataformas e dos aplicativos de mensagens ações relacionadas a três fatores: (i) a utilização de ferramentas que permitam monitorar comportamentos destoantes daqueles considerados mais típicos de um usuário real; (ii) a vedação ao anonimato e (iii) a instrução do usuário⁷².

Trecho de palestra da juíza do Tribunal Constitucional Federal da Alemanha Sibylle Kessal-Wulf, em 2022, na Escola de Magistratura do Estado do Rio de Janeiro (Emerj), é preciso:

Para impedir isso, a liberdade de expressão pode e deve ter limites. A nossa Lei Fundamental alemã optou explicitamente pela democracia defensiva, para que os inimigos da Constituição não possam, invocando as liberdades concedidas pela Lei Fundamental e sob a

69. PACHECO, Denis. *Com fim de programa de checagem de fatos nos EUA, Meta encerra “teatro da autorregulação”*. VEJA. 10 jan. 2025. Disponível em: <https://jornal.usp.br/atualidades/com-fim-de-programa-de-checagem-de-fatos-nos-eua-meta-encerra-teatro-da-autorregulacao/>. Acesso em: 11 jan. 2025.

70. RAIS, *Op. cit.* p. 99.

71. FARAH, *Op. cit.* p. 367-369.

72. AMARAL, *Op. cit.*, Posição 2081.

proteção dessas liberdades, pôr em risco, prejudicar ou destruir a ordem constitucional⁷³.

Para o Ministro do Supremo Tribunal Federal José Dias Toffoli, a qualidade do diálogo na democracia reflete diretamente na sua higidez. Portanto, informações fidedignas e veracidade são atributos alcançáveis por meio do uso ético e transparente das novas tecnologias. Se renunciarmos a esses elementos, colocaremos em risco as conquistas democráticas⁷⁴.

73. KESSAL-WULF, Sibylle. *Fatos Alternativos, fake news, discursos de ódio e liberdade de expressão*. Sybille Kessal-Wulf. Tradução: Cristina Tereza Gaulia e Markus André Hediger. p. 284. Disponível em: https://www.emerj.tjrj.jus.br/revistadireitoemovimento_online/edicoes/volume20_numero2/volume20_numero2_267.pdf. Acesso em: 20 dez. 2024.

74. DIAS TOFFOLI, José Antônio. *Fake news, desinformação e liberdade de expressão*. p. 12. Disponível em: https://biblioteca-digital.tse.jus.br/xmlui/bitstream/handle/bdtse/7624/2019_toffoli_fake_news_desinformacao.pdf?sequence=1&isAllowed=y. Acesso em: 20 dez. 2024.

Anexo

Desinformação ao longo dos Séculos XX e XXI

►1899–1902	-Guerra dos Bôeres (África do Sul)	• O estereótipo “boer” foi popularizado pelo exército britânico para influenciar a opinião pública a apoiar a guerra.
►1915–1923	Genocídio do povo armênio	• Extermínio de milhões de armênios pelo Império Otomano.
►1917	Revolução Russa	• Os bolcheviques utilizaram a propaganda para mobilizar as massas, prometer uma vida melhor e demonizar seus inimigos.
►1921	Cartas Falsas do Correio da Manhã	• Atribuídas a Arthur Bernardes, precipitaram a Revolução de 30.
►1933–1945	Terceiro Reich	• A propaganda nazista, espalhou ódio, racismo e antissemitismo.
►1939	Ataque de Gleiwitz	• A Alemanha nazista montou uma farsa para justificar a invasão da Polônia, dando início à Segunda Guerra Mundial.
►1945–1991	Guerra Fria	• Ambos os blocos (EUA e URSS) utilizaram a desinformação para desacreditar o adversário e justificar suas ações.
►1947–1954	MaCarthyismo	• Nos EUA, o MaCarthyismo espalhou o pânico sobre a infiltração comunista, levando à perseguição de inocentes.
►1960–1980	Ditaduras na América Latina	• As ditaduras militares na América Latina utilizaram a desinformação para justificar a repressão e a violência.
►1962	Crise dos Mísseis em Cuba	• Informações imprecisas e exageradas quase levaram à guerra nuclear.
►1964	Guerra do Vietnã	• Um alegado ataque norte-vietnamita a navios americanos no Golfo de Tonquim justificou a intensificação da guerra.
	Golpe no Brasil	• A desinformação foi ferramenta crucial para justificar a intervenção militar e derrubar o governo de João Goulart.
►1965	Golpe na Indonésia	• Gen. Suharto acusou com fraude o PC de tentativa de golpe e tomou o poder. Houve, pelo menos, 500 mil pessoas executadas.
►1973–1990	Ditadura militar no Chile	• Desinformação foi amplamente utilizada para justificar o golpe.
►1980–1990	Pandemia de HIV/AIDS	• A epidemia foi acompanhada por uma onda de estigmatização e desinformação, associando a doença a grupos específicos.

►1990	Crise Climática	Indústria de combustíveis fósseis usou desinformação para desacreditar a ciência do clima.
	Guerra do Golfo	EUA justificaram a invasão do Iraque com notícia falsa de que soldados do país roubaram incubadoras de bebês do Kuwait.
►1994	Genocídio dos Tutsis	Em 100 dias, cerca de 800 mil pessoas, a maioria da etnia tutsi, foram brutalmente assassinadas por milícias hutus, em Ruanda.
►2000	Movimento Antivacina	O movimento ganhou força com informações falsas sobre os riscos das vacinas, contribuindo para o ressurgimento de doenças.
►2003	Invasão do Iraque	A falsa informação de que o Iraque tinha armas químicas e biológicas justificou a invasão do país pelos EUA.
►2010–2012	Primavera Árabe	A rápida disseminação de notícias falsas e rumores tanto impulsionou como minou movimentos de protesto.
►2013	Jornadas de Junho no Brasil	<i>Fake news</i> nas Redes Sociais acirraram a polarização política.
►2016	Eleição nos EUA	Desinformação nas Redes Sociais influenciou o resultado.
	Brexit	Desinformações nas Redes Sociais influenciaram o resultado do plebiscito pela saída do Reino Unido da União Europeia.
	<i>Impeachment</i> de Dilma Rousseff	Marcado por um ambiente político polarizado, com a circulação de desinformações e narrativas conflitantes.
	Alerta de retaliação nuclear do Paquistão a Israel	Notícia falsa sobre ameaça de Israel ao Paquistão gerou promessa de retaliação nuclear.
►2017	Genocídio de rohingyas	A desinformação foi utilizada para incitar o ódio contra a minoria rohingya em Mianmar.
	Eleições no Quênia	Pesquisa local indicou que 90% dos entrevistados relataram ter tido contato com notícias falsas sobre as eleições.
	<i>MacronLeaks</i> (França)	Eleição presidencial teve ampla utilização de <i>fake news</i> nas Redes Sociais e vazamento de <i>e-mails</i> da campanha de Macron.
►2018/2022	Eleições no Brasil	Nas eleições de 2018 e 2022 houve intensas campanhas de desinformação e manipulação de dados.

► 2019	Protestos na Índia	• A desinformação foi utilizada para incitar a violência durante os protestos contra a Lei de Cidadania da Índia.
	Eleições no Uruguai	• <i>Fake news</i> desacreditaram Lacalle Pou e Daniel Martínez.
	Eleições na Bolívia	• Circularam informações falsas, agravando a polarização política. Após protestos, o presidente Evo Morales renunciou.
	Revolta popular no Chile	• Nos protestos pelo aumento da tarifa do transporte, houve notícias falsas sobre violência, saques e repressão excessiva.
► 2020–2022	Pandemia de Covid-19	• Houve muitas informações falsas sobre a origem do vírus, a eficácia de vacinas e tratamentos e as medidas de distanciamento.
► 2021	Invasão do Capitólio (EUA)	• A invasão do Capitólio foi instigada por uma campanha de desinformação que negava os resultados das eleições.
► 2023	Invasão das sedes dos Três Poderes da República (Brasil)	• Tentativa de golpe foi marcada por muitas <i>fake news</i> incitando violência e deslegitimando as instituições democráticas.

Referências

ALLCOTT, Hunt; GENTZKOW, Matthew. *Social Media and Fake News in the 2016 Election*. Journal of Economic Perspectives. Vol. 31. p. 211-236. Disponível em: <https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.31.2.211>.

AMARAL, Luiz Fernando Prudente do; PRANDO, Rodrigo Augusto. *Fake news: riscos à democracia* (Portuguese Edition). São Paulo, Editora IASP, 2021. *E-book*.

BACHUR, João Paulo. *Desinformação Política, Mídias Digitais e Democracia: Como e por que as fake news funcionam*. Revista Direito Público. Brasília. Vol. 18. p. 436-469. 2021. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5939>.

BINENBOJM, Gustavo. *Fake news como externalidades negativas*. JOTA. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/publicistas/fake-news-como-externalidades-negativas>.

BRASIL. Tribunal Superior Eleitoral. Código Eleitoral. Lei nº 4.737, de 15 de julho de 1965. Brasília: TSE, 1965. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l4737compilado.htm.

BRASIL. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Dispõe sobre os direitos e deveres dos usuários da internet, e sobre os provedores de aplicação, de conexão e de infraestrutura. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

BRASIL. Lei no 14.533, de 11 de janeiro de 2023. Institui a Política Nacional de Educação Digital. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14533.htm#:~:text=LEI%20N%C2%BA%2014.533%2C%20DE%2011%20DE%20JANEIRO%20DE%202023&text=Institui%20a%20Pol%C3%ADtica%20Nacional%20de,30%20de%20outubro%20de%202003.

BRASIL. Senado Federal. Projeto de Lei nº 2.630, de 3 de setembro de 2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Brasília: Senado Federal, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?-codteor=1909983&filename=PL%202630/2020.

BRASIL. Supremo Tribunal Federal. Acórdão ADI 7.261. Relator Ministro Edson Fachin. Sessão de 19/12/2023. Brasília, STF, 2023. p. 6. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=774895965>.

BRASIL. Supremo Tribunal Federal. Acórdão ADPF 572. Relator Ministro Edson Fachin. Sessão de 18/06/2020. Brasília, STF, 2020. p. 16. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=755791517>.

BRASIL. Tribunal Superior Eleitoral. Acórdão AIJE0601771-28.2018.6.00.0000. Relator Ministro Luis Felipe Salomão. Sessão de 28/10/2021. Brasília, TSE, 2021. p. 6, 102, 106. Disponível em: <https://jurisprudencia.tse.jus.br/#/jurisprudencia/pesquisa?expressaoLivre=0601771-28.2018.6.00.0000&tipoDecisao=Ac%25C3%25B3rd%25C3%25A3o%252CResolu%25C3%25A7%25C3%25A3o%252CDecis%25C3%25A3o%2520sem%2520resolu%25C3%25A7%25C3%25A3o¶ms=s>.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.714, de 20 de outubro de 2022. Dispõe sobre o combate à desinformação nas eleições. Brasília: TSE, 2022. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-714-de-20-de-outubro-de-2022>.

BRUNO, Fernanda; ROQUE, Tatiana. A ponta de um iceberg de desconfiança. In: *Pós-Verdade e fake news. Reflexões sobre a guerra de narrativas*. Cobogó Editora. Org Mariana Barbosa. 2019. Rio de Janeiro. E-book.

CARVALHO, Luis Gustavo Grandinetti Castanho de. *Direito de Informação e Liberdade de Expressão*. Rio de Janeiro: Renovar, 1999.

COALIZÃO DIREITOS NA REDE. *Referências Internacionais em Regulação de Plataformas Digitais*. COALIZÃO DIREITOS NA REDE. 2024. p. 66. Disponível em: https://direitosnarede.org.br/wp-content/uploads/2024/04/WEB_V3-Relatorio-sobre-ref-internacionais-em-regulacao-de-plataformas_19-04.pdf.

COMSCORE. Tendências Digitais 2023, ComScore Brasil. Jan. 2023. Brasil. Disponível em: <https://www.comscore.com/por/Insights/Apresentacoes-e-documentos/2023/Tendencias-Digitais-2023>.

DIAS TOFFOLI, José Antônio. *Fake news, desinformação e liberdade de expressão*. Disponível em: https://bibliotecadigital.tse.jus.br/xmlui/bitstream/handle/bdtse/7624/2019_toffoli_fake_news_desinformacao.pdf?sequence=1&isAllowed=y.

DINIZ, Iara. *Só 35 países têm leis específicas contra desinformação, aponta LupaMundi*. LUPA. 6 NOV. 2023. Disponível em: <https://lupa.uol.com.br/jornalismo/2023/11/06/so-35-paises-tem-leis-especificas-contra-desinformacao-aponta-lupamundi>.

EFF-Eletronic Frontier Foundation e Access Now. *Padrões de Direitos Humanos como Linhas de Base para a Regulação de Prestação de Contas das Plataformas – Uma contribuição para o debate brasileiro*. EFF-Eletronic Frontier Foundation e AccessNow. Disponível em: https://www.eff.org/files/2023/07/07/padroes_de_direitos_humanos_como_linhas_de_base_para_a_regulacao_e_prestacao_de_contas_das_plataformas_pt-br.pdf.

FARAH, André. *Desinformação Online, Liberdade de Expressão e Democracia* (Portuguese Edition). Rio de Janeiro, Editora Lumen Juris, 2024. E-book.

FIRPO, Mafê. *Como a Finlândia está ensinando os jovens a não caírem em fake news*. VEJA. 12 jan. 2023. Mundo. Disponível em: <https://veja.abril.com.br/mundo/como-a-finlandia-esta-ensinando-os-jovens-a-nao-cairem-em-fake-news>.

FONSECA, Bruno; SCOFIELD, Laura. *Bolsonaristas usam código “Festa da Selma” para coordenar invasão em Brasília*. Pública. 2023. Disponível em: <https://apublica.org/sentinela/2023/01/bolsonaristas-usam-codigo-festa-da-selma-para-coordenar-invasao-em-brasilia/>.

GAROFALO, Débora. *O que você precisa saber sobre a Política Nacional de Educação Digital*. Revista Educação. 2023. Disponível em: <https://revistaeducacao.com.br/2023/02/17/politica-nacional-de-educacao-digital/>.

Geoengenharia. Disponível em: <https://pt.wikipedia.org/wiki/Geoengenharia>.

Global Disinformation Index Staff. *The quarter billion dollar question: How is Disinformation Gaming Ad Tech?* GDI, 2019. Disponível em: https://disinformationindex.org/wp-content/uploads/2019/09/GDI_Ad-tech_Report_Screen_AW16.pdf.

GÖRGEN, James. *A internet e a armadilha do consenso*. OUTRASPALAVRAS. 2024. Disponível em: <https://outraspalavras.net/tecnologiaemdisputa/a-internet-e-a-armadilha-do-consenso/#s-dfootnote15anc>.

IGF-Internet Governance Forum. *IGF 2024-Annual Meeting Summary Report*. IGF-Internet Governance Forum. 2024. p.45. Disponível em: https://intgovforum.org/en/filedepot_download/305/28529.

KESSAL-WULF, Sibylle. *Fatos Alternativos, fake news, discursos de ódio e liberdade de expressão*. Sybille Kessal-Wulf. Tradução: Cristina Tereza Gaulia e Markus André Hediger. p. 284. Disponível em: https://www.emerj.tjrj.jus.br/revistadireitoemovimento_online/edicoes/volume20_numero2/volume20_numero2_267.pdf.

LESSENSKI, Marin. *How it Started, How it is Going: Media Literacy Index 2022*. OPEN SOCIETY INSTITUTE-SOFIA. 2022. Disponível em: https://osis.bg/wp-content/uploads/2022/10/HowItStarted_MediaLiteracyIndex2022_ENG_.pdf.

LOBO, Ana Paula. *CGI.br sai em defesa do PL 2630 e diz que zerar discussão é um erro*. [nic.br](https://www.nic.br/noticia/na-midia/cgi-br-sai-em-defesa-do-pl-2630-e-diz-que-zerar-discussao-e-um-erro/). 15 abr. 2024. Disponível em: <https://www.nic.br/noticia/na-midia/cgi-br-sai-em-defesa-do-pl-2630-e-diz-que-zerar-discussao-e-um-erro/>.

LUPA e ICFJ. Lupamundi-Mapa das Legislações sobre Desinformação. LUPAMUNDI. Disponível em: <https://lupa.uol.com.br/lupa-mapa-leis-desinformacao/>.

MAIA GOLTZMAN, Elder. *Liberdade de Expressão e Desinformação em Contextos Eleitorais* (Portuguese Edition) p. 39. Belo Horizonte, Forum, 2022. *E-book*.

MARTINS, Helena. Muito além das fake news: o problema da desinformação em meio à crise social. In: *Desinformação: crise política e saídas democráticas para as fake news*. Helena Martins (Org.). Prefácio de Sérgio Amadeu da Silveira. São Paulo, Veneta, 2020. 108 p.

MORAES, Lígia. *Meta começa a testar ‘notas da comunidade’ no Instagram e Facebook nos EUA*. VEJA. 7 mar. 2025. Tecnologia. Disponível em: <https://veja.abril.com.br/tecnologia/meta-comeca-a-testar-notas-da-comunidade-no-instagram-e-facebook-nos-eua/>.

NEWMAN, Nic; FLETCHER, Richard; ROBERTSON, Craig T.; ARGUEDA, Amy Ross; NIELSEN, Rasmus Kleis. *Digital News Report 2024*. Reuters Institute. Reuters Institute for the Study of Journalism. Disponível em: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2024-06/RISJ_DNR_2024_Digital_v10%20lr.pdf.

O'ROURKE, K. C. *John Stuart Mill and Freedom of Expressions – The genesis of a theory*. Taylor & Francis e-Library, 2003. p. 124. Disponível em: <https://epdf.pub/john-stuart-mill-and-freedom-of-expression-the-genesis-of-a-theory-routledge-stu.html>.

PACHECO, Denis. *Com fim de programa de checagem de fatos nos EUA, Meta encerra “teatro da autorregulação”*. Jornal da USP. 10 jan. 2025. Disponível em: <https://jornal.usp.br/atualidades/com-fim-de-programa-de-checagem-de-fatos-nos-eua-meta-encerra-teatro-da-autorregulacao/>.

_____. Inteligências artificiais entram em campo contra e a favor da desinformação. Jornal da USP. 17 nov. 2023. Disponível em: <https://jornal.usp.br/atualidades/inteligencias-artificiais-entram-em-campo-contra-e-a-favor-da-desinformacao/>.

POSETTI, Julie; MATTHEWS, Alice. A short guide to the history of ‘fake news’ and disinformation. International Center for Journalists. 2018. Disponível em: https://www.icfj.org/sites/default/files/2018-07/A%20Short%20Guide%20to%20History%20of%20Fake%20News%20and%20Disinformation_ICFJ%20Final.pdf.

POST, Robert. Participatory Democracy and Free Speech In: *Virginia Law Review*, Volume.97, May 2011, Number 3. Disponível em: <https://virginialawreview.org/wp-content/uploads/2020/12/477.pdf>.

RAIS, Diogo. *Fake News: a conexão entre a desinformação e o direito* (Portuguese Edition). São Paulo, Thomson Reuters Brasil, 2020. *E-book*.

Redação MediaTalks. *Cinco anos de ‘infodemia’: como a desinformação sobre vacinas continua a afetar a saúde pública*. MediaTalks By J&Cia. 11 mar. 2025. Disponível em: <https://mediatalks.uol.com.br/2025/03/11/covid-cinco-anos-e-infodemia-o-legado-da-desinformacao-online/>.

RODRIGUES, Horácio Wanderlei; GRUBBA, Leilane Serratine. *Pesquisa Jurídica Aplicada*. Florianópolis, 2023. Habitus Editora. *E-book*.

ROTHKOPF, David. J. *When the Buzz Bits Back*. Washington Post. Washington. May 11, 2003. Outlook (Comentary). B4-B5. Disponível em: <https://www.researchgate.net/profile/Zhiwen-Hu-4/>

publication/339926961_The_earliest_usage_track-down_of_infodemic/links/5e6c6b6fa6fdcc-f994c66c4c/The-earliest-usage-track-down-of-infodemic.pdf.

SOARES, Magda. *Letramento: um tema em três gêneros*. 3ª ed. Belo Horizonte: Autêntica Editora, 2009.

SUNSTEIN, Cass. *Is Free Speech the Enemy of Democracy?* Disponível em: <https://www.bostonreview.net/articles/cass-sunstein-free-speech-enemy-democracy/>.

UNESCO. *Diretrizes para a Governança das Plataformas Digitais*. UNESCO. 2023. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000387560>. Acesso em: 10 abr. 2025.

VIEIRA, Marcelo Gimenes. *Brasil é prioridade da Meta para ampliar uso comercial do WhatsApp no mundo*. itforum. 23 ago. 2023. Disponível em: <https://itforum.com.br/noticias/brasil-meta-whatsapp-uso-comercial/>.

VOSOUGUI, Soroush; ROY, Deb; ARAL, Sinan. *The spread of true and false news online*. Science. 9 mar. 2018. Disponível em: <https://www.science.org/doi/10.1126/science.aap9559>.

WARDLE, Claire. *Notícias Falsas. Es complicado*. First Draft. 2017. Disponível em: <https://firstdraft-news.org/articles/noticias-falsas-es-complicado/>.

----- DERAKHSHAN, Hossein. *Relatório Desordem Informacional: para um quadro interdisciplinar de investigação e elaboração de políticas públicas*. Disponível em: <https://edoc.coe.int/en/media/11609-desordem-informacional-para-um-quadro-interdisciplinar-de-investigacao-e-elaboracao-de-politicas-publicas.html#>.

Regulação das plataformas digitais no Brasil: desinformação, discurso de ódio e as perspectivas de uma atuação estatal

ELMANO RODRIGUES PINHEIRO FILHO

Sumário: Introdução. 1. Desinformação, discurso de ódio e as plataformas digitais. 2. Regulação de plataformas digitais. 2.1. Abordagens regulatórias na União Europeia, nos Estados Unidos e no Reino Unido. 2.2. Proposta de regulação de plataformas digitais no Brasil. 3. Perspectivas de uma atuação estatal. Considerações finais. Referências.

Introdução

Em maio de 1948, um grupo de cientistas e engenheiros dos Laboratórios Bell se reuniu para nomear uma nova invenção da empresa: um pequeno interruptor e amplificador de sinais elétricos, que decidiram chamar de transistor. Meses depois, um de seus funcionários publicou uma monografia sobre seus estudos, introduzindo um novo termo tão impactante quanto o anterior: o bit². Ao criar uma unidade para quantificar a informação, Claude Shannon conferiu consistência científica e metodológica a décadas de teorias e especulações. Com o avanço do transistor, seu trabalho abriu as portas para o que hoje conhecemos como Era da Informação³.

A Era da Informação⁴, período caracterizado pela rápida transformação na forma como a informação é criada, distribuída e consumida, especialmente a partir do final do século XX, representa uma nova fase na evolução da sociedade, marcada pela centralidade da informação em diversos aspectos da vida cotidiana. As Tecnologias da Informação e Comunicação (TICs), como a internet, computadores e dispositivos móveis, que revolucionaram a maneira como as pessoas se conectam e compartilham conhecimento, são pilares dessa nova era.

Embora tenha trazido muitos benefícios, a Era da Informação também apresenta desafios, como a desinformação e o discurso de ódio que são propagados. Isso se deve ao fato de que, ao contrário do que dissemina sua no-

1. Graduado em Engenharia Elétrica com ênfase em Eletrônica pela Universidade Estadual Paulista (Unesp), pós-graduado em Regulação de Telecomunicações pela Universidade de Brasília (UnB) e mestre em Ciências em Engenharia Elétrica pelo Instituto Militar de Engenharia (IME). Pós-graduando em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio (ITS), em parceria com a Universidade do Estado do Rio de Janeiro (UERJ) e o Centro de Estudos e Pesquisas no Ensino do Direito (CEPED). Exerce o cargo de Especialista em Regulação na Agência Nacional de Telecomunicações (Anatel) desde 2005.

2. GLEICK, James. *A informação: Uma história, uma teoria, uma enxurrada*. 1. ed. São Paulo: Companhia das Letras, 2013. p. 11-12.

3. *Ibidem*, p. 380-381.

4. Termo popularizado pelo filósofo e sociólogo Daniel Bell em seu livro “A Sociedade Pós-Industrial”, publicado em 1973. Bell argumentava que a sociedade estava passando por uma transformação significativa, em que a informação e o conhecimento se tornavam os principais motores da economia e da vida social, em contraste com as eras anteriores, que eram dominadas pela produção industrial e agrícola. Embora a ideia de uma era focada na informação já estivesse em discussão antes, foi Bell quem ajudou a consolidar e difundir o conceito.

ção ingênua, a informação não tem nenhum vínculo essencial com a verdade, existem casos de informações que tentam e conseguem representar a realidade, mas essa não é sua característica definidora. Mentiras, fantasias, e ficções também são informação, e a solução para os problemas causadas pela informação errônea e pela desinformação não é, necessariamente, mais informação⁵.

Nesse contexto, plataformas digitais que interconectam bilhões de usuários⁶ e distribuem quantidade inimaginável de informação, exercem um papel central na disseminação de desinformação e de discurso de ódio, levando, inclusive, a resultados catastróficos⁷. Por essa razão, autoridades governamentais, instituições privadas e comunidade científica têm se debruçado no estudo de formas de lidar com um problema que se propaga exponencialmente.

O propósito deste trabalho é explorar estratégias para combater a desinformação e o discurso de ódio nas plataformas digitais. No entanto, não se pretende abordar o tema de forma exaustiva, uma vez que a complexidade do assunto exigiria uma análise detalhada que ultrapassaria os limites estabelecidos para o trabalho. Portanto, o enfoque será em aspectos específicos da regulação das plataformas digitais.

O objetivo geral deste trabalho é avaliar diferentes modelos de regulação das plataformas digitais que vêm sendo implementados. De forma específica, busca-se: compreender o papel das plataformas digitais na disseminação de discurso de ódio e desinformação; verificar como alguns países tratam a regulação de conteúdo das plataformas; avaliar a proposta de regulação das plataformas digitais no Brasil; investigar como o Projeto de Lei nº 2.630, de 2020, trata da questão da atuação estatal na regulação das plataformas digitais.

A relevância da temática decorre do fato de que as plataformas digitais tornaram-se um dos principais meios de comunicação eletrônica de massa⁸. Diferentemente de outros meios, elas apresentam estruturas algorítmicas que favorecem postagens com maior engajamento, o que, aliado à anonimi-

5. HARARI, Yuval Noah. *Nexus: Uma breve história das redes de informação, da Idade da Pedra à inteligência artificial*. 1. ed. São Paulo: Companhia das Letras, 2024. p. 38-39.

6. O número de usuários ativos nas redes sociais ultrapassou o total de 5 bilhões em 2023, o equivalente a 62,3% da população mundial, de acordo com um relatório anual da agência We are social e da empresa Meltwater. Maiores informações em: KEMP, Simon. *Digital 2024: 5 billion social media users*. Disponível em: <https://wearesocial.com/us/blog/2024/01/digital-2024-5-billion-social-media-users/>. Acesso em: 1 nov. 2024.

7. A exemplo dos massacres de Christchurch e de Mianmar. Maiores informações em: FISHER, Max. *A máquina do caos: como as redes sociais reprogramam nossa mente e nosso mundo*. 1. ed. São Paulo: Todavia, 2023.

8. Como exemplo, segundo dados de setembro de 2024, o consumo de conteúdo de vídeo por meio de plataformas digitais já representa 30,7% do total no Brasil, considerando todos os dispositivos. Maiores informações em: KANTAR IBOPE MEDIA. Kantar Ibope Media, 2024. *Audiência de vídeo*. Disponível em: <https://kantariibopemedia.com/audiencia-de-video/>. Acesso em: 1 nov. 2024.

dade, cria um ambiente propício para a disseminação de informações falsas e discursos extremistas⁹. Portanto, a regulação desse espaço é fundamental para combater a propagação de conteúdos que impactam a convivência social e a democracia, de forma a equilibrar a liberdade de expressão com a necessidade de um ambiente digital seguro e respeitoso. Para a análise do tema, será adotada a metodologia de revisão bibliográfica.

Dessa forma, o presente artigo pretende responder à seguinte questão: como as iniciativas normativas em tramitação no Brasil e no mundo abordam a regulação das plataformas digitais, e quais são os desafios e impactos da criação ou adaptação de entidades regulatórias para combater a desinformação e o discurso de ódio? Para tanto, dividiu-se o artigo em quatro capítulos que buscam avaliar os temas associados. No capítulo 1, serão apresentados conceitos sobre desinformação, discurso de ódio e plataformas digitais. No Capítulo 2, dividido em duas seções, será examinada a evolução da regulação dessas plataformas, destacando a abordagem da União Europeia, dos Estados Unidos e do Reino Unido, além do debate sobre a regulação no Brasil. No Capítulo 3, será feita uma reflexão sobre a atuação estatal na regulação das plataformas digitais, apresentando vantagens e desvantagens de diferentes modelos e a coordenação por diversas entidades no País. Por fim, as considerações finais do trabalho trarão as principais conclusões e sugestões para futuras pesquisas.

1. Desinformação, discurso de ódio e as plataformas digitais

A desinformação não é um fenômeno novo. Desde os tempos antigos, informações errôneas ou enganosas foram usadas como ferramentas de manipulação política e social. Em guerras, por exemplo, a propagação de boatos e informações falsas já era uma estratégia comum¹⁰. Contudo, com o avanço da tecnologia e a invenção de novos meios de comunicação, a desinformação tornou-se mais acessível e disseminada. O prelo, inventado por Johannes Gutenberg por volta de 1440, permitiu a rápida difusão de dados científicos, mas também de fantasias religiosas, mentiras e teorias da conspiração, levando, por exemplo, à onda de caça às bruxas que tomou conta da Europa no começo da era moderna¹¹.

9. FARAH, André. *Desinformação online, liberdade de expressão e democracia: uma proposta de modelo regulatório híbrido*. 1. ed. Rio de Janeiro: Lumen Juris, 2024. p. 76-78.

10. Sun Tzu enfatiza a importância do engano e da manipulação na guerra. Ele sugere que enganar o inimigo é uma estratégia eficaz, pois pode desestabilizá-lo e levá-lo a tomar decisões erradas. Maiores informações em: TZU, Sun. *A arte da guerra: edição completa bilíngue com os 13 capítulos originais*. 1. ed. São Paulo: Edipro, 2021.

11. HARARI, Yuval Noah. *Nexus: Uma breve história das redes de informação, da Idade da Pedra à inteligência artificial*. 1. ed. São Paulo: Companhia das Letras, 2024. p. 111-116.

Embora a desinformação exista há séculos, seu impacto e alcance aumentaram drasticamente nas últimas décadas, como demonstrado pela influência nas eleições dos Estados Unidos e no referendo do Brexit, em 2016, no chamado escândalo da Cambridge Analytica¹², e pela propagação de crenças sem fundamento científico durante a pandemia de Covid-19¹³. Definir desinformação, em consequência, tornou-se uma tarefa mais complexa, especialmente porque o termo é frequentemente substituído por expressões como “notícia falsa” ou “*fake news*”, que nem sempre têm o mesmo significado, o que dificulta ainda mais sua caracterização.

Não obstante essas dificuldades, diversos autores têm se apresentado para definir o tema. Menezes conceitua *fake news* como sendo “notícias desconfiguradas, que acreditam ou que fazem acreditar em algo que é enganoso, não necessariamente intencionais, mas simuladas a partir de fatos falsos ou propriamente verdadeiros, capazes de desviar da verdade, trazer dúvidas, imprecisões e desestabilizar o espaço deliberativo”¹⁴. Por sua vez, Toffoli define notícia fraudulenta como a utilização de “um artifício ou ardil – uma notícia integral ou parcialmente inverídica apta a ludibriar o receptor, influenciando seu comportamento – com o fito de galgar uma vantagem específica e indevida”¹⁵.

Segundo a Organização das Nações Unidas para a Educação, a Ciência e a Cultura (Unesco), o debate sobre *fake news* costuma combinar dois conceitos-chave: a informação incorreta (*misinformation*), que se refere a conteúdos falsos ou enganosos compartilhados sem intenção maliciosa – ou seja, quando o emissor acredita na veracidade da informação – e a desinformação (*disinformation*), caracterizada pela divulgação deliberada de falsidades com o objetivo explícito de enganar ou causar dano. Além dessas, destaca-se uma terceira categoria: a má-informação (*malinformation*), que é a informação baseada na realidade, mas usada para causar danos a uma pessoa, organização ou país¹⁶.

Em que pesem as diferenças dessas definições, em ambas podem ser identificados elementos mínimos de configuração do conceito de desinfor-

12. EMPOLI, Giuliano Da. *Os engenheiros do caos*. 1. ed. 1. reimp. São Paulo: Vestígio, 2020. p. 141-164.

13. FISHER, Max. *A máquina do caos: como as redes sociais reprogramam nossa mente e nosso mundo*. 1. ed. São Paulo: Todavia, 2023. p. 403-411.

14. MENEZES, Paulo Brasil. *Fake News: Modernidade, Metodologia, Regulação e Responsabilização*. 5. ed., rev., ampl. e atual. São Paulo: Editora JusPodivm, 2024. p. 166-167.

15. TOFFOLI, José Antonio Dias. Fake news, desinformação e liberdade de expressão. In: ABBOUD, Georges; NERY JÚNIOR, Nelson; CAMPOS, Roberto (coord.). *Fake news e regulação*. 3. ed. rev. e ampl. São Paulo: Thomson Reuters Brasil, 2021. p. 33.

16. ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA. *Jornalismo, Fake News e Desinformação: manual para educação e treinamento em jornalismo*. Paris, 2019. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000368647>. Acesso em: 09 abr. 2025.

mação, que, segundo Farah, são: a fraude, a manipulação e o dano, ainda que em potencial¹⁷.

O discurso de ódio, por sua vez, também é algo difícil de conceituar. Suas definições variam de acordo com o contexto legal e cultural de cada país. Do ponto de vista internacional, também não há uma definição legal para o discurso de ódio, visto que a caracterização do que é “odioso” é controversa e disputada. Contudo, as Nações Unidas, para efeito de suas políticas, consideram como discurso de ódio “qualquer forma de comunicação que menospreza ou incita violência e discriminação contra indivíduos ou grupos com base em características como raça, etnia, religião, gênero, orientação sexual ou deficiência”¹⁸.

Portanto, “discurso de ódio” e “desinformação” são conceitos distintos, mas que compartilham semelhanças significativas. Ambos têm o potencial de causar danos profundos à sociedade, podem ser utilizados como ferramentas de manipulação e levantam importantes questões sobre responsabilidade e moderação. Além disso, ambos proliferam-se nas plataformas digitais, especialmente nas redes sociais, onde a disseminação rápida e ampla de informações, verdadeiras ou falsas, é uma realidade constante¹⁹. Diante disso, é essencial definir o que são essas plataformas digitais.

Não existe um consenso sobre a definição do termo plataforma digital, do modo que tem sido usado para descrever uma gama de serviços disponíveis na internet, incluindo *marketplaces*, mecanismos de busca, mídias sociais, canais de conteúdo criativo, lojas de aplicativos, serviços de comunicação, sistemas de pagamento e serviços que compõem a chamada economia colaborativa. Segundo a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), uma plataforma online, ou digital, é definida como um serviço digital que facilita as interações entre dois ou mais conjuntos distintos, mas interdependentes de usuários (sejam empresas ou indivíduos), que interagem por meio do serviço de internet²⁰.

As plataformas digitais têm uma série de características econômicas comuns, que incluem efeitos positivos de rede diretos e indiretos (as redes tor-

17. FARAH, André. *Desinformação online, liberdade de expressão e democracia: uma proposta de modelo regulatório híbrido*. 1. ed. Rio de Janeiro: Lumen Juris, 2024. p. 67-70.

18. NAÇÕES UNIDAS. *The UN Strategy and Plan of Action on Hate Speech*. Nova Iorque, 2019. Disponível em: <https://www.un.org/en/hate-speech/un-strategy-and-plan-of-action-on-hate-speech>. Acesso em: 4 nov. 2024.

19. EMPOLI, Giuliano Da. *Os engenheiros do caos*. 1. ed. 1. reimp. São Paulo: Vestígio, 2020. p. 155.

20. ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. *An Introduction to Online Platforms and Their Role in the Digital Transformation*. Paris, 2019. p. 22. Disponível em: <https://doi.org/10.1787/53e5f593-en>. Acesso em: 4 nov. 2024.

nam-se mais úteis à medida que mais usuários juntam-se a elas), subsídios cruzados, escala potencialmente global, geração e uso de um amplo conjunto de dados do usuário para otimizar seus serviços, inovação disruptiva e custos de mudança. Embora muitas dessas características não sejam exclusivas das plataformas digitais, no seu caso a combinação dessas características pode levar a um crescimento explosivo²¹.

Dadas suas características estruturais, as plataformas digitais ocupam posição central na disseminação da desinformação, uma vez que seus algoritmos tendem a privilegiar conteúdos polarizadores, como observa Martins²². Esse mecanismo fortalece bolhas de informação, reforçando vieses e reduzindo a exposição a perspectivas divergentes. Além disso, ao coletarem e segmentarem dados dos usuários, essas plataformas não só amplificam a desinformação, mas também monetizam informações pessoais. Nesse contexto, a autogovernança adotada pelas empresas revela-se insuficiente para conter tais efeitos, tornando indispensável a implementação de mecanismos de regulação estatal que ultrapassem as iniciativas voluntárias das plataformas.

Devido ao papel que desempenham na mediação do debate público e na circulação de informações, as plataformas digitais se inserem no que Jan-Werner Müller definiu como “infraestrutura crítica da democracia” – conjunto de elementos essenciais que sustentam o funcionamento saudável de um regime democrático, a exemplo dos partidos políticos e da imprensa livre²³. São estruturas consideradas vitais, pois sua degradação, captura por interesses antidemocráticos ou disfunção sistêmica pode levar à erosão, ou mesmo ao colapso, da ordem democrática.

Uma vez estabelecido esse marco teórico inicial, passa-se a analisar como a regulação das plataformas digitais está sendo realizada no mundo, e seus impactos no controle da desinformação e do discurso de ódio.

2. Regulação de plataformas digitais

Desde que Gutenberg criou os primeiros tipos móveis, o acesso à informação se expandiu significativamente. A capacidade de reproduzir textos com o mesmo conteúdo e distribuí-los para um número maior de leitores estabeleceu as bases do que hoje se denomina comunicação de massa, um

21. *Ibidem*, p. 11.

22. MARTINS, Helena. *A desinformação em meio à crise do capitalismo e à configuração de uma nova estrutura de mediação social*. Revista Eco-Pós, v. 27, n. 1, p. 330–352, 2024. Disponível em: <https://doi.org/10.29146/eco-ps.v27i1.28045>. Acesso em: 11 abr. 2025.

23. MÜLLER, Jan-Werner. *Democracy Rules*. Nova Iorque: Farrar, Straus and Giroux, 2021.

conjunto de práticas e tecnologias que permitem a distribuição de informações de forma ampla e generalizada, e que inclui os mais diversos e complexos meios, como a televisão, rádio, jornais, revistas, internet e, mais recentemente, as plataformas digitais.

A constante evolução das tecnologias na comunicação de massa tem sido um desafio contínuo para a adaptação do marco normativo e dos sistemas regulatórios às novas realidades. O desenvolvimento da televisão por satélite na década de 1980, por exemplo, trouxe complexidade à regulação estatal, ao possibilitar que sinais de áudio e vídeo originados fora de um país cobrissem uma ampla população, em contraste com a televisão terrestre existente²⁴.

As plataformas digitais, mais uma vez, colocam em questão as formas tradicionais de regulação dos meios de comunicação de massa. As redes sociais, serviços de *streaming* e outros serviços digitais proporcionam uma comunicação mais interativa e personalizada, em contraste com a comunicação unidirecional das mídias programáticas convencionais²⁵. Seus algoritmos de recomendação são projetados para maximizar o engajamento, muitas vezes priorizando conteúdos sensacionalistas, polêmicos ou emocionalmente carregados, exigindo atenção quanto a aspectos como responsabilidade algorítmica e transparência²⁶. Quando se trata de redes sociais, as diversas relações jurídicas que se estabelecem entre aqueles que nelas interagem tornam o objeto da regulação ainda mais complexo²⁷.

A Unesco propõe diversas diretrizes para a governança das plataformas digitais. Entre as principais orientações, destaca-se a obrigação de os Estados garantirem acesso universal à internet, combaterem a exclusão digital e promoverem a alfabetização midiática. As plataformas devem adotar práticas que respeitem os direitos humanos, ser transparentes em relação aos seus processos de moderação e curadoria de conteúdos, e garantir a acessibilidade da informação, e não devem ser responsabilizadas por moderar conteúdos de

24. SARAIVA, Enrique. O novo papel regulatório do Estado e suas consequências na mídia. In: SARAIVA, Enrique; MARTINS, Paulo Emílio Matos; PIERANTI, Octavio Penna (orgs.). *Democracia e regulação dos meios de comunicação de massa*. 1. ed. Rio de Janeiro: Editora FGV, 2008. p. 66.

25. VESTING, Thomas; CAMPOS, Ricardo. Curadoria de conteúdo: regulação de mídias para o século XXI. In: CAMPOS, Ricardo (org.). *O futuro da regulação de plataformas digitais: Digital Services Act (DAS), Digital Markets Act (DMA) e seus impactos no Brasil*. 1. ed. São Paulo: Editora Contracorrente, 2023. p. 37-40.

26. JESUS-SILVA, Thiago Henrique de. *Desinformação e economia política nas plataformas digitais*. Lumina, v. 18, n. 3, p. 117-134, 2024. Disponível em: <https://periodicos.ufjf.br/index.php/lumina/article/view/44963>. Acesso em: 11 abr. 2025.

27. Relações entre rede social e utilizador (ou um sujeito externo) e entre utilizadores de redes sociais (ou entre um utilizador e um sujeito externo). Maiores informações em: FARINHO, Domingos Soares. Delimitação do espectro regulatório de redes sociais. In: ABOUD, Georges; NERY JÚNIOR, Nelson; CAMPOS, Roberto (coord.). *Fake news e regulação*. 3. ed. rev. e ampl. São Paulo: Thomson Reuters Brasil, 2021. p. 51-56.

boa fé. Além disso, os Estados devem criar autoridades reguladoras independentes e com recursos adequados²⁸.

Para lidar com esses desafios de governança, a regulação deve adaptar-se. Segundo Domingos Farinho, a atividade regulatória a que as plataformas digitais estão ou podem ser submetidas divide-se em três categorias: (i) regulação privada ou autorregulação; (ii) regulação pública ou heterorregulação; e (iii) correção ou autorregulação regulada²⁹.

Na regulação privada ou autorregulação o setor privado estabelece suas próprias regras e mecanismos de controle, sem a intervenção direta do Estado. As empresas ou grupos de empresas criam códigos de conduta, diretrizes e sistemas internos de moderação para garantir que suas operações estejam em conformidade com padrões éticos e legais. As políticas de conteúdo de plataformas como Facebook, Twitter e YouTube, que definem o que é permitido ou não em suas plataformas, são exemplos de autorregulação³⁰.

Por sua vez, na regulação pública ou heterorregulação o Estado é responsável pela intervenção externa aos sujeitos regulados, formulando, implementando e fiscalizando a norma. Tal intervenção pode ser feita, basicamente, por meio de uma regulação *ex-ante*, *ex-post* ou responsiva.

A regulação *ex-ante* refere-se à implementação de regras e normas antes que um problema ou risco se materialize. Nessa abordagem, são identificados cenários em que a ocorrência de externalidades negativas é mais provável e, a partir disso, adota-se a proibição ou regulação dessas situações por meio de regras de conduta, com o objetivo de mitigar riscos. A exigência de medidas de transparência nos algoritmos de recomendação com o intuito de evitar manipulações indevidas é um exemplo dessa forma de regulação³¹.

A regulação *ex-post*, por outro lado, é reativa e ocorre depois que um problema ou dano já se materializou. Nesse modelo, as autoridades intervêm apenas quando as entidades violam normas ou quando ocorre uma externalidade

28. ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA. *Diretrizes para a governança das plataformas digitais: salvaguardar a liberdade de expressão e o acesso à informação com uma abordagem multissetorial*. Paris, 2023. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000387560>. Acesso em: 26 nov. 2024.

29. FARINHO, Domingos Soares. Delimitação do espectro regulatório de redes sociais. In: ABBOUD, Georges; NERY JÚNIOR, Nelson; CAMPOS, Roberto (coord.). *Fake news e regulação*. 3. ed. rev. e ampl. São Paulo: Thomson Reuters Brasil, 2021. p. 47.

30. BARROSO, Luna van Brussel. *Liberdade de expressão e democracia na Era Digital: o impacto das mídias sociais no mundo contemporâneo*. 1. reimpressão. Belo Horizonte: Fórum, 2022. p. 204-207.

31. ALBUQUERQUE, Carlos Antônio Menezes de. Observações na moderação de conteúdo: iniciativas legais e sua prática na autorregulação regulada e autorregulação. In: CAMPOS, Ricardo (org.). *O futuro da regulação de plataformas digitais: Digital Services Act (DAS), Digital Markets Act (DMA) e seus impactos no Brasil*. 1. ed. São Paulo: Editora Contracorrente, 2023. p. 394.

negativa. É aplicada, por exemplo, nos casos de responsabilidade intermediária quanto a conteúdos de terceiros em plataformas digitais³².

Por sua vez, a regulação responsiva é um modelo baseado na criação de regras que estimulam o cumprimento voluntário pelos regulados, por meio de um ambiente de diálogo constante destes com o regulador. Esse modelo busca equilibrar a regulação estatal intensa da atividade econômica com sua desregulação extrema³³. O modelo de regulação da Austrália para lidar com questões de desinformação, em que o governo ajusta as medidas regulatórias conforme as novas práticas e tecnologias de plataformas emergem, é um exemplo de sua aplicação³⁴.

Por fim, a autorregulação regulada, também chamada por alguns autores de corregulação, é um sistema intermediário entre a autorregulação pura e a heterorregulação. Nesse modelo, coexistem normas estabelecidas pelo poder público, por organismos ou entidades nacionais e internacionais, e as regras definidas pelos próprios regulados³⁵. Tal abordagem está presente na Lei Alemã para a Melhoria da Aplicação da Lei nas Redes Sociais, ou NetzDG, e que impõe obrigações de transparência e remoção de conteúdo ilegal³⁶, bem como no *Digital Services Act (DSA)* da União Europeia (UE), que exige que códigos de conduta elaborados pelas plataformas sejam acompanhados por órgãos públicos.

Para uma análise mais detalhada dessas abordagens regulatórias, na próxima seção serão exploradas as iniciativas de regulação de plataformas digitais na União Europeia (UE), nos Estados Unidos, no Reino Unido e, subsequentemente, será examinado o caso do Brasil.

2.1 Abordagens regulatórias na União Europeia, nos Estados Unidos e no Reino Unido

A União Europeia tem a capacidade de influenciar mercados globais a partir da criação de regulações locais, fenômeno que Anu Bradford cunhou e de-

32. BIANQUINI, Heloisa. Regulação ex ante, regulação ex post e regulação responsiva: notas exploratórias sobre o processo sancionador da Autoridade Nacional de Proteção de Dados. In: CAMPOS, Ricardo (org.). *O futuro da regulação de plataformas digitais: Digital Services Act (DAS), Digital Markets Act (DMA) e seus impactos no Brasil*. 1. ed. São Paulo: Editora Contracorrente, 2023. p. 268.

33. SCHOLZE, Simone Henriqueta Cossetin; VIEIRA, Vania Lucia Ribeiro; AGUIAR, Alexandre Kehrig Veronese. *Estudo sobre modelo regulatório pró-inovação*. 2024. p. 226.

34. SU, Chunmeizi. Regulating Chinese and North American Digital Media in Australia: Facebook and WeChat as Case Studies. In: FLEW, Terry; MARTIN, Fiona R. *Digital Platform Regulation: global perspectives on internet governance*. 1. ed.. Cham: Palgrave Macmillan, 2022. p. 173-190.

35. SCHOLZE, Simone Henriqueta Cossetin; VIEIRA, Vania Lucia Ribeiro; AGUIAR, Alexandre Kehrig Veronese. *Estudo sobre modelo regulatório pró-inovação*. 2024. p. 66.

36. ALBUQUERQUE, Carlos Antônio Menezes de. Observações na moderação de conteúdo: iniciativas legais e sua prática na autorregulação regulada e autorregulação. In: CAMPOS, Ricardo (org.). *O futuro da regulação de plataformas digitais: Digital Services Act (DAS), Digital Markets Act (DMA) e seus impactos no Brasil*. 1. ed. São Paulo: Editora Contracorrente, 2023. p. 398.

finiu como “Efeito Bruxelas”³⁷. Essa tendência efetivou-se com a aprovação, em 2022, do *Digital Services Act (DSA)*, iniciativa regulatória que visava garantir um ambiente digital seguro e transparente e que tem influenciado alguns países, a exemplo do Brasil. Com enfoque regulatório predominantemente *ex-ante*, busca prevenir problemas ao impor responsabilidades preventivas às plataformas digitais. O DSA estabelece regras claras sobre a moderação de conteúdo, transparência dos algoritmos e fiscalização das plataformas, com ênfase na proteção dos direitos dos usuários e na remoção de conteúdos nocivos. Complementando o quadro regulatório da União Europeia para a economia digital, tem-se o *Digital Markets Act (DMA)*, com enfoque *ex-ante* e aprovado em 2022, que impõe obrigações preventivas a grandes plataformas digitais (*gatekeepers*), como transparência algorítmica e interoperabilidade, a fim de evitar abusos de poder de mercado antes que ocorram.

No que diz respeito à moderação de conteúdo, a legislação europeia não apenas exige que plataformas grandes (com mais de 45 milhões de usuários) tomem medidas rigorosas contra conteúdos ilegais³⁸, como discurso de ódio, e, ainda, exige transparência na moderação e a aplicação de mecanismos de verificação para combater a desinformação³⁹, bem como a criação de sistemas de notificação eficazes para que os usuários possam reportar abusos.

Nos Estados Unidos, a moderação de conteúdo, do ponto de vista legal, manifesta-se, principalmente, pelo uso da Seção 230 do *Communications Decency Act (CDA)*, de 1996, que proporciona certa imunidade às plataformas em relação aos conteúdos de terceiros. Esta imunidade, essencialmente, exime os provedores de conteúdo de serem considerados responsáveis como editores, ou seja, não podem ser responsabilizados pelas publicações dos usuários em suas plataformas, o que inclui discurso de ódio e desinformação. A abordagem regulatória de autorregulação adotada, ao invés de impor regras rígidas de controle *ex-ante* sobre o conteúdo, como ocorre no DSA, permite que as plataformas atuem livremente, com a responsabilidade de moderar conteúdo de boa-fé, sem sofrerem sanções por não removerem

37. BRADFORD, Anu. *The Brussels Effect: How the European Union Rules the World*. Nova Iorque: Oxford University Press, 2020.

38. O conceito de “conteúdo ilegal” no DSA abarca conteúdos como discurso de ódio, terrorismo, discriminação, imagens de abuso sexual infantil, compartilhamento ilegal não consentido de imagens de conteúdo privado, perseguição digital, venda e comercialização de produtos falsos ou ilegais, veiculação não autorizada de material protegido por direitos autorais, entre outros.

39. O DSA não abrange conteúdo de desinformação, na medida que não existem leis específicas reconhecendo sua ilegalidade. Contudo, as regras propostas pelo DSA sobre publicidade, transparência de algoritmos e mitigação de riscos evidenciam as responsabilidades das plataformas também quanto à disseminação de desinformação. Maiores informações em: BARROSO, Luna van Brussel. *Liberdade de expressão e democracia na Era Digital: o impacto das mídias sociais no mundo contemporâneo*. 1. reimpressão. Belo Horizonte: Fórum, 2022. p. 182-194.

rapidamente conteúdos problemáticos, desde que não o façam com a intenção de causar prejuízo⁴⁰.

Essa estrutura contribuiu para o crescimento da economia digital, ao criar um ambiente seguro para empresas como Google e Facebook, sem o temor constante de processos judiciais⁴¹. Contudo, no que se refere ao combate à desinformação e ao discurso de ódio, a Seção 230 é amplamente criticada, uma vez que sua ênfase na não-responsabilidade das plataformas pode dificultar ações mais incisivas contra conteúdos prejudiciais, deixando as plataformas a cargo de políticas próprias, sem um controle estatal efetivo. Por essa razão, há projetos bipartidários, com diferentes abordagens, que buscam redefinir o equilíbrio entre liberdade de expressão e responsabilidade⁴².

No Reino Unido, o *Online Safety Act*, de 2023, visa impor às plataformas digitais um “dever de cuidado”⁴³ para remover conteúdo ilegal ou danoso, com supervisão do regulador dos serviços de comunicações *Office of Communications (Ofcom)*. Esta lei aplica uma abordagem de regulação *ex-ante*, exigindo que certos serviços antecipem e mitiguem riscos relacionados a conteúdos prejudiciais antes de sua disseminação⁴⁴.

No que diz respeito à desinformação e discurso de ódio, o *Online Safety Act* exige que as plataformas adotem medidas para proteger seus usuários, especialmente crianças, de danos *online*, incluindo a remoção de conteúdo nocivo. Contudo, a lei também tem sido criticada por potencialmente restringir a liberdade de expressão, ao forçar plataformas a moderarem proativamente o conteúdo sem uma definição clara de “dano”. O enfoque colaborativo com as plataformas permite uma flexibilidade que pode, por um lado, garantir uma resposta mais ágil, mas, por outro, deixar lacunas em termos de ação decisiva contra conteúdos prejudiciais⁴⁵.

40. ALBUQUERQUE, Carlos Antônio Menezes de. Observações na moderação de conteúdo: iniciativas legais e sua prática na autorregulação regulada e autorregulação. In: CAMPOS, Ricardo (org.). *O futuro da regulação de plataformas digitais: Digital Services Act (DAS), Digital Markets Act (DMA) e seus impactos no Brasil*. 1. ed. São Paulo: Editora Contracorrente, 2023. p. 391-392.

41. TYAGI, Kalpana. Content Competition and Data: Ex ante Regulation to Make Digital Markets Contestable. In: TYAGI, Kalpana; SANDERS, Anselm Kamperman; CAUFFMAN, Caroline. *Digital Platforms, Competition Law, and Regulation: Comparative Perspectives*. 1. ed. Oxford: Hart Publishing, 2024. p. 241-242.

42. A exemplo do *Platform Accountability and Consumer Transparency Act (PACT Act)*. Maiores informações em: CONGRESSIONAL RESEARCH SERVICE. *Section 230: An Overview*. Washington, 2024. Disponível em: <https://www.congress.gov/crs-product/R46751>. Acesso em: 11 abr. 2025.

43. O “dever de cuidado” (ou *duty of care*) na *Common Law* é um princípio jurídico que impõe aos fornecedores de bens e serviços a responsabilidade de prever os possíveis efeitos negativos de suas ofertas e adotar medidas para mitigar tais riscos. O conceito de negligência é baseado nesse dever.

44. SCHOLZE, Simone Henriqueta Cossetin; VIEIRA, Vania Lucia Ribeiro; AGUIAR, Alexandre Kehrig Veronese. *Estudo sobre modelo regulatório pró-inovação*. 2024. p. 145.

45. *Ibidem*, p. 145-146.

Além desses países, merece destaque a abordagem alemã de regulação. A Lei NetzDG, de 2017, enfatiza a proteção dos direitos dos usuários, com foco na moderação de conteúdo e na preservação da diversidade de opiniões, e exige das plataformas a remoção de conteúdos ilegais dentro de prazos específicos, impondo sanções significativas no seu descumprimento. Em casos de controvérsias sobre legalidade de um conteúdo a FSM, instituição de correção reconhecida pelo Departamento Federal de Justiça Alemão, pode ser consultada⁴⁶.

2.2 Proposta de regulação de plataformas digitais no Brasil

No Brasil, ainda não existem normas específicas para regular as atividades das plataformas digitais. A principal legislação sobre o uso da internet é a Lei nº 12.965, de 2014, o Marco Civil da Internet (MCI), que trata do tema apenas para determinar que os provedores de aplicações não são responsáveis pelos conteúdos criados por terceiros e compartilhados em suas plataformas, sendo passíveis de responsabilização apenas se não cumprirem ordens judiciais⁴⁷, e cuja constitucionalidade ainda está sendo discutida no Supremo Tribunal Federal (STF)⁴⁸. Além do MCI, diversos projetos de lei têm sido apresentados com o objetivo de regulamentar as plataformas digitais, destacando-se o Projeto de Lei (PL) nº 2.630, de 2020, que visa instituir a “Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet”.

Conhecido como o “Projeto de Lei das Fake News”, o PL 2.630/2020 foi inicialmente apresentado no Senado Federal com o propósito de regulamentar as plataformas digitais, focando especialmente no combate à desinformação e na promoção da transparência *online*. Entre os temas mais controversos está a criação de novas regras para a moderação de conteúdo, estabelecendo que as plataformas poderão ser punidas se não agirem diligentemente para prevenir práticas ilícitas em seus serviços. Essa abordagem segue o modelo do DSA europeu.

O projeto tem enfrentado dificuldades em sua tramitação, especialmente devido à necessidade de equilibrar transparência, liberdade de expressão e o combate a práticas ilícitas, como a desinformação. Embora a proposta bus-

46. ALBUQUERQUE, Carlos Antônio Menezes de. Observações na moderação de conteúdo: iniciativas legais e sua prática na autorregulação regulada e autorregulação. In: CAMPOS, Ricardo (org.). *O futuro da regulação de plataformas digitais: Digital Services Act (DAS), Digital Markets Act (DMA) e seus impactos no Brasil*. 1. ed. São Paulo: Editora Contracorrente, 2023. p. 392-393.

47. A única exceção é o caso da divulgação de conteúdos sexuais sem o consentimento dos participantes, conhecido como pornografia da vingança, em que ele deverá atuar a partir de simples notificação do usuário.

48. Objeto do Recurso Extraordinário (RE) nº 1.037.396/SP (Tema 987 da Repercussão Geral).

que estabelecer diretrizes para a moderação de conteúdos em plataformas digitais, organizações da sociedade civil^{49, 50} alertam para os riscos de instrumentalização política na regulação da internet, o que poderia resultar em censura indireta, assimetria de poder e fragilização da liberdade de expressão. A ausência de um capítulo robusto sobre deveres de transparência algorítmica ainda traz preocupações quanto à falta de transparência nos critérios de moderação de conteúdo e à vigilância indevida sobre usuários, o que pode impactar o exercício da liberdade de expressão e a privacidade⁵¹.

O Senado Federal aprovou o PL em junho de 2020, e, após algumas alterações, foi encaminhado à Câmara dos Deputados. Na Câmara, o projeto foi analisado nas comissões e, em 2021, um grupo de trabalho apresentou um substitutivo que incluiu novas disposições, como a ampliação da responsabilização das plataformas. Em 2022, o projeto enfrentou resistência e não obteve apoio suficiente para ser pautado⁵².

Com a mudança de governo em 2023, o Executivo enviou uma nova proposta de regulação, modificando alguns aspectos do projeto, como a ampliação da responsabilidade das plataformas quanto a conteúdos prejudiciais. Em abril de 2023, o relator, Deputado Orlando Silva, protocolou seu parecer preliminar, mas o projeto continuou a enfrentar resistência. Em busca de consenso, em junho de 2024, foi instituído grupo de trabalho para analisar e debater o tema⁵³.

3. Perspectivas de uma atuação estatal

Um dos principais desafios que se apresenta ao se debater e propor uma regulação para as plataformas digitais decorre do caráter dinâmico do ambiente digital, que amplifica a incerteza quanto à eficácia de uma possível regulação. De fato, a rapidez e as constantes transformações do mundo digital exigem uma abordagem regulatória criativa e experimental, capaz de lidar

49. INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO. *Nota Técnica sobre os PLS 2927/2020 e PL 2630/2020*. Rio de Janeiro, 2020. Disponível em: <https://itsrio.org/pt/publicacoes/nota-tecnica-its-pls-contra-fake-news/>. Acesso em: 12 abr. 2025.

50. ARTIGO 19. *Nota Técnica Projeto de Lei nº 2.630/2020*. São Paulo, 2020. Disponível em: <https://artigo19.org/2020/08/07/pl-das-fake-news-nota-tecnica-indica-que-atual-proposta-traria-mais-riscos-do-que-beneficios-para-o-combate-as-noticias-falsas/>. Acesso em: 12 abr. 2025.

51. COALIZÃO DIREITOS NA REDE. *PL 2630/20: propostas da CDR para uma lei efetiva e democrática*. CDR, 1 set. 2020. Disponível em: <https://direitosnarede.org.br/2020/09/01/pl-2630-propostas-da-cdr-para-uma-lei-efetiva-e-democratica/>. Acesso em: 12 abr. 2025.

52. NAZARENO, Claudio; PINHEIRO, Guilherme Pereira. *Regulação de plataformas, Fake News e o PL 2630/2020*. Brasília: Câmara dos Deputados, Consultoria Legislativa, 2023. p. 13-18.

53. O grupo de trabalho, no entanto, não chegou a ser sequer instalado, e o prazo para a conclusão de seus trabalhos, estabelecido no Ato do Presidente de 05/06/2024, foi encerrado.

com a complexidade dessa realidade⁵⁴. Nesse contexto, as opções de atuação estatal tornam-se bastante restritas, exigindo não apenas a definição de um modelo regulatório apropriado, mas também a escolha de um órgão com a capacidade e os recursos necessários.

Como exposto em seções anteriores, as propostas de regulação das plataformas digitais têm aplicado, essencialmente, as abordagens de autorregulação (ou regulação privada), de heterorregulação (ou regulação pública) e de autorregulação regulada (ou corregulação).

A autorregulação, ou regulação privada, oferece vantagens como a agilidade na criação de normas e a capacidade de adaptação às especificidades do setor, com a presença de diretrizes claras, sistemas de monitoramento e órgãos de controle independentes. No entanto, suas desvantagens são evidentes. A concentração, em um único ator, do poder de formulação, interpretação e aplicação das regras pode gerar uma falta de *accountability*, afetando aqueles que se encontram fora do sistema autorregulatório. Além disso, a eficácia das sanções pode ser limitada, e os interesses privados podem se sobrepor ao interesse público, favorecendo práticas anticompetitivas e prejudiciais⁵⁵.

Por sua vez, a heterorregulação, ou regulação pública, possui vantagens como a autoridade e legitimidade advindas de um processo democrático, além da força coercitiva da norma e o seu caráter universal. A capacidade de adaptação da lei conforme as necessidades e sua credibilidade são outros pontos positivos⁵⁶. Contudo, a regulação estatal pode ser lenta e enfrentar obstáculos políticos, atrasando sua implementação ou modificação. Além disso, a complexidade das leis e a falta de flexibilidade podem gerar ineficiência. Também há o risco de o regulador abusar de sua autoridade, prejudicando a impessoalidade e favorecendo interesses antidemocráticos⁵⁷.

Já a autorregulação regulada, ou corregulação, combina vantagens dos modelos anteriores, de forma equilibrada e eficiente. Ao permitir que os atores privados participem da formulação das normas, o Estado reconhece suas limitações técnicas, enquanto os regulados têm a oportunidade de adaptar as regras à sua realidade. Isso facilita o cumprimento das normas e o aprendizado

54. MARANHÃO, Juliano; CAMPOS, Ricardo. Fake News e autorregulação regulada das redes sociais no Brasil: fundamentos constitucionais. In: ABBOUD, Georges; NERY JÚNIOR, Nelson; CAMPOS, Roberto (coord.). *Fake news e regulação*. 3. ed. rev. e ampl. São Paulo: Thomson Reuters Brasil, 2021. p. 343-346.

55. FARAH, André. *Desinformação online, liberdade de expressão e democracia: uma proposta de modelo regulatório híbrido*. 1. ed. Rio de Janeiro: Lumen Juris, 2024. p. 100-102.

56. *Ibidem*, p. 138-139.

57. BARROSO, Luna van Brussel. *Liberdade de expressão e democracia na Era Digital: o impacto das mídias sociais no mundo contemporâneo*. 1. reimpressão. Belo Horizonte: Fórum, 2022. p. 306-307.

mútuo entre as partes. Além disso, a possibilidade de ajustes e modificações das regras eleva a corrigibilidade do sistema. No entanto, o modelo pode ser vulnerável à captura de agentes públicos e ao uso da discricionariedade para fins privados, e o equilíbrio entre os interesses privados e o público pode ser difícil de alcançar, comprometendo sua eficácia⁵⁸.

Avaliando-se as vantagens e desvantagens desses três modelos, e considerando o ordenamento jurídico brasileiro e o contexto em que se insere, uma abordagem baseada em corregulação parece ser a mais adequada para a regulação das plataformas digitais no Brasil, com a utilização de uma autoridade especializada como coordenadora do sistema. Tal alternativa vai ao encontro do que fora proposto por diversos especialistas em suas discussões⁵⁹ e que foi incorporada, mesmo que de forma confusa⁶⁰, no substitutivo ao PL nº 2.630/2020.

Um exemplo notável de corregulação no Brasil é o sistema de classificação indicativa de conteúdos audiovisuais. Embora seja coordenado pelo Ministério da Justiça e Segurança Pública (MJSP), a classificação conta com a colaboração das próprias emissoras de televisão, que submetem suas obras à análise com base em critérios previamente definidos pelo poder público. Outro exemplo é o Código Brasileiro de Autorregulamentação Publicitária, conduzido pelo Conselho Nacional de Autorregulamentação Publicitária (Conar). Embora seja um organismo privado, o Conar atua em consonância com princípios constitucionais e legais na promoção da ética na publicidade, recebendo reconhecimento e funcionando de maneira complementar à regulação estatal, exercida pela Secretaria Nacional do Consumidor (Senacon) do MJSP.

No que respeita ao arranjo institucional a ser aplicado, as discussões e propostas afetas ao PL nº 2.630/2020 têm se inclinado para a designação de um órgão já existente como supervisor do sistema⁶¹ e que seria responsável, entre outras coisas, por opinar sobre códigos de condutas elaborados pelas plataformas e realizar estudos sobre o comportamento do setor, com prefe-

58. FARAH, André. *Desinformação online, liberdade de expressão e democracia: uma proposta de modelo regulatório híbrido*. 1. ed. Rio de Janeiro: Lumen Juris, 2024. p. 190-192.

59. BRASIL. Câmara dos Deputados. *Projeto de Lei nº 2630, de 3 de setembro de 2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet*. Brasília: Câmara dos Deputados, 2020. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735&fichaAmigavel=nao>. Acesso em: 1 nov. 2024.

60. BARROSO, Luna van Brussel. *Liberdade de expressão e democracia na Era Digital: o impacto das mídias sociais no mundo contemporâneo*. 1. reimpressão. Belo Horizonte: Fórum, 2022. p. 167.

61. Apesar de já ter sido prevista a criação, na proposta do Governo Federal de março de 2023, de uma Entidade Autônoma de Supervisão. A Comissão Especial de Direito Digital do Conselho Federal da Ordem dos Advogados do Brasil (OAB), na mesma linha dessa proposta, encaminhou ao relator do projeto sugestão de criação de um órgão regulador das plataformas digitais, o Conselho de Políticas Digitais.

rências para o Comitê Gestor da Internet no Brasil (CGI.br) ou para a Agência Nacional de Telecomunicações (Anatel).

O CGI.br é o órgão colegiado responsável pela coordenação e implementação de ações para a governança da internet no Brasil. Criado pela Portaria Interministerial MCT/MC nº 147, de 1995, e alterado pelo Decreto Presidencial nº 4.829, de 2003, tem a atribuição de estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet e diretrizes para a execução do registro de Nomes de Domínio, alocação de Endereço IP e administração pertinente ao Domínio de Primeiro Nível “.br”. Também promove estudos e recomenda procedimentos para a segurança da internet e propõe programas de pesquisa e desenvolvimento que permitam a manutenção do nível de qualidade técnica e inovação no seu uso.

Incluído, inicialmente, no substitutivo apresentado por grupo de trabalho da Câmara dos Deputados, em dezembro de 2021, o CGI.br é visto como um órgão capaz de fornecer diretrizes e recomendações para a autorregulação das plataformas digitais, com enfoque na liberdade e responsabilidade na internet, sem assumir o papel de fiscalizador ou sancionador, o que preservaria a imparcialidade e a atuação técnica⁶². No entanto, críticas apontam que o CGI.br, em seu atual formato, pode sofrer influência de grandes corporações ou do próprio governo⁶³. Além disso, a falta de poder regulatório e a dependência de um modelo de governança multissetorial pode resultar em uma regulação lenta e ineficaz.

Por sua vez, a Anatel, criada pela Lei nº 9.472, de 1997, é uma entidade integrante da Administração Pública Federal indireta, submetida a regime autárquico especial e vinculada ao Ministério das Comunicações. É administrativamente independente e financeiramente autônoma. A Agência tem por objetivo promover o desenvolvimento das telecomunicações do País de modo a dotá-lo de uma moderna e eficiente infraestrutura de telecomunicações, capaz de oferecer à sociedade serviços adequados, diversificados e a preços justos, em todo o território nacional.

Mencionada pelo relator do PL 2.630/2020 como uma opção alternativa para a regulação de plataformas digitais⁶⁴, a Anatel apresenta, como argu-

62. BARROSO, Luna van Brussel. *Liberdade de expressão e democracia na Era Digital: o impacto das mídias sociais no mundo contemporâneo*. 1. reimpressão. Belo Horizonte: Fórum, 2022. p. 283-284.

63. CONGRESSO EM FOCO. *Bancada evangélica critica participação do CGI no PL das Fake News*. Congresso em Foco, 2 maio 2023. Disponível em: <https://congressoemfoco.uol.com.br/area/congresso-nacional/bancada-evangelica-critica-participacao-do-cgi-no-pl-das-fake-news/>. Acesso em: 26 nov. 2024.

64. CONGRESSO EM FOCO. *Anatel poderá assumir regulação da internet, diz Orlando Silva*. Congresso em Foco, 28 abr. 2023. Disponível em: <https://congressoemfoco.uol.com.br/area/congresso-nacional/ao-vivo-em-instantes-orlando-silva-fala-sobre-o-pl-das-fake-news/>. Acesso em: 26 nov. 2024.

mentos favoráveis, a experiência em gestão regulatória, sua infraestrutura consolidada e competência em áreas como economia, proteção de dados e fiscalização, o que poderia facilitar a aplicação de normas já existentes, com custos menores em comparação à criação de um novo órgão⁶⁵. Além disso, sua experiência em poder de polícia, como mostrado nas ações com o Tribunal Superior Eleitoral (TSE)⁶⁶, seria um ponto positivo. No entanto, as críticas são significativas: além da inadequação de sua estrutura consultiva e decisória, a Anatel não possui especialização em temas como direitos digitais e regulação de conteúdo⁶⁷, além de ter sido alvo de auditorias que apontam ineficiência em suas funções no setor de telecomunicações⁶⁸.

Além dessas entidades, cabe destacar o papel que a Autoridade Nacional de Proteção de Dados (ANPD) poderia ocupar nesse ambiente regulatório. Instituída pela Medida Provisória nº 869, de 2018, convertida na Lei nº 13.853, de 8 de julho de 2019, tem como missão zelar pela proteção de dados pessoais, orientada pela Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD). Embora uma atuação mais ampla na regulação de plataformas digitais possa ir além de sua competência original e poderia impactar sua estrutura e orçamentos, o que se traduziria em comprometimento de seus resultados, a ANPD tem um caráter central nas discussões sobre o combate à desinformação devido à evidente relação entre esse tema e a proteção de dados pessoais, especialmente devido ao uso, pelas plataformas digitais, de sistemas automatizados de moderação de conteúdo⁶⁹.

Ao se sopesar as vantagens e desvantagens dessas alternativas, constata-se que nenhuma delas se adequa plenamente ao objeto a ser regulado, especialmente quando se consideram as recomendações de organismos internacionais sobre as características de uma autoridade reguladora de pla-

65. FREIRE, Alexandre; CAMPOS, Ricardo. *A ANATEL como Ente Regulador de Serviços Digitais*. JOTA, 2 maio 2023. Disponível em: <https://www.jota.info/artigos/a-anatel-como-ente-regulador-de-servicos-digitais>. Acesso em: 22 nov. 2024.

66. SOUZA, Nivaldo. *Anatel segue cotada como órgão regulador das plataformas no PL das Fake News*. JOTA, 2 maio 2023. Disponível em: <https://www.jota.info/legislativo/anatel-segue-cotada-como-orgao-regulador-das-plataformas-no-pl-das-fake-news>. Acesso em: 22 nov. 2024.

67. A Anatel não detém competência nem para regular conteúdo e nem para determinar que prestadoras de serviços de telecomunicações procedam ao bloqueio de textos, imagens, vídeos, nomes de domínio, aplicativos ou quaisquer outros conteúdos que sejam expostos, divulgados ou transmitidos pela internet. Ademais, a regulação e fiscalização do conteúdo dos serviços de radiodifusão e ancilares e do serviço de acesso condicionado são de competência, respectivamente, do Ministério das Comunicações (MCOM) e da Agência Nacional de Cinema (Ancine), conforme disposições da Lei nº 4.117, de 1962, e da Lei nº 12.485, de 2011.

68. COALIZAÇÃO DIREITOS NA REDE. *Órgão independente de supervisão das plataformas é essencial, mas não pode ser Anatel*. CDR, 28 abr. 2023. Disponível em: <https://direitosnarede.org.br/2023/04/28/orgao-independente-de-supervisao-das-plataformas-e-essencial-mas-nao-pode-ser-anatel/>. Acesso em: 22 nov. 2024.

69. BRASIL. Câmara dos Deputados. *Projeto de Lei nº 2630, de 3 de setembro de 2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet*. Brasília: Câmara dos Deputados, 2020. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735&fichaAmigavel=nao>. Acesso em: 12 abr. 2025.

taformas digitais. Na visão da Unesco⁷⁰, por exemplo, tal autoridade deve ser independente, livre de pressões políticas, econômicas ou outras, e responder diretamente aos órgãos legislativos. Sua atuação deve ser revista periodicamente por um órgão independente e sujeito a controle judicial, para garantir a transparência e evitar abusos de poder. A designação de seus membros deve ser participativa e transparente, baseada no mérito, e incluir conhecimentos especializados em direitos humanos e ecossistema digital. Além disso, deve contar com recursos financeiros e competências suficientes para cumprir suas responsabilidades de forma eficaz.

Considerações finais

Por meio deste estudo, foi possível apontar o papel das plataformas digitais na propagação do discurso de ódio e desinformação, bem como conhecer as principais abordagens e estruturas que estão sendo implementadas nas tentativas de promover sua regulação.

Cada modelo de regulação das plataformas digitais tem suas vantagens e desvantagens, e a escolha do modelo mais adequado depende do contexto, da natureza do problema a ser resolvido e da flexibilidade necessária. Modelos como a heterorregulação tendem a ser mais rígidos e tradicionais, enquanto a regulação autorregulação e correção oferecem maior flexibilidade e adaptabilidade, mas podem carecer de mecanismos de fiscalização efetivos. Em muitos casos, uma abordagem híbrida, que combine diferentes modelos, pode ser a mais eficaz para lidar com a complexidade e a rapidez das mudanças no ambiente digital.

Para que a regulação das plataformas digitais seja eficiente, é necessário criar uma autoridade regulatória independente, com autonomia técnica e decisória. Essa autoridade deve ser estruturada de forma a garantir sua imparcialidade e eficiência, por meio de um modelo de governança que envolva a sociedade civil e especialistas nas áreas de direitos humanos e tecnologia. Além disso, é imprescindível que a autoridade tenha recursos financeiros e humanos suficientes para cumprir suas funções, sendo submetida a um controle contínuo para assegurar a transparência e evitar abusos de poder.

No Brasil, os avanços na regulação das plataformas digitais têm sido graduais, mas importantes, especialmente em virtude das recentes iniciativas le-

70. ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA. *Diretrizes para a governança das plataformas digitais: salvaguardar a liberdade de expressão e o acesso à informação com uma abordagem multissetorial*. Paris, 2023. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000387560>. Acesso em: 26 nov. 2024.

gislativas no setor da internet. Os obstáculos enfrentados por essas iniciativas refletem a forte oposição, tanto de setores da sociedade quanto das empresas que dominam o mercado tecnológico, à implementação de mecanismos regulatórios mais rígidos. Em decorrência, desafios significativos ainda persistem, como a necessidade de equilibrar a proteção dos direitos individuais, especialmente a liberdade de expressão, com a eficácia das políticas de combate à desinformação e ao discurso de ódio.

Para superar os obstáculos citados deveria ser considerada, na análise do PL 2.630/2020, a opção de emprego, como autoridade reguladora de plataformas digitais, de um órgão independente e diretamente vinculado ao Poder Legislativo, em observância a recomendações de organismos internacionais. O Conselho de Comunicação Social, órgão auxiliar do Congresso Nacional, previsto no art. 224 da Constituição Federal de 1988 e instituído pela Lei nº 8.389, de 1991, poderia, por exemplo, ser considerado para tal fim, dada sua atual função na comunicação social. Para isso, seria necessário realizar ajustes em sua estrutura e competências, de modo a transformá-lo em um órgão executivo, além de seu caráter consultivo.

Diante do exposto, sugere-se que futuras pesquisas se concentrem na comparação da regulação das plataformas digitais com a dos diversos meios de comunicação de massa e o efeito dessa regulação sobre a liberdade de expressão.

Em síntese, as constatações deste estudo evidenciam a complexidade da regulação das plataformas digitais, o que exige um equilíbrio delicado entre inovação tecnológica, direitos fundamentais e controle social. Entretanto, a urgência em adotar medidas para combater o discurso de ódio e a desinformação nas plataformas digitais é evidente, e sua implementação é um passo necessário e inevitável.

Referências

ABBOUD, Georges; NERY JÚNIOR, Nelson; CAMPOS, Roberto (coord.). *Fake news e regulação*. 3. ed. rev. e ampl. São Paulo: Thomson Reuters Brasil, 2021. 448p. ISBN 978-65-5614-752-9.

ARTIGO 19. *Nota Técnica Projeto de Lei nº 2.630/2020*. São Paulo, 2020. Disponível em: <https://artigo19.org/2020/08/07/pl-das-fake-news-nota-tecnica-indica-que-atual-proposta-traria-mais-riscos-do-que-beneficios-para-o-combate-as-noticias-falsas/>. Acesso em: 12 abr. 2025.

BARROSO, Luna van Brussel. *Liberdade de expressão e democracia na Era Digital: o impacto das mídias sociais no mundo contemporâneo*. 1. reimpressão. Belo Horizonte: Fórum, 2022. 327 p. ISBN 978-65-5518-342-9.

BELLI, Luca; ZINGALES, Nicolo. *Platform regulations: how platforms are regulated and how they regulate us. Official outcome of the UN IGF Dynamic Coalition on Platform Responsibility*. 1 ed. Rio de Janeiro: FGV Direito Rio, 2023. 250 p. ISBN 978-85-9597-014-4. Disponível em: <https://repositorio.fgv.br/bitstreams/6a797886-d84e-4e7e-9a3f-71579fd1d70a/download>.

BRADFORD, Anu. *The Brussels Effect: How the European Union Rules the World*. Nova Iorque: Oxford University Press, 2020.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 2630, de 3 de setembro de 2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet*. Brasília: Câmara dos Deputados, 2020. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735&fichaAmigavel=nao>. Acesso em: 1 nov. 2024.

CAMPOS, Ricardo (org.). *O futuro da regulação de plataformas digitais: Digital Services Act (DAS), Digital Markets Act (DMA) e seus impactos no Brasil*. 1. ed. São Paulo: Editora Contracorrente, 2023. 778 p. ISBN 978-65-5396-146-3.

CASTRO, Ricardo Medeiros de; FONSECA, Gabriel Campos Soares da; BRANCO, Pedro Henrique de Moura Gonet. *Estudo sobre cenários de conformação institucional regulatória do ecossistema digital: versão final*. Brasília, 2024, e-book. (1 recurso online 827p).

COALIZAÇÃO DIREITOS NA REDE. *PL 2630/20: propostas da CDR para uma lei efetiva e democrática*. CDR, 1 set. 2020. Disponível em: <https://direitosnarede.org.br/2020/09/01/pl-2630-propostas-da-cdr-para-uma-lei-efetiva-e-democratica/>. Acesso em: 12 abr. 2025.

COALIZÃO DIREITOS NA REDE. *Órgão independente de supervisão das plataformas é essencial, mas não pode ser Anatel*. CDR, 28 abr. 2023. Disponível em: <https://direitosnarede.org.br/2023/04/28/orgao-independente-de-supervisao-das-plataformas-e-essencial-mas-nao-pode-ser-anatel/>. Acesso em: 22 nov. 2024.

CONGRESSIONAL RESEARCH SERVICE. *Section 230: An Overview*. Washington, 2024. Disponível em: <https://www.congress.gov/crs-product/R46751>. Acesso em: 11 abr. 2025.

CONGRESSO EM FOCO. *Bancada evangélica critica participação do CGI no PL das Fake News*. Congresso em Foco, 2 maio 2023. Disponível em: <https://congressoemfoco.uol.com.br/area/congresso-nacional/bancada-evangelica-critica-participacao-do-cgi-no-pl-das-fake-news/>. Acesso em: 26 nov. 2024.

CONGRESSO EM FOCO. *Anatel poderá assumir regulação da internet, diz Orlando Silva*. Congresso em Foco, 28 abr. 2023. Disponível em: <https://congressoemfoco.uol.com.br/area/congresso-nacional/ao-vivo-em-instantes-orlando-silva-fala-sobre-o-pl-das-fake-news/>. Acesso em: 26 nov. 2024.

EMPOLI, Giuliano Da. *Os engenheiros do caos*. 1. ed. 1. reimp. São Paulo: Vestígio, 2020. 190 p. ISBN 978-85-54126-60-5.

FARAH, André. *Desinformação online, liberdade de expressão e democracia: uma proposta de modelo regulatório híbrido*. 1. ed. Rio de Janeiro: Lumen Juris, 2024. 338 p. ISBN 978-85-519-3048-9.

FISHER, Max. *A máquina do caos: como as redes sociais reprogramam nossa mente e nosso mundo*. 1. ed. São Paulo: Todavia, 2023. 544 p. ISBN 978-65-569-2400-7.

FLEW, Terry; MARTIN, Fiona R. *Digital Platform Regulation: global perspectives on internet governance*. 1. ed.. Cham: Palgrave Macmillan, 2022. 327 p. ISBN 978-3-030-95220-4. Disponível em: <https://doi.org/10.1007/978-3-030-95220-4>.

FREIRE, Alexandre; CAMPOS, Ricardo. *A ANATEL como Ente Regulador de Serviços Digitais*. JOTA, 2 maio 2023. Disponível em: <https://www.jota.info/artigos/a-anatel-como-ente-regulador-de-servicos-digitais>. Acesso em: 22 nov. 2024.

GIL, Antonio Carlos. *Como elaborar projetos de pesquisa*. 4. ed. São Paulo: Atlas, 2008. 176 p. ISBN 85-224-3169-8.

GLEICK, James. *A informação: Uma história, uma teoria, uma enxurrada*. 1. ed. São Paulo: Companhia das Letras, 2013. 521 p. ISBN 978-85-359-2266-0.

HARARI, Yuval Noah. *Nexus: Uma breve história das redes de informação, da Idade da Pedra à inteligência artificial*. 1. ed. São Paulo: Companhia das Letras, 2024. 497 p. ISBN 978-85-359-3781-7.

INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO. *Nota Técnica sobre os PLS 2927/2020 e PL 2630/2020*. Rio de Janeiro, 2020. Disponível em: <https://itsrio.org/pt/publicacoes/nota-tecnica-its-pls-contrafake-news/>. Acesso em: 12 abr. 2025.

JESUS-SILVA, Thiago Henrique de. *Desinformação e economia política nas plataformas digitais*. Lumina, v. 18, n. 3, p. 117-134, 2024. Disponível em: <https://periodicos.ufjf.br/index.php/lumina/article/view/44963>. Acesso em: 11 abr. 2025.

KANTAR IBOPE MEDIA. Kantar Ibope Media, 2024. *Audiência de vídeo*. Disponível em: <https://kantaribopemedia.com/audiencia-de-video/>. Acesso em: 1 nov. 2024.

KEMP, Simon. *Digital 2024: 5 billion social media users*. Disponível em: <https://wearesocial.com/us/blog/2024/01/digital-2024-5-billion-social-media-users/>. Acesso em: 1 nov. 2024.

LEVITSKY, Steven; ZIBLATT, Daniel. *Como as democracias morrem*. 1. ed. Rio de Janeiro: Zahar, 2018. 270 p. ISBN 978-85-378-1800-8.

LONGHI, João Victor Rozatti. *Responsabilidade Civil e Redes Sociais: retirada de conteúdo, perfis falsos, discurso de ódio, fake news e milícias digitais*. 2. ed. Indaiatuba: Editora Foco, 2022. 296 p. ISBN 978-65-5515-595-2.

MARTINS, Helena. *A desinformação em meio à crise do capitalismo e à configuração de uma nova estrutura de mediação social*. Revista Eco-Pós, v. 27, n. 1, p. 330-352, 2024. Disponível em: <https://doi.org/10.29146/eco-ps.v27i1.28045>. Acesso em: 11 abr. 2025.

MENEZES, Paulo Brasil. *Fake News: Modernidade, Metodologia, Regulação e Responsabilização*. 5. ed., rev., ampl. e atual. São Paulo: Editora JusPodivm, 2024. 560 p. ISBN 978-85-442-5406-6.

MÜLLER, Jan-Werner. *Democracy Rules*. Nova Iorque: Farrar, Straus and Giroux, 2021.

NAÇÕES UNIDAS. *The UN Strategy and Plan of Action on Hate Speech*. Nova Iorque, 2019. Disponível em: <https://www.un.org/en/hate-speech/un-strategy-and-plan-of-action-on-hate-speech>. Acesso em: 4 nov. 2024.

NAZARENO, Claudio; PINHEIRO, Guilherme Pereira. *Regulação de plataformas, Fake News e o PL 2630/2020*. Brasília: Câmara dos Deputados, Consultoria Legislativa, 2023. 20 p. Disponível em: <https://bd.camara.leg.br/bd/handle/bdcamara/41234>. Acesso em: 29 out. 2024.

SOUZA, Nivaldo. *Anatel segue cotada como órgão regulador das plataformas no PL das Fake News*. JOTA, 2 maio 2023. Disponível em: <https://www.jota.info/legislativo/anatel-segue-cotada-como-orgao-regulador-das-plataformas-no-pl-das-fake-news>. Acesso em: 22 nov. 2024.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA. *Diretrizes para a governança das plataformas digitais: salvaguardar a liberdade de expressão e o acesso à informação com uma abordagem multissetorial*. Paris, 2023. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000387560>. Acesso em: 26 nov. 2024.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA. *Jornalismo, Fake News e Desinformação: manual para educação e treinamento em jornalismo*. Paris, 2019. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000368647>. Acesso em: 09 abr. 2025.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. *An Introduction to Online Platforms and Their Role in the Digital Transformation*. Paris, 2019. Disponível em: <https://doi.org/10.1787/53e5f593-en>. Acesso em: 4 nov. 2024.

SARAVIA, Enrique; MARTINS, Paulo Emílio Matos; PIERANTI, Octavio Penna (orgs.). *Democracia e regulação dos meios de comunicação de massa*. 1. ed. Rio de Janeiro: Editora FGV, 2008. 276 p. ISBN 978-85-225-0664-4.

SCHOLZE, Simone Henriqueta Cossetin; VIEIRA, Vania Lucia Ribeiro; AGUIAR, Alexandre Kehrig Veronese. *Estudo sobre modelo regulatório pró-inovação*. 2024. e-Book. (1 recurso online 304 p).

TYAGI, Kalpana; SANDERS, Anselm Kamperman; CAUFFMAN, Caroline. *Digital Platforms, Competition Law, and Regulation: Comparative Perspectives*. 1. ed.. Oxford: Hart Publishing, 2024. 297 p. ISBN 978-1-50996-940-1. Disponível em: <https://library.oapen.org/handle/20.500.12657/88175>.

TZU, Sun. *A arte da guerra: edição completa bilíngue com os 13 capítulos originais*. 1. ed. São Paulo: Edipro, 2021. ISBN 978-65-5660-049-9.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

3

Políticos em rede: desafios constitucionais no tratamento de perfis de interesse público nas redes sociais

CAROLINA FREITAS GOMIDE DE ARAUJO

Sumário: Introdução. 1. O filtro da Meta: a autorregulação no tabuleiro político. 2. O filtro do Estado: o caminho da regulação brasileira. Considerações finais. Referências.

Introdução

Em 2021, a suspensão das contas de Donald Trump nas redes sociais, motivada pela publicação de conteúdos considerados incitadores de violência durante e após o ataque ao Capitólio dos Estados Unidos, gerou um intenso debate sobre o papel das plataformas digitais na moderação do discurso político e seus impactos na democracia. A decisão de banir um líder mundial de redes como Twitter e Facebook suscitou uma reflexão global sobre os limites da liberdade de expressão e a necessidade de proteger o sistema democrático de manifestações que possam incitar violência ou desinformação.

A situação levantou uma questão central: até que ponto a restrição do discurso de figuras políticas nas redes sociais pode ser compatível com a preservação da democracia e a proteção da liberdade de expressão?

No entanto, essa pergunta pode ser respondida de forma diferente pelos dois principais agentes envolvidos na resposta: as plataformas digitais e o Estado.

As plataformas digitais, que desempenham um papel crucial na comunicação política, passaram a ser vistas como árbitros de um jogo fundamental: a interação entre políticos e seus eleitores. Esse poder de moderação pode impactar diretamente as campanhas eleitorais, o pluralismo político e o direito de participação do eleitorado. Por isso, se as plataformas têm autonomia para decidir sobre o que pode ou não ser postado, suas decisões podem ter implicações profundas no processo democrático. Isso torna essencial uma reflexão sobre os limites dessa moderação e a natureza dos tratamentos diferenciados aplicados às contas de políticos dentro do escopo da autorregulação.

No contexto do Estado brasileiro, o bloqueio de perfis de políticos, especialmente durante períodos eleitorais, tem sido tratado pelos tribunais como uma medida necessária para proteger a ordem democrática. Diferente de outros países, onde a intervenção estatal poderia ser vista como censura, o ju-

1. Mestre em Direito do Estado pela Faculdade de Direito da Universidade de São Paulo (USP). Pós-graduanda em Direito Digital na UERJ/ITS. Pesquisadora visitante na Queen's University, Canadá. Autora dos livros "Cortes Constitucionais Digitais" e "Poder Constituinte Originário das Mulheres no Brasil". Advogada.

diciário brasileiro tem, em diversos casos, entendido pela constitucionalidade da exclusão de perfis políticos em nome da defesa da democracia e da integridade do processo eleitoral.

No campo legislativo, o debate tem avançado com propostas como o Projeto de Lei 2.630/20, que busca regulamentar a questão e sugere um modelo de autorregulação regulada.

Assim, este artigo tem como objetivo compreender como as plataformas digitais e o Estado enfrentam os desafios da moderação de conteúdo em perfis políticos, considerando o equilíbrio entre a garantia da liberdade de expressão e os riscos da disseminação de discursos antidemocráticos em perfis de grande alcance, especialmente os de políticos.

Em síntese, o artigo busca responder à seguinte questão: quais restrições e garantias existem ou estão em debate para a regulação dos discursos políticos pelas plataformas digitais e pelo Estado?

Para tanto, adota-se uma metodologia que combina revisão bibliográfica, análise documental das políticas de moderação de conteúdo da Meta e exame de decisões judiciais e projetos de lei relacionados ao tema no Brasil.

Este estudo, portanto, busca compreender e analisar essas questões a partir de duas perspectivas principais. O primeiro tópico examina as políticas de moderação da Meta, com foco no tratamento dado aos perfis de políticos no contexto de sua autorregulação. Já o segundo tópico explora a posição do Estado brasileiro, analisando decisões judiciais e debates legislativos relacionados ao tratamento de perfis de políticos e partidos no país.

1. O filtro da Meta: a autorregulação no tabuleiro político

Atualmente, um terço da população mundial está no Facebook. As políticas e diretrizes da empresa são aplicáveis a indivíduos de diferentes etnias, gêneros, credos e origens. No entanto, uma análise mais detalhada revela que nem todos os usuários são tratados de forma igualitária nas plataformas da Meta (Instagram e Facebook)², incluindo as contas de políticos.

As próprias regras de conteúdo podem ser diferenciadas entre os usuários, como é o caso da política de Bullying e Assédio, que estabelece regras distintas para proteger pessoas públicas e não públicas de ataques online.³

2. CRUZ, Francisco Brito (Coord.); LANA, Alice; JOST, Iná. Iguais perante as plataformas? Equidade e transparência na moderação de conteúdo em plataformas digitais. *Diagnósticos & Recomendações*, n. 9, jul. 2023.

3. COMITÊ DE SUPERVISÃO DA META. 2021-004-FB-UA – Protestos a favor de Navalny na Rússia. Disponível em: <https://www.oversightboard.com/decision/fb-6yhrxhzr/?lang=pt-br>. Acesso em: 15.01.2025.

No que se refere ao tratamento específico de chefes de Estado, por exemplo, a empresa considera que ameaças de morte a esses indivíduos, ao contrário do que ocorre com outras pessoas, não deveriam ser removidas da plataforma, pois poderiam estar relacionadas a protestos ou movimentos políticos. Um exemplo disso é o caso Slogan de protesto no Irã, onde o Comitê de Supervisão da Meta, órgão responsável por decisões finais em casos complexos de moderação de conteúdo, concluiu que “*marg bar Khamenei*”, traduzido literalmente como “morte ao Khamenei” ou, retoricamente, como “abaixo o Khamenei”, não violaria a política de violência e incitação.⁴

Outra diferença no tratamento das contas de figuras públicas nas plataformas da Meta refere-se à aplicação da chamada “tolerância de interesse público”, a qual permite que conteúdos que, embora violem as políticas da comunidade, permaneçam na plataforma por serem considerados de utilidade pública. Segundo a Meta, embora o orador possa ser um fator importante na análise de se o conteúdo ganhará essa proteção, a empresa não presume que o discurso de políticos seja inerentemente sujeito à tolerância. Ao seu Comitê de Supervisão, no caso Primeiro-ministro do Camboja, a Meta informou que apenas 20% dos conteúdos aos quais foi aplicada essa tolerância, entre junho de 2021 e 2022, foram publicados por políticos.⁵

Além da diferenciação em relação ao tipo de conteúdo permitido para perfis associados à figuras públicas, como políticos, outra distinção aplicada a essas contas está no sistema de revisão, responsável por avaliar se determinado conteúdo viola os padrões da comunidade.

As contas de políticos podem ser submetidas a um sistema chamado de verificação cruzada, cuja ideia, em síntese, é adicionar proteção extra contra possíveis erros de moderação para algumas contas ou conteúdos selecionados antes que uma decisão seja tomada. Bastante criticado, o sistema de verificação cruzada ficou conhecido como o modelo de moderação para VIPs após o vazamento dos chamados Facebook Papers, no segundo semestre de 2021, pela *whistleblower* Frances Haugen.⁶

Esse sistema não é aplicado apenas a contas de políticos e nada indica que todos os políticos recebam esse tratamento diferenciado. Inclusive, segundo a central de transparência da Meta, em outubro de 2021, cerca de 660.000

4. COMITÊ DE SUPERVISÃO DA META. 2022-013-FB-UA – Slogan de protesto no Irã. Disponível em: <https://www.oversightboard.com/decision/fb-zt6ajs4x/?lang=pt-br>. Acesso em: 15.01.2025.

5. COMITÊ DE SUPERVISÃO DA META. 2023-003-FB-MR – Primeiro-ministro do Camboja. Disponível em: <https://www.oversightboard.com/decision/fb-6okjpns3/?lang=pt-br>. Acesso em: 30.05.2024.

6. MILMO, Dan. Facebook revelations: what is in cache of internal documents? The Guardian. Disponível em: <https://www.theguardian.com/technology/2021/oct/25/facebook-revelations-from-misinformation-to-mental-health>. Acesso em 15.01.2025

usuários estavam incluídos na lista de beneficiados com o sistema de verificação cruzada, sendo que nem todos eram políticos.⁷

Por fim, no que diz respeito às sanções que políticos podem sofrer nas plataformas da empresa, é evidente a possibilidade de bloqueio ou suspensão de contas, como exemplificado pelo notório caso de Donald Trump, respaldado pelo Comitê de Supervisão da Meta como uma política adequada a ser adotada pela empresa.

Na ocasião, no entanto, o Comitê de Supervisão da Meta entendeu que não seria possível realizar suspensões ilimitadas, uma vez que isso violaria os direitos humanos, e recomendou que a Meta explicasse seu processo de penalidades nos padrões de comunidade do Facebook e nas diretrizes da comunidade do Instagram, fornecendo aos usuários informações claras sobre as consequências de futuras violações às regras da plataforma.⁸

Considerando a impossibilidade de suspensão de contas por tempo indefinido, conforme entendimento do Comitê, a Meta anunciou em 4 de junho de 2021 que a suspensão de Donald Trump duraria dois anos, com a possibilidade de extensão, caso fosse constatado que ainda existiria um risco para a segurança pública.⁹

Com base nessas regras, o Facebook optou, em 25 de janeiro de 2023, após o período de suspensão de dois anos, por permitir o retorno de Donald Trump à plataforma. A Meta justificou a decisão com a seguinte explicação:¹⁰

A suspensão foi uma decisão extraordinária tomada em circunstâncias extraordinárias. O estado normal das coisas é que o público deve poder ouvir um ex-presidente dos Estados Unidos e um candidato declarado a esse cargo novamente, em nossas plataformas. Agora que o período de suspensão terminou, a questão não é se escolhemos restabelecer as contas do Sr. Trump, mas se ainda existem circunstâncias tão extraordinárias que justifiquem a prorrogação da suspensão além do período original de dois anos.

Para avaliar se o risco grave à segurança pública que existia em janeiro de 2021 diminuiu suficientemente, avaliamos o ambiente atual de acordo com nosso Protocolo de Política de Crise, que in-

7. ZIADY, Hanna. *Facebook kept its own oversight board in the dark on program for VIP users*. Disponível em: <https://edition.cnn.com/2021/10/21/tech/facebook-cross-check-oversight-board/index.html>. Acesso em: 15.01.2025.

8. COMITÊ DE SUPERVISÃO DA META. 2021-001-FB-FBR – *Suspensão do ex-presidente Trump*. Disponível em: <https://www.oversightboard.com/decision/fb-691qamhj/?lang=pt-br>. Acesso em: 15.01.2025.

9. CLEG, Nick. *In Response to Oversight Board, Trump Suspended for Two Years; Will Only Be Reinstated if Conditions Permit*. Meta. 2021. Disponível em: https://about.fb.com/news/2021/06/facebook-response-to-oversight-board-recommendations-trump/?utm_source=chatgpt.com. Acesso em: 15.01.2024

10. CLEG, Nick. *Ending Suspension of Trump's Accounts With New Guardrails to Deter Repeat Offenses*. Meta. 2023. Disponível em: <https://about.fb.com/news/2023/01/trump-facebook-instagram-account-suspension/>. Acesso em: 15.01.2024

cluiu a análise da condução das eleições de meio de mandato nos EUA em 2022 e avaliações de especialistas sobre o ambiente de segurança atual. Nossa determinação é que o risco diminuiu suficientemente, e, portanto, devemos cumprir o prazo de dois anos que estabelecemos. Como tal, estaremos restabelecendo as contas do Sr. Trump no Facebook e Instagram nas próximas semanas. No entanto, estamos fazendo isso com novas salvaguardas para evitar reincidências.

À época, a Meta divulgou que as contas de Trump enfrentariam penalidades aumentadas em caso de reincidência. Caso ele postasse conteúdo que violasse as políticas de conteúdo novamente, o conteúdo seria removido e a conta suspensa mais uma vez por um período de um mês a dois anos, dependendo da gravidade da violação.¹¹

No entanto, em julho de 2024, a Meta divulgou uma mudança em relação ao entendimento sobre a reincidência da conduta de Donald Trump, apontando que:¹²

Com as convenções partidárias se aproximando, incluindo a convenção republicana na próxima semana, os candidatos à Presidência dos Estados Unidos serão em breve formalmente nomeados. Ao avaliar nossa responsabilidade de permitir a expressão política, acreditamos que o povo americano deve poder ouvir os indicados à Presidência nas mesmas condições. Como resultado, o ex-presidente Trump, como candidato do Partido Republicano, não estará mais sujeito às penalidades de suspensão aumentadas. Ao chegar a essa conclusão, também consideramos que essas penalidades foram uma resposta a circunstâncias extremas e extraordinárias, e não precisaram ser aplicadas. Todos os candidatos à Presidência dos EUA continuam sujeitos aos mesmos Padrões da Comunidade que todos os usuários do Facebook e Instagram, incluindo as políticas destinadas a prevenir discursos de ódio e incitação à violência.

Para além do caso Trump, mas também em decorrência dele, a Meta mantém atualmente um sistema de contagem de advertências, possuindo um procedimento padrão de consequências quando determinado número de advertências for alcançado.¹³

11. CLEG, Nick. *Ending Suspension of Trump's Accounts With New Guardrails to Deter Repeat Offenses*. Meta, 2023. Disponível em: <https://about.fb.com/news/2023/01/trump-facebook-instagram-account-suspension/>. Acesso em: 15.01.2024

12. CLEG, Nick. *Ending Suspension of Trump's Accounts With New Guardrails to Deter Repeat Offenses*. Meta, 2023. Disponível em: <https://about.fb.com/news/2023/01/trump-facebook-instagram-account-suspension/>. Acesso em: 15.01.2025

13. META. *Restrição de usuários*. Disponível em: <https://transparency.meta.com/pt-br/enforcement/taking-action/restricting-accounts/>. Acesso em: 15.01.2025

Ademais, também em resposta ao caso Trump, a Meta desenvolveu uma política sobre a restrição de contas de figuras públicas durante agitações civis. A política definiu o conceito de figuras públicas como: “representantes do governo estadual ou nacional, candidatos políticos a esses cargos, pessoas com mais de um milhão de fãs ou seguidores nas redes sociais e pessoas que recebem cobertura substancial de notícias.”¹⁴

A política criada pela Meta determina que em casos de violência ou distúrbios civis contínuos, é possível aplicar restrições diferenciadas para contas de figuras públicas considerando: (i) a gravidade da violação e o histórico da figura pública no Facebook ou no Instagram, incluindo violações atuais e anteriores; (ii) o potencial de influência da figura pública sobre pessoas envolvidas em atos de violência e a relação com elas e (iii) a gravidade dos atos de violência e qualquer lesão corporal relacionada.

Essa política foi interpretada pelo Comitê de Supervisão da Meta no caso Primeiro-ministro do Camboja e resultou em uma recomendação para a suspensão da conta do político. O Comitê entendeu que a repressão política e os atos de violência contra adversários durante os preparativos para as eleições de 2023 no país configuraram ações de violência em andamento, apontando que:¹⁵

A Meta deve esclarecer que a sua política sobre a restrição de contas de figuras públicas é aplicável em contextos nos quais cidadãos estão sob ameaça contínua de violência retaliatória pelo governo. A política deve deixar claro que não se restringe apenas a incidentes isolados de agitação civil e violência, mas é aplicável também quando o governo suprime manifestações políticas preventivamente ou reage a elas com violência ou ameaças de violência.

Embora o Comitê tenha recomendado a suspensão do primeiro-ministro, a Meta optou por não acatar a sugestão, mantendo a conta do político ativa na plataforma.¹⁶

A postura da Meta em relação à moderação de contas de figuras públicas parece ser influenciada, em parte, pelas mudanças na presidência dos Estados Unidos. Essa flexibilidade, embora reflita um ajuste às circunstâncias políticas

14. META Transparency Center. *Restrição de contas de figuras públicas durante agitações civis*. Disponível em: <https://transparency.meta.com/pt-br/enforcement/taking-action/restricting-accounts-by-public-figures>. Acesso em: 15.01.2025.

15. COMITÊ DE SUPERVISÃO DA META. 2023-003-FB-MR – *Primeiro-ministro do Camboja*. Disponível em: <https://www.oversightboard.com/decision/fb-6okjpns3/?lang=pt-br>. Acesso em: 15.01.2025.

16. REUTERS. *Meta rejects recommendation to suspend former Cambodia PM from Facebook*. 2023. Disponível em: <https://www.reuters.com/world/asia-pacific/meta-rejects-recommendation-suspend-former-cambodia-pm-from-facebook-2023-08-30/>. Acesso em: 15.01.2025.

internas, destaca a necessidade de uma regulação mais clara e consistente, tanto nos Estados Unidos quanto em outros contextos globais.

No Brasil, por exemplo, a regulação das contas de interesse público nas redes sociais e a atuação do judiciário nesse campo tornam-se questões centrais para garantir a preservação dos valores democráticos. No próximo tópico, serão abordadas as discussões regulatórias e a atuação do judiciário brasileiro no que se refere à moderação de contas de políticos nas plataformas digitais.

2. O filtro do Estado: o caminho da regulação brasileira

Este tópico visa delinear as principais discussões na legislação e jurisprudência brasileiras sobre o tratamento das contas de interesse público nas plataformas de redes sociais. Embora a regulamentação ainda não tenha sido estabelecida, o judiciário brasileiro está construindo um posicionamento sobre a imunidade parlamentar, a moderação de conteúdo e, também, sobre a constitucionalidade do bloqueio de contas e sua caracterização como censura prévia.

A principal discussão sobre a constitucionalidade do bloqueio de usuários na jurisprudência brasileira ocorreu no âmbito do chamado Inquérito das Fake News (INQ. 4781), criado pelo ministro Dias Toffoli, com relatoria do ministro Alexandre de Moraes. O objetivo era investigar a existência de uma rede virtual de notícias fraudulentas e ataques contra o STF, seus ministros e familiares.¹⁷

Embora o caso não trate somente de contas de políticos, ele trouxe importantes parâmetros sobre a constitucionalidade do bloqueio de perfis em redes sociais quando determinada pelo judiciário. Isso porque, no contexto do inquérito, o ministro Alexandre de Moraes determinou o bloqueio das contas de diversos usuários suspeitos de ataques ao STF e seus ministros, como Roberto Jefferson e Sarah Winter, ambos apoiadores de Jair Bolsonaro e que se enquadrariam no conceito de figuras públicas da Meta.¹⁸

Após a ordem ser cumprida pelas plataformas, as contas apareceram com a mensagem: “Suspensa no Brasil devido a uma ordem judicial”.¹⁹

No entanto, apesar das contas terem tido o acesso inviabilizado no Brasil, subterfúgios de geolocalização possibilitaram que os perfis fossem acessa-

17. CURVELO, Erick. Liberdade de expressão 2.0: a constitucionalidade dos casos de deplatforming no Inquérito das Fake News. *Internet & Sociedade*, v. 1, n. 3, jun. 2021.

18. CURVELO, Erick. Liberdade de expressão 2.0: a constitucionalidade dos casos de deplatforming no Inquérito das Fake News. *Internet & Sociedade*, v. 1, n. 3, jun. 2021.

19. RIBEIRO, G. F. *Conta bolsonarista bloqueada acusa STF de golpe; entenda como a Corte agiu*. UOL. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/07/24/contas-bolsonaristas-suspensas-veja-posts-usados-de-exemplo-em-a-cao-do-stf.htm>. Acesso em: 15.01.2025.

dos através de endereços IP fora do país²⁰, o que levou o ministro Alexandre de Moraes a considerar a ordem parcialmente cumprida, determinando que a decisão anterior deveria ser cumprida de forma integral, “independentemente do acesso a essas postagens se dar por qualquer meio ou qualquer IP, seja do Brasil ou fora dele”.²¹

O Facebook demonstrou indignação e informou que a determinação judicial extrapolaria os limites da jurisdição brasileira. Em resposta, o Ministro Alexandre de Moraes proferiu nova decisão, afirmando que²²:

A suspensão – repita-se, em relação a fatos pretéritos – deve ser total e absoluta, configurando-se descumprimento a permissão dada pelo provedor implicado para a continuidade de divulgação das contas bloqueadas no Brasil, a partir de acessos em outros países. Não se discute a questão de jurisdição nacional sobre o que é postado e visualizado no exterior, mas sim a divulgação de fatos criminosos no território nacional, por meio de notícias e comentários por contas que se determinou o bloqueio judicial. Ou seja, em momento algum se determinou o bloqueio de divulgação no exterior, mas o efetivo bloqueio de contas e divulgação de suas mensagens ilícitas no território nacional, não importando o local de origem da postagem.

Após essa nova decisão, que também aumentou a multa imposta ao Facebook, a empresa anunciou o bloqueio global das contas indicadas, declarando que: “a mais recente ordem judicial é extrema, representando riscos à liberdade de expressão fora da jurisdição brasileira e em conflito com leis e jurisdições ao redor do mundo”.²³

No entanto, as empresas não foram as únicas a reagir à decisão do ministro Alexandre de Moraes. O então presidente Jair Bolsonaro anunciou no Twitter que, por meio da Advocacia Geral da União, ajuizou a Ação Direta de Inconstitucionalidade 6.494 para questionar a constitucionalidade dos bloqueios de contas em redes sociais.

Na Ação Direta de Inconstitucionalidade, sustenta-se que o tribunal deve conferir uma interpretação conforme à Constituição aos artigos 282, I e II, e

20. CURVELO, Erick. Liberdade de expressão 2.0: a constitucionalidade dos casos de deplatforming no Inquérito das Fake News. *Internet & Sociedade*, v. 1, n. 3, jun. 2021.

21. SUPREMO TRIBUNAL FEDERAL. *Inquérito 4781*. Disponível em: <https://www.conjur.com.br/dl/decisao-alexandre-moraes-twitter.pdf>. Acesso em: 15.01.2025

22. SUPREMO TRIBUNAL FEDERAL. *Inquérito 4781*. Disponível em: <https://www.conjur.com.br/dl/decisao-alexandre-moraes-twitter.pdf>. Acesso em: 15.01.2025

23. MERCIER, D. *Pressionado por STF, Facebook bloqueia globalmente contas de apoiadores de Bolsonaro*. El País Brasil. Disponível em: <https://brasil.elpais.com/brasil/2020-08-01/pressionado-por-stf-facebook-bloqueia-globalmente-contas-de-apoiadores-de-bolsonaro.html>. Acesso em: 15.01.2025.

319, II e III, do Código de Processo Penal, bem como aos artigos 15, 19 e 22 do Marco Civil da Internet. Alega-se existir violação à Constituição Federal, nomeadamente à liberdade de manifestação do pensamento (art. 5º, IV e IX, da CRFB/1988), ao livre exercício profissional (art. 5º, XIII, da CRFB/1988) e à cláusula de imunidade material parlamentar (art. 53, caput, da CRFB/1988).

A ação, de relatoria do Ministro Edson Fachin, aguarda julgamento pelo STF.

No entanto, esse não foi o único caso em que a discussão quanto à constitucionalidade dos bloqueios foi levada à Suprema Corte. O posicionamento do tribunal pela constitucionalidade já foi consagrado em caso já julgado pelo plenário.

Na Petição 10.391, o plenário do STF decidiu por maioria manter a decisão do ministro Alexandre de Moraes pela constitucionalidade do bloqueio de contas do Partido da Causa Operária (PCO).

O bloqueio das contas de redes sociais do PCO havia sido determinado monocraticamente em razão de postagens em que o partido pedia a dissolução do STF e atribuía a seus ministros a prática de atos ilícitos. Em sede de agravo, as plataformas alegaram que a medida seria desproporcional e representaria censura, requerendo que fossem indicadas postagens específicas incompatíveis com a Constituição para que fossem removidas.

O plenário do STF, em sua maioria, votou por manter a decisão monocrática do ministro Alexandre de Moraes. Votaram nesse sentido os ministros Gilmar Mendes, Ricardo Lewandowski, Dias Toffoli, Luiz Fux, Luís Roberto Barroso, Edson Fachin, e as ministras Cármen Lúcia e Rosa Weber. Divergiram os ministros Nunes Marques e André Mendonça, que entenderam que o bloqueio das contas nas plataformas configurava censura prévia e contrariava a garantia da liberdade de expressão.

O julgamento foi realizado em plenário virtual e, além do voto do relator, o único voto adicionado à maioria foi o da ministra Rosa Weber. Um ponto interessante desse voto é que, embora tenha votado pela manutenção do bloqueio dos perfis do partido, a ministra destacou que sua decisão se baseava em razões específicas relacionadas à defesa da democracia no caso concreto, deixando claro que seu posicionamento não deveria ser interpretado como uma tese jurídica. Disse a ministra:

Tenho para mim, no entanto, que a relevante questão constitucional suscitada pela parte recorrente reclama maiores reflexões e um debate mais aprofundado no âmbito desta Suprema Corte, debate esse que se mostra incompatível com os naturais limites

derivados do julgamento estritamente virtual. Cuida-se de tema sensível envolvendo pontos de atrito entre valores constitucionais, ora situados em rota de colisão, que ainda não se acha maduro o suficiente para receber, neste específico procedimento cautelar, ora sob julgamento eletrônico, uma solução definitiva desta casa. (...)

Sendo assim, e consideradas as particularidades do caso concreto – expostas no decisum adversado –, acompanho o voto proferido pelo eminente relator, sem firmar, no entanto, tese jurídica a respeito.

Em relação aos ministros que divergiram, ambos apresentaram votos destacados. O ministro Nunes Marques, ao justificar seu posicionamento, afirmou que:

Em síntese, a derrubada de perfis, contas ou canais em redes sociais acaba por afastar, também e completamente, o direito de exposição de ideias com conteúdos lícitos nos mais diversos campos (político, econômico, social, jurídico, histórico, cultural, entre inúmeros outros). Tal medida, além de caracterizar inadmissível censura prévia (art. 220, § 2º, da CF), retira o indivíduo das redes sociais, ambiente de expressão dos direitos inerentes à personalidade, em verdadeiro banimento ou degredo do mundo digital. Mais adequado, portanto, seria excluir apenas o conteúdo eivado de ilicitude.

Mais especificamente quanto à imunidade parlamentar em redes sociais e à possibilidade de bloqueio de contas de políticos, o Supremo Tribunal Federal entende que a imunidade parlamentar se limita a manifestações que guardem relação com o exercício da função legislativa ou que sejam proferidas em razão dela. Nesse contexto, destaca-se o caso do deputado Daniel Silveira que, após vídeo incitando a animosidade entre as Forças Armadas e o STF, teve suas contas nas redes sociais bloqueadas, sua imunidade parlamentar afastada e a denúncia em ação penal recebida, sob o fundamento de que:

A Constituição Federal não permite a propagação de ideias contrárias à ordem constitucional e ao Estado Democrático (CF, artigos 5º, XLIV; e 34, III e IV), tampouco a realização de manifestações nas redes sociais visando ao rompimento do Estado de Direito, com a extinção das cláusulas pétreas constitucionais – Separação de Poderes (CF, artigo 60, § 4º), com a consequente instalação do arbítrio.

A literatura sobre a constitucionalidade da prática ainda é incipiente, mas Roberta Nascimento e Hugo Kalil, concordando com o argumento trazido na Ação Direta de Constitucionalidade supramencionada, defendem que mani-

festação que guarde, ainda que remotamente, relação com o mandato deve ser compreendida na imunidade parlamentar, mesmo que proferida via redes sociais, sendo eventual restrição limitada à manifestação violadora concreta e *a posteriori*, estando vedado o bloqueio de perfil pela Constituição, por se caracterizar censura prévia.²⁴

Para eles, também, qualquer medida cautelar tomada pelo Poder Judiciário que interfira no mandato parlamentar deve ser comunicada à casa legislativa correspondente dentro de 24 horas, para que se delibere sobre sua manutenção em aplicação analógica do disposto no art. 53, da CF.²⁵

Essa também é a posição de alguns projetos de lei que tramitam no legislativo. O Projeto de Lei 2.630/20, também conhecido como Projeto de Lei das Fake News, estende expressamente a imunidade parlamentar para o ambiente digital e cria o conceito de contas que considera como de interesse público. Na última versão do Projeto de Lei, estipulava-se que:²⁶

Art. 33. São consideradas de interesse público, as contas mantidas em redes sociais indicadas como institucionais pelos integrantes da Administração Pública Federal, Estadual e Municipal, direta ou indireta, e pelos seguintes agentes políticos:

I – detentores de mandatos eletivos dos Poderes Executivo e Legislativo da União, dos Estados, do Distrito Federal e dos Municípios;

II – ocupantes, no Poder Executivo, dos cargos de:

- a) Ministro de Estado, Secretário de Estado, Secretário Municipal ou equiparados; e
- b) Presidente, Vice-Presidente e Diretor das entidades da Administração Pública indireta da União, dos Estados, do Distrito Federal e dos Municípios;

§ 1º Os titulares das contas de que trata o caput não poderão restringir a visualização de suas publicações.

24. NASCIMENTO, Roberta Simões; KALIL, Hugo Souto. É possível bloquear perfis de parlamentares nas redes sociais? ADI n. 6.494 é oportunidade para avanços na liberdade de expressão e na imunidade parlamentar. *Jornal Jota*, 16 set. 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/defensor-legis/e-possivel-bloquear-perfis-de-parlamentares-nas-redes-sociais>. Acesso em: 15.01.2025

25. NASCIMENTO, Roberta Simões; KALIL, Hugo Souto. É possível bloquear perfis de parlamentares nas redes sociais? ADI n. 6.494 é oportunidade para avanços na liberdade de expressão e na imunidade parlamentar. *Jornal Jota*, 16 set. 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/defensor-legis/e-possivel-bloquear-perfis-de-parlamentares-nas-redes-sociais>. Acesso em: 15.01.2025

26. BRASIL. *Projeto de lei nº 2.630, de 2020*, e apensados. Disponível em: <https://static.poder360.com.br/2024/06/ultima-versao-PL-2630-2020-fake-news-2023.pdf>

§ 2º As decisões de provedores que constituam intervenção ativa ilícita ou abusiva em contas de interesse público autorizam o ajuizamento de ação judicial para a sua restauração, devendo o Poder Judiciário obrigar os provedores as restabelecerem, no prazo de 24 (vinte e quatro) horas, nos casos em que fique comprovada a sua operação em conformidade com direitos fundamentais e com os princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência.

(...)

§ 6º A imunidade parlamentar material, na forma do art. 53 da Constituição Federal, estende-se aos conteúdos publicados por agentes políticos em plataformas mantidas pelos provedores de redes sociais e mensageria privada

Por sua vez, o Projeto de Lei 3046/22, atualmente em análise na Câmara dos Deputados, propõe atribuir ao Congresso Nacional a decisão final sobre a exclusão ou bloqueio de perfis de parlamentares nas redes sociais, com o seguinte texto:

Art. 8º-E. A exclusão, cancelamento, bloqueio ou suspensão de serviços e funcionalidades da conta ou do perfil em plataforma de rede social, de serviço de mensageria instantânea ou de serviço de chamadas de voz e/ou vídeo de usuário membro do Congresso Nacional constitui medida cautelar de caráter excepcionalíssimo, observadas as seguintes regras:

- I – A fundamentação deve ser robusta, devendo demonstrar cabalmente a indispensabilidade da medida;
- II – A decisão deve conter a indicação de forma clara do conteúdo considerado ilícito que motivou a medida, o tipo penal no qual teria incorrido o Parlamentar, bem como a duração da medida;
- III – A decisão, em qualquer hipótese, deve ter a participação do Ministério Público, vedada a adoção de ofício;
- IV – Salvo no período do recesso forense, a medida cautelar somente pode ser concedida por maioria absoluta dos membros do Supremo Tribunal Federal.

§ 1º Os autos da decisão devem ser remetidos à Casa à qual pertence o Parlamentar em até 24 (vinte e quatro) horas, a quem compete exercer juízo político sobre a decisão, ratificando-a ou suspendendo-a, em procedimento análogo ao previsto no § 2º do art. 53 da Constituição Federal.

O relator do projeto de lei, deputado Nikolas Ferreira, votou pela sua aprovação apontando que a proposta seria acertada “ao transpor para a internet a inviolabilidade constitucional que possuem os parlamentares para expressarem suas opiniões e palavras”²⁷

No entanto, apresentou substitutivo propondo que a especial proteção fosse destinada para contas não apenas de parlamentares, mas de qualquer detentor de mandato eletivo dos Poderes Executivo e Legislativo da União, dos Estados, do Distrito Federal e dos Municípios.

A Constituição do Estado de Goiás, por sua vez, é exemplo de legislação já em vigor que estipula, em seu artigo 12, § 9º, que a inviolabilidade parlamentar também abrange as manifestações realizadas em meios digitais, não ampliando a proteção, no entanto, para os demais detentores de cargo eletivo, como pretende o projeto de lei em tramitação.

Dessa forma, observa-se que o tratamento das contas de interesse público em redes sociais, incluindo bloqueios e moderação de conteúdo, tem gerado debates no Brasil, envolvendo questões constitucionais como a imunidade parlamentar, a liberdade de expressão e os limites da jurisdição nacional.

Considerações finais

As plataformas digitais, como a Meta, exercem um papel fundamental na moderação de conteúdo, utilizando mecanismos como a “tolerância de interesse público” e o “sistema de verificação cruzada” para tratar de maneira diferenciada as contas de figuras públicas, como as de detentores de mandatos eletivos. A sua flexibilidade nas regras aplicáveis e esse público, no entanto, é influenciada, em parte, pelas mudanças na presidência dos Estados Unidos, o que corrobora com a vertente acadêmica que defende a insuficiência de um sistema de autorregulação e a necessidade de uma regulação que traga parâmetros mínimos a serem observados por agente privados.

No cenário regulatório brasileiro, o judiciário tem desempenhado um papel crucial neste debate, com o Supremo Tribunal Federal reafirmando a constitucionalidade do bloqueio de contas de políticos em determinados contextos, especialmente para preservar a ordem democrática e a integridade do processo eleitoral. O STF tem destacado que a imunidade parlamentar não é absoluta, aplicando-se somente a manifestações relacionadas diretamente ao exercício

27. O voto do relator no PL nº 3.046, de 2022 está disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostra-integra?codteor=2347866&filename=Parecer-CCOM-2023-10-19

da função legislativa. A corte também tem reconhecido a importância de limitar abusos que possam prejudicar o debate público e a democracia.

Está pendente de julgamento, no entanto, processo em controle concentrado de constitucionalidade que poderá trazer contornos mais definitivos para a constitucionalidade da prática de bloqueio de contas políticas pelo judiciário, considerando as interpretações de que poderiam configurar censura prévia.

Além disso, o Congresso Nacional também está envolvido na questão, com o Projeto de Lei 2.630/20 propondo um modelo de autorregulação regulada que visaria equilibrar os direitos dos parlamentares e a proteção contra abusos no ambiente digital e o PL 3046/22 que, por sua vez, atribui ao Congresso a decisão final sobre o bloqueio de contas de parlamentares e apresentando novas exigências e limites para as plataformas e para o poder judiciário.

Portanto, a discussão sobre o bloqueio de contas de políticos no ambiente digital envolve uma articulação entre o judiciário, que tem se posicionado sobre as limitações da imunidade parlamentar, e o legislativo, que busca regulamentar a atuação das plataformas e do próprio poder judiciário.

A busca por um equilíbrio entre liberdade de expressão e a proteção da democracia continua a ser um dos maiores desafios em um cenário de crescente protagonismo das redes sociais.

Referências

COMITÊ DE SUPERVISÃO DA META. 2021-001-FB-FBR – *Suspensão do ex-presidente Trump*. Disponível em: <https://www.oversightboard.com/decision/fb-691qamhj/?lang=pt-br>. Acesso em: 15.01.2025.

COMITÊ DE SUPERVISÃO DA META. 2021-004-FB-UA – *Protestos a favor de Navalny na Rússia*. Disponível em: <https://www.oversightboard.com/decision/fb-6yhrxhzr/?lang=pt-br>. Acesso em: 15.01.2025.

COMITÊ DE SUPERVISÃO DA META. 2022-013-FB-UA – *Slogan de protesto no Irã*. Disponível em: <https://www.oversightboard.com/decision/fb-zt6ajs4x/?lang=pt-br>. Acesso em: 15.01.2025.

COMITÊ DE SUPERVISÃO DA META. 2023-003-FB-MR – *Primeiro-ministro do Camboja*. Disponível em: <https://www.oversightboard.com/decision/fb-6okjpns3/?lang=pt-br>. Acesso em: 15.01.2025.

CRUZ, Francisco Brito (Coord.); LANA, Alice; JOST, Iná. Iguais perante as plataformas? Equidade e transparência na moderação de conteúdo em plataformas digitais. Revista: *Diagnósticos & Recomendações*, n. 9, jul. 2023

CLEG, Nick. *Ending Suspension of Trump's Accounts With New Guardrails to Deter Repeat Offenses*. Meta, 2023. Disponível em: <https://about.fb.com/news/2023/01/trump-facebook-instagram-account-suspension/>. Acesso em: 15.01.2025.

CLEG, Nick. *In Response to Oversight Board, Trump Suspended for Two Years; Will Only Be Reinstated if Conditions Permit*. Meta, 2021. Disponível em: https://about.fb.com/news/2021/06/facebook-response-to-oversight-board-recommendations-trump/?utm_source=chatgpt.com. Acesso em: 15.01.2024.

CURVELO, Erick. Liberdade de expressão 2.0: a constitucionalidade dos casos de deplatforming no Inquérito das Fake News. *Internet & Sociedade*, v. 1, n. 3, jun. 2021.

MERCIER, D. *Pressionado por STF, Facebook bloqueia globalmente contas de apoiadores de Bolsonaro*. El País Brasil. Disponível em: <https://brasil.elpais.com/brasil/2020-08-01/pressionado-por-stf-facebook-bloqueia-globalmente-contas-de-apoiadores-de-bolsonaro.html>. Acesso em: 15.01.2025.

META. *Restrição de usuários*. Disponível em: <https://transparency.meta.com/pt-br/enforcement/taking-action/restricting-accounts/>. Acesso em: 15.01.2025.

META Transparency Center. *Restrição de contas de figuras públicas durante agitações civis*. 2024. Disponível em: <https://transparency.meta.com/pt-br/enforcement/taking-action/restricting-accounts-by-public-figures>. Acesso em: 15.01.2025.

NASCIMENTO, Roberta Simões; KALIL, Hugo Souto. É possível bloquear perfis de parlamentares nas redes sociais? ADI n. 6.494 é oportunidade para avanços na liberdade de expressão e na imunidade parlamentar. *Jornal Jota*, 16 set. 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/defensor-legis/e-possivel-bloquear-perfis-de-parlamentares-nas-redes-sociais>. Acesso em: 15.01.2025.

REUTERS. *Meta rejects recommendation to suspend former Cambodia PM from Facebook*. 2023. Disponível: <https://www.reuters.com/world/asia-pacific/meta-rejects-recommendation-suspend-former-cambodia-pm-from-facebook-2023-08-30/> Acesso em: 15.01.2025.

RIBEIRO, G. F. *Conta bolsonarista bloqueada acusa STF de golpe; entenda como a Corte agiu*. UOL. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/07/24/contas-bolsonaristas-suspensas-veja-posts-usados-de-exemplo-em-acao-do-stf.htm>. Acesso em: 15.01.2025.

ZIADY, Hanna. *Facebook kept its own oversight board in the dark on program for VIP users*. Disponível: <https://edition.cnn.com/2021/10/21/tech/facebook-cross-check-oversight-board/index.html>. Acesso em: 15.01.2025.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

EIXO II

Privacidade, Consentimento e Dados Sensíveis

AUTORES

Leandro Alcolumbre

Michel Sachs Feuz

Rainier Garacis

Tessália Mariana Fernandes Pirolla

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

4

A geolocalização como meio de prova digital no processo trabalhista: desafios jurídicos e éticos

TESSÁLIA MARIANA FERNANDES PIROLLA

Sumário: Introdução. 1. Geolocalização como prova digital. 1.1. Aspectos técnicos e probatórios. 2. Regulamentação das provas digitais. 3. Geolocalização e os direitos fundamentais. 3.1. Análise do Processo n.º TST-ROT – 23218-21.2023.5.04.0000 – voto da maioria. 3.2. Análise do Processo n.º TST-ROT – 23218-21.2023.5.04.0000 – voto vencido. 3.3. Tratamento sensível de dados pessoais provenientes da geolocalização. Considerações finais. Referências.

Introdução

A era digital trouxe consigo transformações profundas nas relações sociais, acompanhadas por um aumento significativo na produção e no armazenamento de dados.

Neste contexto, as provas digitais emergem como uma nova classe de meio probatório, capaz de demonstrar fatos ocorridos no ambiente digital ou mediados por tecnologias, com destaque para a prova digital da geolocalização.

A utilização de tais provas, entretanto, suscita discussões importantes sobre sua regulamentação, admissibilidade e impacto nos direitos fundamentais, tais como privacidade e proteção de dados pessoais, demandando uma análise criteriosa da adequação, proporcionalidade e necessidade do uso da medida, de forma a evitar ingerências abusivas e violações indevidas aos direitos dos indivíduos.

Destarte, o presente estudo tem como enfoque a utilização da geolocalização no âmbito trabalhista, como um meio de prova digital, para fins de comprovação de horas extras, analisando suas aplicações práticas e os desafios jurídicos e éticos.

A pesquisa se inicia com uma breve análise dos aspectos doutrinários da geolocalização como espécie de prova digital, notadamente da sua força probante; logo em seguida são abordados aspectos legais que buscam fundamentar e validar a utilização desta diligência probatória.

Após, o estudo analisa a aplicação prática deste meio probante no processo do trabalho, e os seus limites de utilização frente a alguns direitos fundamentais, incluindo, neste tópico, o exame da recente decisão do Tribunal Superior do Trabalho (TST) no processo ROT n.º 23218-21.2023.5.04.0000, que trouxe

1. Analista Jurídica do Ministério Público do Trabalho. Graduada em Direito pela Pontifícia Universidade Católica de São Paulo (PUC-SP), pós-graduada em Direito Processual Civil pelo IBMEC-SP, pós-graduada em Direito Público pela Faculdade de Direito da Universidade de São Paulo (FD-USP), e pós-graduanda em Direito Digital pela Universidade do Rio de Janeiro (UERJ), em parceria com o Instituto de Tecnologia do Rio de Janeiro (ITS-Rio).

critérios relevantes para a admissibilidade da geolocalização como prova digital, mas também apontou sinais de alerta para o perigo de retrocesso social.

Ao final, adiciona-se ao trabalho sucinta abordagem sobre a questão de dados pessoais com inferências sensíveis, e indaga-se: é juridicamente legítimo e eticamente admissível o uso da geolocalização como prova digital para comprovar horas extras em processos trabalhistas, diante dos direitos fundamentais?

A partir das premissas expostas, à luz do panorama jurídico, doutrinário e jurisprudencial, o presente estudo almeja instigar o pensamento crítico da leitora e do leitor, sobre a complexa questão do uso da geolocalização para fins probatórios no âmbito trabalhista.

Para fins de delimitação metodológica, será adotado o método dedutivo de argumentação, a revisão bibliográfica nacional e internacional, e a seleção jurisprudencial, que irá se basear em decisões recentes dos tribunais superiores, especialmente do Tribunal Superior do Trabalho (TST), com destaque para o processo ROT nº 23218-21.2023.5.04.0000.

A escolha considerou a relevância da controvérsia jurídica, a representatividade dos argumentos apresentados e a atualidade das discussões sobre a admissibilidade da geolocalização como meio de prova digital no processo trabalhista.

1. Geolocalização como prova digital

A geolocalização, também conhecida como georreferenciação, é um recurso tecnológico que permite identificar, através de um sistema de coordenadas (latitude e longitude), a posição de uma pessoa, de um estabelecimento ou de um objeto, em um determinado momento, utilizando-se de tecnologias como GPS (*Global Positioning System*), sinais de internet (*Wi-Fi*), sistemas de radiofrequência (*GSM*), endereço de protocolo de internet (endereço IP), entre outras.

Trata-se de um mecanismo que deriva de outras técnicas de posicionamento, tais como os faróis, as estrelas, as bússolas e as ondas de rádio, utilizadas nos tempos primórdios, como forma de o ser humano organizar a sua localização no espaço.

Atualmente, com o avanço das tecnologias de rastreamento e a crescente adesão aos dispositivos móveis, o uso dos dados provenientes desse sistema de referenciação tem se tornado importante não apenas para detectar o posicionamento geográfico, mas também para ser utilizado como meio de prova

em processos judiciais, em especial no âmbito trabalhista que será analisado neste estudo.

Sob essa ótica se insere a prova digital que nada mais é do que a ferramenta capaz de comprovar a ocorrência de um fato “no meio” digital, tal como uma postagem em uma rede social e uma operação financeira em um aplicativo; ou “por meio” digital como, por exemplo, a oitiva de uma testemunha em uma audiência telepresencial e a utilização da geolocalização de um empregado para fins de comprovação de horas extras.

Rennan Thamay e Maurício Tamer² conceituam a prova digital como sendo:

[...] o instrumento jurídico vocacionado a demonstrar a ocorrência ou não de determinado fato e suas circunstâncias, tendo ele ocorrido total ou parcialmente em meios digitais ou, se fora deles, esses sirvam como instrumento de sua demonstração. A prova digital é o meio de demonstrar a ocorrência de um fato ocorrido em meio digital, ou que tem no meio digital um instrumento de demonstração de determinado fato (e) de seu conteúdo.

Neste sentido, cabe analisar alguns atributos a fim de compreender melhor o que vem a ser este meio probatório.

1.1. Aspectos técnicos e probatórios

No tocante às particularidades das provas digitais, podemos mencionar a sua classificação quanto à necessidade de ordem judicial para o seu acesso ou para a sua formação³, destacando as provas digitais que dependem de autorização judicial, tais como a geolocalização, os registros de conexão e aplicação (art. 10, § 1º, da Lei nº 12.965/2014 – Marco Civil da Internet – MCI), as comunicações armazenadas (art. 10, § 2º, do MCI), e as que independem de ordem judicial, isto é, aquelas disponíveis em fontes abertas que são de livre acesso a todas as partes que atuam no processo, como, por exemplo, as disponibilizadas em redes sociais e em sites da internet.

Outrossim, considerando a volatilidade do meio digital, que pode ocasionar a fragilidade da prova produzida, a doutrina e a jurisprudência mencionam a necessidade de a prova digital observar alguns critérios para assegurar a

2. THAMAY, Rennan; TAMER, Mauricio. *Provas no direito digital: conceito da prova digital, procedimentos e provas digitais em espécie*. São Paulo: Thomson Reuters Brasil, 2020. p. 33.

3. CAPANEMA, Walter Aranha. *Manual de direito digital*. Teoria e Prática. Salvador: JusPodivm, 2024. p. 195.

sua validade em um processo, tais como a autenticidade, a integridade e a preservação da custódia.

Neste contexto, Pollyana Soares⁴ cita tais requisitos, esclarecendo que:

A autenticidade deve ser entendida como a qualidade da prova digital que permite a certeza com relação ao autor do fato digital [...]. A integridade está relacionada à qualidade da prova digital que permite a certeza com relação à sua não adulteração desde o momento da realização do fato até a apresentação no processo. [...] Por fim, deve ser preservada a cadeia de custódia da prova, ou seja, é preciso garantir a autenticidade e a integridade em todo processo de produção da prova digital, nas etapas de identificação, coleta, aquisição e preservação.

Assim, a autenticidade pode ser aferida através de algumas ferramentas, tais como assinatura digital; autenticação de dois fatores; registros de *log*; endereço de IP e metadados; bem como a integridade pode ser verificada por meio de *sites* de registros de dados que usam da tecnologia *blockchain* e emitem código *hash* ou carimbo de tempo (*timestamp*), e, por fim, utilizando-se de *sites* de registros de provas digitais, como o *Original My* e o *Verifact*, ou de perícia técnica, é possível averiguar a preservação da cadeia de custódia⁵.

Ainda, importa destacar a distinção entre provas documentais digitais, entendidas como aqueles documentos eletrônicos que atestam um fato em um determinado momento – como e-mails, mensagens de texto e registros históricos de localização armazenados em servidores –, e dados em tempo real, que são informações geradas simultaneamente a sua ocorrência, e obtidos por meio de rastreamento contínuo.

Essa diferenciação é relevante, pois a jurisprudência tem adotado critérios mais rígidos quanto à admissibilidade de dados obtidos em tempo real (dados dinâmicos), dada sua maior potencialidade de invasão à privacidade, inclusive de terceiros não relacionados à investigação, e em virtude da proteção constitucional do artigo 5º, XII. Em contrapartida, o uso de registros georreferenciados históricos (dados estáticos), quando bem delimitado no tempo

4. SOARES, Pollyana Lúcia Rosado. As provas digitais no processo do trabalho. *Revista do Tribunal Regional do Trabalho da 3ª Região*, Belo Horizonte, v. 67, n. 104, jul./dez. 2021. p. 289.

5. LIMA, Andréa Ferreira; NUNES, Vanessa Ester Ferreira; VIEIRA, Carolina Mesquita. Provas digitais no processo do trabalho: a validade do uso da geolocalização. *Revista do Tribunal Superior do Trabalho*, Porto Alegre, v. 90, n. 3, jul./set. 2024. p. 94.

e com finalidade probatória clara, tem recebido maior aceitação nos tribunais, especialmente em demandas criminais⁶.

Além dos desafios citados em relação à força probante das provas digitais, outras questões merecem nossa atenção no que tange à temática das provas digitais – em particular à geolocalização, que é o nosso objeto de estudo –, tais como a alegada falta de regulamentação específica e preocupações atinentes aos direitos fundamentais, em especial ao direito à privacidade e ao sigilo de dados.

2. Regulamentação das provas digitais

De fato, não há uma regulamentação específica que trate das provas digitais. Entretanto, a doutrina e a jurisprudência apontam que há regramentos pontuais que embasam e validam a sua utilização, tais como na Constituição Federal (CF), no Código de Processo Civil (CPC), na Consolidação das Leis do

6. No HC nº 918281/MT, em decisão monocrática do dia 1º de agosto de 2024, o ministro Jesuíno Rissato (Desembargador Convocado do TJDF), acerca da diferença e da admissibilidade da quebra de sigilo de dados informáticos estáticos (geolocalização) e de interceptações das comunicações dinâmicas, entendeu que “(...) III – Na hipótese vertente, observa-se que a determinação judicial rechaçada, em parte, se referiu a dados estáticos antes coletados (registros de geolocalização), relacionados à identificação de usuários que operaram em área delimitada e por intervalo de tempo indicado. Tal situação configura apenas quebra de sigilo de dados informáticos estáticos e se distingue das interceptações das comunicações dinâmicas em si, as quais dariam acesso ao fluxo de comunicações de dados, isto é, ao conhecimento do conteúdo da comunicação travada com o seu destinatário. IV – O tema já foi enfrentado por esta Corte Superior, vejamos: “Na espécie, a ordem judicial direcionou-se a dados estáticos (registros), relacionados à identificação de usuários em determinada localização geográfica que, de alguma forma, possam ter algum ponto em comum com os fatos objeto de investigação por crimes de homicídio. (...) A determinação do Magistrado de primeiro grau, de quebra de dados informáticos estáticos, relativos a arquivos digitais de registros de conexão ou acesso a aplicações de internet e eventuais dados pessoais a eles vinculados, é absolutamente distinta daquela que ocorre com as interceptações das comunicações, (...) A quebra do sigilo de dados, na hipótese, corresponde à obtenção de registros informáticos existentes ou dados já coletados (...) Assim, para que o magistrado possa requisitar dados pessoais armazenados por provedor de serviços de internet, mostra-se satisfatória a indicação dos seguintes elementos previstos na lei: a) indícios da ocorrência do ilícito; b) justificativa da utilidade da requisição; e c) período ao qual se referem os registros (...) Logo, a quebra do sigilo de dados armazenados, de forma autônoma ou associada a outros dados pessoais e informações, não obriga a autoridade judiciária a indicar previamente as pessoas que estão sendo investigadas (...)” (RMS n. 62.143/RJ, Sexta Turma, Rel. Min. Rogério Schietti Cruz, DJe de 8/9/2020). V – Convém registrar que a quebra de sigilo em tela foi decretada por decisão judicial devidamente fundamentada, após pedido expresso da autoridade competente, no seio de investigação formal, tendo, como referência, fatos concretos relacionados ao suposto cometimento de crime grave. VI – Na situação exposta, a r. decisão de origem foi clara ao delimitar tempo e espaço, nos seguintes termos: “a quebra de sigilo de dados telemáticos dos usuários que tenham utilizado os serviços da empresa G B I L e G LLC num raio de 500 metros das coordenadas geográficas Latitude 21 o 35 ‘42.6 ‘S e Longitude 41 o. 28 ‘36.9 ‘W no período abrangido entre 10:00hs e 14:00hs do dia 09/05/2020 (...)” (fl. 112). VII – Contudo, a r. decisão acima extrapolou os limites do entendimento firmado por esta Corte Superior, ao determinar o acesso amplo e irrestrito aos seguintes dados, verbis: “1) que seja dado acesso amplo e irrestrito dos e-mails vinculados aos aparelhos identificados. 2) Que seja fornecido o conteúdo do G. 3) Que seja fornecido o conteúdo do G fotos (incluindo os respectivos metadados – geomarcacão). 4) Que seja fornecido o conteúdo do G D. 5) Que seja fornecida a lista de contatos. 6) Que seja fornecido o histórico de localização, incluindo os trajetos pesquisados no g m, w ou outros que importem a função GPS. 7) Que sejam fornecidas as consultas (pesquisas) realizados pelo usuário (s) do dispositivo. 8) Por fim, que sejam relacionadas as contas do G P, incluindo APPs baixados (downloads) ou comprados, lista de desejos, pessoas e informações das eventuais contas” (fl. 112). VIII – Trata-se de matéria recentemente enfrentada pela Sexta Turma desta Corte Superior, em julgado no qual foi assentada a tese de que dados que refletem informações íntimas (como o acesso irrestrito a fotos e conteúdo de conversas), quando a ordem de quebra de sigilo se voltar a universo indeterminado de pessoas, devem ser afastados desta possibilidade (AgRg no RMS 59.716/RS, Sexta Turma, Rel. Min. Sebastião Reis Júnior, DJe de 17/8/2021). IX – Importante, contudo, sedimentar que a ordem in casu foi dirigida a provedor cuja relação é regida pelo Marco Civil da Internet, o qual não prevê, dentre os requisitos que estabelece para a quebra de sigilo, que a decisão judicial especifique previamente as pessoas objeto da investigação ou que a prova da infração (ou da autoria) possa ser realizada facilmente por outros meios (arts. 22 e 23 da Lei n. 12.965/2014). Entretanto, o referido fundamento não subsiste nos casos em que haja a possibilidade de violação da intimidade e vida privada de pessoas não comprovadamente relacionadas à investigação criminal (AgRg no RMS 59.716/RS, Sexta Turma, Rel. Min. Sebastião Reis Júnior, DJe de 17/8/2021)”. BRASIL. Superior Tribunal de Justiça. *Habeas Corpus* n. 918281 – MT (2024/0198335-0). Relator: Ministro Jesuíno Rissato (Desembargador Convocado do TJDF). Brasília, DF, 02 ago. 2024. Disponível em: <https://www.stj.jus.br>. Acesso em: 17 abr. 2025.

Trabalho (CLT), na Lei Geral de Proteção de Dados (Lei nº 13.709/2018), na Lei de Acesso à Informação (LAI, Lei nº 12.527/2011), no Marco Civil da Internet (MCI, Lei nº 12.965/2014), entre outras.

Sabe-se que o direito à prova é um direito fundamental, previsto na Constituição Federal, que decorre diretamente do direito de ação (art. 5º, inc. XXXV)⁷ e da garantia da ampla defesa (art. 5º, inc. LV)⁸, a qual assegura a todos os litigantes a possibilidade de se produzir as provas necessárias à comprovação dos fatos e das argumentações alegadas em juízo, desde que obtidas por meios lícitos (art. 5º, inc. LVI). Podemos, portanto, considerar que se trata de um direito que abrange, consequentemente, as provas digitais.

O Código de Processo Civil, por sua vez, traz previsão legal genérica no sentido de ser possível a utilização de prova digital uma vez que, em seu artigo 369, outorga às partes “o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz.”⁹, bem como autoriza o juiz a determinar, de ofício ou a requerimento da parte, “as provas necessárias ao julgamento do mérito” (CPC, art. 370).

Tal cláusula aberta fundamenta a validade da prova digital e se coaduna com a ideia de que o Direito está em constante transformação, e, por conseguinte, deve acompanhar os avanços tecnológicos, conforme bem ilustra Fernanda Junqueira e Flávio Higa¹⁰ ao mencionar que:

Como ao Direito – produto cultural que é – se impõe um caminhar *pari passu* com as transformações sociais, a impactar diretamente nos fatos e nos meios de se prová-los, nada mais natural que a produção probatória se apresente, na atual quadratura da história da humanidade, de modo mais requintado, a fazer coro aos avanços tecnológicos.

As provas digitais são, por esse prisma, o substrato de uma sociedade interconectada e deslocada para o espaço virtual, onde se alocam, se armazenam e se transferem milhares de dados, os quais

7. “Art. 5º (...) XXXV – a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito”. BRASIL. Constituição de 1988. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF, 05 de outubro de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 11 jan. 2025.

8. BRASIL. Constituição de 1988. *Op. Cit.*

9. BRASIL. Lei nº 13.105, de 16 de março de 2015. Institui o Código de Processo Civil. Diário Oficial da União, Brasília, DF, 17 mar. 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 11 jan. 2025.

10. JUNQUEIRA, Fernanda; HIGA, Flávio. *Admissibilidade das Provas Digitais na ordem processual: o que se faz na nuvem; fica na nuvem*. Anuario de la Facultad de Derecho. Universidad de Extremadura 38 (2022): 329-348 ISSN: 0213-988X – ISSN-e: 2695-7728. p. 336.

podem deixar rastros e, nessa condição, prestarem-se como meio probante. Daí porque não se discute sua validade.

Ademais, o mesmo diploma legal disciplina, em seus artigos 439 a 441¹¹, os “documentos eletrônicos”, conhecidos na doutrina como sinônimos de “documentos digitais”¹².

Já a Consolidação das Leis do Trabalho é categórica ao atribuir ao juiz “ampla liberdade na direção do processo”, de forma a “determinar qualquer diligência necessária ao esclarecimento” das questões controvertidas (CLT, art. 765)¹³.

Ainda, podemos citar a Lei Geral de Proteção de Dados Pessoais (LGPD, Lei nº 13.709/2018) em seu art. 7º, VI¹⁴; assim como a Lei de Acesso à Informação (LAI, Lei nº 12.527/2011) nos seus artigos 21 e 31¹⁵, e o art. 22¹⁶ do Marco Civil da Internet (MCI, Lei nº 12.965/2014), que permitem, em suma, o acesso a dados pessoais para produção e defesa de provas em juízo.

Adicionalmente, cabe destacar a Resolução CNJ nº 335/2020, que dispõe sobre a política pública de governança e de gestão de processo judicial eletrônico, e institui a Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br), de forma a integrar os tribunais do país; prevendo, inclusive, a adoção de requisitos padronizados para dados e documentos, como, por exemplo, para documentos digitais, nos termos do inciso IV, do artigo 10¹⁷.

11. “Art. 439. A utilização de documentos eletrônicos no processo convencional dependerá de sua conversão à forma impressa e da verificação de sua autenticidade, na forma da lei”, “Art. 440. O juiz apreciará o valor probante do documento eletrônico não convertido, assegurado às partes o acesso ao seu teor”, e “Art. 441. Serão admitidos documentos eletrônicos produzidos e conservados com a observância da legislação específica”. BRASIL. Código de Processo Civil. *Op. Cit.*

12. CAPANEMA, Walter Aranha. *Op. Cit.* p. 204.

13. BRASIL. *Decreto-lei nº 5.452, de 1º de maio de 1943*. Aprova a Consolidação das Leis do Trabalho. Diário Oficial da União, Rio de Janeiro, RJ, 09 ago. 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 11 jan. 2025.

14. “Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...) 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)”. BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 jan. 2025.

15. “Art. 21. Não poderá ser negado acesso à informação necessária à tutela judicial ou administrativa de direitos fundamentais” e “Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais”. BRASIL. *Lei nº 12.527, de 18 de novembro de 2011*. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União, Brasília, DF, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 11 jan. 2025.

16. “Art. 22. A parte interessada poderá, 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”. BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11 jan. 2025.

17. “Art. 10. A política de governança e gestão PDPJ-Br deverá estabelecer também os seguintes requisitos para os dados e documentos: (...) IV – padrões de documentos digitais”. BRASIL. Conselho Nacional de Justiça. *Resolução nº 335, de 29 de setembro de 2020*. Dispõe sobre a governança e a gestão de provas digitais no âmbito do Poder Judiciário. Diário da Justiça Eletrônico, Brasília, DF, n. 250, 1 out. 2020. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3516>. Acesso em: 14 abr. 2025.

Sendo assim, sob a ótica da regulamentação e do princípio da legalidade (art. 5, inc. II¹⁸), considera-se que há substrato legal que fundamente e valide a utilização das provas digitais, bem como não se verifica, de forma geral, proibição à utilização de tal diligência probatória.

Contudo, outras preocupações merecem atenção na utilização de tais provas – em particular no que tange à geolocalização utilizada no âmbito trabalhista –, mormente quanto a alguns princípios e direitos que estão em jogo, e serão analisados adiante.

3. Geolocalização e os direitos fundamentais

Um dos pontos de maior destaque e de discussão acirrada, na doutrina e na jurisprudência, no tocante ao uso da geolocalização – em razão de entendimentos contraditórios –, diz respeito à colisão entre os direitos fundamentais, potencialmente antagônicos, do direito à intimidade/privacidade (CF, 5º, X)¹⁹, à proteção de dados pessoais (CF, 5º, LXXIX)²⁰ e ao sigilo de comunicações telefônicas e telemáticas (CF, 5º, XII)²¹ *versus* o direito à informação e realização da prova, consagrados nos princípios do contraditório e da ampla defesa (CF, 5º, LV)²², como corolários do devido processo legal (CF, 5º, LIV)²³.

De acordo com entendimento consolidado no Supremo Tribunal Federal, “Não há, no sistema constitucional brasileiro, direitos ou garantias que se revistam de caráter absoluto”²⁴. Sendo assim, a solução perpassa pela técnica da ponderação de Robert Alexy²⁵, que se utiliza da “máxima da proporcionalidade” e da aplicação de suas “três máximas parciais” – adequação, necessidade e proporcionalidade em sentido estrito – para resolver conflitos entre

18. “Art. 5º (...) II – ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei”. BRASIL. Constituição de 1988. *Op. Cit.*

19. “Art. 5º (...) 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”. BRASIL. Constituição de 1988. *Op. Cit.*

20. “Art. 5º (...) LXXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”. BRASIL. Constituição de 1988. *Op. Cit.*

21. “Art. 5º (...) 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”. BRASIL. Constituição de 1988. *Op. Cit.*

22. “Art. 5º (...) LV – aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e ampla defesa, com os meios e recursos a ela inerentes”. BRASIL. Constituição de 1988. *Op. Cit.*

23. “Art. 5º (...) LIV – ninguém será privado da liberdade ou de seus bens sem o devido processo legal”. BRASIL. Constituição de 1988. *Op. Cit.*

24. BRASIL. Supremo Tribunal Federal. (Tribunal Pleno). MS n. 23.452/RJ. Relator: Min. Celso de Mello. Julgamento: 16/09/1999. Publicação: 12/05/2000. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur20720/false>. Acesso em: 13 jan. 2025.

25. ALEXY, Robert. *Teoria dos direitos fundamentais*. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008. p. 118.

princípios fundamentais. Tal método é elucidado por Marcelo Novelino²⁶ da seguinte forma:

A adequação entre meios e fins impõe que as medidas adotadas, para serem consideradas proporcionais, sejam aptas a fomentar os objetivos almejados [...] A necessidade (ou exigibilidade) impõe que, dentre os meios aproximadamente adequados para fomentar um determinado fim constitucional, seja escolhido o menos invasivo possível [...] A proporcionalidade em sentido estrito corresponde à “lei material do sopesamento”, segundo a qual “quanto maior for o grau de não satisfação ou de afetação de um princípio, tanto maior terá que ser a importância da satisfação do outro”.

Vale dizer que, diante da análise de um caso concreto, por exemplo, pode-se chegar à conclusão de que uma medida se afigura adequada, necessária e proporcional para a consagração do direito fundamental do contraditório e da ampla defesa, afastando-se a incidência dos direitos fundamentais à privacidade/intimidade, à proteção de dados pessoais e ao sigilo de comunicações telefônicas e telemáticas, mas não de forma a aniquilar tais direitos, mas sim de harmonizá-los com a preponderância do primeiro.

Tal entendimento constou do v. Acórdão do recente julgamento do ROT nº 23218-21.2023.5.04.0000²⁷, da Subseção II Especializada em Dissídios Individuais (SDI II) do Tribunal Superior do Trabalho (TST), que reconheceu a adequação, a necessidade e a proporcionalidade da prova digital da geolocalização, para fins de comprovação de horas extras em um processo trabalhista.

Publicada em 14 de maio de 2024, a referida decisão do TST estabeleceu paradigmas e critérios relevantes para a admissibilidade do uso da geolocalização, os quais merecem ser analisados.

3.1. Análise do processo n.º TST-ROT – 23218-21.2023.5.04.0000 – voto da maioria

Inicialmente, cabe observar que se trata de recurso ordinário interposto pela empresa ré (Banco Santander S.A.), como litisconsorte passivo, em face de decisão do Tribunal Regional do Trabalho da 4ª Região (RS), no mandado de segurança impetrado pelo reclamante bancário, que cassou a decisão do juízo

26. NOVELINO, Marcelo. *Manual de direito constitucional*. Rio de Janeiro: Forense; São Paulo: Método, 2014. p. 504-503.

27. BRASIL. Tribunal Superior do Trabalho. (Subseção II Especializada em Dissídios Individuais – SDI II). ROT nº 23218-21.2023.5.04.0000. Relator Min. Amaury Rodrigues Pinto Junior. Julgamento: 14/05/2024. Publicação: 14/06/2024. Disponível em: <https://jurisprudencia-backend2.tst.jus.br/rest/documentos/4ec98fa07117dd4cd23754bdd6e23c8b>. Acesso em: 15 jan. 2025.

de primeiro grau, na reclamação trabalhista nº 0021835-91.2019.5.04.0341, concedendo parcialmente a segurança para determinar que a autoridade coatora se abstenha de determinar a produção de prova digital de geolocalização requerida pela empresa.

No que tange às leis que respaldam a medida, segundo o relator, a produção de prova digital é amparada por diversos ordenamentos jurídicos, tanto de tribunais internacionais, como as contribuições da Corte Europeia de Direitos Humanos, como por leis brasileiras, notadamente a Lei Geral de Proteção de Dados Pessoais, a Lei de Acesso à Informação e o Marco Civil da Internet, alinhando-se, portanto, com o defendido no item 2 deste estudo.

Em respeito à privacidade e à intimidade, o julgado preconiza, em suma, que haverá priorização de tais direitos quando houver veiculação de dados pessoais referentes a:

(i) crianças, adolescentes (menores) ou pessoas incapazes; (ii) assuntos familiares; (iii) origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas e filiação sindical; (iv) processamento de dados relativos à saúde ou à sexualidade; (v) violência sexual ou doméstica; (vi) dados sensíveis ou de publicação restrita, de acordo com cada legislação nacional aplicável, ou que tenham sido assim considerados na jurisprudência emanada dos órgãos encarregados da proteção jurisdicional dos direitos fundamentais. A transparência e o direito de acesso a informações preponderam nas hipóteses de a pessoa envolvida ter voluntariamente alcançado status público e o processo estiver relacionado aos motivos de sua notoriedade.

Considerando que os dados de geolocalização – para fins de comprovação de horas extras, que é o caso dos autos –, não se incluíam nas hipóteses elencadas, a decisão menciona que a solução para a controvérsia se daria, portanto, pelo equacionamento da “necessidade, adequação e proporcionalidade da providência solicitada”.

Em seguida, citando os princípios atinentes ao âmbito trabalhista da primazia da realidade e da busca da verdade real; e dos princípios processuais da paridade de armas e da inclusão, a decisão afirma que a prova digital da geolocalização é adequada “uma vez que possibilita saber onde estava o trabalhador durante o alegado cumprimento da jornada de trabalho, por meio do monitoramento de antenas de rádio-base”, e é proporcional “pois feita com o menor sacrifício possível ao direito à intimidade”, uma vez que há ressalva expressa de que a prova da geolocalização, para fins de comprovação de horas

extras, deveria ser limitada aos dias e horários apontados na petição inicial como sendo de trabalho realizado, bem como o processo deveria ser mantido em segredo de justiça. Assim, conclui mencionando que a requisição judicial de dados de geolocalização para provar horas extras trabalhadas não viola o direito à privacidade e à proteção de dados do trabalhador²⁸, só se podendo falar em eventual violação ao princípio da intimidade caso as alegações não fossem verdadeiras.

Ato contínuo, no tocante ao sigilo telemático e de comunicações, o julgado aduz que não haveria de se falar em violação a tais direitos uma vez que a prova da geolocalização consistiria em “verificar, em banco de dados, a rádio-base em que se encontrava o aparelho celular do trabalhador durante o alegado horário e período de trabalho”, não se tratando, portanto, de interceptação de mensagens, ligações telefônicas e afins.

Ademais, ao mencionar entendimento da Suprema Corte no HC 91.867²⁹, de relatoria do Min. Gilmar Mendes, que considera a proteção constitucional do artigo 5º, XII, à “comunicação de dados e não dos dados”, o julgado afirma que o sigilo constitucional está atrelado às comunicações de dados, ou seja, às formas de comunicação entre indivíduos; e não aos dados enquanto registro/depósito registral, como ocorre com os dados obtidos através da geolocalização. Ainda, complementou a fundamentação citando outra decisão do Supremo Tribunal Federal (RE n. 418416/SC)³⁰ no sentido de que se considerássemos o sigilo constitucional aos dados, não seria possível sequer estabelecer alguma investigação administrativa.

Logo após, o v. acórdão do TST corrobora seu ponto de vista, mencionando o precedente AgRg no RMS n. 68.487³¹, do Superior Tribunal de Justiça, que entendeu ser adequada, necessária e proporcional a prova digital da geolocalização para apurar um crime de homicídio.

Por fim, o julgado conclui sua convicção, afirmando que seria incoerente os esforços despendidos no desenvolvimento de sistemas – tal como o programa

28. No mesmo sentido: ALBINO, João Pedro Donaire; LIMA, Ana Cláudia Pires Ferreira de. Técnicas de captura de geolocalização para produção de prova judicial. *Revista Direito das Relações Sociais e Trabalhistas*, São Paulo, v. 8, n. 1, p. 216-233, jan./jun. 2022.

29. BRASIL. Supremo Tribunal Federal. (2ª Turma). HC 91.867/PA. Relator: Min. Gilmar Mendes. Julgamento: 24/04/2012. Publicação: 20/09/2012. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=98970411&ext=.pdf>. Acesso em: 15 jan. 2025.

30. BRASIL. Supremo Tribunal Federal. (Tribunal Pleno). RE n. 418.416/SC. Relator: Min. Sepúlveda Pertence. Julgamento: 10/05/2006. Publicação: 19/12/2006. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=2205705>. Acesso em: 15 jan. 2025.

31. BRASIL. Superior Tribunal de Justiça. (5ª Turma). AgRg no RMS n. 68.487/PE. Relator: Min. Ribeiro Dantas. Julgamento: 06/09/2022. Publicação: 15/09/2022. Disponível em: <https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=2210707&tipo=0&nreg=202200716193&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20220915&formato=PDF&salvar=false>. Acesso em: 16 jan. 2025.

VERITAS do Tribunal Regional do Trabalho da 12ª Região³² –, e no treinamento de servidores e magistrados – como o Programa Provas Digitais do TST –, a fim de aperfeiçoarem o uso de provas digitais, para, ao final, repreenderem o uso de tais meios probatórios.

Assim, com base em tais fundamentos expostos, a decisão, tomada por maioria de votos, julgou parcialmente procedente o recurso ordinário do litisconsorte (empresa ré), concedendo apenas parcialmente a segurança pretendida pelo reclamante, no sentido de limitar a prova digital aos dias e horários especificados na exordial, além de determinar o sigilo do processo às partes e ao juiz da causa.

Com efeito, nota-se que tal posicionamento representa um marco no avanço à aceitação e à validação do uso da prova digital da geolocalização no âmbito do processo trabalhista, de forma a nortear as decisões futuras atinentes a esta temática, e evitar decisões contraditórias³³. Todavia, vale frisar que o dilema existente ainda não teve o seu desfecho, e devemos seguir acompanhando o caso, notadamente para compreender qual será o entendimento do STF, a partir do julgamento do Recurso Extraordinário interposto.

Outrossim, corroborando o posicionamento díspar a respeito do tema, cabe ressaltar a existência de corrente vencida, conduzida pelo Min. Aloysio Corrêa da Veiga, Min. Luiz José Dezena da Silva e pela Des. Convocada Margaret Rodrigues Costa, sendo relevante trazer à baila os argumentos que os motivaram a divergir.

3.2. Análise do processo n.º TST-ROT – 23218-21.2023.5.04.0000 – voto vencido

O primeiro ponto importante destacado no voto vencido diz respeito à utilização da geolocalização como medida subsidiária e excepcional, o que equivale a dizer que, havendo outros meios de prova menos invasivos capazes de comprovar as alegações trazidas nos autos, estes deveriam ser utilizados, em

32. Segundo consta do site do Tribunal Regional da 12ª Região, o VERITAS “É um sistema desenvolvido pelo TRT12 para tratamento de dados de geolocalização de telefonia e Google Takeout Localização, com visualização em mapa e expedição de relatório amigável. Os dados de geolocalização podem ser utilizados como prova digital na fase de conhecimento (vínculo, jornada, hora extra, etc) e na fase de execução (bem de família, mapeamento de laranjas, etc)”. Disponível em: <https://portal.trt12.jus.br/sexec-estrutura/provas-digitais>. Acesso em: 16 jan. 2025.

33. A título de exemplo, podemos citar decisões que proíbem o uso da geolocalização: 1.) Do TRT 3ª Região: Autos nº 0010322-07.2022.5.03.0000 (Rel. Angela Ribeiro, 01 ago. 2022); Autos nº 0011685-29.2022.5.03.0000 (Rel. Sérgio de Alencar, 02 dez. 2022); Autos nº 0010813-39.2020.5.03.0079 (Rel. Angela Ribeiro, 07 out. 2022), e 2.) Do TRT 12ª Região: Autos nº 0000658-34.2021.5.12.0000 (Rel. Gisele Alexandrino, 27 out. 2021), e outras decisões que autorizam o uso da geolocalização: Do TRT 12ª Região: Autos nº 0000239-77.2022.5.12.0000 (Rel. Gracio Petrone, 31 ago. 2022) e Autos nº 0000114-12.2022.5.12.0000 (Rel. Narbal Fileti, 28 set. 2022).

detrimento da prova digital³⁴. Assim, o voto sustenta que não se mostra necessária a utilização da geolocalização como primeira prova, uma vez que há o cartão de ponto, por exemplo, menos invasivo ao indivíduo, e que, inclusive, consiste em forma específica de controle prevista em lei, além de obrigação legal intrínseca daqueles que utilizam mão-de-obra assalariada e mediante subordinação, nos termos do artigo 74 da CLT³⁵.

Não bastasse isso, alega que, no caso dos autos, há informação de que o impetrante teria exercido a função de gerência e que não teria direito a horas extraordinárias, demonstrando, portanto, que a produção de tal prova não seria adequada, pois não se prestaria à finalidade pretendida, além de se configurar contraditória. Sendo assim, afirma que a realização da prova da geolocalização, naquele momento, seria abusiva.

Outro ponto relevante evidenciado no voto divergente, relaciona-se com o fato de que a prova da geolocalização tem sido deferida de forma excepcional nos processos criminais para apuração de crimes dolosos e complexos, nos quais tal instrumento teria se mostrado menos gravoso para alcançar a finalidade pretendida, o que se diferenciaria das condições tratadas no processo do trabalho.

Por fim, o voto destaca que não houve fundamentação exauriente no deferimento da prova digital, e que as vantagens do ato na aferição processual da jornada de trabalho não superariam as suas desvantagens quanto à violação à privacidade e à intimidade do indivíduo, motivos esses que serviriam de alerta para o perigo do retrocesso social, por permitirem o uso de meios de prova agressivos de forma corriqueira e indiscriminada.

Com efeito, tais ponderações são de considerável importância e demonstram uma postura mais protecionista e preocupada com os possíveis efeitos que a banalização dos meios tecnológicos possam ocasionar à vida dos indivíduos.

Vale destacar, contudo, que para além dos argumentos explanados, há outros que merecem nossa atenção. Todavia, considerando a limitação do nosso

34. Cabe citar, no mesmo sentido, Enunciado da Associação Nacional dos Magistrados da Justiça do Trabalho (ANAMATRA): 3ª Edição – Aprovados Jornada. Comissões 4-5: Acesso à Justiça e Provas Digitais. Ordem 6: Registros de Geolocalização – meio de prova. Ementa: “Os registros de geolocalização podem ser utilizados como meio de prova em processo judicial, desde que observados os requisitos de necessidade e proporcionalidade, não havendo direito líquido e certo à produção de tal prova, quando os fatos puderem ser demonstrados pelos meios ordinários e menos invasivos da privacidade das partes”. Disponível em: <https://www.anamatra.org.br/jornada/a-jornada/3-edicao-aprovados-jornada>. Acesso em: 20 jan. 2025.

35. “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. § 3º Se o trabalho for executado fora do estabelecimento, o horário dos empregados constará do registro manual, mecânico ou eletrônico em seu poder, sem prejuízo do que dispõe o caput deste artigo. § 4º Fica permitida a utilização de registro de ponto por exceção à jornada regular de trabalho, mediante acordo individual escrito, convenção coletiva ou acordo coletivo de trabalho”. BRASIL. Consolidação das Leis do Trabalho. *Op. Cit.*

objeto de estudo, vamos nos ater, brevemente, a um em especial: a questão de dados pessoais com inferências sensíveis.

3.3. Tratamento sensível de dados pessoais provenientes da geolocalização

Sabe-se que os benefícios da tecnologia na vida cotidiana são imensuráveis. Entretanto, os argumentos que visam à proteção dos direitos fundamentais à privacidade e à intimidade, em face dos meios tecnológicos, são, também, inúmeros e de alto grau de relevância jurídica e social.

Acerca de tal garantia, lecionam Gilmar Mendes e Paulo Branco, ao dizerem que o direito à privacidade e à intimidade é proclamado como resultado da necessidade de o indivíduo “encontrar na solidão a paz e o equilíbrio, continuamente comprometido pelo ritmo da vida moderna”³⁶.

Cabe ressaltar que a preocupação com o desenvolvimento da personalidade e com as interferências ou ataques ilegais ou arbitrários à vida privada se origina em tempos remotos, tal como previsto no art. 17 do Pacto Internacional sobre Direitos Civis e Políticos de 1966 (Decreto nº 592/1992)³⁷ e no art. 11 da Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica, Decreto nº 678/1992)³⁸, e é transportada para os dias atuais, como forma de preservar o direito à privacidade no ambiente digital.

Sob esse prisma, ao incluir a proteção aos dados pessoais, inclusive nos meios digitais, entre o rol de direitos fundamentais consagrados no art. 5º da CF/1988, nota-se que a preocupação com a proteção se expande não só em relação aos dados decorrentes do processo comunicativo entre os indivíduos em sociedade (art. 5º, XII, da CF/1988), como também no que tange aos dados pessoais disseminados pelos indivíduos através de vários meios de comunica-

36. MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional*. São Paulo: Saraiva, 2013, p. 280-281.

37. “Art. 17: 1. Ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação. 2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas”. BRASIL. Decreto nº 592, de 6 de julho de 1992. Atos Internacionais. Pacto Internacional sobre Direitos Civis e Políticos. Promulgação. Brasília, DF: Presidência da República. Disponível em: <https://www.gov.br/mdh/pt-br/navegue-por-temas/atuacao-internacional/organizacao-das-nacoes-unidas-onu/convencoes-internacionais/pacto-internacional-sobre-direitos-civis-e-politicos-1992/pidcp-decreto-no-592-de-6-de-julho-de-1992.pdf>. Acesso em: 19 jan. 2025.

38. “Art. 11: Proteção da Honra e da Dignidade. 1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade. 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação. 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas”. BRASIL. Decreto nº 678, de 6 de novembro de 1992. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso em 19 jan. 2025.

ção social³⁹ (art. 5º, LXXIX, da CF/1988, incluído pela Emenda Constitucional nº 115, de 2022).

Neste contexto, deve ser levado em consideração que, muito embora possa ajudar a comprovar a realização ou não de horas extras, a prova digital da geolocalização pode liberar o acesso a dados que, inicialmente podem sinalizar irrelevantes, mas, após o tratamento, podem revelar características e vulnerabilidades de seus titulares, com alto potencial lesivo e discriminatório, tais como dados sensíveis relativos à religião, opinião política e dados de saúde.

Sob essa ótica, Chiara de Teffé sustenta que ainda que certos dados não sejam formalmente sensíveis e que, em determinado momento pareçam não relevantes, ou que não especifiquem alguém diretamente, “uma vez transferidos, cruzados e/ou organizados, podem resultar em dados bastante específicos sobre determinada pessoa, trazendo informações, inclusive, de caráter sensível sobre ela”⁴⁰.

Neste sentido, a referida autora destaca o enunciado nº 690, aprovado na IX Jornada de Direito Civil do Conselho da Justiça Federal em maio de 2022 que define que “a proteção ampliada conferida pela LGPD aos dados sensíveis deverá ser também aplicada aos casos em que houver tratamento sensível de dados pessoais, tal como observado no §1º do art. 11 da LGPD”⁴¹.

Outrossim, vale ressaltar que tais dados inferidos – entendidos como aqueles que não são diretamente fornecidos pelo titular, mas deduzidos a partir de cruzamentos ou análises automatizadas –, podem representar riscos ainda maiores – do que os dados declarados – à privacidade do indivíduo. Isto porque, por não dependerem de uma manifestação consciente do titular, escapam de seu controle e de sua percepção direta.

Por essa razão, autores como Sandra Wachter e Brent Mittelstadt⁴² entendem que os dados inferidos podem receber padrões mais altos de proteção de dados, como os concedidos a dados sensíveis, em dois momentos: I.) quando dados inferidos ou derivados revelarem diretamente atributos protegidos, tal como a etnia de uma pessoa através do acesso de seu histórico educacional

39. Para melhor análise deste novo prisma de proteção, recomenda-se a seguinte leitura: DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 3. ed. São Paulo: Revista dos Tribunais, 2021.

40. TEFFÉ, Chiara Spadaccini de. *Dados pessoais sensíveis: qualificação, tratamento e boas práticas*. Indaiatuba, SP: Editora Foco, 2022. p. 11 e 39.

41. “Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: (...) § 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”

42. WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: Re-thinking data protection law in the age of Big Data and AI. *Columbia Business Law Review*, v. 2019, Issue 2, p.72. Disponível em: <https://ssrn.com/abstract=3248829>. Acesso em: 16 abr. 2025.

(revelados diretamente), e II.) quando dados pessoais puderem ser mostrados para permitir a inferência de atributos sensíveis (revelados indiretamente) – como, por exemplo, a possibilidade de inferir a raça de uma pessoa através do seu sobrenome ou do seu local de nascimento.

Ainda, podemos mencionar que a vigilância constante e a ausência de limites claros à coleta e ao uso de dados pessoais podem gerar um “efeito inibidor” ou “efeito amedrontador” (*chilling effect*)⁴³, de forma a desencorajar certos indivíduos a praticarem comportamentos lícitos, com receio de serem monitorados ou rastreados, e, conseqüentemente, enfraquecerem direitos fundamentais, como o direito à privacidade, a liberdade de expressão e de associação.

Tal efeito se agrava diante da normalização de ferramentas invasivas, como a utilização da geolocalização em litígios cotidianos. Por essa razão, o uso irrestrito dessa tecnologia pode deseducar a cultura jurídica e social quanto à centralidade da proteção de dados, esvaziando sua função protetiva e contribuindo para um ambiente de vigilância rotineira⁴⁴, especialmente se o Judiciário passar a legitimar tal prática em litígios de pequeno valor, como ações trabalhistas sobre diferenças de horas extras.

Adicionalmente, corre-se o risco de abertura de um precedente perigoso. Se a proteção de dados pessoais for relativizada, isso pode ensejar um efeito dominó, de forma a autorizar que outros ramos do Direito também passem a flexibilizar garantias fundamentais com base em critérios utilitaristas e pragmáticos.

A banalização dessa relativização pode comprometer a solidez dos direitos fundamentais à privacidade e à proteção de dados, que devem ser resguardados de forma equânime em qualquer esfera jurídica. Há o risco, portanto, da exceção se tornar regra.

Com efeito, a proteção de dados deve ser compreendida como valor estruturante do Estado Democrático de Direito e não como um obstáculo à obtenção da verdade processual.

Assim, a partir das premissas delineadas dentro deste estudo, e considerando, sistematicamente, todo o arcabouço normativo-axiológico da Consti-

43. Para melhor compreensão acerca do efeito “chilling”, recomenda-se a seguinte leitura: BÜCHI, Moritz et al. The chilling effects of algorithmic profiling: Mapping the issues. *Computer law & security review*, v. 36, p. 105367, 2020. Disponível em: <https://doi.org/10.1016/j.clsr.2019.105367>. Acesso em: 15 abr. 2025.

44. Neste contexto, vale citar o fenômeno do “capitalismo de vigilância”, descrito por Shoshana Zuboff em sua obra, onde afirma que a captura de dados transforma não só a economia, mas também as relações sociais e laborais, e se alimenta “de todo aspecto de toda a experiência humana”. ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução de George Schlesinger. 1. ed. Rio de Janeiro: Intrínseca, 2020, p. 20.

tuição Federal e dos demais instrumentos legais, nos parece manifestamente desarrazoada a utilização da prova digital da geolocalização para fins de comprovação de horas extras, quando sopesada com o resultado da diligência, *in casu*, meramente patrimonial e corriqueiramente de pequena monta (diferenças de horas-extras).

Seguindo a mesma linha de raciocínio, Walter Vegas Júnior⁴⁵ ressalta que a atuação esperada de um juiz, ao longo de uma instrução probatória que utilize dados provenientes da geolocalização, também deve ser feita de forma sistêmica, destacando que:

É preciso que o juiz, ao eventualmente ser provocado para a produção de um determinado meio de prova, analise a pertinência, relevância e também a respectiva admissibilidade da prova à luz de todo o ordenamento jurídico. Assim como ocorre no âmbito de pesquisas científicas e também em outros contextos investigativos existem limites decorrentes de outros valores consagrados como de maior relevância em cada campo do conhecimento ou de atuação humana, o que fica ainda mais evidente quando se cogita do exercício de parcela de poder em um Estado Democrático de Direito, como aquele albergado na CF/1988.

Considerações finais

As novas tecnologias têm provocado profundas transformações não apenas nas relações sociais, como também têm ocasionado reflexos diretos nos processos judiciais, já que em uma sociedade hiperconectada há produção massiva de dados no mundo digital, os quais podem ser utilizados para a demonstração de fatos alegados em juízo.

Sob essa perspectiva, como forma de acompanhar os avanços tecnológicos e de abarcar os dados produzidos e armazenados no espaço virtual, os meios probatórios também sofreram alterações.

Nesse contexto, insere-se a prova digital, considerada como uma ferramenta capaz de comprovar a ocorrência de um fato produzido no meio digital ou através de um meio digital, como, por exemplo, a utilização da geolocalização no mapeamento da localização e dos deslocamentos de uma pessoa, para fins de comprovação de horas extras em um processo trabalhista.

45. VEGAS JÚNIOR, Walter Rosati. A geolocalização como panaceia no processo do trabalho. *Revista do Tribunal do Trabalho da 2ª Região*, São Paulo, v. 15, n. 30, p. 182-202, jul./dez. 2023.

Da análise do arcabouço jurídico, sob o prisma do princípio da legalidade, é possível verificar que há substrato legal que fundamente e valide a utilização das provas digitais, bem como não se constata vedação legal ao uso de tal diligência probatória.

O imbróglio, contudo, está na aferição da admissibilidade do uso da prova digital da geolocalização frente aos princípios e direitos fundamentais em rota de colisão, notadamente do direito à intimidade/privacidade (CF, 5º, X), à proteção de dados pessoais (CF, 5º, LXXIX) e ao sigilo de comunicações telefônicas e telemáticas (CF, 5º, XII) *versus* o direito à informação e realização da prova, consagrados nos princípios do contraditório e da ampla defesa (CF, 5º, LV).

Com a pesquisa realizada, nota-se que não há entendimento pacífico sobre a temática, inclusive diante da análise do recente julgamento do processo ROT nº 23218-21.2023.5.04.0000, da SDI II do TST, que, apesar de reconhecer, por maioria de votos, a adequação, a necessidade e a proporcionalidade da prova digital da geolocalização, para fins de comprovação de horas extras em um processo trabalhista; traz em seu voto vencido ponderações consideráveis e um alerta para o perigo do retrocesso social, tendo em vista o uso banalizado deste meio de prova.

Em suma, ao adicionar aos argumentos explanados, uma breve análise sobre a questão dos dados pessoais com inferências sensíveis, corrobora-se o entendimento de que a utilização da prova digital da geolocalização, para fins de comprovação de horas extras, mostra-se descabida quando sopesados o arcabouço normativo-axiológico da Constituição Federal e dos demais aparatos legais, com o resultado meramente patrimonial da diligência.

Referências

ALBINO, João Pedro Donaire; LIMA, Ana Cláudia Pires Ferreira de. Técnicas de captura de geolocalização para produção de prova judicial. *Revista Direito das Relações Sociais e Trabalhistas*, São Paulo, v. 8, n. 1, p. 216-233, jan./jun. 2022.

ALEX, Robert. *Teoria dos direitos fundamentais*. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008.

BRASIL. Associação Nacional Dos Magistrados Da Justiça Do Trabalho (ANAMATRA). Comissões 4-5: acesso à justiça e provas digitais. Ordem 6: registros de geolocalização – meio de prova. Disponível em: <https://www.anamatra.org.br/jornada/a-jornada/3-edicao-aprovados-jornada>. Acesso em: 20 jan. 2025.

BRASIL. Conselho Nacional de Justiça. *Resolução nº 335, de 29 de setembro de 2020*. Dispõe sobre a governança e a gestão de provas digitais no âmbito do Poder Judiciário. Diário da Justiça Eletrônico, Brasília, DF, n. 250, 1 out. 2020. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3516>. Acesso em: 14 abr. 2025.

BRASIL. Constituição de 1988. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 11 jan. 2025.

BRASIL. *Decreto nº 592, de 6 de julho de 1992*. Atos Internacionais. Pacto Internacional sobre Direitos Civis e Políticos. Promulgação. Brasília, DF: Presidência da República. Disponível em: <https://www.gov.br/mdh/pt-br/navegue-por-temas/atuacao-internacional/organizacao-das-nacoes-unidas-onu/convencoes-internacionais/pacto-internacional-sobre-direitos-civis-e-politicos-1992/pidcp-decreto-no-592-de-6-de-julho-de-1992.pdf>. Acesso em: 19 jan. 2025.

BRASIL. *Decreto nº 678, de 6 de novembro de 1992*. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso em 19 jan. 2025.

BRASIL. *Decreto-lei nº 5.452, de 1º de maio de 1943*. Aprova a Consolidação das Leis do Trabalho. Diário Oficial da União, Rio de Janeiro, RJ, 09 ago. 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 11 jan. 2025.

BRASIL. *Lei nº 12.527, de 18 de novembro de 2011*. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União, Brasília, DF, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 11 jan. 2025.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11 jan. 2025.

BRASIL. *Lei nº 13.105, de 16 de março de 2015*. Institui o Código de Processo Civil. Diário Oficial da União, Brasília, DF, 17 mar. 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 11 jan. 2025.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 jan. 2025.

BRASIL. Superior Tribunal de Justiça. (5ª Turma). *AgRg no RMS n. 68.487/PE*. Relator: Min. Ribeiro Dantas. Julgamento: 06/09/2022. Publicação: 15/09/2022. Disponível em: <https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=2210707&tipo=0&nreg=202200716193&SeqCgrmaSesao=&CodOrgaoJgdr=&dt=20220915&formato=PDF&salvar=false>. Acesso em: 16 jan. 2025.

BRASIL. Superior Tribunal de Justiça. (Decisão monocrática). *HC n. 918281/MT (2024/0198335-0)*. Relator: Ministro Jesuino Rissato (Desembargador Convocado do TJDF). Julgamento: 01/08/2024. Publicação: 02/08/2024. Disponível em: <https://www.stj.jus.br>. Acesso em: 17 abr. 2025.

BRASIL. Supremo Tribunal Federal. (2ª Turma). *HC n. 91.867/PA*. Relator: Min. Gilmar Mendes. Julgamento: 24/04/2012. Publicação: 20/09/2012. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=98970411&ext=.pdf>. Acesso em: 15 jan. 2025.

BRASIL. Supremo Tribunal Federal. (Tribunal Pleno). *RE n. 418.416/SC*. Relator: Min. Sepúlveda Pertence. Julgamento: 10/05/2006. Publicação: 19/12/2006. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=2205705>. Acesso em: 15 jan. 2025.

BRASIL. Tribunal Superior do Trabalho. (Subseção II Especializada em Dissídios Individuais). *ROT n. 23218-21.2023.5.04.0000*. Relator Ministro Amaury Rodrigues Pinto Junior. Julgamento: 14/05/2024. Publicação: 14/06/2024. Disponível em: <https://jurisprudencia-backend2.tst.jus.br/rest/documentos/4ec98fa07117dd4cd23754bdd6e23c8b>. Acesso em: 15 jan. 2025.

BÜCHI, Moritz et al. The chilling effects of algorithmic profiling: Mapping the issues. *Computer law & security review*, v. 36, p. 105367, 2020. Disponível em: <https://doi.org/10.1016/j.clsr.2019.105367>. Acesso em: 15 abr. 2025.

CAPANEMA, Walter Aranha. *Manual de direito digital*. Teoria e Prática. Salvador: JusPodivm, 2024.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 3. ed. São Paulo: Revista dos Tribunais, 2021.

JUNQUEIRA, Fernanda; HIGA, Flávio. Admissibilidade das Provas Digitais na ordem processual: o que se faz na nuvem; fica na nuvem. *Anuario de la Facultad de Derecho*. Universidad de Extremadura 38 (2022): 329-348. ISSN: 0213-988X –ISSN-e: 2695-7728.

LIMA, Andréa Ferreira; NUNES, Vanessa Ester Ferreira; VIEIRA, Carolina Mesquita. Provas digitais no processo do trabalho: a validade do uso da geolocalização. *Revista do Tribunal Superior do Trabalho*, Porto Alegre, v. 90, n. 3, p. 84-110, jul./set. 2024.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional*. São Paulo: Saraiva, 2013.

NOVELINO, Marcelo. *Manual de direito constitucional*. Rio de Janeiro: Forense; São Paulo: Método, 2014.

SOARES, Pollyana Lúcia Rosado. As provas digitais no processo do trabalho. *Revista do Tribunal Regional do Trabalho da 3ª Região*, Belo Horizonte, v. 67, n. 104, p. 287-295, jul./dez. 2021.

TEFFÉ, Chiara Spadaccini de. *Dados pessoais sensíveis: qualificação, tratamento e boas práticas*. Indaiatuba, SP: Editora Foco, 2022.

THAMAY, Rennan; TAMER, Mauricio. *Provas no direito digital: conceito da prova digital, procedimentos e provas digitais em espécie*. São Paulo: Thomson Reuters Brasil, 2020.

VEGAS JÚNIOR, Walter Rosati. A geolocalização como panaceia no processo do trabalho. *Revista do Tribunal do Trabalho da 2ª Região*, São Paulo, v. 15, n. 30, p. 182-202, jul./dez. 2023.

WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: Re-thinking data protection law in the age of Big Data and AI. *Columbia Business Law Review*, v. 2019, Issue 2, p.01-130. Disponível em: <https://ssrn.com/abstract=3248829>. Acesso em: 16 abr. 2025.

ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução de George Schlesinger. 1. ed. Rio de Janeiro: Intrínseca, 2020.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

5

Limites do consentimento na LGPD

MICHEL SACHS FEUZ

Sumário: Introdução; 1. Limites do Consentimento; 2. Consentimento na LGPD; 3. Limites do Consentimento na Publicidade Personalizada; Considerações Finais.

Introdução

A contemporaneidade é marcada por uma profunda interconexão entre avanços tecnológicos, o surgimento do conceito de sociedade da informação² e a indispensabilidade da coleta e tratamento de dados pessoais, de tal maneira que a informação armazenada em meios digitais se tornou o bem mais precioso³. Em virtude disso, com o surgimento de grandes bancos de dados, e a possibilidade de que um alto fluxo de informações aconteça, o dado passa a representar importante instrumento de poder – não à toa, tem sido chamado de “novo petróleo”⁴.

Nesse contexto, a Lei Geral de Proteção de Dados (LGPD) desponta como marco regulatório fundamental no ordenamento jurídico brasileiro, estabelecendo parâmetros essenciais para a salvaguarda da privacidade em meio à era da informação. Esta legislação, inspirada nos preceitos da Regulação Geral de Proteção de Dados (GDPR), estabelece princípios e diretrizes que buscam equilibrar a crescente necessidade de inovação tecnológica e a proteção efetiva dos direitos individuais relacionados.

O presente estudo se propõe a uma análise dos limites do consentimento no contexto da LGPD. À medida que a sociedade da informação se desenvolve e a tecnologia se torna um agente central nas interrelações sociais e financeiras, é imperativo compreender como os princípios e disposições da LGPD moldam as práticas de coleta, tratamento e consentimento de dados pessoais.

Neste íterim, a evolução tecnológica, voltada predominantemente para a monetização e busca incessante pelo lucro, promoveu a globalização e o processamento massivo de dados. Isso propiciou a criação de uma sociedade informacional, na qual o desenvolvimento econômico está intrinsecamente ligado à captura e utilização de informações dos mais diversos mercados alvos. Contudo, essa transformação não ocorre sem desafios, especialmente no que

1. Pós-graduando em Direito Digital e Novas Tecnologias pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS RIO), em parceria com a Universidade do Estado do Rio de Janeiro (UERJ). Graduado pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Advogado integrante do escritório TozziniFreire Advogados.

2. SENISE, Lisboa, R. *O Direito na Sociedade da Informação IV*. Grupo Almedina (Portugal), 2020.

3. MCAFEE, Andrew; BRYNJOLFSSON, Erik. *A segunda era das máquinas* – Rio de Janeiro: Alta Books, 2014.

4. The Economist. *The world's most valuable resource is no longer oil, but data*. <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 19 jan. 2025.

tange à privacidade dos indivíduos e a concessão dos respectivos consentimentos, viabilizando a reflexão sobre os conceitos subjetivos de liberdade em meio à contemporaneidade.

Nesse cenário, é essencial estudar o consentimento como um dos pilares do tratamento de dados pessoais. O presente trabalho se propõe a lançar luz sobre a intrincada relação entre avanços tecnológicos e o consentimento na coleta de dados pessoais, delineando os desafios e perspectivas que se apresentam diante da crescente digitalização das relações sociais e econômicas.

Assim, pertinente realizar a seguinte reflexão: Quais são os principais limites do consentimento como base legal para o tratamento de dados pessoais sob a perspectiva da LGPD, especialmente em contextos de publicidade personalizada?”

O presente trabalho busca analisar de forma crítica se a base legal do consentimento, na forma em que exigida e delimitada pela LGPD, é suficiente para garantir a autodeterminação informacional dos titulares de dados.

1. Limites do Consentimento

Com o presente trabalho, busca-se verificar quais são os principais desafios enfrentados pela base legal do consentimento da LGPD para que sua efetividade seja mantida, respeitando, de forma clara e específica, a finalidade do tratamento de dados quando da anuência do titular, bem como seu desejo em interromper ou se informar sobre a utilização de seus dados.

Nesta toada, mostra-se fundamental analisar, de forma balanceada, a importância dos dados para o desenvolvimento econômico na sociedade da informação, face às necessidades de se garantir a proteção dos anseios do titular dos dados quando da sua declaração de vontade, de modo que o consentimento dado seja livre, inequívoco, informado, e passível de revogação a qualquer momento.

Em relação ao consentimento, é imperioso o reconhecimento de que se trata de apenas uma das bases legais elencadas na LGPD, isto é, refere-se a uma das possibilidades legalmente previstas para que ocorra o tratamento de dados – e não a única.

Ou seja, quando o titular concede seu consentimento específico, é permitido que o agente de tratamento de dados promova o processamento de suas informações, desde que respeite os ditames legais relacionados.

É importante ressaltar que não há hierarquia entre as hipóteses legais disciplinadas pela LGPD, de forma que uma não prevalece, e nem mesmo depende da outra.

Inclusive, a jurisprudência dos tribunais brasileiros têm convergido para interpretar o art. 7º da LGPD desta maneira, reconhecendo a desnecessidade de concordância do titular para que ocorra o tratamento de dados quando aplicáveis outras bases de tratamento, tal como a de proteção ao crédito, como no exemplo do julgado a seguir destacado:

AGRAVO DE INSTRUMENTO – OBRIGAÇÃO DE FAZER – Decisão que deferiu a tutela de urgência pleiteada pela autora, e determinou à ré Boa Vista Serviços S/A, que se abstinhasse, imediatamente, de divulgar, permitir o acesso ou compartilhar dados pessoais da autora, por meio dos produtos “ACERTA Essencial”, “ACERTA Intermediário”, “ACERTA Completo” e “DATAPLUS”, sem o consentimento dela. Insurgência. Acolhimento em parte. Indícios de exercício regular de direito pela agravante, que mantém cadastros que visam proteção ao crédito, amparada pelo art. 7º, X da LGPD. Contudo, foi constatado o compartilhamento de dados que não guardam relação com a proteção ao crédito, como número do título de eleitor, nome da mãe, estilo de vida, classe social, escolaridade, classe de propensão ao consumo e georreferenciamento. Concessão parcial da ordem, determinando a exclusão de todos os dados que não digam respeito diretamente à proteção do crédito, sendo autorizado o compartilhamento apenas da situação do CPF na Receita Federal; restrições financeiras e atividade de crédito. Recurso parcialmente provido. (...). **No sentir desta relatoria, não se mostra razoável necessitar da concordância para compartilhamento de informações imprescindíveis à atividade de proteção ao crédito (...). Assim, resta clara a intenção do legislador ao prever, em hipóteses distintas, o tratamento de dados pessoais mediante consentimento do titular e para a proteção do crédito, a demonstrar que, neste caso, não há necessidade de consentimento.** (TJSP; Agravo de Instrumento 2086090-11.2022.8.26.0000; Relator (a): João Baptista Galhardo Júnior; Órgão Julgador: 2ª Câmara de Direito Privado; Foro de Ribeirão Preto – 5ª Vara Cível; Data do Julgamento: 01/07/2022; Data de Registro: 01/07/2022)

Pelo exposto, foi observado que o consentimento é uma das bases legais em que se permite o tratamento de dados. Em que pese tal constatação, não se pode perder de vista os desafios encontrados pela definição do consentimento como vetor central para a garantia da proteção de dados pessoais.

Neste aspecto, é diversamente questionada a efetividade de um panorama normativo que centraliza o poder de escolha dos indivíduos como protagonista, embora existam previsões legais, tanto na GDPR, quanto na LGPD, determinando que este seja livre, informado, inequívoco, explícito e específico.

Ressalta-se que o EDPS (European Data Protection Board) possui guia orientativo⁵ acerca do tratamento de dados sob a base legal do consentimento, na perspectiva da GDPR. Em tal estudo, é recomendado que tal base seja evitada quando há desequilíbrio de poder (como em plataformas digitais). O guia destaca ainda que o consentimento deve ser considerada uma base legal apropriada apenas quando é oferecida uma genuína faculdade ao titular quanto a seu aceite ou declínio dos termos oferecidos, ou uma recusa sem detrimento.

No aspecto, referido guia orientativo também destaca que o consentimento deve ser livremente concedido; específico; informado; e inequívoco.

Logo, pode-se entender como principais desafios para manutenção de um consentimento válido (i) a disponibilização de informação insuficiente acerca do tratamento de dados; (ii) eventual existência de vícios de vontade; (iii) consentimento concedido de maneira coercitiva ou forçada, em que o consumidor é compelido a aceitar as políticas de dados para que haja aderência a um determinado serviço oferecido; (iv) desatualização automática; e (v) ausência de mecanismos eficazes para postulação do direito de revogação do consentimento.

2. Consentimento na LGPD

Para tratar da matéria do consentimento na LGPD, é necessário, antes, destacar brevemente o contexto das gerações das Leis de Proteção de Dados na história.

A primeira geração de leis buscou normatizar principalmente a coleta de dados realizada pelo Estado, se preocupando com o massivo processamento de informações da população. Nesta oportunidade, priorizou-se restringir a criação de bancos de dados, que somente poderiam ser desenvolvidos sob concessões estatais.

Com o aumento de tecnologias, e consequentemente do número de bancos de dados, e de agentes atuantes na esfera do tratamento de dados – trans-

5. EUROPEAN DATA PROTECTION BOARD. *Guidelines 05/2020 on consent under Regulation 2016/679*. 2020. Disponível em: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Acesso em: 16 abr. 2025.

cendendo a hegemonia estatal na matéria – foi identificada a necessidade de adequação dos regimes legais, subitamente para tutelar este tipo de relação envolvendo a atividade privada. Desta forma, considerando o aumento desproporcional nas relações de tratamento de dados, tornou-se inviável a manutenção das disposições legislativas que incumbiam somente à atividade estatal regulamentar a criação e funcionamento de todos os bancos de dados existentes.

Anteriormente cabia ao Estado autorizar o compartilhamento de informações de seus cidadãos. No entanto, com a segunda geração de leis, foi determinado que próprio titular seria o responsável por tutelar seus dados, o qual, pela concessão de seu consentimento, declara sua faculdade para que haja a coleta, uso e compartilhamento de seus dados pessoais, por terceiros⁶. Ou, seja, se deu uma ênfase à autonomia individual subjetiva do titular em controlar o fluxo de suas informações pessoais⁷.

Já na terceira geração de leis, verificou-se a importância dada à amplitude do papel protagonista transferido ao titular, na esfera da proteção de dados pessoais, devendo-se destacar a maneira pela qual as normas de proteção de dados pessoais visavam garantir que o indivíduo fosse o agente ativo em todos os fluxos de dados, que lhe eram pertinentes, desde a coleta até o compartilhamento com terceiros.

Assim, foi criado o conceito da “autodeterminação informacional”, uma vez que foi viabilizado, ao consumidor, obter um controle amplo e efetivo sobre as informações inerentes a sua personalidade subjetiva.

Perceptível que, desde a formação da segunda geração, já havia discussões sobre as estratégias legislativas, focadas no poder de escolha dos indivíduos, sendo, neste cenário, que surgem as respostas normativas, marcadas pelas novas gerações legislativas, que visavam corrigir tais pontos, flexibilizando o entendimento legislativo que dispunha do consentimento do consumidor, como vetor central, para que houvesse o tratamento de dados pessoais.

Tais mudanças visavam relativizar a regra geral, mas não foram suficientes para excluir de vez o protagonismo dado ao consentimento dos titulares. O que houve de fato foi uma racionalização e regulamentação do consentimento, tanto é que, pelas novas leis, é indispensável que ele seja livre, informado, inequívoco, explícito e específico.

6. MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. *Big Data: A revolution will transform how we live, work and think*. New York: Houghton Mifflin Publishing, 2013.

7. RODOTÀ, Stefano. *Il diritto di avere*. Roma: Laterza, 2012.

Assim sendo, percebe-se que a anuência do consumidor continua sendo o objeto central das relações de tratamento de dados. Todavia, ele é agora restringido, para que se respeite uma consolidação legítima dos reais anseios do titular.

Tal questão é, inclusive nítida na Lei Geral de Proteção de Dados (Lei 13.709/2018 ou LGPD), que explicita o consentimento como uma das bases legais, para que haja o tratamento de dados pessoais, exigindo, para tanto, que ele seja livre, informado, inequívoco, explícito e específico. Vale ressaltar, também, que, além do consentimento, há nove outras hipóteses reguladas pela Lei, que permitem o processamento das informações pessoais dos titulares.

Neste aspecto, destaca-se o caráter autônomo e individual de cada base legal, não havendo hierarquia de umas com as outras, de forma que o consentimento não é objetivamente imprescindível para que um indivíduo tenha seus dados pessoais como objeto de um fluxo operacional perante terceiros.

Contudo, mesmo em vista da previsão legal, como visto anteriormente, não é fácil, ao consumidor, identificar a real relevância e quantidade do fluxo de seus dados pessoais, em especial, por causa dos nítidos vícios das políticas de privacidade e demais documentos jurídicos, que dependem de clareza e transparência, de modo que não lhe é possibilitado um gerenciamento efetivo de seus dados pessoais e demais informações privadas.

Frente a isso, impulsionada pela liquidez das relações sociais e suas comunicações com a utilização das tecnologias, há uma tendência de que os consumidores se inclinam a preferir benesses e serviços imediatos, em detrimento de sua privacidade e da proteção de seus dados neurais.

No aspecto, se identifica mais uma vulnerabilidade imposta aos consumidores em relação aos processos de tratamento de dados pessoais: a assimetria informacional ante ideologias mercadológicas, que não atendem às expectativas de privacidade, criando embaraços à LGPD, para garantir que haja um consentimento efetivo e que se adeque às reais expectativas e anseios do consumidor.

Vislumbra-se, neste sentido, o conflito da validação do consentimento no contexto da LGPD, ainda mais quando se verifica a ineficiência das políticas de privacidade como meio de controle dos dados pessoais, limitando o real e efetivo controle do titular sobre seus próprios dados.

Não suficiente, há de se denotar que as políticas de privacidade possuem nítidos vícios, tendo em vista a ausência de clareza, transparência e possibilidade de compreensão por consumidores leigos, além de suas constantes

atualizações. Nestas pendências, a falta de poder de barganha do usuário e a demasiada influência de redes sociais, fazem com que o suposto controle pertencente ao titular de seus dados pessoais, pelo mero consentimento concedido, seja apenas uma ilusão.

No tocante à adjectivação do consentimento, válido salientar que, no contexto do direito civil, a trama do consentimento sempre se vinculou aos vícios do negócio jurídico, como o erro e a lesão, sendo que as legislações existentes, nesta matéria, buscavam garantir a efetiva declaração de vontade do contratante, a qual deve ser livre e consciente.

A ausência destes pontos é considerada um defeito no elemento volitivo da formação contratual, denominado “vício do consentimento”, o que viabiliza a anulabilidade do negócio jurídico pactuado sob essas condições. Inclusive, no art. 8º parágrafo 3º da LGPD, há vedação explícita ao tratamento de dados pessoais mediante vício do consentimento.

Agora, em relação às caracterizações do consentimento na LGPD ressalta-se preliminarmente que a informação adequada se traduz pela capacidade que o titular adquire para controlar seus dados, sendo peça fundamental para qualquer processo de tomada de decisão pelo consumidor.

O caráter informacional, em sua forma objetiva, denota a relação do conhecimento transferido por uma pessoa especialista, que detém os meios técnicos inerentes ao processamento de dados, a outra pessoa, leiga, mais vulnerável, ensejando na necessidade de que comunicação transmitida seja ostensiva, clara, perceptível, desde o início, de forma a garantir uma autoproteção ao leigo.

Assim, nota-se que a quantidade de informações deve ser alta o suficiente para possibilitar que o consumidor compreenda, de maneira efetiva e incontroversa, quais são as qualidades e características do bem ou serviço oferecido, bem como os eventuais riscos envolvidos. A LGPD não se ausenta deste racional, ao dispor que a informação, em seu aspecto qualitativo, deve ser clara, adequada e ostensiva, e ao desenvolver, em seu aspecto quantitativo, o rol dos tipos de informação que devem ser transmitidos ao consumidor.

Agora, no tocante ao adjetivo “livre”, pressupõe-se que o consentimento seja baseado no livre-arbítrio do titular e no seu discernimento de poder facultar, conscientemente, dentre as várias opções disponibilizadas, aquela que melhor representa seu real interesse. O foco está na importância de se informar ao cidadão quando a coleta de seus dados é condição essencial para que ele desfrute de um produto ou serviço. Em suma, o dever de que consentimento seja livre se traduz pela indispensabilidade de ele seja sem subordinação,

observando a assimetria de poder para que se garanta a voluntariedade do consentimento concedido pelo usuário.

Ademais, para se analisar o requisito de que o consentimento seja inequívoco, mister acentuar que o princípio da finalidade estipula a condição essencial de que o tratamento de dados goze de propósito específico e explícito. No liame do consentimento, isso se traduz pela exigência de que a declaração de vontade do consumidor seja direcionada para o propósito específico pelo qual seu consentimento foi dado, no âmbito relacional do compartilhamento de seus dados.

Essa imposição visa evitar a existência de consentimentos genéricos, como “para melhorar a experiência”. Portanto, o consentimento inequívoco busca se alinhar a determinada finalidade, de forma que não haja dúvidas se o indivíduo foi informado, de maneira adequada, sobre determinado tratamento de dados, para que ele possa tomar uma decisão livre.

A procura por um consentimento inequívoco implica avaliar de que maneira a configuração padrão de serviços e produtos coleta a quantidade mínima de dados possível. O consentimento granular, que concede ao titular a autorização fragmentada do fluxo de seus dados, reflete a necessidade de um processo decisório específico e inequívoco.

Em circunstâncias especiais, como a participação de terceiros, dados sensíveis, fragilidade do titular e transferência internacional para países com níveis mais baixos de proteção, aplica-se o termo “particular”. A LGPD busca uma “camada adicional” de proteção, exigindo um consentimento especial em que o cidadão concorde deliberadamente com riscos elevados.

A interpretação desse consentimento especial envolve mecanismos que despertem mais a atenção do titular, assegurando que o processo de deliberação seja destacado e inequívoco. O foco está na participação ativa do cidadão no controle dos dados, independentemente do termo específico ou expresso.

3. Limites do Consentimento na Publicidade Personalizada

3.1. Definição e riscos da Publicidade Personalizada

O uso desenfreado dos aplicativos de celulares e redes sociais possibilita que as empresas desenvolvam os perfis sociais das pessoas, de acordo com suas emoções, ou seja, retratos dos estados emocionais dos indivíduos⁸. Assim, é desenvolvida uma atividade empresarial consistente na captação, in-

8. BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2021.

interpretação e utilização de tais informações, as quais são, efetivamente, potencializadoras da difusão de mensagens publicitárias, além de uma análise discriminada do impacto emocional dos anúncios, frente aos consumidores.

Não passa imperceptível, portanto, a existência de uma vigilância imperativa sobre os consumidores, que monitora, desde seus hábitos, históricos de navegação e comportamentos, na rede mundial de computadores, como suas próprias emoções, informações estas que se tornam, sem dúvida alguma, transparentes. Desta feita, não impressiona a expressão adotada por Susanne Lace de “consumidor de vidro”⁹.

Adiante, cumpre verificar que, com a entrada em vigor da Lei Geral de Proteção de Dados, houve a delimitação das hipóteses legais para que o tratamento de dados ocorra, tal como o consentimento.

3.2. Interpretação da LGPD Sobre Duração do Consentimento

Face a preocupação de empresas quanto ao tempo de armazenamento de dados pessoais, em relação às finalidades de tratamento de seus dados, e o tempo de duração de seu consentimento, diversos questionamentos se insurgem quanto à subsistência da anuência do titular, mais especificamente no que diz respeito ao envio de publicidade. Diante do dado cenário, se mostra válida a reflexão sobre qual é o prazo de duração do consentimento disposto pelo titular, e se ele pode ser por tempo indeterminado.

Em simples análise, pode-se perceber que a redação da LGPD não discrimina qual é a extensão temporal do consentimento, e nem mesmo faz menção acerca da possibilidade de consentimento por prazo indeterminado. Entretanto, é possível a obtenção de respostas a partir da interpretação de dispositivos do referido texto legal.

O art. 15 da Lei define as situações que ensejam no término de tratamento de dados:

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;

9. LACE, Susanne. The glass consumer: life in a surveillance society. Bristol: Policy Press, 2005.

- 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.

À vista deste dispositivo, é cabível a interpretação de que o consentimento se exaure ao passo em que finalizado o tratamento dos dados, sendo destacável a hipótese de quando alcançada a sua finalidade, ou o tratamento for desnecessário para tanto, bem como quando ocorrer o *“fim do período de tratamento”*.

De toda sorte, essa menção ao *“período de tratamento”* não significa dizer que sempre deverá haver determinação temporal no consentimento para o tratamento. Observa-se que não há impedimento legal para período indeterminado de tratamento, desde que condizente com a finalidade do tratamento.

O que a LGPD exige é que o consentimento tenha finalidades determinadas (art. 8º, § 4º), sendo que, se esta for compatível com uma indeterminação temporal, o consentimento e o tratamento podem sim ser por prazo indeterminado. Em suma, o que ocorre é que a longevidade da anuência concedida pelo titular é condicionada, não somente à revogação ou não de seu consentimento, mas também à finalidade previamente adotada para o tratamento de seus dados. Assim, exaurindo o objetivo, exaure-se também a autorização.

Observa-se que tal discussão se adequa, inclusive, no contexto do envio de publicidade. Caso o consentimento seja concedido no sentido de autorizar o recebimento de campanhas e promoções de uma determinada empresa que vão surgindo ao longo do tempo, a indeterminação temporal é compatível com a própria finalidade do tratamento consentido pela pessoa.

Por outro lado, caso o consentimento tenha ocorrido somente no sentido de participação em uma campanha ou promoção específica, a finalidade do tratamento está detidamente associada àquela campanha ou promoção. Assim, com o seu término, se encerra também a finalidade e, conseqüentemente, a possibilidade de tratamento – por conta da ausência de consentimento, que é diretamente condicionado ao objetivo do tratamento.

Apesar de a jurisprudência ainda não ter se manifestado sobre o assunto, possível compreender que haverá legalidade no tratamento se a indeterminação temporal for combinada, na forma do art. 8º, § 5º, da LGPD, com meios fáceis e acessíveis de revogação desse consentimento indeterminado, de preferência pelo próprio canal que é feito o envio da publicidade, como acontece em links de *“unsubscribe de mailing”*.

3.3. Boas Práticas Recomendadas

Como forma de prevenção de controvérsias em tratamento de dados e consentimento para envio de publicidade por prazo indeterminado, é recomendável que os agentes de tratamento insiram, nos próprios termos do consentimento, que este seja concedido por prazo indeterminado para o envio das publicidades da empresa que forem surgindo ao longo do tempo, vigorando até que ocorra a opção de revogação do tratamento de dados, pelo titular.

Além disso, por cautela, tem sido recomendado que empresas delimitem em seus sistemas internos um período máximo de guarda de dados, de forma a discriminar o tipo de dado obtido e sua respectiva finalidade, reavaliando, periodicamente, a necessidade de armazenamento tais informações. O cerne da questão se dá no sentido de que os dados devem ser guardados estritamente pelo tempo necessário para que cumpram com uma determinada finalidade previamente definida. Assim, sendo essa finalidade extinta, as informações armazenadas devem ser excluídas, objetivando a garantia de que os agentes de tratamento de dados estejam em conformidade com a LGPD.

Esta orientação é dada similarmente em governos europeus, atendendo às conformidades da GDPR (*General Data Protection Regulation*), que, por sua vez, também não estipula uma data limite para o consentimento concedido pelo titular. A Comissão Europeia¹⁰, já se posicionou no sentido de que dados devem ser guardados pelo menor período possível, observando as razões pelas quais determinadas informações foram coletadas, além do período de tratamento anteriormente pactuado, caso de fato tenha, além de sugerir que empresas definem limites temporais para apagar, ou revisar, as informações obtidas.

O posicionamento de instituições governamentais inglesas não é diferente, o DMA¹¹ (*Data & Marketing Association*), que apesar de reconhecer que a GDPR não especifica um prazo limite para o consentimento, orienta que deve ser considerado o contexto da anuência originalmente concedida, e as expectativas individuais dos consumidores, reforçando que, idealmente, é necessário que os agentes de tratamento tenham justificativa documentada quanto aos prazos que utiliza, a fim de satisfazer os requisitos da GDPR.

10. European Commission. *How long can data be kept and is it necessary to update it? Principles of the General Data Protection Regulation (GDPR)*. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en. Acesso em 15 jan. 2025.

11. DMA. *How long can you rely on consent or legitimate interest? DMA (Data & Marketing Association)*. Disponível em: <https://dma.org.uk/article/how-long-can-you-rely-on-consent-or-legitimate-interest>. Acesso em 15 jan. 2025.

Já a ICO¹² (*Information Commissioner's Office*) se posiciona nas mesmas linhas, criando uma lista de recomendações que devem ser observadas pelos agentes de tratamento, além de se aprofundar nos motivos destas orientações, respondendo questionamentos como: a importância da limitação de armazenamento; o que deve ser feito com os dados pessoais não mais necessários, dentre outros que auxiliam no entendimento do tema.

Considerações finais

O contexto estudado no presente trabalho se relaciona com a complexidade existente nas relações atuais, notadamente no vínculo existente entre os avanços tecnológicos, a coleta e tratamento de dados pessoais, e o consentimento dos titulares à luz da LGPD. Verificou-se, neste cenário, a evolução da sociedade da informação nos campos das interações sociais e financeiras, em que se confere à informação um papel central.

Foi verificado que o consentimento, atualmente, no campo teórico, é mais restrito, limitado, buscando representar o verdadeiro anseio do titular de dados. No entanto, a assimetria informacional dificulta que o consumidor tenha plena ciência sobre como suas informações estão sendo tratadas e utilizadas.

No aspecto, a LGPD exige que o consentimento seja livre, informado, inequívoco, explícito e específico. No entanto, a assimetria informacional dificulta que o consumidor tenha plena ciência sobre como suas informações estão sendo tratadas e utilizadas.

Além disso, para fins de verificação da temporalidade de duração do consentimento é essencial que esta base de tratamento de dados tenha finalidades determinadas. Neste sentido, foi observado que a longevidade da anuência concedida pelo titular é condicionada à finalidade previamente adotada para o tratamento de seus dados, e eventual revogação do consentimento pelo indivíduo.

Por fim, foi visualizado que esse debate também se relaciona ao contexto de publicidade personalizada. Afinal, autorizando o consumidor que o tratamento de seus dados atenda às expectativas de recebimento de campanhas e promoções ao longo do tempo, a indeterminação temporal é compatível com a própria finalidade do tratamento consentido pela pessoa.

Em termos de conclusão, é possível definir que o consentimento, além de uma base legal de tratamento de dados, deve ser visto como um instrumen-

12. ICO. *Storage limitation*. Information Commissioner's Office. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/>. Acesso em 15 jan. 2025.

to para que os titulares possam exercer suas declarações de vontade de forma efetiva, respeitando-se suas reais intenções quando do processamento de suas informações.

Entretanto, é crucial refletir sobre a efetividade do consentimento como mecanismo de controle na prática, especialmente em modelos baseados em vigilância comportamental. Discute-se, ainda, se o consentimento é capaz de garantir autodeterminação informativa ou se, muitas vezes, serve como escudo jurídico para legitimar práticas abusivas.

Neste contexto, é fundamental que os agentes de tratamento de dados adotem práticas que busquem uma maior guarnição da privacidade individual dos titulares de dados, além de viabilizar que estes consigam alcançar a autodeterminação informacional.

É essencial que o consentimento reflita uma escolha consciente e informada, e não represente uma imposição ao consumidor para que usufrua de serviço disponibilizado na rede mundial de computadores, sem que nem ao menos tenha ciência sobre a finalidade e como seus dados pessoais estão sendo utilizados, ou seja sobre aquilo que consentiu.

Assim, imperioso que as empresas respeitem o efetivo racional trazidos pelas regulamentações protetoras de dados pessoais no tocante à validade e efetividade do consentimento dado pelos consumidores. Ainda, devem sempre optar por utilizar referida base legal tão somente se, na prática, o consentimento concedido pelo titular está de fato sendo respeitado, sendo fornecido de maneira livre, específica, informada, e inequívoca.

Não suficiente, deve-se haver uma grande atuação dos órgãos reguladores, como a ANPD, para que fiscalizem a atuação de controladores de dados pessoais, de modo a garantir que não haja extrapolação dos limites do consentimento, impondo sanções nos casos de violação às leis protetivas de dados.

Não se pode perder de vista a necessidade premente de políticas públicas direcionadas para a educação digital da população. A obtenção de um consentimento válido e alinhado com as expectativas dos consumidores demanda não apenas a conformidade legal das empresas, mas também um esforço coletivo para disseminar conhecimentos técnicos e conscientizar a sociedade sobre os impactos do tratamento de dados pessoais. Mediante esse esforço conjunto será possível garantir uma proteção efetiva da privacidade e do real consentimento em meio à era da informação.

Referências

BIONI, Bruno R. *Proteção de dados pessoais: a função e os limites do consentimento*. São Paulo: Grupo GEN, 2021. E-book.

BIONI, Bruno. *Tratado de proteção de dados pessoais*. São Paulo: Grupo GEN, 2020. E-book.

CABRAL, Érico de Pina. *A 'autonomia' no direito privado*. *Revista dos Tribunais*, 2004.

CASTELLS, Manuel. *A era da informação: economia, sociedade e cultura. A sociedade em rede*. Trad. Roneide Venâncio Majers. São Paulo: Paz e Terra, 1999.

CASTELLS, Manuel. *A sociedade em rede*. Trad. Roneide Venâncio Majer; colaboração de Klauss Brandini Gerhardt. 14. ed. São Paulo: Paz e Terra, 2011.

CASTELLS, Manuel. *Redes de indignação e esperança: movimentos sociais na era da internet*. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar, 2017.

DMA. *How long can you rely on consent or legitimate interest?* Disponível em: <https://dma.org.uk/article/how-long-can-you-rely-on-consent-or-legitimate-interest>. Acesso em: 15 jan. 2025.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados*. São Paulo: Thomson Reuters Brasil, 3. ed. 2021.

EUROPEAN COMMISSION. *How long can data be kept and is it necessary to update it? Principles of the General Data Protection Regulation (GDPR)*. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en. Acesso em: 15 jan. 2025.

EUROPEAN DATA PROTECTION BOARD. *Guidelines 05/2020 on consent under Regulation 2016/679*. 2020. Disponível em: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Acesso em: 16 abr. 2025.

GONÇALVES, Carlos R. *Direito civil brasileiro: teoria geral das obrigações*. v. 2. São Paulo: Editora Saraiva, 2023. E-book.

ICO. *Storage limitation*. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/>. Acesso em: 15 jan. 2025.

LACE, Susanne. *The glass consumer: life in a surveillance society*. Bristol: Policy Press, 2005.

LEONARDI, Marcel. *Publicidade personalizada e LGPD*. Disponível em: https://iabbrasil.com.br/wp-content/uploads/2021/08/IAB-BRASIL_PARECER-JURIDICO_LGPD-E-PUBLICIDADE-PERSONALIZADA_MARCEL-LEONARDI.pdf. Acesso em: 18 jan. 2025.

McAFEE, Andrew; BRYNJOLFSSON, Erik. *A segunda era das máquinas*. Rio de Janeiro: Alta Books, 2014.

MIGALHAS. *A questão do consentimento no GDPR*. Migalhas, São Paulo, 22 set. 2018. Disponível em: <https://www.migalhas.com.br/depeso/280485/a-questao-do-consentimento-no-gdpr>. Acesso em: 15 jan. 2025.

MULHOLLAND, Caitlin; MATERA, Vinicius. O tratamento de dados pessoais pelo poder público. In: *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020.

PAESANI, Liliana M. *Direito de informática: comercialização e desenvolvimento internacional do software*. São Paulo: Grupo GEN, 2015. E-book.

PEREIRA, Caio Mário. *Instituições de direito civil: volume IV – direitos reais*. São Paulo: Forense, 2006.

PECK PINHEIRO, Patrícia. *Direito digital aplicado 5.0*. 5. ed. São Paulo: Revista dos Tribunais, 2022.

RODOTÀ, Stefano. *Il diritto di avere*. Roma: Laterza, 2012.

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

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2023.

THE ECONOMIST. The world's most valuable resource is no longer oil, *but data*. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 19 jan. 2025.

VENOSA, Sílvio de Salvo. *Direito civil*. Volume 8. São Paulo: Atlas, 2011.

ZUBOFF, Shoshana. *A era do capitalismo da vigilância: a disputa por um futuro humano na nova fronteira do poder*. Portugal: Relógio D'Água Editores, 2020.

**Desafios práticos de
adequação frente a nova
resolução de transferência
internacional de dados
pessoais (Resolução CD/
ANPD nº19/2024): Análise
dos impactos regulatórios e
operacionais**

RAINIER GARACIS

Sumário: Introdução. 1. O que caracteriza transferência internacional de dados pessoais? 1.1. Aplicabilidade da LGPD 2. Medidas de controle para transferência internacional de dados pessoais apresentadas na LGPD e Resolução CD/ANPD nº19/2024 e seus desafios práticos da implementação. 2.1. Transparência. 2.1.1 Direito a receber cópia dos documentos utilizados para transferência internacional. 3. Documentos formais de privacidade – Garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previsto na LGPD. 3.1. Cláusulas-padrão contratuais. 3.2. Cláusulas-padrão equivalentes e específicas. 3.3. Normas corporativas globais. Considerações finais. Referências.

Introdução

Nos últimos anos, o cenário regulatório global tem enfatizado a proteção de dados pessoais, e a Lei Geral de Proteção de Dados (LGPD) surge como um marco importante nesse contexto. A transferência internacional de dados, regulada pela LGPD e detalhada pela Resolução CD/ANPD nº19/2024, é uma questão que desafia as organizações a adaptarem suas práticas para garantir a conformidade legal e a proteção dos direitos dos titulares. Este artigo explora os aspectos conceituais, regulamentares e operacionais da transferência internacional de dados pessoais, apresentando as diretrizes da LGPD e os desafios impostos pela sua implementação prática.

O conceito de transferência internacional de dados vai além da simples transmissão de informações para fora das fronteiras brasileiras, envolvendo elementos subjetivos e exigências de governança que apenas recentemente foram devidamente abordados. A publicação da Resolução CD/ANPD nº19/2024 trouxe maior clareza a respeito das definições, aplicabilidade e mecanismos regulatórios relacionados a esse tema, fortalecendo o princípio da transparência e destacando a necessidade de medidas específicas para assegurar a proteção de dados.

Nesse contexto, busca-se responder à seguinte pergunta de pesquisa: em que medida a Resolução CD/ANPD nº 19/2024 contribui para a efetiva conformidade das transferências internacionais de dados pessoais realizadas por agentes de tratamento no Brasil? Parte-se da hipótese de que, embora a Resolução represente um avanço na definição de parâmetros legais, sua imple-

1. Graduado pela Universidade Paulista em Direito. cursando pós-graduação em Direito Digital promovida pela Universidade do Estado do Rio de Janeiro (UERJ), Instituto de Tecnologia e Sociedade (ITS Rio) e Centro de Estudos e Pesquisas no Ensino do Direito (CEPED). Atua como analista de privacidade e proteção de dados pessoais no Banco Bradesco desde 2021. Mais informações em: www.linkedin.com/in/rainier-garacis

mentação prática ainda apresenta obstáculos significativos, especialmente no que se refere à aplicabilidade dos mecanismos jurídicos previstos e à capacidade de adequação das organizações.

1. O que caracteriza transferência internacional de dados pessoais?

A transferência internacional de dados pessoais tem seu conceito estabelecido na Lei Geral de Proteção de Dados Pessoais (LGPD) que consiste na ação de transferir dados pessoais para países estrangeiros ou organismos internacionais do qual o país seja membro.

Embora esse conceito aparente ser simples, ele apresenta algumas questões subjetivas das quais apenas após 4 anos da vigência da LGPD houve maior detalhamento delas. Como por exemplo, o elemento principal desse conceito: o que seria *transferência*². Nessa mesma linha de raciocínio, reitera Marcel Leonardi:

É importante compreender que o conceito de “transferência” não se limita ao envio de dados pessoais de um país para outro: o armazenamento de dados pessoais fora do País e o acesso remoto a dados pessoais a partir do exterior igualmente se caracterizam como uma “transferência internacional” para os fins da legislação³.

Dessa forma, com a publicação da Resolução CD/ANPD nº19/2024, o conceito, até então pouco explorado e, em primeira análise, destoante dos demais artigos presentes na LGPD, ganhou a completude e sinergia que era devida para que a discussão do que consistiria transferência internacional e quais as medidas de governanças aptas para realizar esse tipo de tratamento estivesse em foco no ano de 2024 pelo regulador e agentes de tratamentos. Além de reafirmar algumas questões trazidas na LGPD sobre o termo “transferência internacional” e demais princípios (em foco, o da transparência) a resolução trouxe quais seriam os requisitos necessário de serem analisados para que: I) seja possível identificar a existência de transferência internacional e, em momento posterior a identificação, II) identificar a aplicabilidade da

2. Conforme Art. 3º, III da Resolução CD/ANPD nº19/2024 *transferência* consiste em qualquer operação, envolvendo dados pessoais, da qual um agente de tratamento transmite, compartilha e disponibiliza acesso a outro agente de tratamento. Somando-se com o conceito de transferência internacional disposto e, até então, pouco explorado previsto na LGPD, destaca-se que a mera disponibilização de acesso a dados pessoais localizados no Brasil à um agente no exterior, para fins de LGPD, já configura uma transferência internacional, não sendo necessário, por exemplo, o efetivo envio ou armazenamento dessas informações pelo agente fora do país.

3. LEONARDI, Marcel. Tratado de proteção de dados pessoais. In: DONEDA, Danilo et al. (coord.). *Transferência internacional de dados pessoais*. 2. reimp. Rio de Janeiro: Forense, 2021. p. 289.

LGPD e III) se a operação está em conformidade, requisitos esses que serão dissecados adiante⁴.

O elemento chave para caracterizar um tratamento como transferência internacional é identificar, entre os agentes envolvidos, as figuras do exportador (quem disponibiliza, transmite ou compartilha dados pessoais) e do importador (quem recebe ou acessa dados pessoais fora do território brasileiro)⁵. Cabe salientar que a coleta internacional de dados pessoais, seja com o objetivo de realizar oferta ou o fornecimento de bens ou serviços ou realizar o tratamento de dados pessoais de indivíduos localizados no Brasil, não se classifica como transferência internacional de dados pessoais e, por consequência, os agentes envolvidos nessa coleta não precisam cumprir os controles discriminados na Resolução CD/ANPD nº19/2024, sem prejuízo da necessidade de seguir as premissas estabelecidas na LGPD⁶.

1.1 Identificação da Aplicabilidade da LGPD

Outro ponto importante que os controladores devem avaliar ao realizar tratamento que envolvam o envio ou recepção de dados pessoais para ou do exterior é a aplicabilidade da LGPD ou não. Para isso, o regulador indicou que se deve observar o art. 3º da LGPD⁷ (hipóteses de aplicabilidade da lei), concomitantemente, com as hipóteses de exceções apresentadas no art. 8º, §1º da Resolução CD/ANPD nº19/2024:

Art. 8º Aplica-se a Lei nº 13.709, de 14 de agosto de 2018, aos dados pessoais provenientes do exterior sempre que estes sejam objeto de tratamento no território nacional.

§ 1º A Lei nº 13.709, de 14 de agosto de 2018, não se aplica aos dados pessoais provenientes do exterior somente quando ocorrer:

I – trânsito de dados pessoais, sem a ocorrência de comunicação ou uso compartilhado de dados com agente de tratamento situado em território nacional; ou

II – retorno dos dados pessoais, objeto de tratamento no território nacional, exclusivamente ao país ou organismo internacional de proveniência, desde que:

4. SOUZA, A. P. de et al. Soberania digital e a proteção transfronteiriça dos dados pessoais. *Contribuciones a las Ciencias Sociales*, v. 17, n. 9, p. 1-17, 2024.

5. Art. 5º da Resolução CD/ANPD nº19/2024

6. Art. 6º da Resolução CD/ANPD nº19/2024

7. Conforme incisos do art. 3º da LGPD, a LGPD aplica-se quando a operação de tratamento for realizada em território nacional, a atividade de tratamento tenha como objetivo a oferta ou fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional ou os dados pessoais objeto deste tratamento tenha sido coletados no território nacional, independentemente do local onde o agente esteja realizando o tratamento.

- a) o país ou organismo internacional de proveniência proporcione grau de proteção de dados pessoais adequado, reconhecido por decisão da ANPD;
- b) a legislação do país ou as normas aplicáveis ao organismo internacional de proveniência se apliquem à operação realizada; e
- c) a situação específica e excepcional de não aplicação da Lei nº 13.709, de 14 de agosto de 2018, esteja expressamente prevista na decisão de adequação referida na alínea “a”.

Até a publicação do referido regulamento, não havia hipóteses em que o tratamento, enquadrando-se nos critérios do art. 3º da LGPD⁸, afastasse a aplicação da legislação nacional. Todavia, conforme inciso II do artigo acima, caso houver a aplicação de outra legislação e desde que a ANPD reconheça a dispensa da LGPD, é possível que o tratamento de dados pessoais realizados em território nacional fique fora, inclusive, das penas previstas na LGPD, tratando-se de uma inovação relevante em relação a transferência internacional de dados pessoais.

Após esclarecimento sobre o que considerar para identificar um tratamento como transferência internacional de dados pessoais e a hipóteses de aplicabilidade da LGPD, o regulamento traz enfoque específico nos controles necessários para utilização dos mecanismos permissivos de transferência internacional previstos nos arts. 33, II, alínea a, b e c. Quanto aos demais mecanismos do art. 33 da LGPD, esses serão tratados em regulamentações futuras do tema, com exceção daqueles mecanismos que não necessitam de esclarecimentos para sua utilização (já conhecidos ou alvo de outras resoluções emitidas pela ANPD), conforme exposto pela ANPD no art. 1º, parágrafo único da Resolução CD/ANPD nº19/2024⁹, podendo ser utilizados para justificar a transferência internacional de dados pessoais, por exemplo, quando o tratamento for justificado pelas bases legais de execução de contrato, exercício regular de direitos em processos judiciais, administrativos e arbitrais e cumprimento de obrigação legal/ regulatória, essas apenas quando não houver envolvimento de dados pessoais sensíveis, além das bases de proteção da vida ou a incolumidade física do titular, consentimento e execução de política pública ou atribuição legal do serviço público.

8. O art. 3º da LGPD apresenta quais são os critérios para considerar a aplicabilidade da lei.

9. O disposto neste regulamento não exclui a possibilidade da realização de transferência internacional de dados com base nos demais mecanismos previstos no art. 33 da Lei nº 13.709, de 14 de agosto de 2018, que não dependam de regulamentação, desde que atendidas as especificidades do caso concreto e os requisitos legais aplicáveis, conforme estabelecido no art. 9º, II, alínea c da Resolução CD/ANPD nº19/2024.

2. Medidas de controle para transferência internacional de dados pessoais apresentadas na LGPD e Resolução CD/ANPD nº19/2024 e seus desafios práticos da implementação

Conforme visto no capítulo anterior, embora o conceito de transferência internacional não seja novo na legislação nacional de proteção de dados pessoais, alguns dos controles exigidos pelo regulador, demonstraram-se inéditos e amplamente discutíveis, do ponto de vista do meio pelo qual será possível operacionalizá-lo, por exemplo, o direito de o titular solicitar a cópia das cláusulas contratuais que foram utilizadas para firma para a transferência internacional de dados pessoais. Dito isso, este capítulo tem o objetivo de especificar os principais controles apresentados e algumas dificuldades práticas de implementação pelos agentes de tratamento, observando as diversas realidades e níveis de conformidade das empresas no Brasil.

2.1. Transparência

O princípio da transparência da LGPD¹⁰ apresenta-se como um dos principais controles ao longo de toda a resolução. Esse princípio é um norteador em relação aquilo que é realizado com os dados pessoais e possibilita, ao próprio titular exercer seus direitos fundamentais, principalmente, aqueles atrelados a sua personalidade, por exemplo, solicitar a eliminação de dados, relatório de tratamento ou solicitar a cópia dos documentos formalizados com terceiros que realizam a transferência internacional, além de possibilitar o titular a ter uma maior autodeterminação informativa em relação aos seus dados pessoais.

A transparência exigida pelo regulador nesta resolução envolve a divulgação, em página do controlador, da identificação clara sobre a forma, duração, finalidade, país destino, identificação e contatos do controlador, a existência de uso compartilhado dos dados pelo controlador e sua respectiva finalidade, responsabilidades dos agentes que realizarão o tratamento, medidas de segurança envolvida na transferência, quais os direitos dos titulares e meios para exercê-los, incluindo a indicação de canal de atendimento, conforme previsto no regulamento:

Art. 17. O controlador deverá disponibilizar ao titular, em caso de solicitação, a íntegra das cláusulas utilizadas para a realização da transferência internacional de dados, observados os segredos comercial e industrial.
(...)

10. Art. 6º, VI da LGPD: 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.

§ 2º O controlador deverá ainda publicar em sua página na Internet documento contendo informações em língua portuguesa, em linguagem simples, clara, precisa e acessível sobre a realização da transferência internacional de dados (...)

A medida estabelecida pelo regulador aparenta ser de complexa operacionalização, embora essa exigência, sem sombra de dúvidas, visa garantir ao titular a possibilidade de ter maior controle sobre seus dados pessoais.

Todavia, a complexidade origina-se, pois, parte dessas informações necessárias à divulgação possuem probabilidade de variações ao longo do tempo, culminando no risco de ficarem datadas. Veja, a necessidade de divulgar uma lista de empresas, contatos, países e canais de atendimentos de demais controladores envolvidos nessa relação de transferência internacional geram risco do referido documento ficar datado/obsoleto no momento em for publicado pelo controlador, necessitando a criação de processos internos para revisão frequente das informações quando se refere a empresas de grande porte ou multinacionais com grande volume de terceiros envolvidos (clientes, prestadores, órgãos reguladores ou parceiros comerciais), inclusive sendo necessário acionar esses terceiros para garantia da integridade dos dados divulgados.

Além do fator de obsolescência indicado acima, quando se trata de controladores com grande volume de produtos, serviços e/ou parcerias de negócio, apresentar uma relação com dezenas, ou até mesmo centenas, de linhas com todas as informações indicadas na referida resolução aos titulares de dados pessoais pode causar relevante confusão no próprio titular, indo na contramão do objetivo desse controle. Diferentemente do que é encontrado no cenário europeu, cujo tema de privacidade e proteção de dados possui dezenas de anos de maturidade em relação ao cenário brasileiro¹¹, essa medida pode ocasionar dificuldade em identificar o que se busca, levando em conta a efetiva compreensão pelo titular médio, especialmente considerando os níveis atuais de letramento digital no Brasil, haja vista o volume expressivo de informações que serão disponíveis e exigidas pelo próprio regulador. Tornando-se assim, uma medida de controle meramente formal, com pouca ou nenhuma finalidade aparente ao próprio titular, objeto principal desse princípio trazido pela LGPD.

11. Redação trazida pelo website da LGPD/DF: O primórdio da nova cultura de proteção de dados aconteceu na década de 70, na Alemanha, devido ao avanço da computação e da premente e constante preocupação do Estado Alemão para proteger seus cidadãos do que a nação vivenciou no período do regime nazista. Dessa forma, foram criadas as primeiras normas regulatórias que culminaram na legislação de 1978.

Em 1995, foi criada a Diretiva 95/46/CE, da União Europeia, contendo o primeiro regulamento para o bloco, trazendo o conceito de proteção de dados próximos das legislações atuais.

<titulo3>2.1.1 Direito a receber cópia dos documentos utilizados para transferência internacional

Além do critério exposto acima, no que diz respeito à necessidade de transparência ao titular de dados, a ANPD inovou, trazendo mais um controle para que a transparência da transferência internacional de dados pessoais possa ser garantida. Este, estabelece que o titular tenha o direito de solicitar a cópia das cláusulas contratuais¹² que foram utilizadas para firmar o relacionamento com outras empresas envolvidas na transferência internacional de dados.

Sem entrar no mérito da validade desse novo “direito”, uma vez pode-se discutir a legalidade desse inclusão realizada por meio de uma regulamentação criada por autarquia pública federal (ANPD) que dispõe de função regulatória, ou seja, pode editar normas complementares e orientações em relação a LGPD¹³ mas não possui função legislativa para criar novos direitos materiais, função essa do Poder Legislativo, conforme art. 48 da Constituição Federal¹⁴, o estabelecimento desse “direito” apresenta relevante complexidade de cumprimento pelos agentes. Além de complexo, olhado do prisma do titular dos dados pessoais, pode apresentar uma excessividade em relação ao princípio que a justificou, tendo em vista que as principais informações relevantes já estarão detalhadas no site do controlador.

Inclusive, a exceção da disponibilização desses documentos é o respeito ao segredo de negócio/empresarial¹⁵, o que na prática pode ocasionar em um direito sem aplicação. Caso um titular venha a solicitar esses documentos junto aos controladores, é possível que os agentes de tratamento, legitimamente, não os disponibilizem justificando segredo de negócio ou, caso disponibilizem, sem informações relevantes ao próprio titular, apenas texto morto das cláusulas-padrão, sem contexto ou maiores aberturas.

12. As cláusulas contratuais que os titulares podem solicitar suas cópias são aquelas estabelecidas no arts. 17 e 32, parágrafo único e cláusula 14.3 do anexo I da Resolução CD/ANPD nº19/2024: cláusulas-padrão contratuais (ou equivalentes), normas corporativas globais ou cláusulas contratuais específicas, resguardado os segredos empresariais e industriais.

13. Previsto no art. 55-J da LGPD

14. Tal disposição levanta um importante debate jurídico: a imposição desse dever de transparência configura mera regulamentação de dispositivos legais já existentes ou extrapola os limites do poder normativo da ANPD, criando novo direito material? Sob uma interpretação sistemática da LGPD, pode-se argumentar que tal medida encontra lastro nos princípios e direitos previstos na própria lei, especialmente o princípio da transparência (art. 6º, VI), e o direito à informação garantido ao titular (art. 9º e art. 18, VII), que assegura ao titular o acesso a informações claras sobre o tratamento de seus dados e com quem são compartilhados.

Contudo, não há, na LGPD, dispositivo expresso que obrigue o controlador a disponibilizar o conteúdo das cláusulas contratuais firmadas com terceiros, especialmente no que tange à transferência internacional de dados. Ao impor tal exigência, a ANPD poderia estar criando nova obrigação material sem previsão legislativa específica — o que violaria o princípio da reserva legal (art. 5º, II, da CF/88) e configuraria uma usurpação da função legislativa.

Como afirma Celso Antônio Bandeira de Mello no livro Curso de Direito Administrativo, o poder regulamentar “não pode criar direitos ou obrigações novas, mas apenas estabelecer as condições técnicas de operacionalização da norma legal”.

15. Art. 17 da Resolução CD/ANPD nº19/2024

Outra complexidade prática de cumprimento desse item advém da dificuldade que os próprios agentes possam ter no que diz respeito à identificação do envio de determinados dados pessoais acerca de um titular específico para outro país. Sendo necessário para tanto que o agente tenha maturidade, ferramentas e processos bem definidos no que diz respeito a *data mapping/DMM*¹⁶, governança de dados e inventário de tratamento de dados pessoais. Possibilitando identificar de forma simples e rápida qual os documentos que deverão ser disponibilizados ao titular específico que o solicitou, podendo, em alguns casos, a depender dos produtos, serviços ou tamanho do agente de tratamento, ter que disponibilizar dezenas de instrumentos contratuais.

3. Documentos formais de privacidade – Garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previsto na LGPD

Conforme disposto no capítulo 1 “Identificação da Aplicabilidade da LGPD” desse trabalho, um dos mecanismos para transferência internacional é a adoção/formalização de documentos que privacidade que visam garantir a observância e cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD junto aos terceiros envolvidos na transferência internacional de dados pessoais.

Em especial, esses documentos buscam estabelecer condições mútuas entre os agentes de tratamento para que ambos adotem medidas/salvaguardas necessárias para tratar os dados pessoais fora do território nacional em conformidade com a LGPD e demais regulamentações pertinentes. A título de exemplo, estabelecer e demonstrar que ambos os agentes: cumprem obrigações de garantir a transparência ao titular sobre o envio dos dados pessoais, deveres de comunicação ao controlador em caso de incidente de segurança, especial atenção e controles para tratamentos de dados pessoais sensíveis ou de crianças e adolescentes, direitos dos titulares etc.

Embora a existência desses documentos tenha o mesmo propósito, se diferenciam em relação às contrapartes envolvidas na relação, podendo ser formalizados junto a empresas terceiras (cláusulas contratuais) ou com demais

16. Conforme disposto por Leonardo Narciso Marques em *O mapeamento do modelo Data Management Maturity (DMM) à Lei Geral de Proteção de Dados (LGPD)*, p. 54 –55: A LGPD exige uma governança de dados em decorrência aos direitos do Titular dos dados, ou seja, uma gestão dos dados, que seja clara e concisa para garantir como um dado é coletado, o porquê e por quanto tempo ele ficará armazenado/arquivado. Em contrapartida existem as punições legais caso isso seja descumprido. O modelo Data Management Maturity (DMM) fornece práticas para que as empresas executem, outras sejam modificadas para atender aos requisitos da lei. (...) Ao realizar um mapeamento dos dados que é a finalidade de cada categoria e área do DMM a rastreabilidade do dado fica evidente para toda a empresa, usabilidade do dado, tempo em que este deve permanecer dentro da empresa e disponibilidade/comunicação somente para os respectivos setores que realmente tratam este dado.

empresas pertencentes ao mesmo grupo empresarial/econômico (norma corporativas globais), e o caso de uso de cada um deles, conforme discriminado abaixo:

3.1. Cláusulas-padrão contratuais

As cláusulas-padrão contratuais trata-se de documento predefinido pela própria ANPD com objetivo de garantir padronização entre os agentes de tratamento que realizam transferência internacional de dados pessoais, não podendo ter sua redação alterada de nenhuma forma. Com exceção de alguns poucos campos que devem ser customizados/preenchidos para refletir o caso concreto. Elas estabelecem garantias mínimas para que, mesmo em países onde o regime de proteção de dados é diferente do Brasil, os dados pessoais continuem protegidos conforme os padrões exigidos pela LGPD, conforme disposto nos arts. 15 e 16 do referido regulamento:

Art. 15. As cláusulas-padrão contratuais, elaboradas e aprovadas pela ANPD na forma do Anexo II, estabelecem garantias mínimas e condições válidas para a realização de transferências internacionais de dados baseadas no inciso II, alínea «b», do art. 33 da Lei nº 13.709, de 14 de agosto de 2018.

(...)

Art. 16. A validade da transferência internacional de dados, quando amparada na adoção das cláusulas-padrão, pressupõe a adoção integral e sem alteração do texto disponibilizado no Anexo II, mediante instrumento contratual firmado entre o exportador e o importador.

Algumas das dificuldades encontradas com a adoção desse mecanismo como validador da transferência internacional é a negociação com as grandes empresas internacionais de tecnologia e nuvem, por exemplo, (*Big Techs*¹⁷), já que, via de regra, não existe equiparação de poder para negociação com essas entidades, mesmo que, por vezes, atuem como operadoras de dados pessoais, restando ao controlador aderir aos modelos elaborados e impostos por essas empresas (termos de adesão).

Essa dificuldade torna-se concreta no momento em que a ANPD não disponibilizou, após a publicação da Resolução CD/ANPD nº19/2024, alternativa

17. Conforme indicado por Birch, K.; Bronson, K. em *Big Tech*, p. 1, As *Big Techs* são grandes organizações de empresas de tecnologia que atuam na maior parte do globo. A história dessas instituições empresariais está ligada ao processo de globalização mundial. Essas empresas funcionam por meio de um conjunto de inovações nos ramos da tecnologia da informação e da comunicação. Essas empresas são importantes, pois exercem grande influência nas atividades econômicas e culturais das sociedades. As principais são: Microsoft, Apple, Meta, Tencent, Oracle, etc.

para que os agentes tenham outras opções para negociar com essas grandes corporações internacionais, resultando no seguinte dilema: ou há formalização do relacionamento aderindo as cláusulas impostas por essas empresas (em conformidade até dia 23/08/2025 – prazo de adequação) ou não há concretização da contratação da solução almejada, podendo resultar em riscos tecnológicos, dada a paralisia nas negociações, aumento de custo de observância dos agentes e/ou riscos econômicos para as empresas no Brasil¹⁸.

Embora seja possível que os agentes de tratamentos solicitem ao regulador a liberação de uso de cláusulas de transferência internacional equivalente de outras legislações de proteção de dados pessoais (será detalhada a seguir), não existe prazo para retorno dessa avaliação pelo regulador, o que, a depender do caso e urgência da contratação, não será possível aguardar por um prazo indefinido, restando as empresas optar pelas opções indicadas no parágrafo anterior.

3.2. Cláusulas-padrão equivalentes e específicas

As cláusulas-padrão equivalentes são aquelas utilizadas em outras legislações de privacidade e proteção de dados pessoais que podem ser reconhecidas como adequadas pelo regulador e, por consequência, permitidas de serem utilizadas nas formalizações de operações de transferência internacional de dados pessoais¹⁹.

Ainda, há as cláusulas-padrões específicas, tratando-se de mecanismo utilizado como exceção às cláusulas equivalentes e/ou padrões. Ou seja, diante de um caso concreto com tamanha especificidade/unidade, pode ser criada cláusulas específicas para esse caso. Todavia, assim como as equivalentes, a ANPD deve aprovar o uso dessas cláusulas e, serão aprovadas, apenas se os agentes de tratamento que solicitaram a avaliação ao regulador conseguir comprovar a unidade do caso e impossibilidade de utilizar demais medidas existentes no art. 33 para realizar o tratamento almejado²⁰.

Na prática, os casos que exigirão cláusulas específicas deverão ser aqueles em que trate de uma questão relevantemente peculiar e inovadora, uma vez que as bases legais previstas no art. 33, IV da LGPD (execução de contrato, cumprimento de obrigação legal/regulatória e exercício regular de direitos em

18. DE FIGUEIREDO COSTA, R. V. A transferência internacional de dados na Lei nº 13.709/18 e a administração de recursos de terceiros no Brasil. [S.l.], 2019.

19. Art. 18 da Resolução CD/ANPD nº19/2024

20. Arts. 18 §4º e 19 da Resolução CD/ANPD nº19/2024

processos judiciais, administrativo ou arbitrais) devem abarcar grande parte dos casos de transferência internacional de dados pessoais e, não conseguindo justificarem o compartilhamento por essas bases, a adoção das cláusulas-padrões e equivalentes conseguirão suportar de forma adequada²¹.

3.3. Normas corporativas globais

Assim como as cláusulas informadas acima, as normas corporativas globais não se diferem acerca do objetivo pretendido. Todavia, esse documento em questão deve ser utilizado para regulamentar a transferência de dados pessoais entre empresas do mesmo grupo/conglomerado econômico.

Ainda assim, requer aprovação da ANPD e após aprovação, o regulador as tornará públicas²².

O documento apresentará, além do detalhamento dos tratamentos realizados entre as empresas do grupo, lista de entidades vinculadas, papel exercido por cada uma delas no tratamento e os dados de contato de cada organização que efetue tratamento de dados pessoais, regras sobre o processo de revisão das normas corporativas globais e previsão de submissão à prévia aprovação da ANPD e previsão de comunicação à ANPD em caso de alterações nas garantias apresentadas como suficientes de observância dos princípios, direitos do titular e do regime de proteção de dados previsto na Lei nº 13.709, de 14 de agosto de 2018, especialmente na hipótese em que um dos membros do grupo ou conglomerado de empresas estiver submetido a determinação legal de outro país que impeça o cumprimento das normas corporativas²³.

Além de sua função regulatória, as normas corporativas globais também demonstram ao mercado a atenção ao cumprimento do princípio da responsabilização e prestação de contas (*accountability*) ao exigirem que as organizações demonstrem, de forma clara e documentada, a conformidade de suas práticas com os parâmetros estabelecidos pela LGPD. A responsabilização ativa do grupo empresarial é evidenciada tanto na estruturação interna de regras de governança, quanto na obrigação de revisão contínua e comunicação formal de quaisquer alterações relevantes à ANPD, reforçando o compromisso com a proteção de dados pessoais e a transparência frente à autoridade e aos titulares. Como observa Teixeira e Armelim, “[...] não basta o agente ter

21. Vale mencionar que além das bases legais e cláusulas-padrões e equivalentes, ainda é possível que o regulador, no futuro, avalie e aprove países que possuam o mesmo grau de proteção de dados do Brasil, afastando assim a necessidade de adoção de outros mecanismos, conforme estabelecido no art. 10 da Resolução CD/ANPD nº19/2024.

22. Art. 31 da Resolução CD/ANPD nº19/2024

23. Art. 27 da Resolução CD/ANPD nº19/2024

cumprido todas as regras e determinações legais, é preciso que ele a todo tempo registre que cumpriu a lei, utilizando-se das mais diversas formas para que consiga comprovar o atendimento aos preceitos da lei [...]. É de se mencionar a obrigatoriedade da prestação de contas por parte do agente até mesmo quando não houver qualquer descumprimento ou irregularidade”²⁴.

Assim, a implementação de normas corporativas globais exige não só estrutura normativa interna, mas também uma postura contínua de comprometimento com a governança de dados, evidenciada pela revisão constante das práticas adotadas e pela interlocução permanente com a autoridade reguladora.

O principal ônus de utilização/criação dessas normas, além de requerer aprovação do regulador (como visto acima, não há nenhum prazo estabelecido para que essa avaliação ocorra) e necessidade de tornar público um documento que rege processos internos de uma organização/grupo econômico, é a inflexibilidade desse documento. Qualquer alteração, incremento ou remoção de informações exigirá nova avaliação e aprovação pela ANPD, resultando em um documento pouco benéfico para empresas de inovação/médio/grande porte que, frequentemente, buscam melhorias contínuas em seus produtos, serviços e processos.

Além disso, vale destacar o esforço adicional necessário quando as transferências internacionais de dados envolvem a observância simultânea de diferentes regulamentações, como é o caso das transferências bilaterais entre empresas do mesmo grupo econômico estabelecidas em países distintos. Nesses casos, é comum que os agentes de tratamento precisem atender simultaneamente aos requisitos da LGPD e da GDPR, por exemplo, o que torna o processo para utilização das normas mais custoso e intrincado.

Caso haja a intenção de instituir Normas Corporativas Globais (BCRs no caso da GDPR) como mecanismo de transferência, será necessário submeter o documento à avaliação e aprovação da Autoridade Nacional de Proteção de Dados (ANPD), no Brasil, bem como à autoridade de proteção de dados competente na União Europeia, conforme os procedimentos estabelecidos pelo artigo 47 do GDPR.

Considerações finais

A transferência internacional de dados pessoais constitui um elemento central no debate sobre privacidade e proteção de dados, especialmente em

24. TEIXEIRA, Tarcísio; ARMELIM, Rita Maria Gomes da Fonseca. *Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019*. São Paulo: Almedina, 2020.

um mundo cada vez mais interconectado. A LGPD, juntamente com a Resolução CD/ANPD nº19/2024, estabelece diretrizes robustas para garantir que o tratamento de dados ocorra de maneira transparente e segura, mesmo quando envolve múltiplas jurisdições. Apesar disso, a implementação prática dessa norma apresenta desafios significativos, especialmente para organizações de grande porte ou que operam em mercados globais.

Este estudo revelou que, embora as exigências regulamentares reforcem a proteção dos direitos dos titulares, elas também impõem complexidades operacionais e regulatórias, tais como:

- Inexistência de outros mecanismos para resguardar a transferência internacional durante o prazo de adequação concebido;
- Complexidade de criação e manutenção de normas corporativas globais, sendo necessário o envolvimento e aprovação do regulador nacional e internacional, a depender do caso concreto;
- Ausência de definição de prazos para o regulador avaliar as normas corporativas globais e as cláusulas específicas e equivalentes;
- Ausência de disposições específicas e mais flexíveis para agentes de médio e pequeno porte; e
- Estabelecimento de controles complexos e burocráticos para garantia da transparência ao titular.

Além disso, a coexistência de diferentes bases legais e mecanismos para regular transferências internacionais evidencia a importância de um planejamento cuidadoso e de investimentos em governança de dados.

Conclui-se que o sucesso na implementação das medidas previstas na LGPD e na Resolução CD/ANPD nº19/2024 depende de um equilíbrio entre conformidade regulatória e viabilidade operacional, incluindo, principalmente, a definição de outros caminhos para garantir a conformidade dos agentes de tratamento utilizando mecanismos menos onerosos, por exemplo, a publicação de decisão de adequação que considere a União Europeia como território com elevado grau de proteção de dados pessoais, estabelecimento de cláusulas-padrões contratuais mais simples para operações de tratamentos que não possuam alto risco e decisão que reconheça as SCCs (*Standard Contractual Clauses*) da GDPR como cláusulas-padrão equivalentes às nossas. Assim, além das contribuições necessárias do regulador para o cenário nacional de conformidade com a LGPD, as organizações devem buscar não apenas cumprir as exigências legais, mas também desenvolver práticas de privacidade

que agreguem valor aos seus negócios e fortaleçam a confiança dos titulares de dados, facilitando a governança sobre o tema.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Resolução CD/ANPD nº 19, de 23 de agosto de 2024*. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396>. Acesso em: 10 jan. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Transferência internacional de dados pessoais*, de 23 de agosto de 2024. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/assuntos-internacionais/assuntos-internacionais-pt>. Acesso em: 10 jan. 2025.

BIRCH, K.; BRONSON, K. *Big Tech*. Science as Culture, v. 31, n. 1, p. 1-14, 2022. Disponível em: <https://doi.org/10.1080/09505431.2022.2036118>. Acesso em: 10 jan. 2025.

BRASIL. *Lei Geral de Proteção de Dados Pessoais – LGPD: Lei nº 13.709, de 14 de agosto de 2018*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 jan. 2025.

DE FIGUEIREDO COSTA, R. V. *A transferência internacional de dados na Lei nº 13.709/18 e a administração de recursos de terceiros no Brasil*. [S.l.], 2019.

DISTRITO FEDERAL. *LGPD/DF – Histórico*. Disponível em: <https://lgpd.df.gov.br/historico/>. Acesso em: 10 jan. 2025.

LEONARDI, Marcel. Tratado de proteção de dados pessoais. In: DONEDA, Danilo et al. (coord.). *Transferência internacional de dados pessoais*. 2. reimp. Rio de Janeiro: Forense, 2021. p. 289-298.

MARQUES, Leonardo Narciso. *O mapeamento do modelo Data Management Maturity (DMM) à Lei Geral de Proteção de Dados (LGPD)*. 2020. Trabalho de Conclusão de Curso (Graduação) – Pontifícia Universidade Católica de Goiás, Goiânia, 2020. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/1289/1/TCC%202020%20Leonardo%20Narciso%20Marques.pdf>. Acesso em: 10 jan. 2025. p. 54-55.

MELLO, Celso Antônio Bandeira de. *Curso de Direito Administrativo*. 34. ed. São Paulo: Malheiros, 2017, p. 228.

SOUZA, A. P. de et al. Soberania digital e a proteção transfronteiriça dos dados pessoais. *Contribuciones a las Ciencias Sociales*, v. 17, n. 9, p. 1-17, 2024.

TEIXEIRA, Tarcísio; ARMELIM, Rita Maria Gomes da Fonseca. *Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019*. São Paulo: Almedina, 2020.

UNIÃO EUROPEIA, *General Data Protection Regulation – GDPR*, de 27 de abril de 2016: Disponível em: [Regulation – 2016/679 – EN – gdpr – EUR-Lex](https://eur-lex.europa.eu/eli/reg/2016/679/oj) Acessado em 10 jan. 2025.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

7

**Práticas éticas em
Developer Experience:
indicadores e a
autodeterminação
Informativa na LGPD**

LEANDRO ALCOLUMBRE

Sumário: Introdução; 1. A vigilância líquida e direitos fundamentais no trabalho digital; 2. A aplicação de métricas na *Developer Experience*: implicações éticas e jurídicas; 3. Propostas para uma governança ética e responsável de indicadores DX; Considerações finais; Referências.

Introdução

Não há mais dados insignificantes; uma pessoa é demitida com base em um algoritmo que indicou baixa performance. Em um ambiente onde métricas de produtividade são coletadas e analisadas automaticamente, os dados tornam-se determinantes, mesmo sem revelar todo o contexto. Essa pessoa é confrontada com uma decisão fundamentada em informações que não controla e que, muitas vezes, nem compreende completamente.

Esse cenário ilustra o avanço das ferramentas de *People Analytics*, cada vez mais presentes no monitoramento de performance e nas decisões corporativas. Contudo, essas métricas, amplamente adotadas para aumentar eficiência e produtividade, apresentam desafios éticos significativos, especialmente em um contexto de relações assimétricas de poder: como assegurar que os dados utilizados respeitem os direitos fundamentais do colaborador? Até que ponto tais sistemas são transparentes e permitem a autodeterminação informativa, um conceito basilar da Lei Geral de Proteção de Dados (LGPD)?

No mundo contemporâneo, o monitoramento não apenas está disseminado, mas se tornou indispensável, em um movimento que dissolve os limites entre escolha e necessidade, conforme o conceito de pós-panoptismo de Zygmunt Bauman e David Lyon². A compulsoriedade da exposição e o controle invisível tornam os desafios éticos ainda mais urgentes, especialmente em um contexto técnico como o da *Developer Experience* (DX). Nesse sentido, vale formular um questionamento sobre quais seriam os limites éticos e jurídicos para o uso de métricas de performance de desenvolvedores à luz da LGPD e do princípio da autodeterminação informativa.

Este artigo propõe-se a investigar práticas éticas no uso de indicadores de DX, com ênfase na relação entre métricas, autodeterminação informativa

1. Graduado em Direito pela Escola Superior Madre Celeste (ESMAC). Advogado (OAB/PA 39392). Especializando em Direito Digital pela Universidade do Estado do Rio de Janeiro (UERJ), em parceria com o Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS-Rio). Atua profissionalmente com Engenharia de Software e Dados, com foco em *Developer Experience* (DX), *Developer Relations* (DevRel), Acessibilidade digital e Governança de dados. E-mail: leandro.alcolumbre@gmail.com

2. BAUMAN, Zygmunt. *Vigilância líquida: diálogos com David Lyon*. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

e a conformidade com a LGPD. A partir de uma abordagem qualitativa, constrói-se um diálogo entre referências teóricas e práticas do setor, buscando responder, desde uma análise normativa e de um estudo interdisciplinar, como a governança de dados pode alinhar eficiência organizacional e respeito aos direitos individuais.

Para tanto, o texto divide-se em três partes: inicialmente, discute os fundamentos teóricos, conectando conceitos como vigilância líquida e autodeterminação informativa; em seguida, analisa a aplicação prática de métricas na DX e seus impactos éticos e jurídicos; por fim, apresenta propostas para um uso mais responsável e alinhado à legislação, contribuindo para um ambiente de trabalho mais justo e transparente.

1. A vigilância líquida e direitos fundamentais no trabalho digital

Analisar a realidade sob a ótica da literatura ficcional é, muitas vezes, um interessante exercício. Dickens, na obra *Tempos Difíceis*, através da figura de Sissy Jupe, ironiza um mundo onde os dados são usados fora de contexto e com frieza analítica³. George Orwell é frequentemente lembrado pelo emblemático *1984*, em que as pessoas não têm escolha sobre ter seus dados coletados e tratados; os conteúdos passam a estar sob a custódia do Ministério da Verdade, onde se decide o que é ou não correto⁴. Cixin Liu, em *A Floresta Sombria*, avança a crítica ao descrever um futuro em que até caixas de cigarro exibem anúncios e coletam dados continuamente⁵.

Embora duas dessas obras antecedam a internet e a massificação dos dispositivos eletrônicos, elas antecipam elementos do pós-panoptismo. Hoje, especialmente no ambiente de trabalho, cada ação é registrada e tratada, consolidando um modelo de vigilância mais fluido e internalizado⁶. À observação constante do panoptismo tradicional, soma-se a peculiaridade do pós-panóptico: o indivíduo carrega o próprio mecanismo de controle, voluntariamente alimentando o estado de observação contínua por meio de ferramentas que coletam e processam seus dados. Nesse contexto, a ideia

3. DICKENS, Charles. *Tempos difíceis*. São Paulo: Boitempo Editorial, 2014.

4. ORWELL, George. *1984*. Tradução de Alexandre Hubner e Heloisa Jahn. São Paulo: Companhia das Letras, 2009.

5. LIU, Cixin. *A Floresta Sombria*. Rio de Janeiro: Suma, 2017.

6. BAUMAN, Zygmunt. *Vigilância líquida: diálogos com David Lyon*. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

de escolha torna-se ilusória, pois a alternativa de não utilizar tais ferramentas simplesmente não existe⁷.

Por outro lado, a relação de subordinação entre empregador e empregado reforça uma assimetria de poder quando os dados coletados no ambiente tecnológico limitam a capacidade de oposição ou controle do trabalhador diante de decisões tomadas por algoritmos baseados em informações do seu cotidiano profissional⁸. No trabalho digital, o empregado utiliza equipamentos, serviços e até mesmo redes privadas (VPNs) fornecidos pelo empregador. Embora o monitoramento seja legítimo em casos como cibersegurança, o desvio desses dados para fins não explicitados ou não consentidos coloca o trabalhador em uma posição de vulnerabilidade, abrindo espaço para a violação de direitos fundamentais, como privacidade e autodeterminação informativa⁹.

Assim, a proteção dos dados pessoais surge como um contraponto natural ao pós-panóptico, consagrada como um direito humano e fundamental, de modo que já se fala em uma dimensão própria para esta categoria de direitos¹⁰. Em 2022, esse reconhecimento foi explicitado na Constituição Federal por meio da Emenda 115/2022, que incluiu a proteção de dados no rol de garantias fundamentais¹¹. Um pilar central dessa previsão legal é o conceito de autodeterminação informativa. Ele se opõe ao pós-panóptico ao oferecer instrumentos para que o indivíduo compreenda, decida e conteste o uso de seus dados pessoais, especialmente em contextos de trabalho digital, onde a assimetria de poder é ampliada por algoritmos que processam informações do cotidiano

7. BAUMAN, 2013; também BRICALLI, Iafet Leonardi. A vigilância como cultura. *Sociologia & Antropologia*, Rio de Janeiro, v. 10, n. 3, p. 1103-1107, set.-dez. 2020. Disponível em: <https://www.scielo.br/j/sant/a/wjyYxRWtn37DSZ8FrYWmkCL/?lang=pt&format=html>. Acesso em: 15 jan. 2025; SIQUEIRA, Dirceu Pereira; MOREIRA, Mayume Caires. Autodeterminação informativa na sociedade pós-panóptico: novas formas de panoptismo e os direitos da personalidade. *Prisma Jurídico*, São Paulo, v. 22, n. 1, p. 74-91, jan./jun. 2023. Disponível em: <http://doi.org/10.5585/2023.20634>. Acesso em: 15 jan. 2025; VIEIRA, Gustavo Duarte. *Proteção de dados pessoais em práticas de profiling no setor privado*. 2019. 126 f. Dissertação (Mestrado em Direito) – Universidade Federal de Minas Gerais, Belo Horizonte. Disponível em: <https://repositorio.ufmg.br/bitstream/1843/34072/8/Gustavo%20Duarte%20Vieira%20-%20Prote%C3%A7%C3%A3o%20de%20dados%20pessoais%20em%20pr%C3%A1ticas%20de%20profiling-mesclado%281%29.pdf>. Acesso em: 15 jan. 2025

8. BAUMAN, Zygmunt. *Vigilância líquida: diálogos com David Lyon*. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013; VIEIRA, Gustavo Duarte. *Proteção de dados pessoais em práticas de profiling no setor privado*. 2019. 126 f. Dissertação (Mestrado em Direito) – Universidade Federal de Minas Gerais, Belo Horizonte. Disponível em: <https://repositorio.ufmg.br/bitstream/1843/34072/8/Gustavo%20Duarte%20Vieira%20-%20Prote%C3%A7%C3%A3o%20de%20dados%20pessoais%20em%20pr%C3%A1ticas%20de%20profiling-mesclado%281%29.pdf>. Acesso em: 15 jan. 2025

9. VIEIRA, Gustavo Duarte. *Proteção de dados pessoais em práticas de profiling no setor privado*. 2019. 126 f. Dissertação (Mestrado em Direito) – Universidade Federal de Minas Gerais, Belo Horizonte. Disponível em: <https://repositorio.ufmg.br/bitstream/1843/34072/8/Gustavo%20Duarte%20Vieira%20-%20Prote%C3%A7%C3%A3o%20de%20dados%20pessoais%20em%20pr%C3%A1ticas%20de%20profiling-mesclado%281%29.pdf>. Acesso em: 15 jan. 2025

10. SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: DONEDA, Danilo et al. (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

11. BRASIL, *Emenda Constitucional nº 115, de 10 de fevereiro de 2022*. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 15 jan. 2025.

profissional¹². Ao instrumentalizar esse controle, a autodeterminação informativa reforça o protagonismo do indivíduo na gestão de seus dados, alinhando-se à necessidade de equilibrar as relações de poder no ambiente corporativo.

Estas características assimétricas, muitas vezes reconhecidas como parte de uma “obrigação imposta”, encontram expressão na sentença alemã sobre autodeterminação informativa na década de 1980. A decisão tratava do novo censo alemão, composto por 160 perguntas, que coletava dados dos cidadãos e gerava controvérsias devido à obrigatoriedade de preenchimento sob pena de multa, além da possibilidade de retificação e cruzamento com outras bases¹³. Essa preocupação com os desvios de finalidade, levantada tanto por cidadãos quanto por órgãos alemães, demonstrou que não apenas a natureza das informações deve ser analisada, mas também a finalidade e o potencial da hiperconexão tecnológica em criar cenários de vulnerabilidade¹⁴.

Nesse sentido, uma situação análoga ocorre com a coleta de dados durante a jornada de trabalho na área de tecnologia. Ferramentas modernas possibilitam o perfilamento detalhado de trabalhadores com base em suas ações cotidianas, de maneira semelhante ao cruzamento de informações no censo alemão. Embora a criação de perfis, frequentemente embasada em *frameworks* amplamente adotados no mercado, traga benefícios para as organizações – como mensurar o clima organizacional, identificar lacunas e promover boas práticas –, os riscos de comprometer a privacidade individual são evidentes. Assim como no caso do censo, a diversidade de finalidades e a falta de transparência no uso dos dados contrastam facilmente, reforçando a necessidade de uma abordagem ética e responsável no tratamento dessas informações.

Nesse contexto, o conceito de *profiling*, ou perfilamento de dados, surge como uma peça-chave. Ele se refere ao conjunto de técnicas de organização de bases e estatísticas, que podem ou não envolver inteligência artificial, com o objetivo de compreender e prever comportamentos a partir da análise de

12. SIQUEIRA, Dirceu Pereira; MOREIRA, Mayume Caires. Autodeterminação informativa na sociedade pós-panóptico: novas formas de panoptismo e os direitos da personalidade. *Prisma Jurídico*, São Paulo, v. 22, n. 1, p. 74-91, jan./jun. 2023. Disponível em: <http://doi.org/10.5585/2023.20634>. Acesso em: 15 jan. 2025; SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: DONEDA, Danilo et al. (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. VIEIRA, Gustavo Duarte. *Proteção de dados pessoais em práticas de profiling no setor privado*. 2019. 126 f. Dissertação (Mestrado em Direito) – Universidade Federal de Minas Gerais, Belo Horizonte. Disponível em: <https://repositorio.ufmg.br/bitstream/1843/34072/8/Gustavo%20Duarte%20Vieira%20-%20Prote%C3%A7%C3%A3o%20de%20dados%20pessoais%20em%20pr%C3%A1ticas%20de%20profiling-mesclado%281%29.pdf>. Acesso em: 15 jan. 2025;

13. DONEDA, Danilo Cesar Maganhoto. *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. ISBN 978-65-5065-030-8.

14. DONEDA, Danilo Cesar Maganhoto. *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. ISBN 978-65-5065-030-8.

grandes volumes de informações concentradas¹⁵. Dessa forma, nenhum dado é insignificante, já que mesmo uma informação aparentemente desassociada, como um endereço IP ou o histórico de acesso a um sistema, pode ser vinculada a uma pessoa específica quando associada a um identificador único, como um e-mail ou uma credencial de login compartilhada com outras bases. Isso transforma a informação em dado pessoal, sujeitando-a às diretrizes estabelecidas pela Lei Geral de Proteção de Dados¹⁶.

As métricas aplicadas à *Developer Experience* carregam o risco de que os dados utilizados assumam características de informações pessoais, especialmente quando há identificação direta ou indireta. Além disso, o cenário de vigilância líquida se consolida com um panóptico, agora sustentado pelo próprio profissional de tecnologia, por meio de diversos indicadores de atividade e sistemas contínuos de coleta. Nesse contexto, o discurso técnico frequentemente ofusca impactos sociais e jurídicos, ao normalizar práticas de monitoramento sob a justificativa da eficiência. Assim, preocupações éticas tornam-se essenciais para garantir que a inovação esteja em conformidade com as legislações vigentes e respeite o protagonismo dos titulares dos dados. É sob essa perspectiva – em que métricas governança e direitos fundamentais se entrelaçam –, que a discussão se aprofunda a seguir.

2. A aplicação de métricas na developer experience: implicações éticas e jurídicas

O conceito de *Developer Experience* (DX) tem evoluído continuamente, abrangendo dimensões que vão além da simples produtividade individual. Ele integra aspectos holísticos como a fluidez nos processos e práticas, a satisfação das pessoas desenvolvedoras com o ambiente de trabalho e a execução de projetos, além da interação com ferramentas e equipes. Estudos destacam que a DX está intrinsecamente conectada ao conceito de *User Experience* (UX),

15. DONEDA, Danilo Cesar Maganhoto. *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. ISBN 978-65-5065-030-8.; VIEIRA, Gustavo Duarte. *Proteção de dados pessoais em práticas de profiling no setor privado*. 2019. 126 f. Dissertação (Mestrado em Direito) – Universidade Federal de Minas Gerais, Belo Horizonte. Disponível em: <https://repositorio.ufmg.br/bitstream/1843/34072/8/Gustavo%20Duarte%20Vieira%20-%20Prote%C3%A7%C3%A3o%20de%20dados%20pessoais%20em%20pr%C3%A1ticas%20de%20profiling-mesclado%281%29.pdf>. Acesso em: 15 jan. 2025;

16. DONEDA, Danilo Cesar Maganhoto. *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. ISBN 978-65-5065-030-8.; VIEIRA, Gustavo Duarte. *Proteção de dados pessoais em práticas de profiling no setor privado*. 2019. 126 f. Dissertação (Mestrado em Direito) – Universidade Federal de Minas Gerais, Belo Horizonte. Disponível em: <https://repositorio.ufmg.br/bitstream/1843/34072/8/Gustavo%20Duarte%20Vieira%20-%20Prote%C3%A7%C3%A3o%20de%20dados%20pessoais%20em%20pr%C3%A1ticas%20de%20profiling-mesclado%281%29.pdf>. Acesso em: 15 jan. 2025;

dado que a experiência do desenvolvedor afeta diretamente a qualidade e a eficiência do software produzido¹⁷.

Nesse sentido, a DX inclui aspectos como o desempenho colaborativo, a eficácia das ferramentas utilizadas e a dinâmica entre os integrantes da equipe, conforme descrito no *framework* SPACE. Este modelo enfatiza cinco pilares interligados: satisfação e bem-estar, desempenho, atividade, comunicação e colaboração, além de eficiência e fluxo. Tais dimensões revelam que métricas unidimensionais, como número de *commits* ou *pull requests*, não são suficientes para avaliar a experiência do desenvolvedor de maneira completa e significativa¹⁸.

Além disso, a DX está diretamente relacionada à avaliação do desempenho das equipes de desenvolvimento, contexto em que as métricas DORA (*DevOps Research and Assessment*) desempenham um papel fundamental¹⁹. Criadas para medir a eficiência de processos *DevOps*, as métricas DORA se baseiam em quatro indicadores principais: frequência de *deploys*, tempo de implementação de mudanças, taxa de falha de mudanças e tempo médio de recuperação. Esses indicadores permitem avaliar não apenas a produtividade, mas também a estabilidade e a eficácia das equipes, fornecendo uma base quantitativa para otimizações contínuas.

Por fim, a DX também se relaciona com o tempo de carreira e as formas como os desenvolvedores interagem com projetos e ferramentas, permitindo mensurações quantitativas que indicam lacunas e oportunidades de melhoria em ambientes corporativos²⁰. Essa perspectiva integrada evidencia que o conceito de DX transcende métricas isoladas, destacando sua importância no equilíbrio entre inovação e bem-estar no contexto organizacional.

Entretanto, independentemente da abordagem utilizada para acompanhar a *Developer Experience*, suas métricas estão intrinsecamente conectadas ao *People Analytics*. Segundo Zieglmeier e Pretschner²¹, esse conjunto de práticas analíticas é aplicado aos dados dos funcionários com o objetivo de otimizar

17. FAGERHOLM, Fabian; MÜNCH, Jürgen. *Developer Experience: Concept and Definition*. In: INTERNATIONAL CONFERENCE ON SOFTWARE AND SYSTEM PROCESS (ICSSP 2012), Zurich, Switzerland, June 2-3, 2012. Proceedings [...]. IEEE, 2012. p. 73-77. DOI: 10.1109/ICSSP.2012.6225984.

18. FORSGREN, Nicole et al. The SPACE of developer productivity. *Communications of the ACM*, v. 64, n. 6, p. 46-53, 2021. Disponível em: <https://dl.acm.org/doi/10.1145/3454122.3454124>. Acesso em: 15 jan. 2025

19. PINHO, João Gonçalo Mesquita Leite de. *DevOps Approach to Measure Product Quality and Developers' Efficiency*. 2024. Dissertação (Mestrado em Ciência da Computação) – Instituto Superior de Engenharia do Porto, Porto. Disponível em: https://recipp.ipp.pt/bitstream/10400.22/25955/1/Tese_5258.pdf. Acesso em: 15 jan. 2025.

20. LOPES, Jefferson G. M.; OLIVEIRA, Johnatan; FIGUEIREDO, Eduardo. *Evaluating the impact of developer experience on code quality: a systematic literature review*. In: CIBSE 2024: Proceedings of the Latin American Conference on Software Engineering. Belo Horizonte, MG: [s.n.], 2024.

21. ZIEGLMEIER, Valentin; PRETSCHNER, Alexander. *Rethinking People Analytics with Inverse Transparency by Design*. arXiv, 26 jul. 2023. Disponível em: <https://arxiv.org/abs/2305.09813v2>. Acesso em: 15 jan. 2025.

processos de trabalho e aprimorar a tomada de decisões gerenciais. Tradicionalmente, essas práticas se baseiam em métricas quantitativas extraídas de ferramentas digitais utilizadas pelos colaboradores, como plataformas de comunicação, sistemas de rastreamento de tarefas e softwares de produtividade.

A complexidade surge na forma como esses dados são tratados, especialmente no contexto da *Developer Experience*, em que informações começam a ser coletadas já no momento em que o colaborador se autentica no equipamento corporativo. Considere o seguinte cenário hipotético: durante sua jornada de trabalho, uma pessoa desenvolvedora responde a uma pesquisa de satisfação, colabora com colegas na resolução de *bugs* ao responder dúvidas, realiza contribuições técnicas, como *commits*, *pull requests* e revisões de código, e utiliza serviços empresariais relacionados ao desenvolvimento de software.

Cada uma dessas ações é registrada de maneira detalhada, com marcações precisas de data, hora, minuto e segundo, além de vinculadas a identificadores únicos, como credenciais de login. Embora essas métricas revelem muito sobre a jornada de trabalho, elas não capturam aspectos contextuais importantes, como a razão pela qual uma tarefa foi concluída mais lentamente. Por exemplo, não indicam se houve um impacto de acessibilidade, ainda que, por meio do cruzamento de bases, pudesse ser determinado que a pessoa possui uma deficiência.

A análise de identificadores únicos configura perfilamento, transformando ações registradas em dados pessoais, pois permite a identificação direta ou indireta, conforme o art. 12, §2º da LGPD, já discutido neste artigo. Estudos recentes aprofundam essa questão ao propor modelos preditivos baseados em métricas de atividade e familiaridade de desenvolvedores com código, utilizando *Machine Learning*²².

Nesse contexto, as limitações éticas e jurídicas das métricas aplicadas à *Developer Experience* estão relacionadas à necessidade de equilibrar o tratamento de dados estritamente necessário para a manutenção das relações trabalhistas com o tratamento massivo, que frequentemente carece de transparência. Essa falta de clareza nas informações processadas é apontada como um dos principais desafios em práticas de *People Analytics*²³. Além disso, garantir esse equilíbrio e implementar sistemas que promovam a transparência são medidas essenciais para evitar o perfilamento associado à discriminação

22. CHO, Yeongjun et al. *Extending Developer Experience Metrics for Better Effort-Aware Just-In-Time Defect Prediction*. IEEE Access, v. 10, p. 128218-128231, 2022.

23. ZIEGLMEIER, Valentin; PRETSCHNER, Alexander. *Rethinking People Analytics With Inverse Transparency by Design*. arXiv, 26 jul. 2023. Disponível em: <https://arxiv.org/abs/2305.09813v2>. Acesso em: 15 jan. 2025

algorítmica. Essa prática, além de prejudicar colaboradores, causa danos desproporcionais a minorias, agravando desigualdades estruturais²⁴.

Embora a adoção do legítimo interesse como base legal para o tratamento de dados dos colaboradores possa ser defendida, a transparência e a minimização no uso dessas informações são critérios indispensáveis para evitar desvios de finalidade²⁵. Isso se torna especialmente relevante na aplicação de *frameworks* como SPACE e DORA, que utilizam múltiplas métricas para avaliar o ambiente tecnológico das organizações. Além disso, o surgimento constante de ferramentas que ampliam o alcance do panóptico organizacional exige uma análise ética criteriosa, especialmente considerando que o consentimento firmado no contrato de trabalho raramente é verdadeiramente livre e inequívoco²⁶.

Outro aspecto crítico a ser analisado é a potencial colisão de direitos: o exercício regular do direito à iniciativa privada, que justifica o controle para fins de conformidade e cibersegurança, e o direito à proteção de dados pessoais, reconhecido como um direito fundamental²⁷. Para mitigar conflitos, uma abordagem ética que inclua mecanismos de rastreabilidade e transparência ponta a ponta é essencial. Essa prática não apenas garante que os colaboradores compreendam claramente o uso de seus dados, mas também facilita o acompanhamento por representantes coletivos, como sindicatos, quando aplicável.

Nesse sentido, a implementação da autodeterminação informativa no contexto de *Developer Experience* (DX) é central para garantir que o uso de dados atenda tanto às demandas tecnológicas quanto aos direitos individuais. Embora a coleta de dados muitas vezes beneficie os colaboradores ao aprimorar processos e ferramentas, o desafio reside em assegurar que sua utilização seja transparente, voluntária e livre de penalidades, especialmente nos casos em que não há base legal alternativa ao consentimento²⁸.

24. VIEIRA, Gustavo Duarte. *Proteção de dados pessoais em práticas de profiling no setor privado*. 2019. 126 f. Dissertação (Mestrado em Direito) – Universidade Federal de Minas Gerais, Belo Horizonte. Disponível em: <https://repositorio.ufmg.br/bitstream/1843/34072/8/Gustavo%20Duarte%20Vieira%20-%20Prote%C3%A7%C3%A3o%20de%20dados%20pessoais%20em%20pr%C3%A1ticas%20de%20profiling-mesclado%281%29.pdf>. Acesso em: 15 jan. 2025;

25. ZAVANELLA, Fabiano. *Aplicação da Lei Geral de Proteção de Dados nas relações trabalhistas: limites do consentimento do empregado e do legítimo interesse do empregador*. 2023. Tese de Doutorado. Universidade de São Paulo. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2138/tde-06032024-120308/publico/11737207DIC.pdf>. Acesso em: 15 jan. 2025.

26. ZAVANELLA, Fabiano. *Aplicação da Lei Geral de Proteção de Dados nas relações trabalhistas: limites do consentimento do empregado e do legítimo interesse do empregador*. 2023. Tese de Doutorado. Universidade de São Paulo. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2138/tde-06032024-120308/publico/11737207DIC.pdf>. Acesso em: 15 jan. 2025.

27. ZAVANELLA, Fabiano. *Aplicação da Lei Geral de Proteção de Dados nas relações trabalhistas: limites do consentimento do empregado e do legítimo interesse do empregador*. 2023. Tese de Doutorado. Universidade de São Paulo. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2138/tde-06032024-120308/publico/11737207DIC.pdf>. Acesso em: 15 jan. 2025.

28. ZAVANELLA, Fabiano. *Aplicação da Lei Geral de Proteção de Dados nas relações trabalhistas: limites do consentimento do empregado e do legítimo interesse do empregador*. 2023. Tese de Doutorado. Universidade de São Paulo. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2138/tde-06032024-120308/publico/11737207DIC.pdf>. Acesso em: 15 jan. 2025.

Assim, práticas de governança de dados pautadas pela ética e pela conformidade com os parâmetros legais são indispensáveis. No contexto da *Developer Experience*, essas práticas são essenciais para que a inovação tecnológica avance sem comprometer a privacidade dos colaboradores, promovendo um equilíbrio entre o “poder fazer” e o “dever fazer”. A partir dessa perspectiva, explora-se, a seguir, as dimensões técnicas, éticas e jurídicas necessárias para garantir a autodeterminação informativa nas métricas de DX.

3. Propostas para uma governança ética e responsável de indicadores DX

Conforme discutido ao longo deste trabalho, no contexto trabalhista, onde frequentemente se enquadram as análises de *Developer Experience*, duas bases legais são predominantes para o tratamento de dados pessoais, conforme disposto no art. 7º da LGPD: o legítimo interesse, fundamentado na relação de subordinação entre empregador e empregado, e o consentimento. Independentemente da base legal adotada, a transparência desempenha um papel central. Sem ela, a autodeterminação informativa e a prestação de contas pelas empresas tornam-se inviáveis, comprometendo tanto os direitos dos titulares quanto a conformidade legal das organizações.

Para garantir um comportamento transparente na *Developer Experience*, Vieira²⁹ elenca aspectos fundamentais: a identificação clara dos dados coletados, a definição das finalidades para as quais são utilizados, a explicitação de com quem são compartilhados e a indicação das bases legais aplicáveis. Essa transparência é especialmente necessária no uso de *frameworks* como SPACE e DORA, que dependem de indicadores baseados em interações dos colaboradores com ferramentas como GitHub e GitLab, além de métricas relacionadas a taxas de falhas no desenvolvimento de software e respostas a pesquisas de satisfação, entre outros.

Uma solução prática para alcançar essa visibilidade é a implementação da transparência inversa (*Inverse Transparency*), que assegura que os titulares dos dados tenham conhecimento sobre cada acesso realizado às suas informações. Zieglmeier e Pretschner³⁰ propõem uma abordagem em três etapas para operacionalizar esse modelo: monitoramento contínuo dos acessos aos

29. VIEIRA, Gustavo Duarte. *Proteção de dados pessoais em práticas de profiling no setor privado*. 2019. 126 f. Dissertação (Mestrado em Direito) – Universidade Federal de Minas Gerais, Belo Horizonte. Disponível em: <https://repositorio.ufmg.br/bitstream/1843/34072/8/Gustavo%20Duarte%20Vieira%20-%20Prote%C3%A7%C3%A3o%20de%20dados%20pessoais%20em%20pr%C3%A1ticas%20de%20profiling-mesclado%281%29.pdf>. Acesso em: 15 jan. 2025;

30. ZIEGLMEIER, Valentin; PRETSCHNER, Alexander. *Rethinking People Analytics With Inverse Transparency by Design*. arXiv, 26 jul. 2023. Disponível em: <https://arxiv.org/abs/2305.09813v2>. Acesso em: 15 jan. 2025.

dados, armazenamento seguro das informações coletadas e a disponibilização de painéis interativos que detalham como e onde os dados estão sendo utilizados. Essa estrutura não apenas promove o controle pelos titulares, mas também reforça a confiança no uso ético e responsável das métricas de *Developer Experience*.

Essa abordagem requer a integração de ferramentas de *analytics* com sistemas de monitoramento e registros de *logs*. Isso implica que qualquer acesso a dados por consumidores seja registrado com informações precisas de horário (*timestamp*). Os dados coletados devem ser enviados a um banco de dados central por meio de uma interface de programação de aplicação (API) que permita consultas e adição de *logs*. Por fim, um painel deve exibir ao titular cada etapa rastreada do uso de seus dados.

A implementação do rastreamento pode ser adaptada às necessidades específicas da organização ou realizada com ferramentas disponíveis no mercado, como o *CloudTrail* da *Amazon Web Services* (AWS) ou os Registros de Auditoria do *Google Cloud*. Independentemente da solução adotada, é essencial que os dados sejam monitorados com um ponto central de atenção: a criação de painéis de controle acessíveis. Muitas vezes, negligencia-se a acessibilidade desses sistemas, o que compromete a transparência e a autodeterminação informativa.

As diretrizes *Web Content Accessibility Guidelines* (WCAG) estabelecem quatro pilares fundamentais para o desenvolvimento de painéis de controle acessíveis na DX: 1. Perceptível: o conteúdo deve ser apresentado de forma que possa ser percebido por diferentes formatos visuais ou auditivos. 2. Operável: o sistema deve permitir interação por diferentes métodos, como teclado ou dispositivos assistivos. 3. Compreensível: o conteúdo deve ser inteligível para todos, independentemente de deficiências. 4. Robusto: a solução deve ser compatível com tecnologias assistivas diversas e seguir boas práticas de desenvolvimento³¹.

Além de fornecer informações detalhadas sobre onde os dados foram extraídos, como estão sendo tratados e onde estão sendo carregados, essas informações precisam ser exibidas de maneira clara e acessível. Por exemplo, painéis que oferecem contraste adequado, navegação contextualizada e su-

31. FERRAZ, Reinaldo. *Acessibilidade na Web: Boas Práticas para Construir Sites e Aplicações Acessíveis*. São Paulo: Casa do Código, 2020. 246 p. ISBN 978-65-86110-16-6; FERREIRA, Jerusa Gabriela. *O direito à inclusão digital das pessoas com deficiência visual no Brasil*. Orientadora: Luciani Coimbra de Carvalho. 2023. 136 f. Dissertação (Mestrado em Direito) Faculdade de Direito, Universidade Federal de Mato Grosso do Sul, Campo Grande, 2023. Disponível em: [HTTPS://repositorio.ufms.br/retrieve/1405298f-0d01-4a60-a759-a9f2ee19f004/Disserta%3a7%3a3o%20da%20Jerusa%20-%2007-09-2023%20-%20FINAL.pdf](https://repositorio.ufms.br/retrieve/1405298f-0d01-4a60-a759-a9f2ee19f004/Disserta%3a7%3a3o%20da%20Jerusa%20-%2007-09-2023%20-%20FINAL.pdf). Acesso em: 15 jan. 2025.

porte a softwares leitores de tela ampliam a transparência e proporcionam ao titular uma compreensão completa do uso de seus dados³².

Estudos sobre transparência inversa demonstram que sua aplicação pode aumentar a confiança dos colaboradores nas ferramentas corporativas, além de promover maior engajamento entre desenvolvedores de software. Isso resulta em benefícios diretos para o ambiente organizacional, ao melhorar o clima e fomentar o protagonismo dos colaboradores³³. Essa conexão é natural, dado que a transparência depende de arquiteturas de controle que garantam o acompanhamento ponta a ponta³⁴.

Adicionalmente, independentemente da base legal utilizada, é fundamental que os painéis listem todas as utilizações dos dados. Nos casos em que o colaborador opte por desativar o compartilhamento de determinados dados, a organização pode recorrer à anonimização, ocultando identificadores únicos, mas preservando dados de contribuição por recortes que atendam ao contexto da DX. Um painel centralizado pode, ainda, facilitar a abertura de chamados para a correção de eventuais imprecisões, assegurando que os dados sejam consumidos de forma confiável e estejam em conformidade com as normas aplicáveis.

A adoção dessas boas práticas representa, para as organizações, uma oportunidade de incorporar a privacidade e a transparência como fundamentos da arquitetura de sistemas. Isso oferece aos colaboradores da área de tecnologia um ambiente que incentiva a confiança e o uso ético de seus dados pessoais. Por um lado, promove conformidade com padrões normativos; por outro, contribui para a retenção de talentos, ao garantir que, no contexto da *Developer Experience*, a satisfação e o clima organizacional sejam otimizados com o respeito à privacidade dos colaboradores.

32. FERRAZ, Reinaldo. *Acessibilidade na Web: Boas Práticas para Construir Sites e Aplicações Acessíveis*. São Paulo: Casa do Código, 2020. 246 p. ISBN 978-65-86110-16-6; FERREIRA, Jerusa Gabriela. *O direito à inclusão digital das pessoas com deficiência visual no Brasil*. Orientadora: Luciani Coimbra de Carvalho. 2023. 136 f. Dissertação (Mestrado em Direito) Faculdade de Direito, Universidade Federal de Mato Grosso do Sul, Campo Grande, 2023. Disponível em: [HTTPS://repositorio.ufms.br/retrieve/1405298f-0d01-4a60-a759-a9f2ee19f004/Disserta%3%a7%c3%a3o%20da%20Jerusa%20-%2007-09-2023%20-%20FINAL.pdf](https://repositorio.ufms.br/retrieve/1405298f-0d01-4a60-a759-a9f2ee19f004/Disserta%3%a7%c3%a3o%20da%20Jerusa%20-%2007-09-2023%20-%20FINAL.pdf). Acesso em: 15 jan. 2025.

33. ZIEGLMEIER, Valentin; PRETSCHNER, Alexander. *Rethinking People Analytics With Inverse Transparency by Design*. arXiv, 26 jul. 2023. Disponível em: <https://arxiv.org/abs/2305.09813v2>. Acesso em: 15 jan. 2025.

34. VIEIRA, Gustavo Duarte. *Proteção de dados pessoais em práticas de profiling no setor privado*. 2019. 126 f. Dissertação (Mestrado em Direito) – Universidade Federal de Minas Gerais, Belo Horizonte. Disponível em: <https://repositorio.ufmg.br/bitstream/1843/34072/8/Gustavo%20Duarte%20Vieira%20-%20Prote%3%A7%C3%A3o%20de%20dados%20pessoais%20em%20pr%C3%A1ticas%20de%20profiling-mesclado%281%29.pdf>. Acesso em: 15 jan. 2025.

Considerações finais

A *Developer Experience* (DX) tem se consolidado no mercado como um conjunto de práticas voltadas a maximizar a produtividade e melhorar a satisfação dos colaboradores. De um lado, são utilizadas ferramentas e métricas para elevar a eficiência. De outro, busca-se aprimorar a experiência de uso e o bem-estar das pessoas desenvolvedoras. Este estudo explorou essas oportunidades, mas também destacou os desafios éticos relacionados à vigilância excessiva, ao uso de dados sem diretrizes claras e ao desequilíbrio de poder típico das relações laborais.

No contexto analisado, apresentaram-se perspectivas fundamentadas na autodeterminação informativa e na transparência como pilares essenciais. Essas práticas permitem criar métricas de desempenho com responsabilidade ética e alinhamento normativo. Por exemplo, o uso de mecanismos como monitoramento rastreável e perfilamento ético pode assegurar maior equilíbrio no tratamento de dados. A transparência, por sua vez, deve incluir acessibilidade e acesso facilitado às informações sobre o uso de dados. Independentemente da base legal utilizada (como legítimo interesse ou consentimento), é fundamental que os colaboradores possam acompanhar o ciclo completo de seus dados e estejam cientes de cada etapa.

Espera-se que a aplicação dessas práticas vá além da conformidade normativa, promovendo confiança nos colaboradores. A transparência pode atuar como um fator de retenção de talentos, uma vez que demonstra respeito aos direitos individuais e incentiva um ambiente mais ético e colaborativo. Adicionalmente, a disseminação dessas práticas entre as equipes de desenvolvimento pode influenciar positivamente o comportamento dos profissionais, estimulando o design de produtos que respeitem a privacidade dos usuários finais.

Ao adotar essas práticas, as organizações têm a oportunidade de alinhar inovação tecnológica, ética e privacidade. Isso não apenas fortalece a reputação da empresa junto a consumidores finais, mas também cria um diferencial competitivo ao unir eficiência organizacional e responsabilidade social.

Referências

BAUMAN, Zygmunt. *Vigilância líquida*: diálogos com David Lyon. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BRASIL. *Emenda Constitucional nº 115, de 10 de fevereiro de 2022*. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 15 jan. 2025.

BRICALLI, Iafet Leonardi. A vigilância como cultura. *Sociologia & Antropologia*, Rio de Janeiro, v. 10, n. 3, p. 1103-1107, set.-dez. 2020. Disponível em: <https://www.scielo.br/j/sant/a/wjyYxRWt-n37DSZ8FrYWmkCL/?lang=pt&format=html>. Acesso em: 15 jan. 2025

CHO, Yeongjun et al. *Extending Developer Experience Metrics for Better Effort-Aware Just-In-Time Defect Prediction*. IEEE Access, v. 10, p. 128218-128231, 2022.

DICKENS, Charles. *Tempos difíceis*. São Paulo: Boitempo Editorial, 2014.

DONEDA, Danilo Cesar Maganhoto. *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. ISBN 978-65-5065-030-8.

FAGERHOLM, Fabian; MÜNCH, Jürgen. *Developer Experience: Concept and Definition*. In: INTERNATIONAL CONFERENCE ON SOFTWARE AND SYSTEM PROCESS (ICSSP 2012), Zurich, Switzerland, June 2-3, 2012. Proceedings [...]. IEEE, 2012. p. 73-77. DOI: 10.1109/ICSSP.2012.6225984.

FERRAZ, Reinaldo. *Acessibilidade na Web: Boas Práticas para Construir Sites e Aplicações Acessíveis*. São Paulo: Casa do Código, 2020. 246 p. ISBN 978-65-86110-16-6

FERREIRA, Jerusa Gabriela. *O direito à inclusão digital das pessoas com deficiência visual no Brasil*. Orientadora: Luciani Coimbra de Carvalho. 2023. 136 f. Dissertação (Mestrado em Direito) Faculdade de Direito, Universidade Federal de Mato Grosso do Sul, Campo Grande, 2023. Disponível em: <HTTPS://repositorio.ufms.br/retrieve/1405298f-0d01-4a60-a759-a9f2ee19f004/Disserta%c3%a7%c3%a3o%20da%20Jerusa%20-%2007-09-2023%20-%20FINAL.pdf>. Acesso em: 15 jan. 2025.

FORSGREN, Nicole et al. The SPACE of developer productivity. *Communications of the ACM*, v. 64, n. 6, p. 46-53, 2021. Disponível em: <https://dl.acm.org/doi/10.1145/3454122.3454124>. Acesso em: 15 jan. 2025.

LIU, Cixin. *A Floresta Sombria*. Rio de Janeiro: Suma, 2017.

LOPES, Jefferson G. M.; OLIVEIRA, Johnatan; FIGUEIREDO, Eduardo. *Evaluating the impact of developer experience on code quality: a systematic literature review*. In: CIBSE 2024: Proceedings of the Latin American Conference on Software Engineering. Belo Horizonte, MG: [s.n.], 2024.

ORWELL, George. 1984. Tradução de Alexandre Hubner e Heloisa Jahn. São Paulo: Companhia das Letras, 2009.

PINHO, João Gonçalo Mesquita Leite de. *DevOps Approach to Measure Product Quality and Developers' Efficiency*. 2024. Dissertação (Mestrado em Ciência da Computação) – Instituto Superior de Engenharia do Porto, Porto. Disponível em: https://recipp.ipp.pt/bitstream/10400.22/25955/1/Tese_5258.pdf. Acesso em: 15 jan. 2025.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: DONEDA, Danilo et al. (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

SIQUEIRA, Dirceu Pereira; MOREIRA, Mayume Caires. Autodeterminação informativa na sociedade pós-panóptico: novas formas de panoptismo e os direitos da personalidade. *Prisma Jurídico*,

São Paulo, v. 22, n. 1, p. 74-91, jan./jun. 2023. Disponível em: <http://doi.org/10.5585/2023.20634>. Acesso em: 15 jan. 2025.

VIEIRA, Gustavo Duarte. *Proteção de dados pessoais em práticas de profiling no setor privado*. 2019. 126 f. Dissertação (Mestrado em Direito) – Universidade Federal de Minas Gerais, Belo Horizonte. Disponível em: <https://repositorio.ufmg.br/bitstream/1843/34072/8/Gustavo%20Duar-te%20Vieira%20-%20Prote%C3%A7%C3%A3o%20de%20dados%20pessoais%20em%20pr%C3%A1ticas%20de%20profiling-mesclado%281%29.pdf>. Acesso em: 15 jan. 2025

ZAVANELLA, Fabiano. *Aplicação da Lei Geral de Proteção de Dados nas relações trabalhistas: limites do consentimento do empregado e do legítimo interesse do empregador*. 2023. Tese de Doutorado. Universidade de São Paulo. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2138/tde-06032024-120308/publico/11737207DIC.pdf>. Acesso em: 15 jan. 2025.

ZIEGLMEIER, Valentin; PRETSCHNER, Alexander. *Rethinking People Analytics With Inverse Transparency by Design*. arXiv, 26 jul. 2023. Disponível em: <https://arxiv.org/abs/2305.09813v2>. Acesso em: 15 jan. 2025.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

EIXO III

Neurotecnologia e neurodados

AUTORES

Daniele Dimas Ramos Garuti

Desirée Marcelle da Cunha

Larissa Almeida Del Lhano

Larissa Boullosa Magnavita de Oliveira

Nicole Julie da Silva Rodrigues

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

8

Neurodireitos e dados sensíveis: a proteção da mente na era digital

DESIRÉE MARCELLE DA CUNHA

Sumário: Introdução. 1. Neurodados na era das ICM e o limbo jurídico da privacidade cerebral. 2. Riscos à privacidade dos dados neurais. 2.1. Riscos associados ao hackeamento dos dados neurais. 2.2. Coleta e uso indevidos de dados neurais em desfavor do consumidor. 3. Panorama das iniciativas de regulamentação no Brasil e no mundo. 4. Necessidade de regulação e enquadramento dos dados neurais enquanto dados pessoais sensíveis. Considerações finais. Referências.

The mind is the sanctuary of our innermost selves, and that private world must be protected. YUSTE, Rafael.²

Introdução

A partir de uma abordagem qualitativa, de caráter exploratório e analítico, fundamentada em pesquisa bibliográfica e documental, o presente estudo tem como objetivo examinar os riscos associados à coleta e utilização de dados neurais, bem como defender seu enquadramento jurídico como dados pessoais sensíveis.

Para tanto, foram analisados estudos doutrinários, artigos científicos, relatórios institucionais e normativos nacionais e internacionais, permitindo uma reflexão crítica sobre os desafios regulatórios impostos pelas novas tecnologias neurodigitais, à luz da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e do princípio da proteção da dignidade da pessoa humana.

Nesse contexto, através das pesquisas que deram ensejo ao estudo em questão, foi possível identificar a enorme evolução das Interfaces Cérebro-Máquina (ICM), sistemas que possibilitam a comunicação entre o cérebro e dispositivos externos, permitindo ao usuário interagir com o meio que o cerca.

É relevante destacar que a *Neuralink*, uma das empresas pioneiras no desenvolvimento de dispositivos implantáveis de ICM, realizou o primeiro implante em um ser humano em janeiro de 2024³. O chip, denominado “*Telepathy*”, possui mais de mil eletrodos responsáveis por registrar a atividade dos neurônios.

1. Advogada. Assessora jurídica na Secretaria de Estado de Educação do Rio de Janeiro. Bacharel em Direito pela Universidade do Estado do Rio de Janeiro (UERJ). Pós-graduanda em Direito Digital pela Universidade do Estado do Rio de Janeiro (UERJ), em parceria com o Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS-Rio).

2. Tradução livre: “Há de se proteger o cérebro como o santuário da nossa mente porque aí é gerada a identidade humana”. Disponível em: <https://magazine.columbia.edu/article/need-protect-data-our-brains>. Acesso em: 18 jan. 2025.

3. *ELON Musk's Neuralink implants brain chip in first human*. Reuters. 30 jan. 2024. Disponível em: <https://www.reuters.com/technology/neuralink-implants-brain-chip-first-human-musk-says-2024-01-29/>. Acesso em: 20 dez. 2024.

De acordo com o site oficial da *Neuralink*, o objetivo primordial do dispositivo é restaurar a autonomia de pacientes com condições de saúde graves, além de “desbloquear o potencial humano no futuro”⁴, o que revela a ambição da empresa de, a longo prazo, empregar sua tecnologia para promover uma simbiose entre o ser humano e a máquina, possibilitando a criação de uma espécie de “super-humano”.

Para se entender a relevância do tema, espera-se que o mercado global de Interfaces Cérebro-Máquina passe de 1.74 bilhões de dólares em 2022 para 6.2 bilhões de dólares em 2030⁵, tornando-se cada vez mais popular.

Tendo isso em vista, surge a preocupação em torno da coleta, armazenamento e tratamento dos dados neurais dos usuários, bem como a respeito da privacidade mental e segurança destes dispositivos.

Todavia, a legislação atual não consegue abarcar todas as hipóteses e especificidades para a adequada proteção jurídica da mente, de modo que há pouco ou quase nada sendo regulado a respeito da proteção dos dados neurais utilizados por estes dispositivos.

Em especial, sequer há normativa delimitando dados neurais enquanto dados pessoais sensíveis, apesar da natureza das informações coletadas, por si, já revelar o grau de risco a que ficam submetidos os usuários.

Dessa forma, este trabalho parte da hipótese de que o reconhecimento jurídico dos dados neurais como dados pessoais sensíveis configura condição indispensável para a efetiva tutela da privacidade mental no ordenamento jurídico brasileiro.

1. Neurodados na era das ICM e o limbo jurídico da privacidade cerebral

O dado neural pode ser compreendido como qualquer informação obtida, direta ou indiretamente, da atividade do sistema nervoso central do paciente, mediante interações cérebro-computador⁶.

4. “Our mission: Create a generalized brain interface to restore autonomy to those with unmet medical needs today and unlock human potential tomorrow.”. *Neuralink*. Disponível em: <https://neuralink.com/>. Acesso em: 22 dez. 2024.

5. ALOHALY, Manar. *The brain computer interface market is growing – but what are the risks?*. Global Economic Forum. 14 jun. 2024. Disponível em: [https://www.weforum.org/stories/2024/06/the-brain-computer-interface-market-is-growing-but-what-are-the-risks/#:~:text=The%20brain%20computer%20interface%20\(BCI,to%20%246.2%20billion%20by%202030](https://www.weforum.org/stories/2024/06/the-brain-computer-interface-market-is-growing-but-what-are-the-risks/#:~:text=The%20brain%20computer%20interface%20(BCI,to%20%246.2%20billion%20by%202030). Acesso em: 28 dez. 2024.

6. BRASIL. CÂMARA DOS DEPUTADOS. *Projeto cria regras para proteger dados obtidos a partir do sistema nervoso central*. 06 jul. 2021. Disponível em: https://www.camara.leg.br/noticias/769507-PROJETO-CRIA-REGRAS-PARA-PROTEGER-DADOS-OBTIDOS-A-PARTIR-DO-SISTEMA-NERVOSO-CENTRAL%E2%80%A8?utm_source=chatgpt.com. Acesso em 11 dez. 2024.

Esse procedimento é comumente realizado através de dispositivos Interfaces Cérebro-Máquina (ICM), cuja tecnologia é capaz de medir a atividade cerebral e traduzi-la em comandos para um computador ou outro dispositivo, permitindo que os usuários controlem máquinas e dispositivos usando apenas seus pensamentos⁷.

No entanto, apesar de os novos dispositivos de neurotecnologia oferecerem grandes promessas para a saúde, produtividade e entretenimento, eles também implicam sérios riscos à privacidade, especialmente no que diz respeito ao uso indevido de dados neurais pelas empresas que detêm essas tecnologias, o que se agrava tendo em vista a incipiente ou quase inexistente legislação protetiva.

Importante esclarecer que os dispositivos ICM podem ser invasivos ou não invasivos, com base no método de interação com o cérebro: métodos invasivos requerem a inserção de eletrodos no córtex cerebral, através de uma cirurgia intracraniana, como aqueles idealizados pela *Neuralink*; já os métodos não-invasivos utilizam os eletrodos externamente no couro cabeludo (o mais comum são os sinais captados por meio de eletroencefalograma – EEG)⁸.

Trazendo luz especificamente para os métodos invasivos de utilização de ICM, objeto central deste trabalho, observa-se a significativa vulnerabilidade do usuário em relação ao controle sobre os seus dados neurais.

Isso ocorre porque, ao ser implantado no cérebro, e conectado diretamente a um computador, o dispositivo possibilita a coleta e o processamento imediato das informações cerebrais.

Sendo assim, há insegurança quanto ao nível de proteção destes dados, e até que ponto o usuário teria capacidade plena para o desenvolvimento das suas atividades, discernimento das suas atividades e exteriorização da sua vontade.

Ou seja, a pessoa humana perde o controle da própria mente para os detentores de tais tecnologias, sem saber, inclusive, quais dados estão sendo coletados, como estão sendo armazenados, para o que estão sendo usados e se há segurança adequada para possíveis vazamentos ou invasões de terceiros.

A situação é alarmante, pois, atualmente, no Brasil, não existe uma regulamentação específica para a proteção dos dados neurais, os quais, por sua vez, sequer são considerados como dados pessoais sensíveis.

7. PEKSA, Janis.; MAMCHUR, Dmytro. *State-of-the-Art on Brain-Computer Interface Technology*. Sensors 2023, 23, 6001. p. 1. Disponível em: <https://doi.org/10.3390/s23136001>. Acesso em 13 dez. 2024.

8. SCHUH, Anderson R. et al. *Desenvolvimento de Um Simulador Controlado por Interface Cérebro-Computador Não Invasiva para Treinamento na Utilização de Cadeira de Rodas*. RENOTE, Porto Alegre, v. 11, n. 3, 2013. p.3. Disponível em: <https://www.seer.ufrgs.br/index.php/renote/article/view/44716>. Acesso em 28 dez. 2024.

Isso evidencia a necessidade urgente de o direito acompanhar as inovações tecnológicas, a fim de garantir a proteção da pessoa humana, especialmente considerando o status de direito fundamental atribuído à proteção dos dados pessoais pela Constituição brasileira.

Desse modo, se torna imprescindível a correta definição e o adequado enquadramento dos neurodados, a fim de plenamente tutelar a proteção jurídica da mente, que possui alta complexidade e cujas informações são altamente sensíveis – os dados neurais estão relacionados à saúde, posição política, ideológica e religiosa, preferências, convicções, sensações, emoções e memórias.

Considerando o exposto, é possível conjecturar a respeito dos possíveis riscos ao titular de dados neurais quando suas informações são tratadas por empresas de neurotecnologia.

2. Riscos à privacidade dos dados neurais

Because it accesses the centre of our mental activity, neurotechnology bypasses all of the filters that exist in the body. YUSTE, Rafael.⁹

Um estudo realizado por cientistas da Universidade da Califórnia, em Berkeley, no ano de 2011, demonstrou ser possível usar exames cerebrais para reconstruir trechos de filmes que as pessoas haviam assistido anteriormente.¹⁰

Aproximadamente doze anos depois, em 2023, foi possível recriar a música “*Another Brick in the Wall, Part. I*”, da banda Pink Floyd, a partir de ondas cerebrais captadas por uma tecnologia de IA, de pacientes que ouviam a canção em estado de inconsciência, demonstrando que a atividade elétrica do cérebro pode ser decodificada e usada para reconstruir música.¹¹

Os resultados apresentados revelam que a exposição indiscriminada dos neurodados, sem a devida regulamentação, pode gerar consequências devastadoras, especialmente se utilizados para fins ilícitos, o que só atesta a urgência do tema.

Neste ponto, respaldando a necessidade de se atentar aos riscos das neurotecnologias, estudos identificaram mais de 300 vulnerabilidades em dispo-

9. Tradução livre: “Porque ela acessa o centro de nossa atividade mental, a neurotecnologia ultrapassa todos os filtros que existem no corpo”. Disponível em: <https://www.cnic.es/en/noticias/rafael-yuste-because-it-accesses-centre-our-mental-activity-neurotechnology-bypasses-all>. Acesso em: 18 jan. 2025.

10. MAKASDJIAN, Roxanne. *New video of how scientists reconstruct the movies in our minds*. UC Berkeley News. 21 dez. 2011. Disponível em: <https://news.berkeley.edu/2011/12/21/new-visionreconstructionvideo/>. Acesso em: 12 jan 2025.

11. TU, Lucy. *Neuroscientists Re-create Pink Floyd Song from Listeners’ Brain Activity*. Scientific American. 15 ago. 2023. Disponível em: <https://www.scientificamerican.com/article/neuroscientists-re-create-pink-floyd-song-from-listeners-brain-activity/>. Acesso em: 12 jan. 2025.

sitivos de neurotecnologia, incluindo falhas que permitiriam a interceptação de sinais e o controle remoto do dispositivo¹².

Exemplo desta vulnerabilidade é o risco de acesso não autorizado a dados pessoais sensíveis dos usuários, a partir da captação de sinais neurais, constatado no experimento realizado ainda no ano de 2012, por pesquisadores das Universidades de Oxford, Berkeley e Geneva, que conseguiram obter informações pessoais das pessoas através do uso de um *headset* para jogos virtuais.¹³

As informações coletadas apenas observando as ondas cerebrais captadas pelo headset utilizado, diziam respeito a senhas de cartão de crédito, a localização de suas casas, mês de nascimento, identificação de pessoas conhecidas, nome do banco e o cartão bancário preferido pelo usuário.¹⁴

Semelhante ao estudo conduzido em 2012, Frank *et al*¹⁵, em artigo publicado no ano de 2017, demonstrou a possibilidade de inferir informações privadas de um usuário, analisando suas atividades cerebrais em resposta a estímulos visuais subliminares.

Os 27 participantes do experimento foram expostos a imagens por apenas 13,3 milissegundos, insuficientes para percepção consciente, mas que geraram respostas neurais detectáveis – os resultados indicaram que um invasor poderia, potencialmente, extrair informações sensíveis sem o conhecimento do usuário¹⁶.

Importante mencionar também o estudo realizado com pacientes portadores do mal de Parkinson, em que se constatou uma melhora significativa em relação à incapacidade motora dos participantes após realização de tratamento a partir de estimulação cerebral, porém muitos deles relataram um sentimento de que tinham perdido parte de suas personalidades¹⁷, o que demonstra a possibilidade de alteração das características mais individuais dos usuários, construídas no decorrer de uma vida.

12. TARKHANI, Zehnra *et al.* *Enhancing the Security & Privacy of Wearable Brain-Computer Interfaces*. Disponível em: <https://doi.org/10.48550/arXiv.2201.07711>. Acesso em 23 dez. 2024.

13. MARTINOVIC, Ivan *et al.* On the feasibility of {Side-Channel} attacks with {Brain-Computer} interfaces. In: *21st USENIX Security Symposium (USENIX Security 12)*. 2012. p. 143-158. Disponível em: <https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final56.pdf>. Acesso em: 12 jan. 2025.

14. *Ibid.*

15. FRANK, Mario *et al.* *Using EEG-Based BCI Devices to Subliminally Probe for Private Information*. arXiv preprint arXiv:1312.6052, 2013. Disponível em: <https://arxiv.org/pdf/1312.6052>. Acesso em: 12 jan. 2025.

16. *Ibid.*

17. FERNANDES, Samuel. *Eficaz para tratar Parkinson, estimulação cerebral pode ter relação com distúrbios de comportamento*. Folha. 29 jun. 2024. Disponível em: <https://www1.folha.uol.com.br/ciencia/2024/06/eficaz-para-tratar-parkinson-estimulacao-cerebral-pode-ter-relacao-com-disturbios-de-comportamento.shtml>. Acesso em: 13 jan. 2025.

2.1. Riscos associados ao hackeamento dos dados neurais

Além disso, há também a possibilidade de hackeamento ou manipulação do cérebro, ou seja, *hackers* podem acessar sinais neurais transmitidos entre o dispositivo e outros sistemas, obtendo informações pessoais, o que violaria a privacidade mental dos cidadãos.

Não se trata de uma hipótese inimaginável, afinal, em 2017, a agência americana responsável pela regulação de alimentos e medicamentos (FDA) nos Estados Unidos, anunciou o *recall* de 465 mil marcapassos implantados em pacientes no país, que se encontravam vulneráveis a ações de *hackers*.¹⁸

De acordo com o órgão, as falhas de segurança identificadas permitiam que pessoas não autorizadas acessassem o sistema do equipamento e modificassem comandos de programação, o que poderia resultar em danos ao paciente pela depleção rápida da bateria ou administração de estímulos inapropriados, o que poderia, inclusive, levá-los a óbito.¹⁹

Nesse contexto, no caso das Interfaces Cérebro-Máquina, há o risco potencial de um software malicioso (vírus) afetar o dispositivo e causar danos ao usuário. Assim, como os pensamentos integram o sistema operacional do dispositivo implantado no cérebro, os dados neurais estarão sujeitos aos mesmos problemas de armazenamento e transmissão que outros dados comuns, de forma tal que *hackers* poderão corromper ou de alguma forma alterar os dados/pensamentos.

Estudiosos apontam²⁰ que um caminho óbvio para *hackers* será a leitura dos pensamentos.

Ou seja, *hackers* poderiam, eventualmente, interceptar e bloquear ou interceptar e alterar mensagens e, como uma ICM transmite atividade neural, é possível imaginar que técnicas de interceptação existentes também sejam aplicadas para interceptar os dados neurais – e, quando isso acontecer, nenhum pensamento será privado ou seguro.

A manipulação dos sinais neurais é uma das consequências de um hackeamento, afetando o comportamento ou estado emocional da pessoa que utiliza o dispositivo; poderia ocorrer, teoricamente, o *input* de dados falsos em uma ICM, influenciando os pensamentos, decisões ou funções motoras de um usuário.

18. HERN, Alex. *Hacking risk leads to recall of 500,000 pacemakers due to patient death fears*. The Guardian. Tecnologia. 31 ago. 2017. Disponível: <https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update>. Acesso em: 12 jan. 2025.

19. *Ibid.*

20. FOSS, Rebecca. *Brain-Computer Interfaces: A New Frontier for Hackers*. UMGC Global Media Center. 25 out. 2021. Disponível em: <https://www.umgc.edu/news/archives/2021/10/brain-computer-interfaces-a-new-frontier-for-hackers>. Acesso em: 12 jan 2025.

Ou seja, o usuário de dispositivos cerebrais também está exposto à riscos à sua saúde física, pois a manipulação de sinais neurais pode causar alterações no funcionamento do cérebro, levando a danos físicos ou psicológicos.

Indo mais além, podemos imaginar a possibilidade de cibercriminosos alterarem a memória, ameaçar apagá-la ou reescrevê-la, ou mesmo modificar as respostas emocionais de uma pessoa, à distância, o que envolve não somente questões éticas quanto ao consentimento, como reforça a necessidade de uma regulação específica da proteção de dados neurais.

O hackeamento é uma possibilidade, pois muitos dispositivos ICM utilizam conexões sem fio, como Bluetooth ou Wi-Fi, para transmitir dados entre o cérebro e computadores externos, de modo que estas conexões podem ser pontos de entrada para *hackers*.

Ou seja, se a mente humana for violada, por consequência direta, viola-se a própria dignidade do indivíduo, sua identificação pessoal, personalidade, tudo aquilo que constitui o ser em sua essência e individualidade. Não somente o vazamento de dados é um risco, como também o apagamento ou mesmo a manipulação, alterando que a pessoa é e será.

2.2. Coleta e uso indevidos de dados neurais em desfavor do consumidor

Não se pode olvidar também do risco de utilização indevida de dados neurais para *marketing* abusivo, comprometendo a autonomia cognitiva dos consumidores.

Ou seja, sem perceber, os indivíduos podem ser levados a acreditar que tomaram decisões por vontade própria, quando, na verdade, foram guiados por estratégias baseadas em seus dados neurais²¹.

Assim, sinais neurais dos usuários que revelem intenções e pré-disposições de compra, por exemplo, poderiam ser extraídos, sem consentimento, e usados na criação de padrões de consumo.

Os sinais cerebrais podem indicar interesse em um produto ou hesitação em comprar algo, de modo que plataformas de e-commerce poderiam usar essas informações para oferecer promoções ou ajustar preços em tempo real, explorando o estado mental do consumidor²².

21. TORRES, Edgar P et al. *EEG-Based BCI Emotion Recognition: A Survey*. *Sensors* (Basel, Switzerland) vol. 20,18 5083. 7 set. 2020. p. 3. Disponível em: [doi:10.3390/s20185083](https://doi.org/10.3390/s20185083). Acesso em: 19 jan. 2025.

22. LEE, Joseph. *Brain-computer interfaces and dualism: a problem of brain, mind, and body*. *AI & Soc* 31, 29–40 (2016). Disponível em: <https://doi.org/10.1007/s00146-014-0545-8>. Acesso em: 19 jan. 2025.

Exemplo da captação de intenções através de sinais neurais, ocorreu com o teste implementado pela Frito-Lay (Pepsico) que se utilizou de EEG (eletroencefalograma) para testar como as pessoas reagiam a diferentes *designs* de embalagens de chips, a partir de suas respostas cerebrais.²³

Segundo o teste, pacotes brilhantes e de cores vivas faziam os consumidores se sentirem culpados, associando o produto a hábitos alimentares inadequados; já os pacotes foscos e de cores mais sutis não despertavam sentimento de culpa nos consumidores. Com base nesses resultados, a Frito-Lay alterou suas embalagens para torná-las menos brilhantes, o que resultou em melhores respostas dos consumidores e em um aumento nas vendas.²⁴

Além do mais, há o risco de algumas tecnologias de ICM potencialmente induzirem mudanças no estado emocional de uma pessoa, como relaxamento ou excitação, o que pode ser explorado para aumentar a receptividade a mensagens publicitárias – o dispositivo poderia, durante uma campanha publicitária, induzir sensações de confiança ou otimismo, tornando o consumidor mais propenso a aceitar uma oferta.

Pode-se asseverar, portanto, que a manipulação de consumidores com base em dados neurais é uma possibilidade real, especialmente à medida que as tecnologias de interface cérebro-máquina se tornam mais sofisticadas, o que levanta questões éticas e jurídicas profundas, exigindo regulamentação adequada para proteger a autonomia e a privacidade dos indivíduos.

Conclui-se, pois, que os dados neurais podem ser utilizados em desfavor dos seus titulares, sem consentimento, bem como podem, eventualmente, estarem vulneráveis a manipulações e a ataques *hackers*. Por isso, o direito precisa se ater a estes novos dilemas, se antevendo a possíveis resultados danosos aos indivíduos.

3. Panorama das iniciativas de regulamentação no Brasil e no mundo

No cenário internacional, é possível identificar alguns avanços em prol da regulamentação dos neurodireitos. Todavia, ainda são iniciativas pontuais, que se desenvolvem vagarosamente, não conseguindo acompanhar apropriadamente os avanços de empresas da área de neurotecnologia.

23. BURKITT, Laurie. *Neuromarketing: Companies Use Neuroscience for Consumer Insights*. 29 out. 2009, atualizado em 16 jul. 2012. Disponível em: <https://www.forbes.com/forbes/2009/1116/marketing-hyundai-neurofocus-brain-waves-battle-for-the-brain.html>. Acesso em: 12 jan. 2025.

24. *Ibid.*

Nesse contexto, a fundação *Neurorights Foundation* – organização sem fins lucrativos que promove o desenvolvimento ético da neurotecnologia – divulgou, em abril de 2024, um relatório no qual identificou que as proteções de privacidade de dados da indústria de neurotecnologia eram frequentemente fracas ou inexistentes, revelando um cenário preocupante de fragilidade regulatória e exposição dos indivíduos à coleta e uso indevido de dados neurais.²⁵

Entretanto, alguns países já possuem legislações significativamente desenvolvidas em relação à temática. O Chile é um exemplo paradigmático, sendo o primeiro país no mundo a assegurar a proteção legal dos neurodireitos, em setembro de 2021, por meio da Lei nº 21.383/2021, que modificou o artigo 19 de sua Constituição.²⁶ Além disso, outros países da América Latina, como Argentina e México, estão atualmente deliberando sobre legislações análogas.

Inspirado pela iniciativa Chilena, os Estados Unidos reconheceram igualmente a relevância da promulgação de legislações voltadas à proteção dos neurodireitos.

Exemplo disto é que, em 2023, o estado do Colorado aprovou uma lei que classifica dados neurais como dados sensíveis, impondo restrições sobre sua coleta e uso sem o consentimento do usuário²⁷.

Já em 2024, a Califórnia incluiu explicitamente os dados neurais como dados pessoais sensíveis na *California Consumer Privacy Act* (CCPA), proibindo também que empresas vendam ou compartilhem esses dados sem o consentimento do titular²⁸.

No plano internacional, destaca-se ainda a Recomendação da OCDE sobre Inovação Responsável em Neurotecnologia (OECD/LEGAL/0457)²⁹, adotada em 2019, a qual constitui o primeiro marco normativo global voltado especificamente à regulação ética das neurotecnologias. Tal recomendação define neurotecnologia como os dispositivos e procedimentos utilizados para aces-

25. GENSER, Jared et al. *Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies*. Disponível em: https://www.perseus-strategies.com/wp-content/uploads/2024/04/FINAL_Consumer_Neurotechnology_Report_Neurorights_Foundation_April-1.pdf. Acesso em: 23 dez. 2024.

26. GUZMÁN H. Lorena. *Chile: Pioneirismo na proteção dos neurodireitos*. UNESCO. 21 mar. 2022, atualizado em 13 out. 2023. Disponível em: <https://courier.unesco.org/en/articles/chile-pioneering-protection-neurorights>. Acesso em: 23 dez. 2024.

27. JOHNSON, Thora. *Colorado Enacts Nation's First Privacy Law to Protect Consumer Brainwaves: What it Means for Life Sciences and Health Tech Companies*. Orrick. 01 maio 2024. Disponível em: <https://www.orrick.com/en/Insights/2024/04/Colorado-Enacts-Nations-First-Privacy-Law-to-Protect-Consumer-Brainwaves>. Acesso em: 26 dez. 2024.

28. MOENS, Jonathan. *California Passes Law Protecting Consumer Brain Data*. The New York Times. 29 set. 2024, atualizado em 30 set. 2024. Disponível em: <https://www.nytimes.com/2024/09/29/science/california-neurorights-tech-law.html>. Acesso em: 23 dez. 2024.

29. OCDE, *Recommendation of the Council on Responsible Innovation in Neurotechnology*, OECD/LEGAL/0457. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0457#dates>. Acesso em: 19 abr. 2025.

sar, monitorar, investigar, avaliar, manipular e/ou emular a estrutura e a função dos sistemas neurais de pessoas naturais.

O objetivo principal da mencionada recomendação, formalmente adotada por 39 países, é orientar governos e agentes inovadores na antecipação e enfrentamento dos desafios éticos, jurídicos e sociais que decorrem dessas tecnologias, promovendo, simultaneamente, um ambiente favorável à inovação responsável.

Ressalte-se que a OECD/LEGAL/0457 é estruturada em nove princípios fundamentais, entre os quais se destacam a proteção de dados cerebrais pessoais, a avaliação de segurança, o fortalecimento da supervisão regulatória e a prevenção de usos indevidos.

Em complemento, para auxiliar na implementação de tais diretrizes, a OCDE lançou, em abril de 2024, o *Neurotechnology Toolkit*³⁰, um guia prático destinado aos formuladores de políticas públicas que atuam com regulação de tecnologias emergentes.

No Brasil, embora de forma gradual e morosa, observam-se iniciativas pontuais visando à regulamentação legal dos dados neurais. Atualmente tramitam dois projetos de Lei a respeito do tema: o PL nº 1229/21³¹ e o PL nº 522/2022³², ambos de autoria do Deputado Carlos Henrique Gaguim. O PL de 2021, inspirado na lei Chilena, propõe uma alteração na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), a fim de conceituar dado neural e regulamentar sua proteção³³, já o PL de 2022, embora similar, traz um teor mais técnico e aprofundado.

Um avanço mais significativo, a nível estadual, ocorreu no ano de 2023, no qual foi aprovada a PEC 298/2023, que alterou a Constituição do Rio Grande do Sul, passando a prever que todo o indivíduo possui o direito à integridade mental, como uma proteção inalienável contra a manipulação decorrente dos avanços da neurociência e da neurotecnologia³⁴.

30. OCDE. *Neurotechnology Toolkit*. Paris: OECD, abr. 2024. Disponível em: <https://www.oecd.org/content/dam/oecd/en/topics/policy-sub-issues/emerging-technologies/neurotech-toolkit.pdf>. Acesso em: 18 abr. 2025.

31. BRASIL. Câmara dos Deputados. *Projeto de Lei nº 1229/21, de 06 de abril de 2021. Modifica a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), a fim de conceituar dado neural e regulamentar a sua proteção*. Brasília: Câmara dos Deputados, 2021. Disponível em: <https://abrir.link/PL1229-21>. Acesso em: 19 jan. 2025.

32. BRASIL. Câmara dos Deputados. *Projeto de Lei nº 522/22, de 09 de março de 2022. Modifica a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), a fim de conceituar dado neural e regulamentar a sua proteção*. Brasília: Câmara dos Deputados, 2022. Disponível em: <https://abrir.link/PL522-22>. Acesso em: 19 jan. 2025.

33. BRASIL. CÂMARA DOS DEPUTADOS. *Projeto cria regras para proteger dados obtidos a partir do sistema nervoso central*. Câmara dos Deputados. 06 jul. 2021. Disponível em: https://www.camara.leg.br/noticias/769507-PROJETO-CRIA-REGRAS-PARA-PROTEGER-DADOS-OBTIDOS-A-PARTIR-DO-SISTEMA-NERVOSO-CENTRAL%E2%80%A8?utm_source=chatgpt.com. Acesso em 11 dez. 2024.

34. MUA, Cíntia Teresinha Burhalde; SILVEIRA, Paulo Antonio Caliendo Velloso da. *Proteção ao neurodireito e à integridade mental na Constituição do RS*. CONJUR. 5 jan. 2024. Disponível em: <https://www.conjur.com.br/2024-jan-05/protecao-ao-neurodireito-a-integridade-mental-na-constituicao-do-rs/>. Acesso em: 08 jan. 2025.

No mesmo ano, em 2023, surgiu o Projeto de Lei nº 2.174, de autoria de Rubens Pereira Júnior, com a pretensão de criar uma legislação autônoma, abarcando a proteção do cérebro e do sistema nervoso, e objetivando incluir os neurodireitos na categoria de direitos fundamentais.

Existe ainda uma Proposta de Emenda Constitucional, de nº 29/2023, que busca “incluir, entre os direitos e garantias fundamentais, a proteção à integridade mental e à transparência algorítmica”, alterando o artigo 5.º, LXXX, da CF/88.

Todavia, a temática ainda merece um tratamento a nível nacional, consolidando adequadamente a proteção voltada aos dados neurais, em lei específica, de modo propor um tratamento especial a estes dados tão complexos, que imprescindivelmente devem ser compreendidos como dados pessoais sensíveis, para melhor regulação, conforme será explicitado a seguir.

4. Necessidade de regulação e enquadramento dos dados neurais enquanto dados pessoais sensíveis

It's always too early to assess a technology until it's suddenly too late. IENCA, Marcello³⁵.

Apesar das iniciativas brasileiras existentes já representarem um avanço, é preciso se atentar à busca por uma regulamentação robusta e específica que preveja uma proteção completa à privacidade mental.

Porém, o primeiro passo para se buscar uma adequada regulamentação é a partir da compreensão do dado neural enquanto dado pessoal sensível, a fim de se conceber uma proteção especial a estes dados, que revelam informações íntimas de seus titulares.

Afinal, embora a maior empresa do setor da atualidade afirme usar sua tecnologia para tratar condições médicas não atendidas atualmente, o objetivo a longo prazo da empresa é criar super-humanos, de forma a melhorar as habilidades dos indivíduos, para que consigam acompanhar a evolução da tecnologia, situação que já não parece tão distópica.

E na mesma gradação em que aumentam as pesquisas sobre melhoramento humano, através da conexão do cérebro às máquinas, também se acentuam as preocupações acerca da ética, privacidade, responsabilidade e proteção dos dados tratados nestes procedimentos, conforme visto anteriormente.

35. Tradução livre: É sempre cedo demais para avaliar uma tecnologia, até que, de repente, seja tarde demais.

Assim, pode-se inferir, à luz das neurotecnologias emergentes, que o futuro aponta para uma simbiose entre máquina e humano, onde a mente está diretamente ligada à internet; por conseguinte, se os dados neurais não forem protegidos, não mais constituirão parte do indivíduo, mas bens de propriedade de grandes empresas, sem que o titular tenha ingerência alguma sobre o processo de coleta, armazenamento e manuseio de suas próprias informações pessoais.

Observa-se, com isso, que os dados neurais possuem inegavelmente natureza de dados pessoais sensíveis, haja vista que a mente humana é capaz de armazenar diversas informações íntimas, de elevada importância e sensibilidade.

É certo que há na doutrina divergência a respeito da taxatividade ou não do rol do art. 5º, II, da LGPD, que elenca os dados pessoais sensíveis³⁶.

Porém, mostra-se mais acertado o entendimento de Caitlin Mulholland, ao sustentar que o rol possui caráter exemplificativo, de modo a abarcar outras hipóteses não previstas expressamente em que serão identificados os dados pessoais que tenham natureza considerada sensível³⁷.

Afinal, conforme complementa Chiara de Teffé, conceber um rol fechado aos dados sensíveis poderia excluir demandas e manifestações do indivíduo que, diante do avanço social e tecnológico, requeiram proteção ampliada.³⁸

Além do mais, Teffé explicita que considerar o rol dos dados sensíveis enquanto exemplificativo, coaduna com o fundamento da categoria desses dados, com a sua natureza diretamente relacionada a aspectos existenciais da pessoa humana, bem como com o entendimento de que a proteção de dados pessoais é considerada direito da personalidade³⁹.

Cabe mencionar ainda que até mesmo parte da doutrina que entende ser o rol dos dados pessoais sensíveis taxativo, também considera que caso um dado considerado não sensível, quando tratado, se revele, no caso concreto, capaz de fornecer informações sensíveis, este também poderá receber o tratamento como se dado sensível fosse, vide art. 11, §1, da LGPD⁴⁰.

36. LGPD, Art. 5º, 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.

37. MULHOLLAND, Caitlin. *Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais*. Migalhas. 2020. Disponível em: <https://migalhas.uol.com.br/coluna/migalhas-devulnerabilidade/329261/dadospessoais-sensiveis-e-consentimento-na-lei-geral-de-protecao-de-dados-pessoais>. Acesso em: 13 jan. 2025.

38. TEFFÉ, Chiara Antonia Spadaccini de. *Dados pessoais sensíveis: uma análise funcional da categoria e das hipóteses de tratamento*. 2022. 310 f. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2022. p. 86.

39. *Ibid.*, p. 85.

40. PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. *Compliance digital e LGPD*. São Paulo: Revista dos Tribunais, Thomson Reuters, 2021. p. 119.

Assim, é imprescindível que para se idealizar uma lei para o tratamento de dados neurais – o que se considera mais adequado, vide a complexidade de tais dados, que possuem peculiaridades e riscos diferenciados –, se parta da concepção de dado neural como dado pessoal sensível, de modo que a disciplina passe a usufruir de um tratamento mais rigoroso em relação aos demais dados, como a exigência de consentimento de forma específica e destacada para finalidades específicas, com base no que aduz o art. 8º da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).⁴¹

Isto se deve ao fato de que, tratando-se de dados neurais, cujo conteúdo pode revelar aspectos profundos da vida psíquica e emocional de um indivíduo, o consentimento não pode ser considerado uma mera formalidade. Pelo contrário, deve refletir a plena compreensão das consequências do tratamento, bem como o respeito à autonomia do titular, em consonância com os princípios bioéticos da autonomia, beneficência, não maleficência e justiça.

Nesse mesmo sentido, o documento da OCDE “*Neurotechnology Toolkit*” de abril de 2024⁴², anteriormente citado, recomenda expressamente o estabelecimento de estruturas robustas de consentimento voltadas à coleta, uso e/ou compartilhamento de dados neurais e de biometria cognitiva, de modo a garantir que tal consentimento seja não apenas informado e específico, mas também revogável a qualquer tempo, assegurando-se, assim, a proteção efetiva da autonomia e da privacidade mental dos indivíduos.

Ou seja, a base legal aplicada aos dados sensíveis impõe às organizações uma camada adicional de segurança com o objetivo de conter acessos indevidos ou vazamentos, o que acarretaria um prejuízo maior aos titulares desses dados, justamente por sua natureza⁴³.

Portanto, o que se pretende com a categorização é gerar uma regulação mais rigorosa, com intuito de melhor proteger a pessoa humana, no que tange à sua privacidade mental e ao controle de seus dados neurais.

Destaque-se que, em razão da alta proteção que os dados pessoais considerados sensíveis requerem, o art. 46 da LGPD impõe aos agentes de tratamento a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações aci-

41. TEFFÉ, Chiara Antonia Spadaccini de. *op. cit.* p. 151/152.

42. OCDE. *Neurotechnology Toolkit*. Paris: OECD, abr. 2024. Disponível em: <https://www.oecd.org/content/dam/oecd/en/topics/policy-sub-issues/emerging-technologies/neurotech-toolkit.pdf>. Acesso em: 18 abr. 2025.

43. FLEMING, Maria Cristina. *LGPD: diferenças no tratamento de dados pessoais e dados pessoais sensíveis*. CONJUR. 6 mar. 2021. Disponível em: <https://www.conjur.com.br/2021-mar-06/fleming-diferencas-tratamento-dados-pessoais-sensiveis/>. Acesso em: 13 jan. 2025.

dentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito⁴⁴.

É por isso que, ao enquadrar os dados neurais na categoria de dados pessoais sensíveis, busca-se trazer um arcabouço de alta proteção ao titular desses dados, que carregam consigo alta complexidade e sensibilidade, pois dizem respeito a informações íntimas, sentimentos, sensações, memórias, pré-disposições políticas, convicções religiosas e filosóficas, dentre outras questões afetas à mente humana, de modo que a empresa que vier a tratar dados neurais, precisará adotar práticas, de modo a estar em conformidade com a LGPD.

Ademais, admitindo-se a classificação dos dados neurais como dados pessoais sensíveis, é possível, inclusive, conjecturar cenários futuros que evidenciam a importância de sua proteção jurídica específica.

Suponha-se, por exemplo, que um plano de saúde passe a exigir o uso de dispositivos para detectar a predisposição de seus beneficiários a doenças neurológicas, como Alzheimer ou epilepsia, utilizando essas informações para restringir a concessão de cobertura ou ajustar valores de mensalidade. Em um cenário em que os dados neurais são juridicamente reconhecidos como dados pessoais sensíveis, tal prática seria vedada, à luz do art. 11, §4º, da Lei Geral de Proteção de Dados Pessoais, por configurar tratamento discriminatório.

De modo semelhante, imagine-se que uma fintech utilize dispositivos de Interface Cérebro-Máquina (ICM) para captar dados relacionados a padrões de impulsividade, aversão ao risco ou estilo de tomada de decisão, com o intuito de estimar a probabilidade de inadimplência de consumidores.

O enquadramento desses dados como pessoais sensíveis implicaria a submissão do tratamento às restrições previstas no art. 11 da LGPD, exigindo, entre outros requisitos, consentimento específico, finalidade legítima e proporcional e o respeito à vedação de decisões automatizadas com efeitos discriminatórios, nos termos do art. 20. A descon sideração dessas exigências poderia ensejar responsabilização civil e administrativa da empresa, notadamente por afronta ao princípio da não discriminação e à proteção da dignidade do titular.

Importa também destacar o Guia Orientativo sobre o Tratamento de Dados Pessoais pelo Poder Público (versão 2.0, jun. 2023)⁴⁵, o qual evidencia que os

44. LGPD, Art. 46. 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.

45. ANPD. Guia Orientativo. *Tratamento de Dados Pessoais pelo Poder Público*. Jun/2023. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 19 abr. 2025.

dados pessoais sensíveis, nos termos do art. 5º, II, da LGPD, estão submetidos a um regime jurídico protetivo mais rigoroso, exigindo do agente público maior cautela e responsabilidade quanto ao seu tratamento.

Assim, essa exigência se justifica pela natureza potencialmente discriminatória ou estigmatizante desses dados, como ocorre, por exemplo, no contexto da divulgação de resultados de estudos em saúde pública, hipótese na qual a própria LGPD veda expressamente a revelação de dados pessoais sensíveis (art. 13, § 1º).

A referida orientação reforça a necessidade de aplicação de salvaguardas específicas sempre que se tratar de informações capazes de expor aspectos íntimos da pessoa natural, o que, por analogia, se mostra especialmente relevante para o tratamento de dados neurais, diante de sua alta sensibilidade e risco à privacidade mental.

Nesse sentido, pode-se concluir que violar a privacidade mental de uma pessoa, a partir de um tratamento indevido de dados neurais, implicaria diretamente em um dano à própria dignidade da pessoa humana, transgredindo sua própria essência.

Além do mais, enquadrando-se os dados neurais na categoria de sensíveis, empresas que coletam, armazenam e tratam estes dados precisariam criar relatórios internos, garantir a criação de um estado de *compliance* e considerar a adoção do “*Privacy by Design*” (proteção e privacidade desde a concepção e em todo o ciclo do tratamento de dados pessoais), de modo a proporcionar avaliações prévias de impacto, medidas técnicas e organizacionais adequadas e *accountability* em todo o processo⁴⁶.

Não obstante, a partir dessa categorização imprescindível aqui defendida para o adequado tratamento de dados neurais, é importante que a legislação que venha tratar sobre neurodireitos, imponha àqueles que manuseiam tais informações altamente sensíveis, o respeito aos seguintes direitos: Liberdade Cognitiva, Privacidade Mental, Integridade Mental e Continuidade Psicológica.⁴⁷

Ou seja, é imperativo assegurar a “liberdade cognitiva”, de modo que os titulares de dados possam optar por utilizar ou se abster de utilizar estimulações cerebrais e quaisquer outras técnicas capazes de alterar seu estado mental. Ademais, é necessário proteger o direito à “privacidade mental”, tornando ilegal a leitura da mente de alguém sem o seu consentimento, além

46. TEFFÉ, Chiara Antonia Spadaccini de. *op. cit.* p. 233.

47. IENCA, Marcello. ANDORNO, Roberto. *Towards new human rights in the age of neuroscience and neurotechnology*. Life Sci Soc Policy 13, 5 (2017). Disponível em: <https://doi.org/10.1186/s40504-017-0050-1>. Acesso em: 12 jan. 2025.

de garantir salvaguardas à “integridade mental”, resguardando os titulares de dados contra invasões maliciosas ao cérebro. Por fim, deve-se assegurar a “continuidade psicológica”, protegendo os indivíduos contra tratamentos ou aprimoramentos que possam comprometer seu senso de identidade ou a percepção de continuidade de sua pessoa ao longo da vida⁴⁸.

Nesse sentido, a legislação vigente mostra-se insuficiente para assegurar a proteção dos dados neurais, que abarcam emoções, pensamentos e atividades cerebrais, cuja natureza é intrinsecamente complexa e cujos riscos decorrentes do seu manejo inadequado ainda permanecem incertos.

Em razão disto, a proteção apropriada dos neurodados enquanto dados sensíveis demanda uma abordagem mais abrangente e especializada, que contemple suas características únicas e os riscos a eles inerentes⁴⁹.

Considerações finais

Do exposto, é possível concluir que existe um vácuo legislativo no que tange à proteção específica de dados neurais, o que representa um risco significativo, considerando o rápido avanço das neurotecnologias e seus potenciais perigos para os usuários. As regulamentações atuais são insuficientes para garantir a proteção adequada dos indivíduos frente aos dispositivos invasivos que conectam cérebros a computadores, o que impõe a necessidade de o direito evoluir e se antecipar aos problemas modernos emergentes.

A solução mais adequada, conforme defendido neste trabalho, é a partir da compreensão dos dados neurais como dados pessoais sensíveis, conferindo-lhes uma proteção especial. Ao conceituar adequadamente o dado neural, para enquadrá-lo enquanto sensível, é possível aplicar um tratamento mais rigoroso à sua regulamentação, uma vez, como observado, o rol do artigo 5º, inciso II da LGPD é meramente exemplificativo, permitindo a inclusão de situações ainda não previstas, que envolvam riscos significativos aos usuários.

Para além disso, a fim de assegurar uma proteção jurídica mais eficaz da mente, é imprescindível a criação de uma legislação específica sobre neurodireitos, que aborde em seu escopo, de maneira abrangente, direitos fundamentais essenciais, como a liberdade cognitiva, a privacidade, a integridade mental e a continuidade psicológica.

48. *Ibid.*

49. CABRAL, Anna Cecília Moreira. *Regulação da proteção de dados no âmbito da neurotecnologia e dos neurodireitos*. 2024. 122 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Fundação Getúlio Vargas, Rio de Janeiro, 2024. p. 31.

Em síntese, os dados neurais podem ser considerados a última fronteira da privacidade humana, o que revela a urgente necessidade de desenvolver uma nova estrutura regulatória. Portanto, para uma regulação eficaz dos dados neurais, é preciso tratá-los como dados pessoais sensíveis, levando em consideração, também, os direitos decorrentes dessa proteção, a fim de se antever e resguardar a mente humana de eventuais danos, quiçá irreversíveis.

Referências

ALOHALLY, Manar. *The brain computer interface market is growing – but what are the risks?*. Global Economic Forum. 14 jun. 2024. Disponível em: [https://www.weforum.org/stories/2024/06/the-brain-computer-interface-market-is-growing-but-what-are-the-risks/#:~:text=The%20brain%20computer%20interface%20\(BCI,to%20%246.2%20billion%20by%202030](https://www.weforum.org/stories/2024/06/the-brain-computer-interface-market-is-growing-but-what-are-the-risks/#:~:text=The%20brain%20computer%20interface%20(BCI,to%20%246.2%20billion%20by%202030). Acesso em: 28 dez. 2024.

ANPD. Guia Orientativo. *Tratamento de Dados Pessoais pelo Poder Público*. Jun/2023. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 19 abr. 2025.

BRASIL. CÂMARA DOS DEPUTADOS. *Projeto cria regras para proteger dados obtidos a partir do sistema nervoso central*. 06 jul. 2021. Disponível em: https://www.camara.leg.br/noticias/769507-PROJETO-CRIA-REGRAS-PARA-PROTEGER-DADOS-OBTIDOS-A-PARTIR-DO-SISTEMA-NERVOSO-CENTRAL%E2%80%A8?utm_source=chatgpt.com. Acesso em 11 dez. 2024.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 1229/21, de 06 de abril de 2021. Modifica a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), a fim de conceituar dado neural e regulamentar a sua proteção*. Brasília: Câmara dos Deputados, 2021. Disponível em: <https://abrir.link/PL1229-21>. Acesso em: 19 jan. 2025.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 522/22, de 09 de março de 2022. Modifica a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), a fim de conceituar dado neural e regulamentar a sua proteção*. Brasília: Câmara dos Deputados, 2022. Disponível em: <https://abrir.link/PL522-22>. Acesso em: 19 jan. 2025.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)*. Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 157, p. 59-64, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 jan. 2025.

BURKITT, Laurie. *Neuromarketing: Companies Use Neuroscience for Consumer Insights*. 29 out. 2009, atualizado em 16 jul. 2012. Disponível em: <https://www.forbes.com/forbes/2009/1116/marketing-hyundai-neurofocus-brain-waves-battle-for-the-brain.html>. Acesso em: 12 jan. 2025.

CABRAL, Anna Cecilia Moreira. *Regulação da proteção de dados no âmbito da neurotecnologia e dos neurodireitos*. 2024. 122 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Fundação Getúlio Vargas, Rio de Janeiro, 2024. p. 31.

ELON Musk's Neuralink implants brain chip in first human. Reuters. 30 jan. 2024. Disponível em: <https://www.reuters.com/technology/neuralink-implants-brain-chip-first-human-musk-says-2024-01-29/>. Acesso em: 20 dez. 2024.

FERNANDES, Samuel. *Eficaz para tratar Parkinson, estimulação cerebral pode ter relação com distúrbios de comportamento*. Folha. 29 jun. 2024. Disponível em: <https://www1.folha.uol.com.br/ciencia/2024/06/eficaz-para-tratar-parkinson-estimulacao-cerebral-pode-ter-relacao-com-disturbios-de-comportamento.shtml>. Acesso em: 13 jan. 2025.

FLEMING, Maria Cristina. *LGPD: diferenças no tratamento de dados pessoais e dados pessoais sensíveis*. CONJUR. 6 mar. 2021. Disponível em: <https://www.conjur.com.br/2021-mar-06/fleming-diferencas-tratamento-dados-pessoais-sensiveis/>. Acesso em: 13 jan. 2025.

FOSS, Rebecca. *Brain-Computer Interfaces: A New Frontier for Hackers*. UMGC Global Media Center. 25 out. 2021. Disponível em: <https://www.umgc.edu/news/archives/2021/10/brain-computer-interfaces-a-new-frontier-for-hackers>. Acesso em: 12 jan 2025.

FRANK, Mario *et al.* *Using EEG-Based BCI Devices to Subliminally Probe for Private Information*. arXiv preprint arXiv:1312.6052, 2013. Disponível em: <https://arxiv.org/pdf/1312.6052>. Acesso em: 12 jan 2025.

GENSER, Jared *et al.* *Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies*. Disponível em: https://www.perseus-strategies.com/wp-content/uploads/2024/04/FINAL_Consumer_Neurotechnology_Report_Neurorights_Foundation_April-1.pdf. Acesso em: 23 dez. 2024.

GUZMÁN H. Lorena. *Chile: Pioneirismo na proteção dos neurodireitos*. UNESCO. 21 mar. 2022, atualizado em 13 out. 2023. Disponível em: <https://courier.unesco.org/en/articles/chile-pioneering-protection-neurorights>. Acesso em: 23 dez. 2024.

HERN, Alex. *Hacking risk leads to recall of 500,000 pacemakers due to patient death fears*. The Guardian. Tecnologia. 31 ago. 2017. Disponível: <https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update>. Acesso em: 12 jan. 2025.

IENCA, Marcello. ANDORNO, Roberto. *Towards new human rights in the age of neuroscience and neurotechnology*. *Life Sci Soc Policy* 13, 5 (2017). 27 p. Disponível em: <https://doi.org/10.1186/s40504-017-0050-1>. Acesso em: 12 jan. 2025.

JOHNSON, Thora. *Colorado Enacts Nation's First Privacy Law to Protect Consumer Brainwaves: What it Means for Life Sciences and Health Tech Companies*. Orrick. 01 maio 2024. Disponível em: <https://www.orrick.com/en/Insights/2024/04/Colorado-Enacts-Nations-First-Privacy-Law-to-Protect-Consumer-Brainwaves>. Acesso em: 26 dez. 2024.

LEE, Joseph. *Brain-computer interfaces and dualism: a problem of brain, mind, and body*. *AI & Soc* 31, 29-40 (2016). Disponível em: <https://doi.org/10.1007/s00146-014-0545-8>. Acesso em: 19 jan. 2025.

MAKASDJIAN, Roxanne. *New video of how scientists reconstruct the movies in our minds*. UC Berkeley News. 21 dez. 2011. Disponível em: <https://news.berkeley.edu/2011/12/21/new-visionreconstructionvideo/>. Acesso em: 12 jan 2025.

MARTINOVIC, Ivan *et al.* *On the feasibility of {Side-Channel} attacks with {Brain-Computer} interfaces*. In: *21st USENIX Security Symposium (USENIX Security 12)*. 2012. p. 143-158. Disponível em: <https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final56.pdf>. Acesso em: 12 jan. 2025.

MOENS, Jonathan. *California Passes Law Protecting Consumer Brain Data*. The New York Times. 29 set. 2024, atualizado em 30 set. 2024. Disponível em: <https://www.nytimes.com/2024/09/29/science/california-neurorights-tech-law.html>. Acesso em 23 dez. 2024.

MUA, Cíntia Teresinha Burhalde; SILVEIRA, Paulo Antonio Caliendo Velloso da. *Proteção ao neurodireito e à integridade mental na Constituição do RS*. CONJUR. 5 jan. 2024. Disponível em: <https://www.conjur.com.br/2024-jan-05/protecao-ao-neurodireito-a-integridade-mental-na-constituicao-do-rs/>. Acesso em: 08 jan. 2025.

MULHOLLAND, Caitlin. *Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais*. Migalhas. 2020. Disponível em: <https://migalhas.uol.com.br/coluna/migalhas-de-vulnerabilidade/329261/dadospessoais-sensiveis-e-consentimento-na-lei-geral-de-protecao-de-dados-pessoais>. Acesso em: 13 jan. 2025.

NEURALINK. Disponível em: <https://neuralink.com/>. Acesso em: 22 dez. 2024.

OCDE. *Neurotechnology Toolkit*. Paris: OECD, abr. 2024. Disponível em: <https://www.oecd.org/content/dam/oecd/en/topics/policy-sub-issues/emerging-technologies/neurotech-toolkit.pdf>. Acesso em: 18 abr. 2025.

OCDE, *Recommendation of the Council on Responsible Innovation in Neurotechnology*, OECD/LEGAL/0457. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0457#dates>. Acesso em: 19 abr. 2025.

PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. *Compliance digital e LGPD*. São Paulo: Revista dos Tribunais, Thomson Reuters, 2021.

PEKSA, Janis.; MAMCHUR, Dmytro. *State-of-the-Art on Brain-Computer Interface Technology*. Sensors 2023, 23, 6001. 28 p. Disponível em: <https://doi.org/10.3390/s23136001>. Acesso em 13 dez. 2024.

SCHUH, Ânderson R. et al. *Desenvolvimento de Um Simulador Controlado por Interface Cérebro-Computador Não Invasiva para Treinamento na Utilização de Cadeira de Rodas*. RENOTE, Porto Alegre, v. 11, n. 3, 2013. p.3. Disponível em: <https://www.seer.ufrgs.br/index.php/renote/article/view/44716>. Acesso em 28 dez. 2024.

TARKHANI, Zehnra et al. *Enhancing the Security & Privacy of Wearable Brain-Computer Interfaces*. Disponível em: <https://doi.org/10.48550/arXiv.2201.07711>. Acesso em 23 dez. 2024.

TEFFÉ, Chiara Antonia Spadaccini de. *Dados pessoais sensíveis: uma análise funcional da categoria e das hipóteses de tratamento*. 2022. 310 f. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2022.

TORRES, Edgar P et al. *EEG-Based BCI Emotion Recognition: A Survey*. Sensors Basel, Switzerland) vol. 20,18 5083. 7 set. 2020. 36 p. Disponível em: doi:10.3390/s20185083. Acesso em: 19 jan. 2025

TU, Lucy. *Neuroscientists Re-create Pink Floyd Song from Listeners' Brain Activity*. Scientific American. 15 ago. 2023. Disponível em: <https://www.scientificamerican.com/article/neuroscientists-re-create-pink-floyd-song-from-listeners-brain-activity/>. Acesso em: 12 jan. 2025.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

9

Big Brother na Era da Neurotecnologia: Neurodireitos e a Proteção dos Neurodados no Brasil

NICOLE JULIE DA SILVA RODRIGUES

Sumário: Introdução. 1. “1984” revisitado e a ascensão das Neurotecnologias. 1.1. Neurodireitos: Fundamentos Éticos e Jurídicos. 2. Impactos das Neurotecnologias na privacidade e a proteção dos neurodados no ordenamento jurídico brasileiro. Considerações finais. Referências.

Introdução

As transformações recentes no campo das neurotecnologias trazem à tona questões éticas, jurídicas e sociais sobre a privacidade mental, principalmente no que diz respeito à transparência nos reais propósitos por trás de suas criações. Assim como George Orwell, em sua obra distópica “1984”, advertiu acerca das ameaças que envolvem o controle totalitário e da vigilância extrema, o desenvolvimento das interfaces cérebro-computador (BCI) e de tecnologias capazes de acessar ou manipular dados cerebrais nos coloca diante de desafios que ultrapassam a ficção. Em um contexto onde o pensamento se torna decodificável, a proteção da dignidade humana demanda a construção de uma nova classe jurídica: os neurodireitos.

No Brasil, a discussão sobre neurotecnologias ainda é emergente, mas os avanços neurocientíficos e o crescente interesse de governos e empresas privadas mostram a necessidade de regulação específica. A capacidade dessas tecnologias de captar sinais cerebrais e transformar dados em informações monetizáveis revela riscos consideráveis à privacidade mental. A título de exemplo, é possível imaginar uma empresa que utilize dispositivos vestíveis para captar e interpretar sinais cerebrais de seus funcionários como forma de medir produtividade e foco. Em outro cenário, uma escola pode adotar tecnologias BCI para identificar o nível de atenção dos alunos em sala de aula, sob o argumento de personalização do ensino, sem que os estudantes ou seus responsáveis compreendam integralmente os riscos envolvidos.

Nesse contexto, o presente artigo investiga o problema da ausência de normativas adequadas para proteger os neurodados no ordenamento jurídico brasileiro, abordando a relevância dos neurodireitos como mecanismos para salvaguardar os dados cerebrais. Como destacado por Rieger, a mente humana é a essência do seu ser, seu tesouro pessoal e, por isso, sua proteção é uma

1. Pós-Graduada em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio (ITS Rio), em parceria com a Universidade do Estado do Rio de Janeiro (UERJ) e o Centro de Estudos e Pesquisa no Ensino do Direito (CEPED). Graduada em Direito pela Universidade Federal Fluminense.

necessidade nessa era de avanços neurotecnológicos². Logo, este trabalho busca responder em que medida o ordenamento jurídico brasileiro está apto a assegurar e efetivar os neurodireitos diante do avanço das neurotecnologias, principalmente no que diz respeito à proteção de dados neurais. Parte-se da hipótese de que a legislação brasileira ainda não é suficiente para lidar com os riscos específicos trazidos pelas neurotecnologias, sendo necessária a criação de regime normativo específico que contemple a proteção dos neurodados dentro da Lei Geral de Proteção de Dados..

O objetivo geral é analisar o impacto das neurotecnologias na privacidade mental e propor soluções jurídicas que garantam a proteção dos neurodados no Brasil. Ao decorrer dos dois capítulos, busca-se determinar os desafios éticos e jurídicos associados ao uso de neurotecnologias; identificar as principais propostas legislativas nacionais sobre o tema e, por fim, destacar adaptações legislativas, como é o caso do Projeto de Lei nº 522/2022, o qual busca conceituar dado neural e regulamentar a sua proteção, alterando a LGPD. Propõe-se, a partir disso, a criação de um regime normativo especial dentro da LGPD que contemple os neurodados, com regras específicas sobre consentimento, privacidade, segurança e limitação de finalidades.

Metodologicamente, esta pesquisa utiliza abordagem qualitativa, com análise bibliográfica como base principal, especialmente as contribuições de Marcello Ienca e Rafael Yuste. Esses autores destacam que as neurotecnologias apresentam riscos únicos – e até irreversíveis – à privacidade mental, sendo fundamental a criação de neurodireitos para proteger os indivíduos contra a manipulação mental e o uso indevido de dados cerebrais. Por fim, será considerada a necessidade de atuação de órgãos fiscalizadores, em especial, a atuação da ANPD, para garantir a efetividade da regulamentação proposta.

Diante disso, o presente estudo reafirma a importância de se discutir a regulamentação das neurotecnologias no Brasil, destacando o neurodireito como elemento essencial para tutelar o cérebro dos indivíduos contra riscos de manipulação mental e invasões à privacidade.

1. “1984” revisitado e a ascensão das neurotecnologias

A obra “1984”, de George Orwell, ao construir a sua ficção distópica, narra uma nação controlada pelo Grande Irmão, o qual é considerado pela socie-

2. RIEGER, Poliene Fernanda Souza Nascimento. *Privacidade mental e liberdade cognitiva: perspectivas e desdobramentos para novos direitos fundamentais no contexto de desenvolvimento e aplicação de neurotecnologia*. 2023, p. 59. IBEDP, Brasília, 2022. Disponível em: <http://52.186.153.119/handle/123456789/4239>. Acesso em: 15 jan. 2025.

dade como onipresente e infalível. Apesar de desconhecido, o Grande Irmão, junto ao Núcleo do Partido e o Partido Exterior, consegue impor um regime de vigilância e controle totalitário sobre os indivíduos, a fim de que a estrutura hierárquica sempre permaneça imutável.

Por não existir leis, o controle feito pela “Polícia das Ideias” é dever do Partido, sendo o principal responsável pela vigilância constante da sociedade e da linguagem. O desenvolvimento de treinamentos mentais relacionados às palavras ‘criminterrupção’ e ‘duplipensar’ são suficientes para suprimir o pensamento individual, limitar a capacidade das pessoas de pensar de forma crítica e impedir rebeliões contra a estrutura do governo³.

Enquanto a criminterrupção é capaz de sustar e corrigir, como por instinto, qualquer pensamento subversivo, o duplipensar é o fato de um indivíduo absorver e acreditar em duas ideias contraditórias como verdadeiras, sem ao menos perceber a contradição⁴. Tais mecanismos de controle mental foram essenciais para que os cidadãos odiassem os inimigos do governo e amassem incondicionalmente o Grande Irmão e a sua estrutura totalitária.

Constata-se que o crime de pensamento é o alicerce do controle do Grande Irmão e do Partido, visto que, a partir da supressão da liberdade individual e do controle mental, os indivíduos eram incapazes de pensar de forma contrária aos ideais do Partido. Dessa forma, qualquer pensamento capaz de contradizer ou questionar os ensinamentos do Grande Irmão era punível, ao contrário, por exemplo, do Direito Penal Brasileiro, que não intervém nos atos de cogitação e respeita a esfera íntima do indivíduo e, por isso, por mais reprovável e ilícito que um pensamento seja, este não possui relevância jurídica.

Dessa forma, verifica-se que o poder emanado por este líder alcançava os níveis mais íntimos de qualquer indivíduo, que é o pensamento e, assim, havia a supressão da individualidade. Apesar da obra “1984” ser uma ficção científica distópica e utópica, esta continua sendo de tamanha relevância para antecipar os desafios éticos e jurídicos que a ciência e a tecnologia podem representar no futuro. Torna-se essencial iniciar a discussão acerca das neurotecnologias e das preocupações associadas ao tema da privacidade mental.

Como seres tecno dependentes, o avanço tecnológico ao longo das décadas transformou o papel da tecnologia como uma simples ferramenta facilitadora para ser parte integrante de cada indivíduo. E, no contexto da saúde

3. ORWELL, George. 1984. Tradução de Alexandre Hubner e Heloisa Jahn. São Paulo: Companhia das Letras, 2009., p. 247 – 254.

4. IDEM, p. 249 e 252.

integrada ao desenvolvimento de inteligência artificial, a partir da década de 1990 – denominada como a “Década do Cérebro” –, a neurociência tem sido potencializada, graças também aos investimentos bilionários na área.

De acordo com o *The NeuroRights Foundation*, organização sem fins lucrativos criada com o objetivo de assegurar os direitos humanos contra o uso indevido da neurotecnologia ou o seu abuso, a neurotecnologia pode ser definida como toda e qualquer tecnologia capaz de registrar ou interferir na atividade cerebral, principalmente no que diz respeito às interfaces cérebro-computador⁵.

Por muitos anos, tecnologias capazes de interferir na atividade cerebral eram consideradas irreais e distantes da realidade, mas hoje o cenário se inverte com a inserção das novas neurotecnologias em nosso cotidiano. As interfaces cérebro-computador, conduzem a comunicação entre o cérebro e o mundo exterior, imprimindo dados cerebrais ou até mesmo modificando a atividade cerebral. A forma de comunicação BCI se exterioriza de múltiplas formas, principalmente no meio clínico, sendo a mais conhecida a eletroencefalografia (EEG), capaz de registrar sinais cerebrais ao longo de execuções de tarefas sensoriais⁶.

Importa destacar que a neurociência aliada com as neurotecnologias estão alcançando patamares sequer vistos. Doenças como Parkinson, depressão, ansiedade, autismo, paralisia cerebral, entre outras doenças que causam sofrimento e limitações aos pacientes, são exemplos de patologias que estão sendo objetos de estudo da neurociência com o objetivo de curar doenças – antes incuráveis –, amenizar deficiências e promover qualidade de vida aos pacientes acamados.

O cientista Rafael Yuste já afirma que há expectativas concretas em nossa realidade de pensamentos humanos serem modificados ou codificados ao usar neurotecnologia, já que os nossos pensamentos, memórias e escolhas são gerados pelo impulso coordenado de circuitos neurais em nossos cérebros⁷. Por isso, diversas interfaces cérebro-computador, conseguem deduzir informações privadas sobre nós e nossas predileções, sendo dados relevantes não só na área médica, mas também no ramo do neuromarketing, no qual empresas reproduzem técnicas de neuroimagem para descobrir preferências

5. THE NEURORIGHTS FOUNDATION. *The Challenge: Advances in Neurotechnology Have Far Outpaced Global, National, and Corporate Governance*. Disponível em: <https://neurorightsfoundation.org>. Acesso em: 14 jan. 2025.

6. IENCA, Marcello; ANDORNO, Roberto. *Towards new human rights in the age of neuroscience and neurotechnology*. Life Sciences, Society and Policy, p. 3. Vol. 13, n. 5. 26 abr. 2017. Disponível em: <https://doi.org/10.1186/s40504-017-0050-1>. Acesso em: 25 dez. 2024.

7. MIRANDA, Maria Lucilia Moraes de; NASCIMENTO, et al. *Neurodireito – colisões dos direitos fundamentais dentro da razoabilidade e proporcionalidade*. Revista Ibero-Americana de Humanidades, Ciências e Educação, p. 174. REASE, v. 9, n. 12, 29 dez. 2023. Disponível em: <https://doi.org/10.51891/rease.v9i12.12746>. Acesso em: 14 jan. 2025.

e intenções dos consumidores ou até mesmo criá-las e orientá-las de acordo com o seu interesse.

Atualmente, dispositivos vestíveis como os famosos smartwatches e outros *wearables* e *neurogadgets* – que nos pertence atualmente de forma quase “indissociável” também são considerados neurotecnologias por conseguirem captar sinais cerebrais que transmitam o nosso comportamento, preferências, sentimentos, que serão transformados em dados que serão examinados por algoritmos e depois monetizados. Nita Farahany, professora da Universidade Duke, afirma que no caso dos smartwatches, os “sensores cerebrais são justamente parecidos com sensores de frequência cardíaca encontrados nos smartwatches ou em anéis que medem a temperatura do corpo quando captam a atividade elétrica no cérebro”⁸.

Sendo assim, se antes não era possível ultrapassar as fronteiras da mente humana, as neurotecnologias estão evoluindo em níveis que estão descortinando tal possibilidade. O desenvolvimento das neurotecnologias estão nos permitindo entender que o cérebro deve ser tutelado de forma especial. Isso porque, em nosso ordenamento jurídico, não conseguimos designar nas bases legais uma tutela do cérebro, mas apenas tutela sobre outros bens jurídicos, como manifestações do pensamento, liberdade de consciência, entre outros.

O nosso ordenamento jurídico precisa se debruçar sobre todo o corpo humano, mas especialmente o cérebro. Portanto, da mesma forma como Orwell previu os perigos relacionados ao controle mental e a ausência de privacidade mental, as neurotecnologias, apesar de ter múltiplos benefícios, sobretudo na área médica, devem ser objeto de discussão sobre os desafios e riscos associados de forma que a privacidade de todos os indivíduos sejam respeitados e consigam equilibrar de forma harmônica com os avanços tecnológicos.

1.1. Os Neurodireitos são os novos direitos humanos?

A discussão sobre a tutela do cérebro, a priori, deve pairar-se sobre o fato de que a mente humana é considerado o “último refúgio de liberdade pessoal e autodeterminação”⁹, tendo em vista o maior grau de intimidade subjetiva, capaz de criar e estimular as nossas crenças, discernimentos, sentimentos, ou seja, tudo que remete a nossa individualidade.

8. BBC. *Neurotecnologia e privacidade mental: os desafios éticos e legais do avanço tecnológico*. Disponível em: <https://www.bbc.com/portuguese/articles/c88jmpl902lo>. Acesso em: 07 jan. 2025.

9. MIRANDA, Maria Lucilia Moraes de; NASCIMENTO, et al. *Neurodireito – colisões dos direitos fundamentais dentro da razoabilidade e proporcionalidade*. Revista Ibero-Americana de Humanidades, Ciências e Educação, p. 168. REASE, v. 9, n. 12, 29 dez. 2023. Disponível em: <https://doi.org/10.51891/rease.v9i12.12746>. Acesso em: 14 jan. 2025.

A área da neurotecnologia é considerada uma área estratégica e lucrativa para empresas privadas e países, que almejam possuir domínio e influência sobre neurotecnologias aliadas à inteligência artificial. Nos últimos anos, é possível perceber a intensificação da corrida neurotecnológica de implantes cerebrais, sobretudo entre China, com a estatal Neijing Xinzhida e os EUA, com a empresa Neuralink, fundada pelo empresário Elon Musk.

O chip cerebral denominado “Link” já está sendo implantado em humanos desde o ano passado¹⁰. Resumidamente, esses chips são utilizados para recolher atividade elétrica feita por nossos neurônios e podem ser implantados no córtex cerebral ou na superfície da cabeça. Assim, toda atividade neural é captada pelos eletrodos e transportada a um processador que interpreta esses sinais¹¹. A função de tecnologias de inteligência artificial consiste em traduzir os sinais elétricos recebidos em comandos especiais.

As neurotecnologias permitem que os dados humanos possam ser acessados, coletados ou até mesmo manipulados. Através das interfaces cérebro-computador (BCI), estamos mais próximos da decodificação do pensamento ou do aperfeiçoamento da capacidade cognitiva ao conectar o cérebro diretamente a redes digitais. Por isso, diante da necessidade de assegurar a autonomia e a personalidade humana, surge uma nova classe de direitos humanos de personalidade, os neurodireitos, cujo objetivo é regulamentar o uso ético e moderado dessas novas neurotecnologias relacionadas ao cérebro humano.

Os neurodireitos surgem em um contexto onde o sistema internacional de proteção de direitos humanos não conseguia oferecer uma condução adequada aos inúmeros riscos que afloram do desenvolvimento e aplicação das neurotecnologias. De acordo com Marcello Ienca, os neurodireitos podem ser definidos:

Os neurodireitos são um subcampo da investigação neuroética que lida com a ética, princípios legais, sociais ou naturais de liberdade ou direito. relacionados ao domínio cerebral e mental de uma pessoa; isto é, são regras normativas fundamentais para a proteção e preservação do cérebro humano e da mente¹².

10. CNN BRASIL. *Neuralink faz 1º implante de chip cerebral em humano, diz Elon Musk*. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/neuralink-faz-1o-implante-de-chip-cerebral-em-humano-diz-elon-musk/>. Acesso em: 07 jan. 2025.

11. G1. *Implantação de chip cerebral da ‘Neuralink’, de Elon Musk, divide opiniões de especialistas; veja como funciona*. Disponível em: <https://bit.ly/4fav75V>. Acesso em: 02 jan. 2024.

12. IENCA, Marcello. *On Neurorights*. Front. Hum. Neurosci. 15:701258. 2021, p.6. Disponível em: <https://www.frontiersin.org/journals/human-neuroscience/articles/10.3389/fnhum.2021.701258/full>. Acesso em: 07 jan. 2025. Texto Original: “First of all, let us consider the very notion of “neurorights.” Neurorights can be defined as the ethical, legal, social or natural principles of freedom or entitlement relating to a person’s cerebral and mental domain; that is, the fundamental normative rules for the protection and preservation of the human brain and mind. Consequently, neuroright studies are a subfield of neuroethical and neurolegal inquiry that deals with the ethical, legal, social or natural principles of freedom or entitlement related to a person’s cerebral and mental domain; that is, the fundamental normative rules for the protection and preservation of the human brain and mind”.

IENCA aborda que há cinco novos direitos humanos que se relacionam com a personalidade dos indivíduos e que podem ser identificados no contexto dos neurodireitos, tais sejam o direito à identidade pessoal, o direito ao livre arbítrio, o direito à integridade mental, o direito ao acesso equitativo e o direito à proteção contra vieses algorítmicos (uso de tecnologias de *machine learning*)¹³.

Ao observar infinitas preocupações éticas e legais no âmbito das neurotecnologias e da proteção à dignidade humana, é vital destacar o importante trabalho – o qual alavancou a discussão sobre os neurodireitos – realizado pelos pesquisadores Rafael Yuste, Sara Goering, entre outros, em colaboração, os quais foram importantes para o desenvolvimento do estudo e dos avanços envolvendo os neurodireitos ao redor do mundo.

Na pesquisa realizada por esses autores e publicada na Revista *Nature*, Rafael Yuste e os demais pesquisadores delimitam as quatro principais áreas de preocupação no que se refere as neurotecnologias e inteligência artificial¹⁴, a saber, a privacidade mental e consentimento, a autonomia e a identidade pessoal, o direito ao aumento cognitivo e direito à proteção contra vieses.

Como objetivo desta pesquisa, constata-se que a proteção à privacidade mental se mostra relevante em contexto global, visto que há diversas preocupações sobre a transparência de iniciativas e projetos envolvendo neurotecnologias, principalmente sobre a capacidade de ocorrência de falhas e vazamento na privacidade de dados neurais.

A Empresa Neuralink e o implante de chip cerebral “Link” em humanos, por exemplo, são alvo de discussões acerca das consequências éticas e o limite de seu uso pelo setor privado. Como avalia o especialista em tecnologia, Arthur Igreja sobre o tema, “as implicações éticas e morais são irrestritas e infinitas nesse caso, já que estamos tratando da coleta de dados na fonte, o que é difícil imaginar algo que seja mais sensível, que possa dizer mais sobre o indivíduo”¹⁵. Há a necessidade de debate sobre as novidades legislativas brasileiras rumo a um marco regulatório capaz de preservar os dados cerebrais, a fim de assegurar a intimidade e o último refúgio de liberdade pessoal e autodeterminação dos indivíduos.

13. IENCA, Marcello; ANDORNO, Roberto. *Towards new human rights in the age of neuroscience and neurotechnology*. Life Sciences, Society and Policy. Vol. 13, n. 5. 26 abr. 2017, p. 13 – 14. Disponível em: <https://doi.org/10.1186/s40504-017-0050-1>. Acesso em: 25 dez. 2024.

14. YUSTE, R., GOERING, S., ARCAS, B. et al. *Four ethical priorities for neurotechnologies and AI*. *Nature* 551, 159–163 (2017). Disponível em: <https://www.nature.com/articles/551159a>. Acesso em 07/10/2024.

15. INFOMONEY. Elon Musk x China: o que está em jogo na corrida pelos chips cerebrais?. Disponível em: <https://bit.ly/48e-tcuQ>. Acesso em: 02 dez. 2024.

2. Impactos das Neurotecnologias na privacidade e a proteção dos neurodados no ordenamento jurídico brasileiro

O direito à privacidade remonta ao século 19, com o artigo “the right to privacy”, de Samuel Warren e Louis Brandeis, e a sua discussão é potencializada inicialmente com a evolução das tecnologias e atualmente com as neurotecnologias. Nesse viés, os autores Rafael Yuste, Sarah Goering, e outros acreditam que, no que se refere ao direito à privacidade e consentimento, os cidadãos devem ter a habilidade e o direito de manter seus neurodados de forma privada, ou seja, devem exercer o “direito de ficar/estar sozinho”¹⁶.

A corrida legislativa que busca assegurar o direito à neuroproteção e neutralizar os riscos inerentes do uso ou abuso indevido e não transparente das neurotecnologias – que podem trazer riscos à mente e as funções cerebrais dos indivíduos – começa com iniciativas internacionais, como a Recomendação sobre Inovação Responsável em Neurotecnologia, publicada pela OCDE, a qual apresenta disposições sobre liberdade cognitiva e privacidade mental, o Ethical Issues of Neurotechnology: Report, publicada pela Unesco em 2021¹⁷.

No Brasil, há duas iniciativas legislativas de relevância e urgência no cenário da regulamentação das neurotecnologias. A primeira diz respeito à Proposta de Emenda à Constituição nº 23, que seguiu o exemplo da Emenda à Constituição nº 115/2023, o qual incluiu a proteção de dados pessoais no rol de direitos e garantias fundamentais. A PEC visa incluir a proteção à integridade mental e à transparência algorítmica como fundamentos básicos para o crescimento e aplicação científica e tecnológica.

Importa destacar que o Chile, seguindo as diretrizes e preocupações levantadas por Rafael Yuste e outros pesquisadores, foi o primeiro país a buscar a positivação constitucional, ao alterar a sua Constituição e inserir os neurodireitos entre os direitos fundamentais à neuroproteção no país, mais especificamente o direito à privacidade mental, o direito à identidade, o direito ao livre arbítrio, o direito contra os processos automatizados de tomada de decisão e o direito ao acesso equitativo do aumento cognitivo¹⁸.

16. IENCA, Marcello; ANDORNO, Roberto. *Towards new human rights in the age of neuroscience and neurotechnology*. Life Sciences, Society and Policy. Vol. 13, n. 5. 26 abr. 2017, p. 13 – 14. Disponível em: <https://doi.org/10.1186/s40504-017-0050-1>. Acesso em: 25 dez. 2024.

17. LEGAL GROUNDS INSTITUTE. *Direito Civil e Novas Tecnologias: contribuições à Comissão de Juristas responsável pela atualização do Código Civil*. Op. cit., p. 174.

18. KREPSKY, Giselle Marie; CIPRIANI, Thiago. *Neurodireitos: Uma Comparação entre a proposta de emenda constitucional do Chile e a proposta de alteração da Lei Geral de Proteção de Dados do Brasil*. In: Anais do CIDHTP Blumenau (SC): FURB, 2022. Disponível em: <https://www.even3.com.br/anais/dignidadehumanaedireito/496373-neurodireitos--uma-comparacao-entre-a-proposta-de-emenda-constitucional-do-chile-e-a-proposta-de-alteracao-da-lei/>. Acesso em: 25 dez. 2024.

Tendo em vista a complexidade do tema, a Reforma do Código Civil (atual Lei nº 10.406/2002) busca agregar ao rol dos direitos da personalidade uma nova dimensão, a saber, os neurodireitos. De acordo com os pesquisadores José Filho e Amanda Martins:

O atual Artigo 13 do Código Civil preocupa-se com a disposição sobre o próprio corpo, limitando-a quando houver prejuízo à integridade física ou aos bons costumes. Além disso, o referido artigo proíbe dispor sobre o próprio corpo, exceto por exigência médica. **Ainda que, a rigor, o cérebro humano esteja contemplado enquanto órgão, não há proteção expressa à liberdade, privacidade e integridade mental.** Com isso, torna-se necessário ampliar o quadro de direitos humanos para que as liberdades e os direitos fundamentais continuem sendo protegidos diante do avanço da neurotecnologia¹⁹. (grifos nossos)

Logo, em um contexto onde o cérebro precisa estar contemplado enquanto órgão em regulação específica e adequada, a proposta legislativa de Reforma ao Código Civil acrescenta os neurodireitos ao Capítulo II do Código Civil, como parte indissociável da personalidade e as mesmas características dos direitos das personalidades, isto é, não podem ser transmitidas, renunciadas ou limitadas: Art. X – Os neurodireitos são parte indissociável da personalidade e recebem a mesma proteção, não podendo ser transmitidos, renunciados ou limitados.

I – São considerados neurodireitos as proteções que visam preservar a privacidade mental, a identidade pessoal, o livre arbítrio, o acesso justo à ampliação ou melhoria cerebral, a integridade mental e a proteção contra vieses, das pessoas naturais a partir da utilização de neurotecnologias.

II – São garantidos a toda pessoa natural os seguintes neurodireitos:

- a) direito à liberdade cognitiva: é vedado o uso de neurotecnologias de forma coercitiva ou sem consentimento;
- b) direito ao livre arbítrio: direito de tomar decisões livres e competentes no uso de interfaces cérebro-máquina, sem manipulação de pensamentos, sentimentos ou estados mentais;
- c) direito à privacidade mental: direito de proteção contra o acesso não autorizado ou não desejado a dados cerebrais, vedada a venda ou transferência comercial;
- d) direito à integridade mental: direito à não manipulação da atividade mental por neurotecnologias, sendo vedada a alteração ou eliminação do controle sobre o próprio comportamento sem consentimento;

19. LEGAL GROUNDS INSTITUTE. *Direito Civil e Novas Tecnologias: contribuições à Comissão de Juristas responsável pela atualização do Código Civil*, p. 176 Disponível em: <https://legalgroundsinstitute.com/blog/atualizacao-do-codigo-civil-como-oportunidade-para-codificacao-dos-neurodireitos/>. Acesso em: 07 jan. 2025.

e) direito de continuidade da identidade pessoal e da vida mental: proteção contra alterações na identidade pessoal ou coerência de comportamento, sendo vedadas alterações não autorizadas no cérebro ou nas atividades cerebrais;

f) direito ao acesso justo: direito de acesso justo e equitativo a tecnologias de aprimoramento ou extensão das capacidades cognitivas que deve ser guiado pelos princípios da justiça e da equidade;

g) direito à proteção contra vieses: são vedadas práticas discriminatórias ou enviesadas a partir de dados cerebrais.

Parágrafo Único – Os neurodireitos e o uso ou acesso a dados cerebrais poderão ser

regulados por normas específicas, desde que preservadas as proteções e garantias

conferidas aos direitos de personalidade, bem como os direitos
elencados no inciso

II acima. (grifos nossos)²⁰

Diante da análise da proposta legislativa, percebe-se que o direito à privacidade mental, presente na Proposta Legislativa, assim como os demais neurodireitos previstos pela Neurorights Foundation, é associado à convicção de que quaisquer neurodados – ou dados cerebrais – recolhidos através da medição de atividade de operação neural podem impactar de forma desmedida e profunda e, por isso, esta categoria de dados pessoais deve ser objeto de regulamentação específica, conforme disposto no art. X, inciso II, Parágrafo Único, da Reforma do CC, a fim de estabelecer normas capazes de equilibrar a necessidade de inovação e a regulamentação adequada para tratar a natureza complexa dos dados cerebrais codificados ou manipulados por neurotecnologias.

Por isso, torna-se relevante a Proposta Legislativa que visa reformar o Código Civil, pois significa um avanço contra os riscos adversos pelo desenvolvimento neurotecnológico, visto que estes riscos passam pelos nossos direitos de personalidade, os quais são direitos absolutos estendidos para tutelar a dignidade da pessoa humana, sendo, portanto, indisponíveis.

No que se refere ao direito à proteção da privacidade como direito fundamental da personalidade e a proteção aos neurodados no nosso ordenamento jurídico, o Brasil buscou, através da Proposta de Lei ordinária nº 1.229/2021 alterar a Lei nº 13.709/2018, ou melhor, a Lei Geral de Proteção de Dados. É válido salientar que, apesar da LGPD ter sido promulgada em 2018, marcando a era da sociedade da informação e a proteção aos direitos da personalidade, já

20. Idem, p. 179.

se faz necessária a análise dos neurodados, visto que a Lei precisa se adequar aos novos desafios relacionados à liberdade cognitiva do indivíduo e a sua privacidade e autonomia mental. Todos os indivíduos merecem que seus dados cerebrais possuam proteção regulatória contra toda e qualquer neurotecnologia que possa coletar dados sensíveis e íntimos do indivíduo.

Nesse contexto, o Projeto de Lei nº 1.229/2021, apesar de retirado pelo próprio autor, visava acrescentar ao marco regulatório da LGPD a importante conceituação de dados neurais, estabelecendo uma nova classe jurídica de dados pessoais sensíveis referentes à saúde e regulamentar a coleta e tratamento desses dados.

Os pesquisadores Marcelo Ienca e Roberto Andorno, ao discorrer sobre a proteção à privacidade, abordam que a primeira preocupação deve ser se as normas jurídicas tradicionais são suficientes para abranger os dados contidos e gerados por nossas mentes²¹. Como vimos anteriormente, a LGPD, apesar de recente, não possui definições e direcionamentos jurídicos no que se refere à coleta e tratamento de dados cerebrais, sendo insuficiente para assegurar a proteção à privacidade dos neurodados.

Outra consideração feita pelos pesquisadores é que “tais dados devem ser tratados de forma justa para fins específicos e com base no consentimento da pessoa em causa ou em qualquer outra base legítima prevista por lei”²². Logo, como as bases legais para o tratamento de dados pessoais sensíveis estão dispostas no art. 11 da LGPD, faz-se necessário indagar qual(is) bases legais serão suficientes para comprovar e legitimar o tratamento e o uso de dados pessoais sensíveis, como é o caso dos neurodados.

Por isso, considerando que o Direito é contingente e sofre de uma dupla carência, isto é, o fato do direito estar sempre a mercê dos fatos sociais e a insuficiência que o direito sofre quando ele vai se subsumir a um fato social que pode não ser mais o mesmo²³, é imprescindível que as iniciativas e os debates legislativos sejam potencializadas, visto que o nosso ordenamento jurídico está longe de esgotar o tema e, por isso, torna-se indispensável a proposição de normas específicas para regular os neurodireitos, mas principalmente regular acerca do uso e acesso aos dados cerebrais.

21. IENCA, Marcello; ANDORNO, Roberto. *Towards new human rights in the age of neuroscience and neurotechnology*. Life Sciences, Society and Policy. Vol. 13, n. 5. 26 abr. 2017, p. 12. Disponível em: <https://doi.org/10.1186/s40504-017-0050-1>. Acesso em: 25 dez. 2024.

22. IDEM, pag 12. Texto Original: “such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law”.

23. LEGAL GROUND INSTITUTE. *Seminário Regulação De Neurodireitos*. Youtube, 6 mar. 2024. Disponível em: <https://www.youtube.com/watch?v=WSZoPTiV16U&t=11264s>. Acesso em: 07 jan. 2025.

Atualmente, há um projeto de Lei em tramitação no Congresso Nacional que busca alterar a LGPD para incluir a proteção dos neurodados: o PL 522/2022, na Câmara dos Deputados. Este Projeto possui objetivos semelhantes ao PL arquivado, a fim de preservar a privacidade dos indivíduos, mas é mais amplo do que o PL anterior, visto que aborda definições de dado neural e interface cérebro-computador, a regulamentação do tratamento de dados neurais e a necessidade do consentimento explícito e específico do titular, os direitos dos titulares de dados neurais e a responsabilidade dos controladores:

Art. 1º Esta Lei modifica a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), a fim de conceituar dado neural e regulamentar a sua proteção.

Art. 2º O art. 5º da Lei nº 13.709, de 14 de agosto de 2018, passa a vigorar com as seguintes alterações:

“Art. 5º 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, dado neural, quando vinculado a uma pessoa natural; XX – dado neural: qualquer informação obtida, direta ou indiretamente, da atividade do sistema nervoso central e cujo acesso é realizado por meio de interfaces cérebro-computador, ou qualquer outra tecnologia, invasivas ou não-invasivas;

XXI – interface cérebro-computador: qualquer sistema eletrônico, óptico ou magnético que colete informação do sistema nervoso central e a transmita a um sistema informático ou que substitua, restaure, complemente ou melhore a atividade do sistema nervoso central em suas interações com o seu ambiente interno ou externo; XXII – neurotecnologia: conjunto de dispositivos, métodos ou instrumentos não farmacológicos que permitem uma conexão direta ou indireta com o sistema nervoso.” (NR)

Art. 3º O Capítulo II da Lei nº 13.709, de 14 de agosto de 2018, passa a vigorar acrescido da seguinte Seção II-A: “**Seção II-A Do Tratamento de Dados Neurais**

Art. 13-A O tratamento de dados neurais somente ocorrerá quando:

I – o titular ou o responsável legal consentir, de forma específica e destacada, para finalidades específicas, mesmo em circunstâncias clínicas ou nos casos em que a interface cérebro-computador tenha a capacidade de tratar dados com o titular inconsciente;

II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) realização de estudos por órgão de pesquisa, garantida a anonimização dos dados pessoais sensíveis; b) proteção da vida ou da incolumidade física do titular ou de terceiro; c) tutela da saúde, exclusivamente, em procedimento rea-

lizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

Parágrafo único. O pedido de consentimento para o tratamento de dados neurais deve indicar, de forma clara e destacada, os possíveis efeitos físicos, cognitivos e emocionais de sua aplicação, as contraindicações bem como as normas sobre privacidade e as medidas de segurança da informação adotadas.

Art. 13-B É vedado o uso de qualquer interface cérebrocomputador ou método que possa causar danos à identidade individual do titular dos dados, prejudicar sua autonomia ou sua integridade psicológica.

Art. 13-C É vedada a comunicação ou o uso compartilhado entre controladores de dados neurais com objetivo de obter vantagem econômica.

Art. 13-D Não se aplicam aos dados neurais as exceções previstas no inciso I e inciso II, alínea 'a', do art. 4º.

Art. 13-E O Estado tomará medidas para assegurar o acesso equitativo aos avanços da neurotecnologia. ²⁴. (grifos nossos)

Logo, seguindo o exemplo do Projeto de Lei supracitado, esta pesquisa propõe a criação de um regime normativo especial dentro da LGPD que contemple os neurodados como categoria de dados pessoais sensíveis, com regras específicas sobre consentimento informado, segurança da privacidade e da informação e limitação estrita de finalidades de tratamento. Esse regime deve reconhecer os neurodados e exigir, como regra, que qualquer coleta ou manipulação seja precedida por consentimento livre, específico e destacado, excetuando as hipóteses em que o tratamento ou coleta de dados seja feito sem fornecimento de consentimento de titular. Além disso, o tratamento de tais dados deve se restringir a finalidades legítimas e compatíveis com a dignidade da pessoa humana, vedando sua utilização para fins discriminatórios, que podem causar danos à identidade individual do titular dos dados, prejudicando sua autonomia ou sua integridade psicológica.

Entretanto, torna-se válido salientar que, em que pese o Projeto de Lei nº 522/2022 representar um importante passo para a proteção de neurodados em nosso arcabouço jurídico, a sua eficácia está interligada a capacidade de enfrentar desafios técnicos e operacionais. Um dos pontos críticos consiste na definição de órgãos fiscalizadores com competência especializada para operar em cenários de alto grau de complexidade tecnológica, como é o caso das neurotecnologias BCI.

24. BRASIL. PL 522/2022. Modifica a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados pessoais), a fim de conceituar dado neural e regulamentar a sua proteção. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2276604>. Acesso em: 25 dez. 2024.

A Autoridade Nacional de Proteção de Dados (ANPD), embora represente um avanço no cenário da proteção de dados pessoais ao estabelecer normas e diretrizes para a sua implementação, ainda carece de capacidade técnica, recursos humanos especializados e infraestrutura tecnológica compatível com a natureza dos neurodados. Logo, considerando que os dados neurais envolvem informações biométricas e comportamentais e dados extraídos diretamente do sistema nervoso central, faz-se necessário o fortalecimento e reestrutura da ANPD, através de (1) criação de uma diretoria técnica voltada exclusivamente à proteção dos neurodados; (2) a capacitação de servidores em ética das neurotecnologias e inteligência artificial aplicada a neurotecnologias; (3) cooperação técnica com universidades, centros de pesquisa em neurociência e órgãos como o Conselho Nacional de Justiça e o Ministério Público Federal, para padronização de boas práticas e compartilhamento de dados regulatórios e (4) articulação com eventuais agências reguladoras voltadas a tecnologias emergentes que venham a ser instituídas, entre outras condutas necessárias.

É válido salientar que a proteção dos dados cerebrais e a privacidade mental é essencial para a preservação existencial e de tudo que é subjetivo no indivíduo, ou melhor, a sua essência e, por isso, criar um arcabouço jurídico que busque garantir a tutela de todos os aspectos do cérebro e dos nossos direitos da personalidade se torna essencial também para que os dados pessoais sensíveis dos indivíduos não sofram ameaças externas e conduções abusivas e indevidas de outros indivíduos, empresas e governos com a sua operacionalização para manipulação e controle de informações. Para maior eficácia do Projeto, destaca-se a importância de educação digital e ética neurotecnológica para a sociedade civil, com campanhas públicas que alertem sobre os direitos dos titulares de neurodados e riscos da exposição dos dados neurais.

Apesar da obra “1984” e a figura do Grande Irmão retratarem um cenário com previsões distópicas, o contexto atual e o potencial de evolução das neurotecnologias no futuro associado a ascensão de governos totalitários ou abuso e falta de transparência de empresas que buscam o lucro de forma cega e desenfreada, pode nos trazer muita lucidez sobre a necessidade de debater sobre o tema, instigar iniciativas públicas e privadas que buscam assegurar os direitos humanos contra o uso indevido ou abusivo da neurotecnologia, como a organização sem fins lucrativos Neurorights Foundation, mas principalmente de propor normas jurídicas, como a Proposta de Lei nº 522/2022, capazes de esclarecer conceituações e como o uso e a coleta de dados cerebrais devem ser coletadas e tratadas por empresas e governos, além de definir as bases

legais que podem ser corretamente usadas, a fim de tutelar o nosso direito à privacidade mental e, conseqüentemente, a nossa essência.

Considerações finais

Diante da análise desta pesquisa, conclui-se a urgência em compreender a privacidade mental dentro de um cenário global, em que novas tecnologias possuem o potencial de tratar e coletar dados, a fim de decodificar o pensamento ou até mesmo aprimorar o potencial cognitivo do cérebro, mas principalmente para assegurar a existencialidade do sujeito e evitar conduções abusivas de governos ou empresas que buscam instrumentalizar as informações obtidas por meio de tecnologias BCI para fins ilícitos e controladores.

Entre os principais resultados, destaca-se a necessidade urgente de adaptação legislativa no ordenamento jurídico brasileiro. A análise mostrou que as iniciativas legislativas que buscam positivar os neurodireitos com status constitucional em nossa Carta Magna e como parte integrante do rol dos direitos da personalidade em nosso Código Civil são de suma importância, principalmente quando examinamos o famoso caso chileno, visto que, como as neurotecnologias estão ganhando espaço em nosso cotidiano, torna-se ainda mais urgente criar regulamentações específicas que visam garantir a proteção dos neurodados, no que se refere a coleta e tratamento desses dados pessoais sensíveis, contra qualquer tentativa de uso indevido ou manipulação de dados cerebrais dos indivíduos.

Nesse sentido, a pesquisa destacou como de prioritária atenção o Projeto de Lei nº 522/2022 que serve como exemplo inspirador para a criação de um arcabouço jurídico robusto que consiga equilibrar inovação tecnológica com respeito à privacidade mental. Nesse cenário, destaca-se a importância de se definir base(s) legal(is) sólida(s) para a proteção dos neurodados, tendo em vista a necessidade de aprimorar a tutela jurídica do cérebro e incluir disposições específicas sobre neurodados, de modo a garantir que o tratamento dessas informações respeite a autonomia do titular e impeça possíveis manipulações. Ademais, é necessário que o consentimento seja obtido de forma explícita e informada, considerando os possíveis impactos cognitivos e emocionais da coleta e tratamento dessas tecnologias.

Defende-se também a criação de um regime especial dentro da Lei Geral de Proteção de Dados. Essa proposta visa preencher as lacunas normativas existentes e assegurar que os dados neurais, por refletirem a intimidade da mente humana, sejam tutelados com o mais alto grau de proteção legal. Além

disso, reconhece-se a necessidade do fortalecimento da ANPD para que possa atuar na proteção dos dados neurais no indivíduo, ao estabelecer normas e diretrizes para a sua implementação.

Portanto, infere-se que a regulamentação das neurotecnologias, sobretudo no que se refere ao direito à privacidade mental, torna-se indispensável para evitar abusos e assegurar que os avanços sejam revertidos em prol da humanidade, reafirmando a dignidade humana e a proteção dos dados cerebrais mesmo em tempos de transformações neurotecnológicas.

Referências

AGÊNCIA BRASIL. *Neurotecnologia avança, cientistas pedem proteção à privacidade mental*. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2024-03/neurotecnologia-avanca-cientistas-pedem-protecao-privacidade-mental>. Acesso em: 07 jan. 2025.

AGÊNCIA BRASIL. *PEC propõe proteção à privacidade mental na era das neurotecnologias*. Disponível em: <https://noticias.uol.com.br/ultimas-noticias/agencia-brasil/2024/03/10/pec-propoe-protecao-a-privacidade-mental-na-era-das-neurotecnologias.htm>. Acesso em: 07 jan. 2025.

BBC. *Elon Musk x China: o que está por trás da corrida pelos chips cerebrais*. Disponível em: <https://www.bbc.com/portuguese/articles/c88jmpl902lo>. Acesso em: 07 jan. 2025.

BBC. *Neurotecnologia e privacidade mental: os desafios éticos e legais do avanço tecnológico*. Disponível em: <https://www.bbc.com/portuguese/articles/c88jmpl902lo>. Acesso em: 07 jan. 2025.

BRASIL. *PL 522/2022. Modifica a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), a fim de conceituar dado neural e regulamentar a sua proteção*. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2276604>. Acesso em: 25 dez. 2024.

BRASIL. *Projeto de Lei nº 1229, de 2021. Dispõe sobre a proteção dos neurodireitos e estabelece diretrizes éticas para o uso de neurotecnologias*. Disponível em: <https://bit.ly/48hzCt9>. Acesso em: 25 dez. 2024.

BRASIL. *Senado Federal. Proposta de Emenda à Constituição n. 29, de 2023. Altera a Constituição Federal para incluir, entre os direitos e garantias fundamentais, a proteção à integridade mental e à transparência algorítmica*. Disponível em: <https://bit.ly/3BMYyWt>. Acesso em: 25 dez. 2024.

CNN BRASIL. *Neuralink faz 1º implante de chip cerebral em humano, diz Elon Musk*. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/neuralink-faz-1o-implante-de-chip-cerebral-em-humano-diz-elon-musk/>. Acesso em: 07 jan. 2025.

FRAZÃO, Ana. *'Neurocapitalismo' e o negócio de dados cerebrais. Os nossos pensamentos e a nossa identidade pessoal estão em risco?* Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/neurocapitalismo-e-o-negocio-de-dados-cerebrais-25092019>. Acesso em: 25 dez. 2024.

FRAZÃO, Ana; MULHOLLAND, Caitlin. *Podcast Direito Digital com Ana Frazão e Caitlin Mulholland: Episódio 21: Neurodireitos*. Março 2023. Disponível em: <http://www.podcastdireitodigital.com/>. Acesso em: 25 dez. 2024.

G1. *Implantação de chip cerebral da 'Neuralink', de Elon Musk, divide opiniões de especialistas; veja como funciona*. Disponível em: <https://bit.ly/4fav75V>. Acesso em: 02 jan. 2024.

IENCA, Marcello. *On Neurorights*. Front. Hum. Neurosci. 15:701258. 2021. Disponível em: <https://www.frontiersin.org/journals/human-neuroscience/articles/10.3389/fnhum.2021.701258/full>. Acesso em: 07 jan. 2025.

IENCA, Marcello; ANDORNO, Roberto. *Towards new human rights in the age of neuroscience and neurotechnology*. Life Sciences, Society and Policy. Vol. 13, n. 5. 26 abr. 2017. Disponível em: <https://doi.org/10.1186/s40504-017-0050-1>. Acesso em: 25 dez. 2024.

INFOMONEY. *Elon Musk x China: o que está em jogo na corrida pelos chips cerebrais?*. Disponível em: <https://bit.ly/48etcuO>. Acesso em: 02 dez. 2024.

KREPSKY, Giselle Marie; CIPRIANI, Thiago. *Neurodireitos: Uma Comparação entre a proposta de emenda constitucional do Chile e a proposta de alteração da Lei Geral de Proteção de Dados do Brasil*. In: *Anais do Congresso Internacional Dignidade Humana em Tempos de Pandemia: direito e democracia no Brasil contemporâneo*. Anais. Blumenau (SC): FURB, 2022. Disponível em: <https://www.even3.com.br/anais/dignidadehumanaedireito/496373-neurodireitos--uma-comparacao-entre-a-proposta-de-emenda-constitucional-do-chile-e-a-proposta-de-alteracao-da-lei/>. Acesso em: 25 dez. 2024.

LEGAL GROUNDS INSTITUTE. *Direito Civil e Novas Tecnologias: contribuições à Comissão de Juristas responsável pela atualização do Código Civil*. Disponível em: <https://legalgroundsinstitute.com/blog/atualizacao-do-codigo-civil-como-oportunidade-para-codificacao-dos-neurodireitos/>. Acesso em: 07 jan. 2025.

LEGAL GROUND INSTITUTE. *Seminário Regulação De Neurodireitos*. Youtube, 6 mar. 2024. Disponível em: <https://www.youtube.com/watch?v=WSZoPTiV16U&t=11264s>. Acesso em: 07 jan. 2025.

MIRANDA, Maria Lucilia Morais de; NASCIMENTO, Adriana Galvão do; BRAGA, Indira Maria Alencar; MALAFAIA, Tatiane Maria Gama da Silva; BIZOTTO, Beatriz Lucia Salvador; GLAIMO, Thays de Mello. *Neurodireito – colisões dos direitos fundamentais dentro da razoabilidade e proporcionalidade*. Revista Ibero-Americana de Humanidades, Ciências e Educação – REASE, v. 9, n. 12, 29 dez. 2023. Disponível em: <https://doi.org/10.51891/rease.v9i12.12746>. Acesso em: 14 jan. 2025.

ORWELL, George. 1984. Tradução de Alexandre Hubner e Heloisa Jahn. São Paulo: Companhia das Letras, 2009.

POSSA, Alisson Alexsandro. *A concretização da dignidade humana na era das neurotecnologias: o direito à liberdade cognitiva como neurodireito na ordem constitucional brasileira*. Dissertação de Mestrado. Brasília, 2022. Disponível em: https://repositorio.idp.edu.br/bitstream/123456789/4688/1/Dissertação_ALISSON%20ALEXSANDRO%20POSSA_Mestrado_2022.pdf. Acesso em: 25 dez. 2024.

THE NEURORIGHTS FOUNDATION. *The Challenge: Advances in Neurotechnology Have Far Outpaced Global, National, and Corporate Governance*. Disponível em: <https://neurorightsfoundation.org>. Acesso em: 14 jan. 2025.

RIEGER, Poliene Fernanda Souza Nascimento. *Privacidade mental e liberdade cognitiva: perspectivas e desdobramentos para novos direitos fundamentais no contexto desenvolvimento e aplicação de neurotecnologia*. 2023. 85 f. (Mestrado Profissional em Revista Ibero-Americana de Humanidades, Ciências e Educação-REASE Revista Ibero-Americana de Humanidades, Ciências e Educação. São Paulo, v.9.n.12. dez. 2023. ISSN – 2675 – 3375183 Direito) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2022. Disponível em: <http://52.186.153.119/handle/123456789/4239>. Acesso em: 15 jan. 2025.

VENTURA, Dora Fix. *Um retrato da área de Neurociência e comportamento no Brasil*. Psicologia: Teoria e Pesquisa* [online]. 2010, v. 26, n. spe, p. 123. Disponível em: <https://doi.org/10.1590/S0102-37722010000500011>. Epub 13 dez. 2010. ISSN 1806-3446. Acesso em: 07 jan. 2025.

YUSTE, Rafael. *Recommendations for Responsible Development and Application of Neurotechnologies*. Publicado online em 19 abr. 2021. Disponível em: <https://doi.org/10.1007/s12152-021-09468-6>. Acesso em: 25 dez. 2024.

YUSTE, Rafael; GENSER, Jared; HERMMAN, Stephanie. *It's Time for Neuro-Rights*. *Horizons*, n. 18, 2021. Disponível em: <https://www.perseus-strategies.com/wp-content/uploads/2021/03/Neuro-Rights-Horizons-Winter-2021.pdf>. Acesso em: 25 dez. 2024.

YUSTE, Rafael et al. *Four ethical priorities for neurotechnologies and AI*. *Nature*. 551. Pp. 159-163. 09 nov. 2017. Disponível em: <https://www.nature.com/articles/551159a>. Acesso em: 25 dez. 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

10

Governança na era das novas tecnologias e as relações de trabalho: riscos de discriminação e desafios regulatórios da IA

LARISSA ALMEIDA DEL LHANO

Sumário: Introdução. 1. A Inteligência Artificial: diferentes classificações e empregabilidades. 2. IA no contexto laboral: potencialidades e desafios. 3. Governança e os possíveis caminhos para mitigação da discriminação algorítmica. Considerações finais. Referências.

Introdução

Diante da Quarta Revolução Industrial, as tecnologias se tornam cada vez mais presentes no cotidiano, alterando diversas relações econômicas e humanas na sociedade por conta de suas potencialidades². Assim, cumpre ressaltar, dentre diversas tecnologias emergentes, o protagonismo da inteligência artificial (IA), ferramenta disruptiva e com caráter de uso geral³. Devido às suas múltiplas aplicações e diferentes classificações, não há consenso sobre uma definição única, sendo entendida como um conceito “guarda-chuva”⁴.

No contexto empresarial, existem diversas formas de utilização da IA⁵, desde a realização de tarefas simples de forma automatizada, até mesmo na substituição parcial de intervenção humana em situações decisórias. Como exemplo, pode-se citar a utilização de IA como norteadora das tomadas de decisão da empresa em questões laborais, seja no momento de contratação, seja para monitoramento da produtividade do trabalhador no desempenho de suas funções⁶.

Dessa forma, o presente artigo aborda alguns dos desafios e impactos existentes, além de possíveis medidas para mitigação de riscos no uso de IA no contexto corporativo, considerando o emprego dessa tecnologia no âmbito das relações de trabalho.

A hipótese é a de que existem riscos no uso de IA no contexto laboral de uma corporação e independentemente da finalidade de uso do sistema, sendo

1. Advogada. Pós-graduanda em Direito Digital pela Universidade do Estado do Rio de Janeiro (UERJ) em parceria com o ITS Rio. Pesquisadora voluntária do Grupo Empresa, Desenvolvimento e Responsabilidade (EDResp – UFJF). Graduada em Direito pela Universidade Federal de Juiz de Fora (UFJF).

2. SCHWAB, Klaus. *A Quarta Revolução Industrial*. 1 ed. São Paulo: Edipro, 2016.

3. ABRUSIO, Juliana; ARAUJO, André Eduardo Dorster. Inteligência artificial: decisões automatizadas e discriminação nas relações de trabalho. *Revista de Direito do Trabalho e Seguridade Social*. vol. 223. ano 48. p. 321–343. São Paulo: Ed. RT, mai./jun. 2022. Disponível em: <http://revistadoatribunais.com.br/maf/app/document?stid=st-rl&marg=DTR-2022-9190>. Acesso em: 20 ago. 2024.

4. KORKMAZ, Maria Regina Rigolon. *Decisões automatizadas: explicação, revisão e proteção na era da inteligência artificial*. São Paulo: Thomson Reuters Brasil, 2023.

5. PINHEIRO, Caroline da Rosa. BREGA, Gabriel Ribeiro. Inteligência Artificial e *Compliance* – a (in)suficiência dos marcos de proteção de dados. *Revista Semestral de Direito Empresarial*, n. 28, p. 161-196, jan./jun. 2021. Disponível em: <https://rsde.com.br/artigos/inteligencia-artificial-e-compliance-a-insuficiencia-dos-marcos-de-protecao-de-dados/>. Acesso em: 17 out. 2024.

6. ADAMS-PRASSL, Jeremias. What if your boss was an algorithm? The rise of Artificial Intelligence at Work. *Comparative Labor Law & Policy Journal* 123. vol. 41, p. 1-30. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3661151. Acesso em: 18 jan. 2025.

necessária uma reflexão acerca de medidas de governança que podem ser aplicadas, a fim de evitar cenários de discriminação algorítmica. A pesquisa realizada é teórica e de natureza normativa, valendo-se do método dedutivo, com revisão bibliográfica e análise documental.

O artigo tem o objetivo de responder à seguinte pergunta: Considerando os riscos do uso de IA no âmbito corporativo, como a governança pode contribuir para uma implementação ética dessa tecnologia, de forma que cenários de discriminação algorítmica em relações de trabalho sejam mitigados?

O trabalho foi dividido em 3 (três) partes, além da introdução e considerações finais. Inicialmente, são apresentados conceitos relevantes para a compreensão do trabalho, além de breve contextualização sobre a inteligência artificial e suas classificações enquanto tecnologia disruptiva. Na segunda parte, é feita uma explanação do uso de IA no âmbito corporativo, sendo dado destaque para seus impactos, positivos e negativos, em relações de trabalho, seja para a empresa ou o trabalhador. O terceiro tópico trata de medidas de governança possíveis de implementação para mitigar cenários de discriminação algorítmica, além de analisar brevemente o cenário regulatório da IA nos contextos internacional e nacional.

Por fim, apresenta-se a conclusão, considerando os objetivos, hipóteses e metodologia delineados anteriormente. A presente pesquisa não tem o intuito de esgotar o debate sobre o tema, mas contribuir com discussões em andamento acerca da utilização de IA em relações laborais.

1. A Inteligência Artificial: diferentes classificações e empregabilidades

Apesar de não ser uma tecnologia criada recentemente, os últimos anos, sendo dado destaque para 2023 e 2024, foram altamente marcados pelo crescimento do protagonismo da IA e por debates acerca de sua regulação ao redor do mundo⁷. No cenário internacional, pode-se citar a aprovação do Regulamento Europeu (*Artificial Intelligence Act*) no primeiro semestre de 2024, a atualização dos princípios orientadores criados em 2019 pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE) sobre o tema, bem como a publicação de uma resolução pela Organização das Nações Unidas (ONU), com o intuito de fomentar a proteção de direitos humanos e uma IA segura.

7. PINHEIRO, Caroline da Rosa. ROCHA, Matheus Mazzoni. DEL LHANDO, Larissa Almeida. Governança e Inteligência Artificial: (in)certezas sobre substituição humana nos conselhos de administração. *Anais do XIII Encontro Internacional do Conpedi Uruguai – Montevideu. Governo Digital, Direito e Novas Tecnologias I*, p. 4-25. Disponível em: <http://site.conpedi.org.br/publicacoes/351f5k20/nhf03e63/LWCi1rkteY4fOjiA.pdf> Acesso em: 06 out. 2024.

No Brasil, está em tramitação o Projeto de Lei (PL) n.º 2.338/2023⁸, que busca ser o marco regulatório nacional específico da IA⁹, e que recebeu em dezembro de 2024 novo texto substitutivo. Influenciado pelo regulamento da União Europeia, o projeto de lei brasileiro conta com uma estrutura baseada em riscos dos sistemas dessa tecnologia, possibilitando que o monitoramento e adoção de medidas mitigatórias e/ou sancionatórias seja proporcional a cada contexto de aplicação.

A preocupação com a regulação da IA é pertinente, pois apesar de seus variados benefícios, existe por parte de diversos setores, no âmbito público e no privado, a preocupação quanto à sua utilização de forma ética e responsável pelos agentes de IA¹⁰, por ser uma ferramenta que desafia as estruturas regulatórias já existentes e em vigor¹¹.

Além das variadas aplicações da IA, cumpre destacar algumas das classificações existentes em relação a essa tecnologia. Inicialmente, são trazidos os conceitos de IA fraca e forte: o primeiro tipo de sistema – e único existente até o momento – tem como finalidades realizar tarefas específicas considerando sua programação, enquanto o sistema forte seria capaz de realizar qualquer tarefa, devido à sua habilidade de aprendizado contínuo¹².

Ainda, é feita menção ao sistema de aprendizado de máquina (*machine learning*), em que seus algoritmos são capazes de aprender com experiências anteriores, aperfeiçoando sua atuação¹³, e que pode ser realizado de forma supervisionada ou por reforço¹⁴.

Não obstante, pode ser feita alusão à classificação de aplicação de IA de forma concentrada ou fragmentada. Ao passo que a primeira utiliza de forma mais

8. BRASIL. Senado Federal. *Projeto de Lei n.º 2.338, de 2023. Dispõe sobre o uso da Inteligência Artificial*. Brasília, DF: Congresso Nacional. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 11 dez. 2024.

9. Apesar de não haver uma legislação específica em vigor sobre IA, outras legislações brasileiras relacionam-se ao tema, como a Lei Geral de Proteção de Dados Pessoais, o Código Civil, o Código de Defesa do Consumidor. In: BARBOSA, Leonardo Figueiredo; PINHEIRO, Caroline da Rosa. *Inteligência artificial no Brasil: avanços regulatórios*. *Revista de Informação Legislativa: RIL*, Brasília, DF, v. 60, n. 240, p. 11–41, out./dez. 2023. Disponível em: https://www12.senado.leg.br/ril/edicoes/60/240/v60_n240_p11. Acesso em: 06 set. 2024.

10. No presente trabalho considera-se o conceito de “agente de inteligência artificial” disposto no PL n.º 2.338/2023 em seu art. 4º, VIII: “desenvolvedores, fornecedores e aplicadores que atuem na cadeia de valor e na governança interna de sistemas de inteligência artificial, nos termos definidos por regulamento”. BRASIL. Senado Federal. *Projeto de Lei n.º 2.338, de 2023. Dispõe sobre o uso da Inteligência Artificial*. Brasília, DF: Congresso Nacional. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 11 dez. 2024.

11. KORKMAZ, Maria Regina Rigolon. *Decisões automatizadas: explicação, revisão e proteção na era da inteligência artificial*. São Paulo: Thomson Reuters Brasil, 2023.

12. KORKMAZ, Maria Regina Rigolon. *Decisões automatizadas: explicação, revisão e proteção na era da inteligência artificial*. São Paulo: Thomson Reuters Brasil, 2023.

13. PINHEIRO, Caroline da Rosa. BREGA, Gabriel Ribeiro. *Inteligência Artificial e Compliance – a (in)suficiência dos marcos de proteção de dados*. *Revista Semestral de Direito Empresarial*, n. 28, p. 161-196, jan./jun. 2021. Disponível em: <https://rsde.com.br/artigos/inteligencia-artificial-e-compliance-a-insuficiencia-dos-marcos-de-protecao-de-dados/>. Acesso em: 17 out. 2024.

14. KORKMAZ, Maria Regina Rigolon. *Decisões automatizadas: explicação, revisão e proteção na era da inteligência artificial*. São Paulo: Thomson Reuters Brasil, 2023.

robusta e radical o sistema, a aplicação fragmentada usa diferentes tecnologias, de forma isolada e em diversos níveis, para atingir os objetivos da corporação¹⁵. Considerando os objetivos deste trabalho, essa última será foco de análise.

Diante da aplicação fragmentada, Chiu e Lim¹⁶ dividem os sistemas de IA em três classificações distintas: (i) incremental/ facilitadora; (ii) radical/disruptiva; e (iii) fundamental/estrutural, que nivelam as ferramentas a partir de uma análise dos possíveis impactos na governança de uma empresa e seu nível de complexidade.

Sistemas de IA utilizados de forma incremental podem ser exemplificados como os que atuam no auxílio de atividades específicas, visando maior eficiência à atividade humana, além de colaborar com a redução de custos na realização da função; a aplicação radical estaria relacionada com a realização de atividades antes reservadas a humanos, ocorrendo uma substituição; e a fundamental é a de caráter mais disruptivo, trabalhando com substituições completas de humano em uma função por um sistema de IA¹⁷.

Sem considerar se a IA é utilizada de forma incremental ou mais robusta na corporação, existem diferentes riscos em seu uso, pois até mesmo a aplicação fragmentada e incremental da IA pode gerar resultados discriminatórios, a depender da finalidade de sua utilização e seu manejo. A preocupação cresce, principalmente, quando se trata de IA's com caráter de aprendizado de máquina (*machine learning*), uma vez que têm a capacidade de realizar cruzamentos de informações de seus bancos de dados, aprimorando seus sistemas e, assim, conseguem alcançar resultados que inicialmente podem não ter sido previstos completamente por seus desenvolvedores¹⁸.

2. IA no contexto laboral: potencialidades e desafios

O acelerado avanço das tecnologias e suas múltiplas formas de aplicação tem gerado alterações nas relações sociais, marcadas pela denominada hiperconexão e configurando uma sociedade regida por dados e controlada por algoritmos¹⁹.

15. PORTUGAL GOUVÊA, Carlos. *A Estrutura da Governança Corporativa*. São Paulo: Quartier Latin, 2022

16. CHIU, Iris H.-Y.; LIM, Ernest WK. Technology vs ideology: how far will artificial intelligence and distributed ledger technology transform corporate governance and business?. *Berkeley Bus. LJ*, v. 18, p. 1-18, 11 nov. 2020. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3695006. Acesso em: 17 ago. 2024.

17. CHIU, Iris H.-Y.; LIM, Ernest WK. Technology vs ideology: how far will artificial intelligence and distributed ledger technology transform corporate governance and business?. *Berkeley Bus. LJ*, v. 18, p. 1-18, 11 nov. 2020. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3695006. Acesso em: 17 ago. 2024.

18. PIRES, Thatiane Cristina Fontão; SILVA, Rafael Peteffi da. A responsabilidade civil pelos atos autônomos da inteligência artificial: notas iniciais sobre a resolução do Parlamento Europeu. *Rev. Bras. Polít. Públicas*, Brasília, v. 7, n° 3, 2017 p. 238-254. Disponível em: <https://www.arqcom.uniceub.br/RBPP/article/viewFile/4951/3643>. Acesso em: 10 dez. 2024.

19. REQUIÃO, Maurício. COSTA, Diego Carneiro. Discriminação Algorítmica: ações afirmativas como estratégia de combate. *Civillistica.com*, a. 11, n. 3, 2022. Disponível em: <http://civillistica.com/discriminacao-algoritmica/>. Acesso em: 03 jan. 2025.

No âmbito corporativo, as alterações também são perceptíveis, uma vez que empresas, buscando aumentar a produtividade de suas atividades e otimizar seus processos de gestão, têm implementado tecnologias em diferentes graus e finalidades²⁰, como para auxílio em tomadas de decisão, análise de dados, monitoramento de métricas e até mesmo da produtividade e desempenho de seus colaboradores, foco do presente trabalho, modificando o papel ocupado por empregado e empregador nas relações laborais²¹.

Tal cenário, por um lado, aumenta a possibilidade de uma gestão empresarial acerca das atividades laborais desempenhadas²², permitindo a redução de custos operacionais, aumento de eficiência e da celeridade em processos internos²³, considerando o cenário de concorrência empresarial vivenciado no mercado.

Entretanto, destaca-se que a arquitetura relacional que surge nesse cenário é fortemente marcada pelo monitoramento e controle construídos pelo capitalismo de vigilância²⁴, que tem influenciado as práticas do mercado. A gestão algorítmica, portanto, é entendida como a utilização de sistemas algorítmicos que se valem de dados rastreados que podem ser utilizados em atividades de monitoramento, atribuição de tarefas e supervisão de trabalhos²⁵.

O contexto de monitoramento lida com um alto volume de dados, nem sempre qualificados, que podem ser interpretados conforme os interesses da empresa, como na formação de *profiling*²⁶ de trabalhadores para análise e monitoramento de produtividade e, de forma não intencional, promover discrimi-

20. SANTOS, Rodrigo Coimbra. GRAMINHO, Vivian Maria Caxambu. Discriminação algorítmica nas relações de trabalho e princípio da Lei Geral de Proteção de Dados. *Sequência*, v. 45, n. 96, p. 1-31, 2024. Disponível em: <https://www.scielo.br/j/seq/a/9FGhvr75HYSdGMRfKnJ9FZd/?format=pdf&lang=pt>. Acesso em: 02 jan. 2025.

21. SANTOS, Rodrigo Coimbra. GRAMINHO, Vivian Maria Caxambu. Discriminação algorítmica nas relações de trabalho e princípio da Lei Geral de Proteção de Dados. *Sequência*, v. 45, n. 96, p. 1-31, 2024. Disponível em: <https://www.scielo.br/j/seq/a/9FGhvr75HYSdGMRfKnJ9FZd/?format=pdf&lang=pt>. Acesso em: 02 jan. 2025.

22. DE STEFANO, Valerio. Automação, inteligência artificial e proteção laboral: padrões algorítmicos e o que fazer com eles. In: *Futuro do Trabalho: os efeitos da revolução digital na sociedade*. CARELLI, Rodrigo de Lacerda; CAVALCANTI, Tiago Muniz; FONSECA, Vanessa Patriota da (org.). Brasília: ESMPU, 2020. Disponível em: https://escola.mpu.mp.br/publicacoes/obras-avulsas/e-books-esmpu/futuro-do-trabalho-os-efeitos-da-revolucao-digital-na-sociedade/@@download/arquivo/Livro_Futuro+do+Trabalho.pdf. Acesso em: 07 out. 2024.

23. PORTUGAL GOUVÊA, Carlos. *A Estrutura da Governança Corporativa*. São Paulo: Quartier Latin, 2022.

24. ZUBOFF, Shoshana. *The age of Surveillance Capitalism: the fight for a human future at the new frontier of power*. Nova Iorque: Public Affairs, 2019.

25. ALGORITHMIC management in the workplace. *Internacional Labour Organization*. Disponível em: <https://www.ilo.org/algorithmic-management-workplace>. Acesso em: 17 abr. 2025.

26. O fenômeno pode ser entendido como a geração de correlações de cunho estatístico e natureza preditiva, relacionados a determinados indivíduos ou grupos, baseados em suas características. In: VIEIRA, Gustavo Duarte. *Proteção de dados pessoais em práticas de profiling no setor privado*. Dissertação (Mestrado em Direito) – Faculdade de Direito da Universidade Federal de Minas Gerais. Belo Horizonte, 2019, p. 25. Disponível em: <http://hdl.handle.net/1843/34072>. Acesso em: 10 out. 2024.

nação algorítmica através dos *inputs* e *outputs* do sistema, o que pode ensejar em impactos negativos aos direitos e oportunidades dos trabalhadores²⁷.

É comum prevalecer o entendimento de que uma decisão tomada por sistemas de IA seja mais clara e assertiva que uma decisão tomada por um humano, mas tal posicionamento precisa ser ponderado, considerando a opacidade dos algoritmos e falta de transparência sobre o funcionamento do sistema são fatores que impactam na geração de vieses e na confiabilidade acerca da qualidade dos dados e como ocorreu seu processamento²⁸.

Ainda, a utilização sem limitações de tecnologias para análises preditivas e monitoramentos pode gerar impactos à privacidade dos indivíduos, bem como o livre desenvolvimento de sua personalidade, pois muitas vezes são disponibilizados aos sistemas mais dados dos que os necessários para as análises pretendidas, criando uma arquitetura de controle fora do alcance do cidadão para mudanças, podendo ser equiparada à estrutura de “ditadura dos algoritmos”, de Stefano Rodotà²⁹.

Um exemplo de mecanismos de monitoramento individual de trabalhadores considerando o contexto de tecnologias e meio digital é a utilização de *bossware*s, que se popularizaram com o crescimento de situações de teletrabalho, principalmente em decorrência da pandemia da Covid-19. O termo refere-se a aplicativos e *softwares* de computador, que são capazes de rastrear movimentos de *mouse*, ativar webcams e microfones, fazer capturas de telas e outras tantas ações de monitoramento, muitas vezes sem que o trabalhador perceba³⁰. Tal ferramenta, além de ter funcionalidades que permitem construir perfis e entender padrões de comportamento do trabalhador, pode servir como fonte de dados para alimentar sistemas de IA na busca por soluções de aumento de produtividade que sejam benéficas aos objetivos da corporação mas, em contrapartida, se não utilizada de forma transparente e diligente, pode ensejar em violações de direitos fundamentais dos trabalhadores, como o da privacidade³¹.

27. FONSECA, Bruno Blum. Inteligência artificial e a proteção dos dados pessoais no recrutamento de trabalhadores: desafios e perspectivas. In: BRANCO, Sérgio; TEFFÉ, Chiara Spadaccini de (Coords.). *Regulação digital: Perspectivas Jurídicas sobre Tecnologia e Sociedade*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2024, p. 299-319. Disponível em: <https://itsrio.org/pt/publicacoes/regulacao-digital-dialogos-da-pos-graduacao-em-direito-digital/>. Acesso em: 23 ago. 2024.

28. FRAZÃO, Ana; GOETTENAUER, Carlos. Black box e o direito face à opacidade algorítmica. In: BARBOSA, Mafalda Miranda; NETTO, Felipe Braga; SILVA, Michael César; FALEIROS JÚNIOR, José Luiz de Moura (Coords.). *Direito digital e inteligência artificial: diálogos entre Brasil e Europa*. Indaiatuba, SP: Editora Foco, 2021, p. 27-42. Disponível em: https://www.academia.edu/45811453/Black_Box_e_o_direito_face_%C3%A0_opacidade_algor%C3%ADtmica. Acesso em: 25 out. 2024.

29. RODOTÀ, Stefano. *Il mondo nella rete: Quali i diritti, quali i vincoli*. Roma: Laterza & Figli – Gruppo Editoriale L'Espresso, 2019.

30. BOSSWARE is coming for almost every worker: the software you might not realize is watching you. *The Guardian*. Disponível em: <https://www.theguardian.com/technology/2022/apr/27/remote-worksoftware-home-surveillance-computer-monitoring-pandemic>. Acesso em: 18 abr. 2025.

31. MUNN, Luke. Expansive and Invasive: Mapping the “Bossware” used to monitor workers. *Surveillance & Society*, n. 22, v. 2, p. 104-119. Disponível em: <https://ojs.library.queensu.ca/index.php/surveillance-and-society/index>. Acesso em: 18 abr. 2025.

Nessa toada, considerando que sistemas de IA são treinados e alimentados com dados, deve haver um cuidado em relação às limitações da ferramenta e à qualidade das informações inseridas no banco dos sistemas, para que não ocorra um incentivo à criação de padrões enviesados e discriminatórios durante a utilização dos sistemas³². Ademais, a análise realizada pela IA relaciona-se a dados históricos, que podem carregar consigo padrões e vieses correspondentes à época em que foram gerados, influenciando na análise final e não atendendo ao princípio da não-discriminação.

Ressalta-se que, sendo a relação de trabalho assimétrica, em que o polo contratado está em posição de vulnerabilidade em relação ao contratante, cumpre destacar o protagonismo que o conceito de gestão algorítmica tem tomado. Definida como o fenômeno que utiliza diferentes procedimentos algorítmicos para gerenciar o trabalho nas corporações, através da coleta e armazenamento de informações para posterior análise, capazes de alterar a estrutura organizacional e as condições de trabalho existentes³³, a gestão algorítmica ressalta as assimetrias existentes, ao reforçar uma estrutura de concentração de poder e pouca transparência nas mãos do empregador, podendo reforçar a ocorrência de impactos discriminatórios.

Apesar de ser mais comum sua análise no contexto de trabalho de plataformas, a OIT esclarece que, diante de uma sociedade cada vez mais digital, bem como a ocorrência da pandemia de Covid-19, a gestão algorítmica também passou a ocorrer em contextos de trabalho mais tradicionais, sendo implementada a partir de estruturas de organização já consolidadas³⁴.

O controle e monitoramento do trabalhador por meio de algoritmos devem ser analisados com cautela, uma vez que a gestão algorítmica pode abarcar questões relacionadas a planejamento, controle, comando e coordenação de atividades laborais, impactando diretamente na concepção tradicional de relação de trabalho. Sua implementação pode contar com a combinação de diferentes ferramentas tecnológicas, como *big data*, *machine learning*, monitoramento por geolocalização, e utilização de *wearables* para coleta de métri-

32. KORKMAZ, Maria Regina Rigolon. *Decisões automatizadas: explicação, revisão e proteção na era da inteligência artificial*. São Paulo: Thomson Reuters Brasil, 2023.

33. ADAMS-PRASSL, Jeremias. What if your boss was an algorithm? The rise of Artificial Intelligence at Work. *Comparative Labor Law & Policy Journal* 123. vol. 41, p. 1-30. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3661151. Acesso em: 18 jan. 2025.

34. INTERNATIONAL LABOUR ORGANIZATION. *World employment and social outlook: The role of digital labour the world of work*. [s.l.: s.n.]. Disponível em: <https://www.ilo.org/publications/flagship-reports/role-digital-labour-platforms-transforming-world-work>. Acesso em: 05 out. 2024.

cas, automatizando ou auxiliando na atividade humana de monitoramento e processos decisórios³⁵.

A implementação de tecnologias nesse cenário pode ensejar em uma larga coleta de dados pessoais e informações referentes à privacidade do indivíduo, que quando interpretados de maneira equivocada podem viabilizar a ocorrência de vieses discriminatórios de diferentes naturezas – relacionados ao gênero, raça e faixa etária, por exemplo –, colocando em risco o bem-estar do trabalhador no ambiente laboral e a proteção de seus direitos.

Diante disso, é importante salientar que o direito ao trabalho deve ser efetivado a todos os seres humanos, sem qualquer distinção³⁶, englobando os contextos de contratação, a manutenção do emprego e o oferecimento de condições de trabalho dignas. No Brasil, a Constituição Federal de 1988 tem como alguns de seus princípios a igualdade (art. 5º) e a não discriminação dos cidadãos (art. 3º). Ainda, a Lei n.º 9.029/1995³⁷ trata especificamente da vedação de práticas discriminatórias de acesso ao trabalho ou manutenção nele em decorrência de questões relacionadas a estado civil, cor, deficiência e demais questões que são alvo de discriminação.

Nesse ínterim, algumas medidas são necessárias para estabelecer direitos dos trabalhadores em um contexto de uso de IA, como a transparência acerca da coleta e análise de dados, a efetivação do direito à revisão de decisões automatizadas³⁸, bem como a criação de mecanismos que promovam a autodeterminação dos trabalhadores, a fim de evitar que o gerenciamento seja utilizado de maneira abusiva³⁹. Assim, cumpre analisar, na próxima seção, boas práticas de governança corporativa para a manutenção de um trabalho humano digno e com proteção de direitos, diante de um cenário de acelerada inovação e ainda pouca regulação da IA.

35. BAIocco, Sara; FERNANDEZ-MACÍAS, Enrique; RANI, Uma; PESOLE, Annarosa. The Algorithmic Management of work and its implications in different contexts. Background paper n. 9. *International Labour Organization*, 2022. Disponível em: <https://www.ilo.org/publications/algorithmic-management-work-and-its-implications-different-contexts>. Acesso em: 02 out. 2024.

36. É feita referência à Convenção n.º 111 da Organização Internacional do Trabalho (OIT), que dispõe da discriminação decorrente de relações de emprego e profissão. In: BRASIL. *Decreto-Lei nº 10.088, de 5 de novembro de 2019*. Consolida atos normativos editados pelo Poder Executivo Federal que dispõem sobre a promulgação de convenções e recomendações da Organização Internacional do Trabalho – OIT ratificadas pela República Federativa do Brasil. OIT. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10088.htm#art5. Acesso em: 17 set. 2024.

37. BRASIL. *Lei Federal n.º 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: https://www.planalto.gov.br/ccivil_03/leis/l9029.htm#:~:text=LEI%20N%C2%BA%209.029%2C%20DE%2013, trabalho%2C%20e%20d%C3%A1%20outras%20provid%C3%AAs. Acesso em: 14 set. 2024.

38. Tal disposição já era tratada na Lei n.º 13.709/2018 (LGPD), em seu artigo 20, que dispõe sobre o direito do titular de dados solicitar a revisão de decisões automatizadas, em determinados contextos, inclusive no profissional, caso impacte em seus interesses. BRASIL. *Lei n.º 13.709 de 14 de agosto de 2018*. Lei Geral de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 ago. 2024.

39. BAIocco, Sara; FERNANDEZ-MACÍAS, Enrique; RANI, Uma; PESOLE, Annarosa. The Algorithmic Management of work and its implications in different contexts. Background paper n. 9. *International Labour Organization*, 2022. Disponível em: <https://www.ilo.org/publications/algorithmic-management-work-and-its-implications-different-contexts>. Acesso em: 02 out. 2024.

3. Governança e os possíveis caminhos para mitigação da discriminação algorítmica

Como tratado anteriormente, nos últimos anos as discussões acerca de implementação, regulação e desafios para um uso ético da IA têm aumentado, o que se reflete em um movimento de estabelecimento de legislações e normativas ao longo do mundo. Nesse sentido, no Brasil, a preocupação do legislador com os possíveis riscos advindos do uso de IA é refletida ao longo de todo o PL n.º 2.338/2023, considerando seu texto substitutivo de dezembro de 2024: seu Capítulo III trata das classificações de risco traçadas; o Capítulo IV dispõe sobre as práticas de governança em sistemas de alto risco; e o Capítulo VI busca articular questões relacionadas às boas práticas e governança de forma geral, quando se trata de sistemas de IA.

Considerando a sensibilidade do tema, o legislador classificou, no texto do PL 2.338/2023, sistemas de IA com a finalidade de utilização no contexto laboral como sistemas de alto risco, em seu art. 14, III:

Art. 14 Consideram-se sistemas de inteligência artificial de alto risco aqueles desenvolvidos e utilizados para as seguintes finalidades e nos seguintes contextos: [...] III – recrutamento, triagem, filtragem, avaliação de candidatos, tomadas de decisões sobre promoções ou cessações de relações contratuais de trabalho, repartições de tarefas e controle e avaliação do desempenho e do comportamento das pessoas nas áreas de emprego, gestão de trabalhadores e acesso ao emprego por conta própria. (Brasil, 2024).

A classificação acima colacionada verifica-se como assertiva, por ser um contexto que lida com alto volume de dados pessoais relacionados aos trabalhadores, alguns até sendo dados pessoais sensíveis, que podem fomentar violação de direitos⁴⁰. Sua utilização, portanto, deve ter um rigor maior, a fim de evitar a ocorrência de danos⁴¹.

Ademais, mesmo que o Brasil ainda não possua um marco legal específico sobre a regulação da IA aprovado, não significa que o tema ainda não seja abordado por outras legislações. Neste trabalho, destaca-se a LGPD, que além de determinar o procedimento a ser seguido para um tratamento de dados pessoais efetivo, o *caput* do art. 20 determina que é direito do titular de

40. TEFFÉ, Chiara Spadaccini de. *Dados pessoais sensíveis: qualificação, tratamento e boas práticas*. Indaiatuba: Editora Foco, 2022.

41. FRAZÃO, Ana. Por que regular a inteligência artificial? Reflexões sobre os riscos e as incertezas inerentes à utilização da tecnologia. In: Cueva et al (Orgs.). *Direitos Fundamentais e Novas Tecnologias – Homenagem ao Professor Danilo Doneda*. Rio de Janeiro, RJ: Editora GZ, 2024, p. 3-26.

dados poder solicitar a revisão de decisões automatizadas, quando forem tomadas com base no tratamento de seus dados pessoais e que impactem seus interesses, dentre outras finalidades, na definição de perfil de natureza pessoal ou profissional⁴².

Considerando o exposto, também é feita referência às disposições trazidas pela ISO 38.507/2023⁴³, publicada pela Associação Brasileira de Normas Técnicas (ABNT) em outubro de 2023 acerca da governança eficaz da Inteligência Artificial. O documento trata da importância da utilização de IA de forma responsável, devendo sempre ocorrer a verificação de riscos e os parâmetros éticos por parte do órgão diretivo da organização que utiliza ou dará início ao uso de IA destacando questões como oportunidades, riscos e responsabilidades nessa prática. O objetivo, portanto, é que seja mantida a estratégia de alcance dos objetivos da organização de forma eficaz, bem como das partes relacionadas.

Destaca-se, também, a alínea “c” do item 2.4. “Desenvolver capacidades humanas e preparar-se para a transformação do mercado de trabalho”, disposto no documento de princípios orientadores da OCDE – *Recommendation of the Council on OECD Legal Instruments Artificial Intelligence*⁴⁴ –, atualizado em 2024, que menciona de forma direta a necessidade de articulação conjunta de diferentes sujeitos para a estruturação de diretrizes que, além de trabalhar em um uso ético e responsável da IA em contextos laborais, também faça do ambiente de trabalho um local seguro. Tal recomendação reforça a importância de debate acerca do tema, visto que é um documento de natureza internacional. Ao ensejo:

c) Os governos também devem trabalhar em estreita colaboração com as partes interessadas para promover o uso responsável da IA no trabalho, melhorar a segurança dos trabalhadores, a qualidade dos empregos e dos serviços públicos, fomentar o empreendedorismo e a produtividade e garantir que os benefícios da IA sejam compartilhados de forma ampla e justa.

42. Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. BRASIL. *Lei n.º 13.709 de 14 de agosto de 2018*. Lei Geral de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 ago. 2024.

43. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC TR 38507: Tecnologia da informação — Governança de TI — Implicações de governança do uso de inteligência artificial pelas organizações. ABNT, 2023. Disponível em: <https://www.abntcolecao.com.br/colecao.aspx>. Acesso em: 15 dez. 2024.

44. No original: 2.4. *Building human capacity and preparing for labour market transformation (...)* c) Governments should also work closely with stakeholders to promote the responsible use of AI at work, to enhance the safety of workers, the quality of jobs and of public services, to foster entrepreneurship and productivity, and aim to ensure that the benefits from AI are broadly and fairly shared. In: ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Recommendation of the Council on Artificial Intelligence. OECD Legal Instruments*. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. Acesso em: 16 abr. 2025, p. 10 (tradução livre).

Assim, é crucial que o PL n.º 2.338/2023 seja articulado com outras legislações, como a LGPD e a Constituição Federal, não sendo possível assumir que apenas um documento seja capaz de atender a demandas de garantias e proteção em um tema de tamanha importância. Ainda, diante da existência de normativas não vinculantes aplicáveis ao tema, bem como a importância de um ecossistema de governança, destaca-se a relevância de regulação e autorregulação atuarem de forma complementar. Verifica-se, portanto, que a construção de uma estrutura de governança eficaz demanda uma análise multissetorial acerca do caso⁴⁵.

Ainda, em relação a questões mais técnicas, deve-se ter cuidado com a criação, treinamento e utilização de sistemas de IA em contextos de alto risco, uma vez que são pautados em dados, e não realizam diferenciações em relação à sua qualidade ou correlações com questões externas ao banco de dados com que são alimentados, mas sim sobre os objetivos para os quais foram desenvolvidos. Estabelecer e cumprir com um protocolo de monitoramento e reparo é importante para garantir seu bom funcionamento, evitando o estabelecimento de vies indesejado. Nesse sentido, Chiara de Teffé⁴⁶ dispõe que:

Para que os algoritmos sejam justos, é preciso fiscalizá-los, repará-los e aprimorá-los. Dessa forma, além de se ter uma regulamentação adequada, que privilegie a transparência e a explicação quanto às decisões algorítmicas, o princípio da não discriminação deve estar presente desde a concepção dos sistemas de inteligência artificial – tanto na parte técnica dessa construção quanto na garantia da diversidade dos times responsáveis pelo desenvolvimento dos algoritmos –, sendo aplicado em todo o ciclo de vida desses sistemas.

Nesse sentido, no âmbito de governança⁴⁷, a corporação deve ter um programa que seja de fato eficaz, e que sua implementação garanta a prote-

45. TEFFÉ, Chiara Spadaccini; MEDON, Filipe. A utilização de inteligência artificial em decisões empresariais: notas introdutórias acerca da responsabilidade civil dos administradores. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Coord.). *Inteligência artificial e direito: ética, regulação e responsabilidade*. Editora Revista dos Tribunais, 2019.

46. TEFFÉ, Chiara Spadaccini de. *Dados pessoais sensíveis: qualificação, tratamento e boas práticas*. Indaiatuba: Editora Foco, 2022. p.29.

47. O conceito de governança corporativa encontra-se estabelecido pelo Instituto Brasileiro de Governança Corporativa (IBGC) como “o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. As boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico ao longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum”. In: INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. *Código das melhores práticas de governança corporativa*. 5 ed. São Paulo: IBGC, 2015, p. 20.

ção dos direitos do trabalhador. Um programa pautado em práticas de *ethics bluewashing*⁴⁸, somente para atender a requisitos do mercado, cria um cenário de insegurança jurídica sobre o funcionamento dos sistemas e o impacto de fato gerado aos afetados, e aumenta ainda mais a relação assimétrica entre empregado e empregador. Nesse sentido, deve-se observar um alinhamento de interesses da empresa, pautada predominantemente por questões econômicas, com questões de cunho social, por parte dos trabalhadores⁴⁹.

Por fim, cumpre ressaltar que as práticas de governança e a regulação de utilização da IA não devem ser traduzidas como freios à inovação e desenvolvimento empresarial, mas sim como uma busca pelo equilíbrio entre proteção de direitos e desenvolvimento. Conforme disposto por Ana Frazão⁵⁰:

É preciso entender que a tecnologia não é neutra nem necessariamente boa. Tudo depende de como ela é utilizada e de como são administrados determinados conflitos, tais como o existente entre inovação e proteção de direitos fundamentais. (...) o maior problema dos tempos atuais é que a tecnologia, incluindo a inteligência artificial, tem sido escolhida e colocada em uso sem os devidos cuidados e muitas vezes sem nenhum tipo de *accountability*, por agentes econômicos que priorizam seus interesses em detrimento dos consumidores, da sociedade e da própria democracia.

Considerações finais

Diante do exposto, o presente artigo teve como objetivo demonstrar, que a utilização de IA no cenário corporativo apresenta desafios e riscos que devem ser observados de forma atenta, especialmente quando se trata de sua utilização no contexto de relações de trabalho.

Apesar de a aplicação de sistemas de IA no âmbito corporativo ter o objetivo de auxiliar no aumento de produtividade e redução de custos da empresa

48. Segundo Luciano Floridi (tradução livre): “A má prática em realizar alegações infundadas ou enganosas sobre, ou implementar medidas superficiais em nome dos valores éticos e benefícios de processos digitais, produtos, serviços ou outras soluções, visando parecer mais ético digitalmente do que na realidade é”. No original: “*Ethics bluewashing = def. the malpractice of making unsubstantiated or misleading claims about, or implementing superficial measures in favour of, the ethical values and benefits of digital processes, products, services, or other solutions in order to appear more digitally ethical than one is*”. In: FLORIDI, Luciano. Translating Principles into Practices of Digital Ethics: five risks of being unethical. *Philosophy & Technology*, v. 32, n. 2, p. 185-193, 23 mai. 2019. Springer Science and Business Media LLC. Disponível em: <https://doi.org/10.1007/s13347-019-00354-x>. Acesso em: 31 ago. 2024.

49. ARTUR, Karen. Compliance trabalhista: entre o comportamento e as instituições. In: PINHEIRO, Caroline da Rosa (org.). *Compliance: entre a teoria e a prática. Reflexões contemporâneas e análise dos programas de integridade das companhias listadas no Novo Mercado*. 1 ed. São Paulo: Foco, 2022, p.119-125.

50. FRAZÃO, Ana. Por que regular a inteligência artificial? Reflexões sobre os riscos e as incertezas inerentes à utilização da tecnologia. In: Cueva et al (Orgs.). *Direitos Fundamentais e Novas Tecnologias – Homenagem ao Professor Danilo Doneda*. Rio de Janeiro, RJ: Editora GZ, 2024, p. 5.

em suas operações, sendo objetivos legítimos considerando a competitividade empresarial, é importante ter atenção a intercorrências que a utilização dessa tecnologia pode gerar, como cenários de discriminação de trabalhadores da corporação⁵¹.

A gestão algorítmica, por inserir tecnologias no contexto laboral para reduzir custos operacionais e aumentar eficiência da empresa no mercado diante de maior controle, previsibilidade e monitoramento, deve ser alvo de uma análise cautelosa, uma vez que o exercício dessa supervisão depende de uma análise ampla de dados coletados dos trabalhadores, que nem sempre estão cientes de todos os processos aos quais são submetidos.

Outra ponderação importante a ser feita é a de que algoritmos não possuem a mesma habilidade que os seres humanos em estabelecer determinadas correlações, como levar em conta valores e características da corporação em uma tomada de decisão, ponderando os dados aos quais possuem acesso. A análise de um sistema de IA considera os *outputs* e *inputs* que recebe, bem como sua base de dados, não atingindo o mesmo patamar que a inteligência humana. Ainda, os vieses discriminatórios podem decorrer tanto de cruzamentos de dados não previstos anteriormente, quanto em decorrência do “retrato” da sociedade em que as informações foram geradas ou ponto de vista de seus programadores.

Dessa forma, é importante que boas práticas que promovam a proteção de direitos e uma utilização ética de IA sejam implementadas pelas corporações, como a realização de auditorias algorítmicas periódicas dos sistemas para correção e monitoramento de vieses, elaboração de relatórios de impacto e códigos de ética, a fim de trazer maior transparência aos indivíduos que podem ser afetados pela tecnologia, contínua supervisão humana do funcionamento de sistemas de IA e medidas que assegurem aos trabalhadores transparência e direito à explicação em tomadas de decisão realizadas de forma automatizada.

Ademais, a definição tradicional de governança corporativa precisa ser revisitada constantemente, diante do cenário de crescente aprimoramento da IA enquanto ferramenta disruptiva, para que se mantenha alinhada às necessidades do momento presente, e seja de fato uma ferramenta importante para a efetivação de direitos.

51. MATIAS, João Luís Nogueira. MORAIS JÚNIOR, Ricardo Antônio Maia de. Discriminação Algorítmica na relação de emprego: eficiência econômica, inteligência artificial e fragilidade do empregado. *Revista TST*, vol. 90, n. 2, p. 128-147, abr./jun. 2024. Disponível em: <https://revista.tst.jus.br/rtst/article/view/67/80>. Acesso em: 12 nov. 2024.

Por fim, ressalta-se a importância da regulação da IA, que não deve ser entendida como uma tentativa de restringir a inovação, mas uma medida promotora de equilíbrio entre desenvolvimento e proteção de direitos e garantias fundamentais. Dessa maneira, autorregulação e regulação (considerando tanto a de IA, em tramitação, quanto as legislações de cunho trabalhista e demais aplicáveis já em vigor) devem atuar de forma conjunta, uma vez que a autorregulação, por si só, encontra limites de eficácia, visto que em um contexto corporativo, principalmente quando se analisam relações de trabalho, há uma relação assimétrica, não só informacional quanto de poder, que pode trazer insegurança diante da existência de distintos interesses, que podem entrar em conflito.

O objetivo final, portanto, é que a governança corporativa de uma empresa seja estabelecida de forma eficaz e funcional, colaborando para um cenário de trabalho digno e respeitoso, bem como sejam evitados cenários de discriminação e violação de direitos por parte de sistemas de IA.

Referências

ABRUSIO, Juliana; ARAUJO, André Eduardo Dorster. Inteligência artificial: decisões automatizadas e discriminação nas relações de trabalho. *Revista de Direito do Trabalho e Seguridade Social*. vol. 223. ano 48. p. 321-343. São Paulo: Ed. RT, mai./jun. 2022. Disponível em: <http://revistadostribunais.com.br/maf/app/document?stid=st-rql&marg=DTR-2022-9190>. Acesso em: 20 ago. 2024.

ADAMS-PRASSL, Jeremias. What if your boss was an algorithm? The rise of Artificial Intelligence at. Work. *Comparative Labor Law & Policy Journal* 123. vol. 41, p. 1-30. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3661151. Acesso em: 18 jan. 2025.

ADAMS-PRASSL, Jeremias. Gestão Algorítmica e o Futuro do Trabalho. In: *Futuro do Trabalho: os efeitos da revolução digital na sociedade*. CARELLI, Rodrigo de Lacerda; CAVALCANTI, Tiago Muniz; FONSECA, Vanessa Patriota da (org.). Brasília: ESMPU, 2020. Disponível em: https://escola.mpu.mp.br/publicacoes/obras-avulsas/e-books-esmpu/futuro-do-trabalho-os-efeitos-da-revolucao-digital-na-sociedade/@@download/arquivo/Livro_Futuro+do+Trabalho.pdf. Acesso em: 07 out. 2024.

ALGORITHMIC management in the workplace. *International Labour Organization*. Disponível em: <https://www.ilo.org/algorithmic-management-workplace>. Acesso em: 17 abr. 2025.

ARTUR, Karen. Compliance trabalhista: entre o comportamento e as instituições. In: PINHEIRO, Caroline da Rosa (org.). *Compliance: entre a teoria e a prática. Reflexões contemporâneas e análise dos programas de integridade das companhias listadas no Novo Mercado*. 1 ed. São Paulo: Foco, 2022, p.119-125.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC TR 38507: Tecnologia da informação – Governança de TI – Implicações de governança do uso de inteligência artificial pelas organizações*. ABNT, 2023. Disponível em: <https://www.abntcolecao.com.br/colecao.aspx>. Acesso em: 15 dez. 2024.

BAIOCCO, Sara; FERNANDEZ-MACÍAS, Enrique; RANI, Uma; PESOLE, Annarosa. The Algorithmic Management of work and its implications in different contexts. Background paper n. 9. *International Labour Organization*, 2022. Disponível em: <https://www.ilo.org/publications/algorithmic-management-work-and-its-implications-different-contexts>. Acesso em: 02 out. 2024.

BARBOSA, Leonardo Figueiredo; PINHEIRO, Caroline da Rosa. Inteligência artificial no Brasil: avanços regulatórios. *Revista de Informação Legislativa: RIL*, Brasília, DF, v. 60, n. 240, p. 11– 41, out./dez. 2023. Disponível em: https://www12.senado.leg.br/ril/edicoes/60/240/v60_n240_p11. Acesso em: 06 set. 2024.

BOSSWARE is coming for almost every worker: the software you might not realize is watching you. *The Guardian*. Disponível em: <https://www.theguardian.com/technology/2022/apr/27/remote-worksoftware-home-surveillance-computer-monitoring-pandemic>. Acesso em: 18 abr. 2025.

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: 12 ago. 2024.

BRASIL. *Lei n.º 13.709 de 14 de agosto de 2018*. Lei Geral de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 ago. 2024.

BRASIL. *Lei Federal n.º 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: https://www.planalto.gov.br/ccivil_03/leis/l9029.htm#:~:text=LEI%20N%C2%BA%209.029%2C%20DE%2013,trabalho%2C%20e%20d%C3%A1%20outras%20provid%C3%Aancias. Acesso em: 14 set. 2024.

BRASIL. *Decreto-Lei n.º 10.088, de 5 de novembro de 2019*. Consolida atos normativos editados pelo Poder Executivo Federal que dispõem sobre a promulgação de convenções e recomendações da Organização Internacional do Trabalho – OIT ratificadas pela República Federativa do Brasil. OIT. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10088.htm#art5. Acesso em: 17 set. 2024.

BRASIL. Senado Federal. *Projeto de Lei n.º 2.338, de 2023. Dispõe sobre o uso da Inteligência Artificial*. Brasília, DF: Congresso Nacional. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 11 dez. 2024.

CHIU, Iris H.-Y.; LIM, Ernest WK. Technology vs ideology: how far will artificial intelligence and distributed ledger technology transform corporate governance and business?. *Berkeley Bus. LJ*, v. 18, p. 1-18, 11 nov. 2020. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3695006. Acesso em: 17 ago. 2024.

DE STEFANO, Valerio. Automação, inteligência artificial e proteção laboral: padrões algorítmicos e o que fazer com eles. In: *Futuro do Trabalho: os efeitos da revolução digital na sociedade*. CARELLI, Rodrigo de Lacerda; CAVALCANTI, Tiago Muniz; FONSECA, Vanessa Patriota da (org.). Brasília: ESMPU, 2020. Disponível em: https://escola.mpu.mp.br/publicacoes/obras-avulsas/e-books-esmpu/futuro-do-trabalho-os-efeitos-da-revolucao-digital-na-sociedade/@@download/arquivo/Livro_Futuro+do+Trabalho.pdf. Acesso em: 07 out. 2024.

FLORIDI L. Soft ethics, the governance of the digital and the General Data Protection Regulation. *Phil. Trans. R. Soc.* 2018. Disponível em: <http://dx.doi.org/10.1098/rsta.2018.0081>. Acesso em: 28 ago. 2024.

FLORIDI, Luciano. Translating Principles into Practices of Digital Ethics: five risks of being unethical. *Philosophy & Technology*, v. 32, n. 2, p. 185-193, 23 mai. 2019. *Springer Science and Business Media LLC*. Disponível em: <https://doi.org/10.1007/s13347-019-00354-x>. Acesso em: 31 ago. 2024.

FONSECA, Bruno Blum. Inteligência artificial e a proteção dos dados pessoais no recrutamento de trabalhadores: desafios e perspectivas. In: BRANCO, Sérgio; TEFFÉ, Chiara Spadaccini de (Coords.). *Regulação digital: Perspectivas Jurídicas sobre Tecnologia e Sociedade*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2024, p. 299-319. Disponível em: <https://itsrio.org/pt/publicacoes/regulacao-digital-dialogos-da-pos-graduacao-em-direito-digital/>. Acesso em: 23 ago. 2024.

FRAZÃO, Ana; GOETTENAUER, Carlos. Black box e o direito face à opacidade algorítmica. In: BARBOSA, Mafalda Miranda; NETTO, Felipe Braga; SILVA, Michael César; FALEIROS JÚNIOR, José Luiz de Moura (Coords.). *Direito digital e inteligência artificial: diálogos entre Brasil e Europa*. Indaiatuba, SP: Editora Foco, 2021, p. 27-42. Disponível em: https://www.academia.edu/45811453/Black_Box_e_o_direito_face_%C3%A0_opacidade_algor%C3%ADmica. Acesso em: 25 out. 2024.

FRAZÃO, Ana. Por que regular a inteligência artificial? Reflexões sobre os riscos e as incertezas inerentes à utilização da tecnologia. In: Cueva *et al* (Orgs.). *Direitos Fundamentais e Novas Tecnologias – Homenagem ao Professor Danilo Doneda*. Rio de Janeiro, RJ: Editora GZ, 2024, p. 3-26.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. *Código das melhores práticas de governança corporativa*. 5 ed. São Paulo: IBGC, 2015, p. 20.

INTERNATIONAL LABOUR ORGANIZATION. *World employment and social outlook: The role of digital labour in the world of work*. [s.l.: s.n.]. Disponível em: <https://www.ilo.org/publications/flagship-reports/role-digital-labour-platforms-transforming-world-work>. Acesso em: 05 out. 2024.

KORKMAZ, Maria Regina Rigolon. *Decisões automatizadas: explicação, revisão e proteção na era da inteligência artificial*. São Paulo: Thomson Reuters Brasil, 2023.

MATIAS, João Luís Nogueira. MORAIS JÚNIOR, Ricardo Antônio Maia de. Discriminação Algorítmica na relação de emprego: eficiência econômica, inteligência artificial e fragilidade do empregado. *Revista TST*, vol. 90, n. 2, p. 128-147, abr./jun. 2024. Disponível em: <https://revista.tst.jus.br/rtst/article/view/67/80>. Acesso em: 12 nov. 2024.

MUNN, Luke. Expansive and Invasive: Mapping the “Bossware” used to monitor workers. *Surveillance & Society*, n. 22, v. 2, p. 104-119. Disponível em: <https://ojs.library.queensu.ca/index.php/surveillance-and-society/index>. Acesso em: 18 abr. 2025.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Recommendation of the Council on Artificial Intelligence. OECD Legal Instruments*. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. Acesso em: 16 abr. 2025, p. 10.

PINHEIRO, Caroline da Rosa. BREGA, Gabriel Ribeiro. Inteligência Artificial e *Compliance* – a (in)suficiência dos marcos de proteção de dados. *Revista Semestral de Direito Empresarial*, n. 28, p. 161-196, jan./jun. 2021. Disponível em: <https://rsde.com.br/artigos/inteligencia-artificial-e-compliance-a-insuficiencia-dos-marcos-de-protecao-de-dados/>. Acesso em: 17 out. 2024.

PINHEIRO, Caroline da Rosa. ROCHA, Matheus Mazzoni. DEL LHANO, Larissa Almeida. Governança e Inteligência Artificial: (in)certezas sobre substituição humana nos conselhos de administração. *Anais do XIII Encontro Internacional do Conpedi Uruguai – Montevideu. Governo Digital, Direito e Novas Tecnologias I*, p. 4-25. Disponível em: <http://site.conpedi.org.br/publicacoes/351f5k20/nhf03e63/LWCi1rkteY4fOjiA.pdf>. Acesso em: 06 out. 2024.

PIRES, Thatiane Cristina Fontão; SILVA, Rafael Peteffi da. A responsabilidade civil pelos atos autônomos da inteligência artificial: notas iniciais sobre a resolução do Parlamento Europeu. *Rev. Bras. Polít. Públicas*, Brasília, v. 7, nº 3, 2017 p. 238-254. Disponível em: <https://www.arqcom.uniceub.br/RBPP/article/viewFile/4951/3643>. Acesso em: 10 dez. 2024.

PORTUGAL GOUVÊA, Carlos. *A Estrutura da Governança Corporativa*. São Paulo: Quartier Latin, 2022.

REQUIÃO, Maurício. COSTA, Diego Carneiro. Discriminação Algorítmica: ações afirmativas como estratégia de combate. *Civilistica.com*, a. 11, n. 3, 2022. Disponível em: <http://civilistica.com/discriminacao-algoritmica/>. Acesso em: 03 jan. 2025.

RODOTÀ, Stefano. *A vida na sociedade da vigilância – a privacidade hoje*. Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano. *Il mondo nella rete: Quali i diritti, quali i vincoli*. Roma: Laterza & Figli – Gruppo Editoriale L'Espresso, 2019.

SANTOS, Rodrigo Coimbra. GRAMINHO, Vivian Maria Caxambu. Discriminação algorítmica nas relações de trabalho e princípio da Lei Geral de Proteção de Dados. *Sequência*, v. 45, n. 96, p. 1-31, 2024. Disponível em: <https://www.scielo.br/j/seq/a/9FGhvr75HYSdGMRfKnJ9FZd/?format=pdf&lang=pt>. Acesso em: 02 jan. 2025.

SCHWAB, Klaus. *A Quarta Revolução Industrial*. 1 ed. São Paulo: Edipro, 2016.

TEFFÉ, Chiara Spadaccini de; MEDON, Filipe. A utilização de inteligência artificial em decisões empresariais: notas introdutórias acerca da responsabilidade civil dos administradores. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Coord.). *Inteligência artificial e direito: ética, regulação e responsabilidade*. Editora Revista dos Tribunais, 2019.

TEFFÉ, Chiara Spadaccini de. *Dados pessoais sensíveis: qualificação, tratamento e boas práticas*. Indaiatuba: Editora Foco, 2022.

VIEIRA, Gustavo Duarte. *Proteção de dados pessoais em práticas de profiling no setor privado*. Dissertação (Mestrado em Direito) – Faculdade de Direito da Universidade Federal de Minas Gerais. Belo Horizonte, 2019. Disponível em: <http://hdl.handle.net/1843/34072>. Acesso em: 10 out. 2024.

ZUBOFF, Shoshana. *The age of Surveillance Capitalism: the fight for a human future at the new frontier of power*. Nova Iorque: Public Affairs, 2019.

IA Generativa e tratamento de dados pessoais: uso do legítimo interesse para o tratamento de imagens para treinamento de IA generativa – o caso Meta

DANIELE DIMAS RAMOS GARUTI

Sumário: Introdução. 1. Lei Geral de Proteção de Dados. 1.1. Bases legais para o tratamento de dados pessoais – legítimo interesse. 2. Inteligência Artificial Generativa. 3. Legítimo interesse como base legal para o tratamento de imagens para treinamento de IA Generativa. 4. Avaliação da decisão da ANPD sobre a base legal utilizada pelo Facebook. Considerações finais. Referências.

Introdução

Sabemos que a Inteligência Artificial Generativa é uma tecnologia que está trazendo diversas facilidades para o dia a dia, para o trabalho e até para o lazer daqueles que se utilizam do ambiente da internet. Entretanto, é importante considerar que para que a tecnologia possa funcionar, é necessário o treinamento dela com diversos dados reais retirados da internet.

Neste sentido, quando tal treinamento envolve a utilização de imagens/fotografias publicamente disponibilizadas online torna-se imprescindível considerarmos a forma como tais imagens estão sendo tratadas no âmbito de tal treinamento, bem como qual o nível de proteção deve ser aplicado a elas. Por serem imagens que possivelmente possuem a representação física de um indivíduo, seu tratamento deverá ser realizado em observância aos princípios e exigências da Lei Geral de Proteção de Dados – LGPD, por se tratarem de dados pessoais, entre elas a utilização de uma hipótese legal legítima para seu tratamento.

O presente estudo tem como objetivo avaliar se é juridicamente aceitável o uso da base legal do legítimo interesse para o tratamento de imagens coletadas a partir das redes sociais Facebook e Instagram para fins de treinamento da Inteligência Artificial Generativa da Meta (antigo Facebook), tendo como base a análise de Notas Técnicas publicadas pela Autoridade Nacional de Proteção de Dados em que a autoridade avalia a política de privacidade da Meta e o tratamento de dados pessoais contidos em imagens/fotografias realizado pela empresa em relação à sua Inteligência Artificial Generativa, avaliando se tais imagens devem ser consideradas dados pessoais sensíveis e tendo em vista as restrições aplicadas ao tratamento de dados pessoais sensíveis de acordo com a LGPD.

Foram avaliados, portanto, os tipos de dados coletados pela Meta para o treinamento de sua Inteligência Artificial Generativa, bem como qual a finali-

1. Advogada. Graduada em Direito pela Universidade Presbiteriana Mackenzie e pós-graduanda em Direito Digital pelo Instituto de Tecnologia e Sociedade (ITS-RJ) em parceria com a Universidade do Estado do Rio de Janeiro. Atua na área de Propriedade Intelectual, Tecnologia da Informação e Proteção de Dados pelo escritório Trench Rossi Watanabe.

dade de sua utilização durante o treinamento indicado, além de avaliarmos a possibilidade de inferência de dados pessoais sensíveis a partir dos dados coletados para, então ser verificada a legalidade da utilização da base legal do legítimo interesse para justificar o tratamento de dados pessoais decorrentes do treinamento.

1. Lei Geral de Proteção de Dados

Em pleno século XXI, em um ambiente cada vez mais tecnológico e digital em que os dados dos indivíduos estão cada vez mais disponíveis e públicos, tornou-se imprescindível abordar questões de privacidade e proteção de dados.

Conforme devidamente apontado por Doneda, “a privacidade está fortemente ligada à personalidade e ao seu desenvolvimento, para o qual é elemento essencial, em uma complexa teia de relações ainda a ser completamente vislumbrada pelo direito e pelas ciências sociais.”²

A legislação brasileira, comumente chamada de Lei Geral de Proteção de Dados, a Lei nº 13.709/2018, ou “LGPD”, que regula o tratamento de dados pessoais de pessoas físicas, coletados física ou digitalmente, entrou em vigor em 2020. A LGPD tem por objetivo proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural.³

Neste sentido, a LGPD estabelece diversos princípios que devem ser observados durante o tratamento de dados pessoais, entre eles, os princípios da necessidade, da adequação e da transparência, que devem ser sempre levados em consideração. Dessa forma, o tratamento de dados pessoais deverá ser realizado limitando-se aos dados mínimos necessários para a realização de suas finalidades, não utilizando-se dados além daqueles proporcionais à finalidade do tratamento (necessidade); em compatibilidade com as finalidades informadas ao titular (adequação); e garantindo aos titulares informações claras e precisas sobre as atividades realizadas (transparência).

Além disso, a LGPD define também diversas situações, bases legais, em que empresas ou indivíduos (controladores, conforme definição legal), podem legalmente tratar dados pessoais, das quais falaremos um pouco adiante.

2. DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. Thomson Reuters, 2021.

3. BRASIL. *Lei Federal nº 13.709/2018 (LGPD)*. Brasília, 2018.

1.1 Bases legais para o tratamento de dados pessoais – legítimo interesse

Conforme mencionado acima, a LGPD estabeleceu diversas hipóteses para as quais os agentes de tratamento estariam autorizados a tratar dados pessoais durante suas operações. Além disso, a legislação brasileira também estabeleceu que, a depender do nível de discriminação que um determinado dado pessoal poderia causar ao ser tratado de maneira indevida, tal dado pessoal deveria ter um tratamento mais rigoroso.

Dessa forma, a LGPD estabeleceu bases legais diversas para os dois tipos de dados pessoais definidos em sua redação: dados pessoais e dados pessoais sensíveis.

De acordo com a legislação, dado pessoal representa “informação relacionada a pessoa natural identificada ou identificável”⁴. Já dados pessoais sensíveis são definidos como 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”.⁵

Neste sentido, e conforme mencionado acima, o legislador entendeu por certo adotar hipóteses legais distintas para dados pessoais⁶ e dados pessoais sensíveis⁷ sob as quais os controladores de dados pudessem basear suas operações de tratamento de dados pessoais.

4. BRASIL. *Lei Federal nº 13.709/2018 (LGPD)*. Brasília, 2018.

5. BRASIL. *Lei Federal nº 13.709/2018 (LGPD)*. Brasília, 2018.

6. 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. BRASIL. *Lei Federal nº 13.709/2018 (LGPD)*. Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 08 de janeiro de 2025.

7. 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. BRASIL. *Lei Federal nº 13.709/2018 (LGPD)*. Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 08 de janeiro de 2025.

Em sua maioria, as bases legais para ambas as modalidades de dados pessoais descritas na legislação são equivalentes entre si, porém, destacamos que, ao determinar as hipóteses em que dados pessoais sensíveis poderiam ser tratados de forma legal pelos controladores, o legislador não incluiu o legítimo interesse como uma opção aplicável.

Em linhas gerais, o legítimo interesse pode ser entendido como “a autorização para que o intérprete avalie (pondere) no caso concreto os direitos e valores em jogo para, ao final, concluir pela possibilidade de tratamento de dados sem o consentimento do titular”⁸.

Ainda, conforme descrito por Oliveira e Cots, no âmbito do tratamento de dados pessoais entende-se por “interesse” aquilo que é importante ou desejável pelo controlador, enquanto “legítimo” é entendido como a característica de ser o interesse justificado ou amparado pelo bom senso ou pela lei.⁹

Portanto, para avaliarmos se o legítimo interesse está presente em uma relação, é necessário avaliar se o tratamento dos dados pessoais proposto é relevante para uma determinada atividade e justificado em relação ao controlador.

Dessa forma, por se tratar de uma hipótese em que o controlador (intérprete) possui maior liberdade de interpretação, o legislador entendeu por bem não permitir que o tratamento dos dados pessoais que, em seu entendimento, possuem uma possibilidade maior de acarretar dano ao seu titular em caso de tratamento indevido (dados pessoais sensíveis), pudesse ser baseado em tal hipótese legal, impondo, dessa forma, uma restrição maior ao seu tratamento.

Além disso, de acordo com a Autoridade Nacional de Proteção de Dados (ANPD) o tratamento de dados pessoais utilizando-se da base legal do legítimo interesse deve ser precedido de um teste, chamado de teste de balanceamento, em que se avalia a proporcionalidade entre os interesses do controlador e os impactos e os riscos aos direitos e liberdades dos titulares¹⁰. Dessa forma, é necessário que sejam realizadas determinadas “avaliações sobre os riscos envolvidos no tratamento e que sejam considerados objetivamente quais são os impactos sobre os direitos e liberdades fundamentais dos titulares”¹¹.

8. BESSA, Leonardo. *Privacidade e proteção de dados pessoais: a categorização das bases legais na LGPD. Inteligência Artificial Generativa no Direito*. 5 anos de LGPD. Revista dos Tribunais, 2024.

9. OLIVEIRA, Ricardo; COTS, Márcio. *O Legítimo Interesse*. O Legítimo Interesse e a LGPD. Revista dos Tribunais, 2021. E-book.

10. ANPD. *Guia Orientativo – Hipóteses legais de tratamento de dados pessoais – legítimo interesse*. 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em: 14 abr. 2025.

11. ANPD. *Guia Orientativo – Hipóteses legais de tratamento de dados pessoais – legítimo interesse*. 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em: 14 abr. 2025.

Neste sentido, é necessário, portanto, fazer a seguinte reflexão: por ser uma base legal bastante interpretativa, ou seja, depende de uma análise da relevância do tratamento dos dados pessoais para a realização de uma determinada atividade com uma finalidade específica, esta base legal, especialmente quando utilizada pelas chamadas *big techs*, grandes empresas de tecnologia que possuem determinado controle sobre o mercado, pode gerar uma avaliação deturpada dos princípios anteriormente mencionados e dos riscos envolvidos no tratamento de dados pessoais, uma vez que a avaliação da necessidade e da adequação do tratamento dos dados pessoais se dará por quem é o beneficiário de tal tratamento e não por aqueles que “sofrerão” as consequências de tal atividade.

2. Inteligência Artificial Generativa

Passamos agora a tratar da tecnologia objeto do estudo apresentado no presente artigo, apresentando um resumo para entendimento de sua aplicação para então serem avaliadas as hipóteses de tratamento de dados pessoais envolvidas no treinamento de tal tecnologia.

A Inteligência Artificial Generativa (IA Generativa) é uma tecnologia que tem por objetivo criar novos conteúdos, seja em forma de texto, áudio, imagem ou vídeo, através do aprendizado de máquina. Ou seja, a IA Generativa opera na forma da coleta e tratamento de um grande volume de dados (sejam eles dados pessoais ou não) e utilização de redes neurais artificiais, conhecidas também como *deep learning*, para treinamento de seus sistemas com o objetivo de “aprender” com os padrões e estruturas desses dados.

Com esse “aprendizado” a IA Generativa consegue identificar tais padrões e estruturas e utilizá-los para gerar novos conteúdos, nas mesmas formas mencionadas acima, que se diferem daqueles utilizados para seu treinamento, mas que seguem os mesmos modelos contidos neles.

Dessa forma, as tecnologias de IA Generativa operam capturando características estatísticas dos dados pelos quais foi treinada para criar novos exemplos do conteúdo solicitado que sejam semelhantes aos reais. Isso somente é possível diante do grande volume de dados que é utilizado para seu treinamento, trazendo assim a possibilidade da tecnologia não só classificar informações, mas também criar conteúdo baseado nos modelos contidos em sua base de dados.

Neste sentido, este treinamento realizado para que a IA Generativa possa “aprender” os padrões e estruturas a serem seguidas deve ser realizado com

informações e dados reais, que podem ser obtidos de dados e informações públicas que são disponibilizadas na internet. Este procedimento é chamado de raspagem.

Ocorre que, em se tratando de dados e informações disponíveis publicamente, tais dados e informações podem conter também dados pessoais, conforme definidos anteriormente, e, portanto, a atividade referente à sua utilização para treinamento da IA Generativa, ou seja, a raspagem e treinamento da IA Generativa, deve ser baseada em uma das hipóteses legais para tratamento de dados pessoais estabelecida pela LGPD.

Isso porque, uma imagem/fotografia que permita a identificação de um indivíduo representado nela deve ser considerado um dado pessoal uma vez que identifica ou torna identificável uma determinada pessoa física.

Além disso, em se tratando de imagens que retratam pessoas enquadradas em grupos considerados “minorias”, o tratamento de suas imagens, além de ser considerado um dado pessoal, também poderia, a depender de sua utilização, gerar inferências de dados considerados sensíveis, fazendo com que, portanto, dados inicialmente considerados “comuns” possam ser transformados em dados pessoais sensíveis.

Neste sentido, a Unesco aponta que, por utilizar dados que podem ser considerados pessoais em seu treinamento, a IA Generativa pode acabar por violar leis de proteção de dados, tal como o Regulamento Geral sobre Proteção de Dados (GDPR) da União Europeia, uma vez que, após treinado com tais dados, as informações recebidas pela IA Generativa não podem ser removidas do sistema, ou seja, torna-se impossível que a IA Generativa “esqueça-se” de tais informações.¹²

3. Legítimo interesse como base legal para o tratamento de imagens para treinamento de IA Generativa

Como mencionado acima, entre os dados utilizados pela IA Generativa, é possível identificar a possibilidade de treinamento de tais tecnologias utilizando como base imagens/fotografias publicamente disponíveis na internet.

Ocorre que, por muitas vezes, e como foi o caso da Meta que será discutido mais adiante, o controlador dos dados utiliza-se da base legal do legítimo inte-

12. UNESCO. *Guia para a IA generativa na educação e na pesquisa*. 2024. Disponível em: https://unesdoc.unesco.org/in/documentViewer.xhtml?v=2.1.196&id=p::usmarcdef_0000390241&file=/in/rest/annotationSVC/DownloadWatermarkedAttachment/attach_import_0880195e-d225-4872-bc95-e36b69d17343%3F_%3D390241por.pdf&locale=en&multi=true&ark=/ark:/48223/pf0000390241/PDF/390241por.pdf#509_24_guia_IA_INT_Portuguese.indd%3A.15084%3A2017. Acesso em: 18 abr. 2025.

resse para basear o tratamento de dados pessoais relacionado ao treinamento da base de dados de tecnologias de IA Generativa.

Entretanto, conforme amplamente apresentado acima, a base legal do legítimo interesse não pode ser utilizada pelos controladores para basear o tratamento de dados pessoais sensíveis. Dessa forma, apresenta-se, portanto, o seguinte questionamento: seria o tratamento de imagens que contenham pessoas físicas, por si só, um tratamento de dados pessoais sensíveis considerando a possibilidade de inferência de diversos tipos de dados pessoais sensíveis a partir de tais imagens?

Ora, não parece razoável estabelecer que qualquer tratamento de imagens, fotografias mais precisamente, que contenha a representação de uma pessoa física revele dados pessoais sensíveis e, portanto, tenha de ser realizado com base em uma hipótese legal de tratamento de dados pessoais estabelecida no artigo 11 da LGPD (bases legais para o tratamento de dados pessoais sensíveis).

Na verdade, é preciso avaliar o tipo de tratamento que está sendo realizado com tal imagem/fotografia, e se este tratamento tem por objetivo inferir dados 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, para só então tal tratamento ser considerado uma atividade realizada com dados pessoais sensíveis e, portanto, sujeita às bases legais descritas no artigo 11 da LGPD.

Isso porque, além da imagem, outros dados inicialmente considerados unicamente dados pessoais, a depender do tipo de tratamento a que são submetidos, podem gerar inferências relacionadas a dados pessoais sensíveis. Isso ocorre, por exemplo, com dados de geolocalização, uma vez que, a depender do local a que se referem podem gerar inferências relacionadas a informações sobre a origem racial, convicção religiosa, entre outros.

Assim, mostra-se bastante relevante identificar o tipo de tratamento a ser realizado com determinado dado para que seja possível identificar a qual categoria tal tratamento se refere, seja um tratamento de dados pessoais ou um tratamento de dados pessoais sensíveis.

Por exemplo, caso uma imagem seja utilizada para identificar uso de tatuagens, símbolos religiosos, vestimentas, entre outros, com o objetivo de definir a convicção religiosa de determinados indivíduos, este dado pode ser considerado um dado pessoal sensível, uma vez que se relaciona ao rol de dados sensíveis definido pela LGPD.

Neste sentido, conforme mencionado por Fachinetti, a interpretação que tem sido utilizada na Europa é a de que imagens/fotografias podem ser consideradas apenas dados pessoais quando o objetivo do tratamento não esteja relacionado ao seu caráter potencialmente sensível, não atingindo, assim, o nível de dados pessoais sensíveis.¹³

Além disso, o próprio considerando número 51 do GDPR estabelece que apenas serão considerados dados biométricos as imagens que sejam processadas por meios técnicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular¹⁴, o que vai em linha com o entendimento aqui apresentado, de que o objetivo do tratamento deve ser considerado para definição da caracterização da imagem como dado sensível ou não.

Se a atividade de tratamento de dados não tiver por finalidade a obtenção de dados relacionados à categoria dos dados pessoais sensíveis, não haverá que se falar em tratamento de dados pessoais sensíveis, sendo que, portanto, tal tratamento não precisará estar baseado em uma das hipóteses de tratamento de dados listadas no artigo 11 da LGPD, mas sim em uma das hipóteses prevista no artigo 7º da LGPD, o que abarca, portanto o legítimo interesse.

Dessa forma, considerando o uso de imagens para o treinamento de IA Generativa sem o objetivo de identificação de um titular ou aferição de quaisquer categorias de dados pessoais sensíveis, mas sim de determinação de padrões e estruturas presentes nas imagens utilizadas para o treinamento, mostra-se perfeitamente legal e aplicável, o uso do legítimo interesse para basear as atividades de tratamento de dados pessoais referentes ao uso de imagens/fotografias para o treinamento *deep learning* da tecnologia de IA Generativa.

4. Avaliação da decisão da ANPD sobre a base legal utilizada pela Meta (Facebook)

Conforme mencionado acima, o uso da base legal do legítimo interesse para basear a atividade de tratamento de dados pessoais relacionada à raspagem e ao treinamento de IA Generativa foi a escolha tomada pela Meta para basear o seu uso de imagens/fotografias coletadas em suas redes sociais (Facebook e Instagram).

13. FACHINETTI, Aline. *LGPD: fotos, inferências e a sensibilidade de dados pessoais. Uma análise sobre inferências e o seu impacto na sensibilidade dos dados pessoais*. 2019.

14. UNIÃO EUROPEIA. Considerando número 51. Regulamento Geral de Proteção de Dados da União Europeia. 2016. Disponível em: <https://gdpr-text.com/pt/read/recital-51/>. Acesso em: 18 jan. 2025.

Com o conhecimento do fato mencionado acima, a ANPD realizou uma análise da política de privacidade da Meta para avaliar a legalidade das atividades de tratamento de dados pessoais realizadas pela Meta.

Neste sentido, a ANPD publicou duas Notas Técnicas relacionadas ao uso pela Meta de imagens para treinamento de sua IA Generativa, em que discute a publicização de informações acerca do uso dos dados pessoais dos usuários das redes sociais, além da base legal utilizada pela empresa para basear o uso de imagens para treinamento de sua tecnologia.

Ao avaliar a atividade mencionada, em sua primeira Nota Técnica, a ANPD apontou que o uso da base legal do legítimo interesse não seria adequada para o tratamento de dados pessoais realizada pela Meta, conforme demonstrado abaixo:

A hipótese legal do legítimo interesse, nesse contexto, conforme disposto no Canal de Privacidade do controlador, parece não estar em consonância com as normas brasileiras de proteção de dados pessoais. Isso ocorre uma vez que o tratamento de dados pessoais em virtude do legítimo interesse do controlador ou de terceiros encontra-se fundamentado no art. 7º, IX, da LGPD.¹⁵

Em continuação, a ANPD esclareceu que tal entendimento teria por base a consideração de imagens/fotografias, por si só como dados pessoais sensíveis, considerando a possibilidade de tratamento indiscriminado de tais dados, sem considerar a real atividade e real finalidade do tratamento indicado:

O tratamento de dados pessoais sensíveis, nas circunstâncias ora analisadas, somente poderia ser realizado quando amparado em uma das hipóteses legais dispostas no art. 11 da LGPD, uma vez que o tratamento indiscriminado de fotografias, imagens, vídeos e gravações de áudios, especialmente por meio de uso de sistemas de inteligência artificial, pode revelar vinculações políticas, religiosas, sindicais e sexuais dos titulares, que já se caracterizam, de imediato, como dados sensíveis, conforme definição do art. 5º, inciso II da LGPD.¹⁶

Entretanto, em sua segunda Nota Informativa, após explicações trazidas pela Meta, a ANPD alterou o seu entendimento e esclareceu que informações pessoais retiradas de imagens/fotografias, por si só, não caracterizariam dados pessoais sensíveis, conforme disposto abaixo:

15. ANPD. *Nota Técnica nº 27/2024/FIS/CGF/ANPD*. 2024. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nt-27.pdf>. Acesso em: 08 jan. 2025.

16. ANPD. *Nota Técnica nº 27/2024/FIS/CGF/ANPD*. 2024. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nt-27.pdf>. Acesso em: 08 jan. 2025.

Assim, informações pessoais não estruturadas contidas em fotografias, áudios e imagens de vídeos, por si só, não constituem dados pessoais sensíveis que, consoante o art. 5º, II, da LGPD, se referem ao 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.¹⁷

Assim, a ANPD entendeu, de forma mais razoável, que a caracterização de uma informação pessoal presente em imagens/fotografias coletadas e tratadas pela Meta a partir de suas redes sociais (Facebook e Instagram) para treinamento de sua IA Generativa, após esclarecimentos da forma como tais informações são tratadas pela Meta, não constituem dados pessoais sensíveis, uma vez que as medidas aplicadas pela Meta para garantir a segurança das informações tratadas limita em grande parte a possibilidade de identificação de seus titulares, não tendo por objetivo, portanto, a inferência de dados pessoais sensíveis, como podemos observar abaixo:

Nesse sentido, a identificação ou a possibilidade de reidentificação de usuários e não usuários, inclusive no que se refere a dados pessoais sensíveis, seria bastante limitada em virtude das próprias características do tratamento de dados pessoais e em razão das medidas técnicas de segurança implementadas para evitar essa situação.¹⁸

Dessa forma, é possível observar uma mudança no entendimento da ANPD a partir do recebimento de informações adicionais fornecidas pela Meta sobre a atividade de tratamento realizada com as imagens/fotografias, o que demonstra que a forma e o objetivo do tratamento são importantes para a caracterização de tal informação como um dado pessoal sensível ou não.

Neste sentido, consideramos que a decisão tomada pela ANPD, de considerar a forma e o objetivo do tratamento para a caracterização dos dados pessoais como sensíveis ou não, é extremamente importante para que a proteção apresentada pela LGPD aos dados pessoais sensíveis não seja enfraquecida. Dessa forma, apenas dados que tenham de fato as características mencionadas acima para caracterização como dados sensíveis, possuirão as proteções adicionais apresentadas pela LGPD.

17. ANPD. *Nota Técnica nº 39/2024/FIS/CGF/ANPD*. 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_anpd-0140555-nota-tecnica.pdf. Acesso em: 08 jan. 2025.

18. ANPD. *Nota Técnica nº 39/2024/FIS/CGF/ANPD*. 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_anpd-0140555-nota-tecnica.pdf. Acesso em: 08 jan. 2025.

Considerações finais

Com as informações trazidas e avaliadas, foi possível identificar a legalidade do uso da hipótese legal do legítimo interesse para basear o uso de imagens/fotografias para o treinamento de IA Generativa, mais especificamente, o caso da Meta.

Apesar de a princípio indicar pela ilegalidade na utilização de tal base legal para basear a atividade em comento, em posterior avaliação aos fatos, a ANPD entendeu que a finalidade da atividade realizada pela Meta não incluía a inferência de dados pessoais sensíveis de tais imagens/fotografias, tampouco a utilização de tais informações para fins do treinamento de sua IA Generativa.

Dessa forma, a ANPD se mostrou bastante razoável em considerar, conforme amplamente discutido, que a finalidade do tratamento das imagens/fotografias é bastante relevante e deve ser considerada ao ser avaliada a legalidade da base legal escolhida para basear o legítimo tratamento de tais imagens/fotografias. Deve-se, portanto, avaliar se há a inferência ou não de dados sensíveis a partir do tratamento para, posteriormente, verificar a possibilidade de utilização de bases legais aplicáveis apenas a dados pessoais, contidas no art. 7º da LGPD, e que não podem ser utilizadas para legitimar o tratamento de dados pessoais sensíveis.

Entretanto, é importante observarmos que, conforme já apontado pelo *European Data Protection Supervisor* (EDPS), o uso de tecnologias de raspagem pode ocasionar uma certa perda de controle relacionada às finalidades do tratamento dos dados coletados, uma vez que os dados pessoais são coletados sem o conhecimento dos titulares e podem ser utilizados, pela própria IA Generativa, para finalidades distintas da qual tenham sido inicialmente coletadas¹⁹, podendo acarretar em um uso não avaliado anteriormente e que pode não ter como base legal mais adequada o legítimo interesse.

Assim, não obstante a decisão relacionada ao caso da Meta, a discussão apresentada neste artigo acende um alerta acerca do tratamento de imagens à luz da base legal do legítimo interesse. Neste sentido, apenas a decisão sobre o caso da Meta não é suficiente para identificarmos aprofundar o entendimento da ANPD acerca deste tratamento. Portanto, faz-se necessário que a citada autoridade se aprofunde no tema com a publicação de, por exemplo, um guia orientativo acerca do uso da base legal do legítimo interesse para o

19. EDPS. *Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI Systems*. 2024. Disponível em: https://www.edps.europa.eu/system/files/2024-06/24-06-03_genai_orientations_en.pdf. Acesso em: 18 abr. 2025.

tratamento de imagens com menção expressa acerca da possibilidade de inferência de dados sensíveis a partir de tal tratamento, bem como acerca dos usos secundários possivelmente realizados pela IA Generativa.

Assim, seja pelo seu dever de regulação, seja pelo histórico de abusos no uso de dados pessoais na jurisdição brasileira, a ANPD não pode se esquivar de enfrentar os limites do uso do legítimo interesse para o tratamento de imagens, e, especialmente, em conexão com o treinamento de IA Generativa.

Referências

ANPD. *Guia Orientativo – Hipóteses legais de tratamento de dados pessoais – legítimo interesse*. 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em: 14 abr. 2025.

ANPD. *Radar Tecnológico. Inteligência Artificial Generativa*. 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/radar_tecnologico_ia_generativa_anpd.pdf. Acesso em: 08 jan. 2025.

ANPD. *Nota Técnica nº 39/2024/FIS/CGF/ANPD*. 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_anpd-0140555-nota-tecnica.pdf. Acesso em: 08 jan. 2025.

ANPD. *Nota Técnica nº 27/2024/FIS/CGF/ANPD*. 2024. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nt-27.pdf>. Acesso em: 08 jan. 2025.

BESSA, Leonardo. *Privacidade e proteção de dados pessoais: a categorização das bases legais na LGPD. Inteligência Artificial Generativa no Direito*. 5 anos de LGPD. Revista dos Tribunais, 2024.

BRASIL. *Lei Federal nº 13.709/2018 (LGPD)*. Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 08 jan. 2025.

DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. Thomson Reuters, 2021.

EDPS. *Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI Systems*. 2024. Disponível em: https://www.edps.europa.eu/system/files/2024-06/24-06-03_genai_orientations_en.pdf. Acesso em: 18 abr. 2025.

FACEBOOK. *Como a Meta usa informações para modelos e recursos de IA generativa*. Disponível em: <https://www.facebook.com/privacy/genai>. Acesso em: 18 abr. 2025.

FACHINETTI, Aline. *LGPD: fotos, inferências e a sensibilidade de dados pessoais. Uma análise sobre inferências e o seu impacto na sensibilidade dos dados pessoais*. 2019.

FALCÃO, Daniel; PEROLI, Kelvin. *Imagem, dado pessoal sensível?* Disponível em: https://www.conjur.com.br/2022-mai-28/observatorio-constitucional-imagem-dado-pessoal-sensivel/#_ftn8. Acesso em: 09 jan. 2025

ICO. *Legitimate Interest Assessment template*. <https://ico.org.uk/media/about-the-ico/disclosure-log/4017958/ic-109330-z1w4-attachment-2.pdf>. Acesso em: 18 abr. 2025.

OLIVEIRA, Ricardo; COTS, Márcio. *O Legítimo Interesse*. O Legítimo Interesse e a LGPD. Revista dos Tribunais, 2021.

PINHEIRO, Patrícia Peck. *Proteção de dados pessoais: comentários à Lei n. 13.709/2018 LGPD*. São Paulo. Saraiva Educação, 2018.

PORTO, Fábio; ARAÚJO, Valter; GABRIEL, Anderson. *Inteligência Artificial Generativa no Direito*. Revista dos Tribunais, 2024.

UNESCO. *Guia para a IA generativa na educação e na pesquisa*. 2024. Disponível em: https://unesdoc.unesco.org/in/documentViewer.xhtml?v=2.1.196&id=p::usmarcdef_0000390241&file=/in/rest/annotationSVC/DownloadWatermarkedAttachment/attach_import_0880195e-d225-4872-bc95-e36b69d17343%3F_%3D390241por.pdf&locale=en&multi=true&ark=/ark:/48223/pf0000390241/PDF/390241por.pdf#509_24_guia_IA_INT_Portuguese.indd%3A.15084%3A2017. Acesso em: 18 abr. 2025.

UNIÃO EUROPEIA. *Regulamento Geral de Proteção de Dados da União Europeia*. 2016. Disponível em: <https://gdpr-info.eu/>. Acesso em: 08 jan. 2025.

UNIÃO EUROPEIA. *Regulamento Geral de Proteção de Dados da União Europeia*. 2016. Disponível em: <https://gdpr-text.com/pt/read/recital-51/>. Acesso em: 18 jan. 2025.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

12

**Entre o algoritmo e
a decisão humana: a
abrangência do art. 20
da LGPD na análise de
compatibilidade de perfis
através do uso de inteligência
artificial em processos de
recrutamento e seleção**

LARISSA BOULLOSA MAGNAVITA DE OLIVEIRA

Sumário: Introdução. 1. As plataformas ATS e o uso de inteligência artificial na triagem de candidatos. 2. Direitos dos titulares em decisões unicamente automatizadas: reflexões sobre o art. 20 da LGPD. 3. A imprecisão do direito à explicação: entre a limitação e a proteção do titular. 4. Convergência entre algoritmos e decisão humana: zona cinzenta? Considerações finais. Referências.

Introdução

Com o contínuo desenvolvimento da tecnologia, a sociedade alcançou um contexto marcado pelo protagonismo da inteligência artificial (IA), sendo um mecanismo utilizado atualmente em diversos âmbitos sociais com o intuito de auxiliar o ser humano em suas tarefas, poupando tempo e esforço. Portanto, pode-se dizer que o surgimento e a implementação de novos produtos digitais e soluções tecnológicas com o uso da inteligência artificial se encontra em um número crescente, conduzindo também um aumento de ocasiões em que decisões que afetem a vida de pessoas sejam tomadas através de algoritmos.

Esse movimento tem atingido diversos campos corporativos, passando a interagir com diferentes áreas nas organizações, seja através de análises de comportamento do consumidor e previsões de demanda, auxílio nas tomadas de decisão a partir da análise de dados internos e externos ao negócio, avaliação de risco de crédito e detecção de fraudes, análise de desempenho de colaboradores e a automatização dos processos de recrutamento e seleção na triagem de candidatos.

No que tange ao último recorte citado, faz-se imperioso destacar os impactos que esta prática pode trazer para as organizações e para os titulares dos dados pessoais frente aos riscos em relação à justiça e à privacidade dos dados. A utilização de plataformas digitais que disponibilizam funcionalidades que fazem a triagem automatizada de candidatos através de sistemas algorítmicos pode influenciar diretamente o futuro profissional de uma pessoa sem estar imune a falhas, seja por deficiências tecnológicas ou pelo uso de bases incompletas ou enviesadas, podendo levar a decisões equivocadas ou até mesmo discriminatórias.

Embora os pontos favoráveis ao emprego da inteligência artificial no âmbito dos recursos humanos sejam clarividentes posto a diminuição de custos e

1. Advogada, DPO e Consultora Jurídica. Pós-graduanda em Direito Digital pela Universidade do Estado do Rio de Janeiro (UERJ) em parceria com o ITS Rio. Graduada em Direito pela Universidade Salvador (UNIFACS). Bacharela em Humanidades pela Universidade Federal da Bahia (UFBA).

os ganhos em eficiência e celeridade para as empresas, faz-se evidente a necessidade de mecanismos que assegurem a revisão dessas decisões, garantindo que erros ou injustiças possam ser corrigidos e que o processo seletivo respeite os direitos fundamentais dos candidatos.

Neste contexto, o art. 20 da Lei Geral de Proteção de Dados (LGPD) emerge como uma salvaguarda essencial, ao garantir aos titulares dos dados o direito de solicitar a revisão de decisões unicamente automatizadas que afetem seus interesses. Esse dispositivo busca assegurar que as decisões automatizadas não sejam tomadas de forma arbitrária ou discriminatória, promovendo um equilíbrio entre o uso da tecnologia e o respeito aos direitos individuais.

Todavia, a aplicação prática do art. 20 em processos de recrutamento e seleção ainda enfrenta desafios. Embora em algumas soluções a decisão final geralmente recaia sobre o recrutador humano, a triagem automatizada desempenha um papel determinante na exclusão ou avanço de candidatos nas etapas iniciais do processo. Essa dinâmica híbrida entre decisões automatizadas e humanas levanta a questão sobre a real abrangência do direito à revisão garantido pela LGPD, que ao mencionar apenas as decisões unicamente automatizadas em seu dispositivo legal, evidencia uma carência de aperfeiçoamentos para dar ao comando legal a efetividade necessária, deixando dúvidas quanto à extensão do conceito e lacunas capazes de comprometer a proteção pretendida. Para tanto, o presente artigo visa refletir crítica e sistematicamente a respeito da abrangência do art. 20 da LGPD frente a decisões complexas no contexto da análise de compatibilidade de perfis nos processos de recrutamento e seleção, sendo imperioso analisar o sistema protetivo de dados em sua essência, para além de uma interpretação meramente positivista.

Desta forma, estrutura-se a presente pesquisa em quatro capítulos, iniciando-se por uma contextualização sobre as plataformas *Applicant Tracking System* (ATS) e as diferentes modalidades do uso de inteligência artificial na triagem de candidatos, compreendendo, inclusive, a participação da pessoa recrutadora no processo decisório. Na seção subsequente, traz-se sobre o art. 20 da LGPD e o direito da revisão, entendendo-o como mitigador de riscos na ocorrência de decisões automatizadas, sem deixar de evidenciar, contudo, os seus desafios práticos. Na terceira seção, serão enfrentadas questões a respeito da efetividade do direito à explicação, com foco nas limitações e desafios impostos pela redação normativa. A análise se concentrará na interpretação da norma, especialmente no que diz respeito à sua aplicação em decisões híbridas, ou seja, aquelas que envolvem tanto a atuação de algoritmos

quanto a intervenção humana. Doravante, no quarto capítulo será abordada a questão da convergência entre algoritmos e decisões humanas na análise de compatibilidade de perfis nos processos de recrutamento e seleção, com foco em analisar a lacuna que emerge da interação entre esses dois elementos no contexto dos processos decisórios frente a direta e significativa influência algorítmica nas decisões das pessoas recrutadoras.

Por fim, será apresentada a síntese conclusiva, seguida das referências utilizadas para a conclusão do presente artigo.

1. As plataformas ATS e o uso de inteligência artificial na triagem de candidatos

Nos dias de hoje, a inteligência artificial deixou de ser apenas uma tecnologia emergente e assumiu um papel de destaque no mundo corporativo, trazendo um novo paradigma social para as relações interpessoais e interinstitucionais. Sua aplicação em diversos setores empresariais tem transformado a maneira como as organizações gerenciam informações e tomam decisões estratégicas, otimizando a produtividade e permitindo uma maior agilidade na resposta às demandas do mercado.

Quando relacionamos este contexto com o mercado de recrutamento e seleção, entende-se que este recorte corporativo está em constante atualização, já havendo uma severa modernização quando posto em comparação à época em que as vagas de emprego eram anunciadas em jornais e o processo de triagem de candidatos era conduzido de forma manual, envolvendo grandes esforços operacionais nos departamentos de recursos humanos das empresas, bem como tempo e custos nada desprezíveis². Para além disso, tem-se que ao longo do tempo, a seleção deixou de ser vista como um sistema meramente classificatório e eliminatório de candidatos, adquirindo importância estratégica para tornar a qualidade da seleção uma vantagem competitiva para a organização³, sendo possível compreender o surgimento de novas possibilidades que tornaram o processo seletivo mais efetivo e dinâmico.

Ante o exposto, as plataformas *Applicant Tracking System* (ATS) surgiram como uma resposta à crescente demanda por soluções que facilitassem a gestão de processos seletivos em empresas que recebem centenas de currículos

2. JUNQUEIRA, Thiago. *Discriminação: o desafio da inteligência artificial em processos seletivos*. Disponível em: <https://veja.abril.com.br/economia/discriminacao-o-desafio-da-inteligencia-artificial-em-processos-seletivos>. Acesso em: 05 jul. 2024.

3. CIPRIANO, Gael Santos; CERIBELI; Harrison Bachion; MACIEL, Gustavo Nunes; CAMPOS, Rita de Cássia Legal. *Inteligência artificial nos processos de seleção de RH*. *Revista Estudos de Administração e Sociedade*, n.2, v.6. Niterói: Universidade Federal Fluminense, 2021.

para preencher uma única vaga. De tal maneira, essas plataformas foram desenvolvidas para centralizar e organizar as candidaturas, permitindo que as pessoas recrutadoras pudessem acessar, classificar e gerenciar as informações e o desempenho dos candidatos de forma mais ágil.

Inicialmente, os sistemas ATS eram basicamente bancos de dados avançados, capazes de armazenar informações de currículos e acompanhar o progresso dos candidatos em cada etapa do processo seletivo. Com o tempo, no entanto, a necessidade de tornar esses sistemas mais eficientes levou à integração de tecnologias mais sofisticadas como a inteligência artificial, que, por sua vez, atualmente se apresenta de diferentes formas dentro deste contexto, frente o crescimento do mercado:

Não só o Brasil, como o mundo, viu crescer o número das chamadas *HR Techs*, que são as *startups* que atuam no desenvolvimento de tecnologias para o desenvolvimento, recrutamento e seleção de pessoas. Em 2017, o Google fomentou cerca de 20 *startups*; no final de 2020, o número chegou a 373. Tais *startups* ajudam a desmistificar o uso da inteligência artificial, e mostram que seu uso não precisa ter o formato somente de um robô, mas que também está presente em *softwares* que podem guardar dados extremamente relevantes quando mineradores de forma a buscar uma integração entre o candidato e a empresa⁴.

Dessa forma, diversos são os posicionamentos das *HR Techs* existentes, bem como variados são os parâmetros adotados na implementação de IA em suas funcionalidades, sobretudo na triagem de candidatos. Neste viés, algumas empresas se manifestam no sentido de que em que pese a tecnologia seja eficiente, ainda é necessário um direcionamento humano. Como reflexo deste entendimento, pode-se dizer que entre as funcionalidades mais encontradas no mercado de ATS envolvendo atuação algorítmica nas análises de compatibilidade de perfis na triagem de candidatos, tem-se: (i) o ranqueamento de candidatos; (ii) o *match* de talentos; (iii) a reprovação automatizada através de *score* e; (iv) a análise preditiva.

No ranqueamento, o usuário da plataforma pode determinar critérios de forma prévia, como experiência profissional, formação acadêmica e outros requisitos da vaga, enquanto a inteligência artificial analisa os currículos dos candidatos e os organiza em um *ranking*, priorizando aqueles que atendem

4. ARBEX, Gabriela. *Estudo mapeia HR Techs do Brasil e aponta enorme potencial de crescimento*. Disponível em: <https://forbes.com.br/forbes-tech/2020/06/exclusivo-estudo-mapeia-rh-techs-do-brasil-e-aponta-enorme-potencial-de-crescimento/>. Acesso em: 03 jan. 2025.

melhor aos critérios estabelecidos, sem necessariamente aprová-los ou reprová-los. Logo, a decisão final de contratação ou reprovação fica à cargo do recrutador responsável, ou seja, a palavra final é dada por um humano.

Neste sonar, o *match* de talentos se apresenta em uma lógica parecida, tratando-se de uma hipótese em que por meio de algoritmos de *machine learning*, o sistema avalia os currículos dos candidatos e os compara com os critérios personalizados pelo recrutador com base na descrição da vaga divulgada, identificando aqueles que possuem maior compatibilidade. Esta análise considera não apenas palavras-chave presentes no currículo, como também padrões mais complexos, como sinônimos, contexto e experiências relacionadas. Em seguida, o recrutador se depara com *tags* atribuídas aos candidatos, identificando se possui “alto, médio ou baixo *fit*” com a vaga. Com observância ao resultado da avaliação de cada critério escolhido, a decisão de reprovar ou avançar com o candidato se dá pela pessoa recrutadora.

Adicionalmente às modalidades anteriores, porém com premissas diferentes, também é possível se deparar com a reprovação automatizada através de *score*, caso em que as plataformas ATS são programadas para reprovar automaticamente os candidatos que não atendem a determinados critérios básicos definidos pelo recrutador ou pela própria ferramenta, não atingindo um *score* pré-determinado para continuidade no processo. Por fim, mas não se limitando, algumas plataformas viabilizam uma análise preditiva, mecanismo para prever o potencial de sucesso de um candidato na vaga em questão, analisando dados históricos de contratações anteriores e identificando características comuns entre os profissionais que tiveram bom desempenho em cargos similares, por exemplo.

Ante o exposto, percebe-se que o uso de algoritmos para tomar decisões críticas pode levar o titular de dados pessoais a reprovações injustas, especialmente quando as bases de dados utilizadas para treinar a inteligência artificial são limitadas ou enviesadas, cenário que requer uma tutela revisória. Não tão somente, a falta de transparência nos critérios utilizados pelos algoritmos em algumas modalidades pode dificultar a contestação de decisões por parte dos candidatos, colocando em risco o cumprimento de legislações como a Lei Geral de Proteção de Dados.

Tendo este contexto em vista, o próximo capítulo será dedicado a explorar a LGPD, com ênfase no art. 20, que garante aos titulares dos dados pessoais o direito de solicitar a revisão de decisões unicamente automatizadas.

2. Direitos dos titulares em decisões unicamente automatizadas: reflexões sobre o art. 20 da LGPD

O tópico anterior constatou que atualmente as atividades e interações corporativas estão cada vez mais intermediadas pela inteligência artificial, de forma que o uso desta tecnologia na triagem de candidatos em processos seletivos tem ganhado diversas modalidades de aplicação, proporcionado relevantes benefícios para os departamentos de *talent acquisition* e vantagens significativas para as organizações, sobretudo no que se refere a escala e velocidade das operações.

Por outro lado, surge também uma necessidade em viabilizar uma análise detalhada dos diversos aspectos envolvidos no processo decisório mediado por algoritmos. Isto porque o uso da inteligência artificial pode gerar resultados que ensejam preocupações, seja em razão do cometimento de erros objetivos, seja pela existência de fatores que tornem estes resultados questionáveis por apresentar parcialidade, viés, opacidade, tendências discriminatórias, dentre outros aspectos problemáticos⁵. Neste sentido, empreende-se uma compreensão da Lei Geral de Proteção de Dados como parâmetro mitigatório destes riscos, disciplinando em seu art. 20 o direito do titular dos dados pessoais à explicação das decisões tomadas unicamente com base em tratamento automatizado, a saber:

Artigo 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (Redação dada pela Lei nº 13.853, de 2019).

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais⁶.

5. WIMMER, Miriam; DONEDA, Danilo. “Falhas de IA” e a intervenção humana em decisões automatizadas: parâmetros para a legitimação pela humanização. *Dossiê – Inteligência Artificial, Ética e Epistemologia*, vol.18, n.100. Brasília: Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, 2021.

6. BRASIL. Lei 13.709/2018. *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: 19 jan. 2025.

Embora tenha-se que a lógica do direito à explicação e do direito à revisão de decisões automatizadas que impacta o titular dos dados tenha sido inaugurada no Brasil através do art. 5º da Lei nº 12.414/2011, a qual Lei de Cadastro Positivo, que inclui entre os direitos do cadastrado, o de solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados, a sua inserção no microssistema de proteção de dados pessoais ampliou o campo de aplicabilidade⁷. Corroborando neste sentido, o cenário de recrutamento e seleção se insere neste contexto não apenas por afetar diretamente o interesse do titular que se candidatou para uma vaga de trabalho, mas também emprega mecanismos automatizados para definir o perfil profissional do candidato. Essa situação demanda atenção especial, dado que a relação entre candidatos e empresas empregadoras é marcada por uma desigualdade estrutural, na qual a empresa contratante é detentora de maior poder econômico e informacional.

De tal maneira, essa hipossuficiência do candidato em relação à empresa empregadora torna a proteção de dados ainda mais relevante, haja vista estarem mais vulneráveis a práticas abusivas ou discriminatórias, especialmente em um cenário onde decisões importantes como a contratação podem ser tomadas por sistemas automatizados sem a devida transparência e controle. Embora o uso de inteligência artificial possa trazer a ideia de maior transparência no processo de recrutamento e seleção, uma vez que a análise das etapas enfrentadas por uma pessoa candidata pode ser convertida em um resultado inteiro, ou seja, é possível que a IA expresse em porcentagens a desenvoltura da pessoa durante o processo⁸, informações enviesadas ou errôneas obtidas a partir de banco de dados podem deturpar o processo de triagem e privar candidatos aptos de boas oportunidades⁹.

Neste contexto, acrescenta-se que é possível que o aprendizado da máquina induza um viés, discriminando e repetindo preconceitos anteriores, visto que “os processos automatizados são treinados para procurar padrões históricos de sucesso e a lógica empregada sugere que o que levou ao sucesso no passado, levará novamente ao sucesso no futuro”¹⁰. Ou seja, se a maioria das

7. LIMA, Taisa Maria Macena; SÁ, Maria de Fátima Freire de. Inteligência artificial e Lei Geral de Proteção de Dados Pessoais: o direito à explicação nas decisões automatizadas. *Revista Brasileira de Direito Civil – RBDCivil*. Belo Horizonte, v. 26, p. 232, 2020.

8. ALBERTO, Leonardo de Andrade; YASUOKA, Renan Takeshi; PIERANTI, Octavio Penna. *O uso de inteligência artificial nos processos de recrutamento e seleção: reflexões introdutórias*. São Paulo: Simpósio dos Programas de Mestrado Profissional, 2021, p.1144.

9. SANKIEVICZ, Alexandre; PINHEIRO, Guilherme Pereira. Aspectos da proteção de dados nas relações de trabalho. In: DONEDA, Danilo... [et al.]. *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021, p. 510.

10. O'NEIL, Cathy. *Algoritmos da destruição em massa*. Santo André: Editora Rua do Sabão, 2021, p. 32.

contratações de uma empresa tiver sido de homens, por exemplo, alguns dados, ainda que indiretamente relacionados a termos femininos, poderão sofrer uma qualificação negativa. Este ocorrido, por sua vez, foi visto em 2015 na empresa Amazon, que utilizava uma plataforma digital que analisava os currículos enviados de forma automatizada atribuindo notas de 1 a 5 para cada candidato. Mesmo não tendo se valido do gênero como *input*, o algoritmo foi capaz de identificá-lo por meio de alguns termos utilizados nos currículos e, como resultado, desenvolveu um viés a favor dos homens – historicamente, o gênero predominante nas empresas de tecnologia¹¹. Mesmo tentando editar e corrigir a programação, com o intuito de torná-la neutra a esses termos específicos, os especialistas em *machine learning* contratados da empresa concluíram que não poderiam impedir que outras correlações discriminatórias fossem criadas pelas máquinas, de forma que a ferramenta foi descontinuada da organização.

Portanto, é fundamental que as empresas adotem práticas que garantam a conformidade com a legislação vigente e com diretrizes éticas, assegurando que os candidatos tenham acesso a explicações claras sobre os critérios utilizados nas decisões automatizadas e a possibilidade de revisão por um agente humano, tendo em vista que a tutela revisiva, ao se voltar às decisões que afetam o interesse do titular de dados, afasta qualquer interesse meramente especulativo ou sem fundamento jurídico relevante. Desta forma, é legítimo que um candidato queira descobrir se foi reprovado do processo seletivo porque foi discriminado por conta da idade ou do gênero, a exemplo de mulheres em idade em fértil¹².

Ocorre que, conquanto a previsão legislativa já seja um avanço, os parâmetros legais para o exercício do direito à explicação podem não ser suficientes para assegurar a autonomia informativa do titular dos dados pessoais e para concretizar a principiologia sistematizada no art. 6º da Lei Geral de Proteção de Dados, em especial, os princípios do livre acesso (inc. IV), da transparência (inc. VI) e da não discriminação (inc. IX)¹³. É sabido que a preferência do legislador se deu para resguardar o segredo comercial e industrial das empresas, ou seja, em manter intocáveis as informações mais estratégicas por trás do desenvolvimento da aplicação em alguns contextos, apresentando um prejuízo

11. JUNQUEIRA, Thiago. *Discriminação: o desafio da inteligência artificial em processos seletivos*. Disponível em: <https://veja.abril.com.br/economia/discriminacao-o-desafio-da-inteligencia-artificial-em-processos-seletivos>. Acesso em: 16 abr. 2025.

12. ALMEIDA, Dayse Coelho de. *Lei Geral de Proteção de Dados e novos direitos do empregado na decisão automatizada*. Disponível em: <https://www.migalhas.com.br/depeso/356587/lgpd-e-novos-direitos-do-empregado-na-decisao-automatizada>. Acesso em: 19 jan. 2025.

13. LIMA, Taisa Maria Macena; SÁ, Maria de Fátima Freire de. Inteligência artificial e Lei Geral de Proteção de Dados Pessoais: o direito à explicação nas decisões automatizadas. *Revista Brasileira de Direito Civil – RBDCivil*. Belo Horizonte, v. 26, p. 233, 2020.

para o titular. Dito isto, o direito à revisão de decisões automatizadas somente ocorrerá caso se saiba que o tratamento automatizado esteja ocorrendo, o que muitas vezes pode ser mascarado, principalmente nas relações de contratação, pelo poder de controle inerente a essa relação¹⁴.

Um outro aspecto relevante se dá também no § 2º, no qual é explicitado que a auditoria pela Autoridade Nacional de Proteção de Dados (ANPD), somente ocorrerá caso o agente de tratamento se recuse a fornecer tais informações, o que limita ainda mais o poder fiscalizatório dessa Autoridade, fragilizando o exercício dos direitos do titular¹⁵, mencionando-se ainda o fato de que é discricionária a decisão da ANPD de realizar ou não a auditoria. Contudo, as limitações do texto normativo não se esgotam nestes aspectos, carecendo ainda de outros aprofundamentos que colocam em indagação a abrangência do art. 20 da LGPD em decisões híbridas, ou seja, decisões tomadas por um humano através de análise algorítmica.

Perante o explanado, buscar-se-á, no próximo capítulo, trazer contrapontos pautados no ponto de vista interpretativo da legislação em relação às decisões híbridas, preocupando-se em evidenciar as lacunas existentes no texto normativo brasileiro de proteção de dados pessoais ao limitar seu escopo a decisões unicamente automatizadas.

3. A imprecisão do direito à explicação: entre a limitação e a proteção do titular

Conforme o cenário apresentado, tem-se que o art. 20 da Lei Geral de Proteção de Dados apresenta algumas discussões em relação à efetividade do direito à explicação, bem como revela uma timidez em seu texto normativo na medida em que restringe o direito à explicação às decisões unicamente automatizadas. Desta forma, as decisões que forem o resultado simultâneo da automação e da decisão humana não são alcançadas pela previsão normativa¹⁶, ao menos à primeira vista.

Atinente a esta problemática, o mesmo cenário é encontrado diante ao regulamento europeu, o qual *General Data Protection Regulation* (GDPR), que consigna em seu art. 22 o direito à explicação. Neste sentido, algumas po-

14. LIMA, Francisco Gérson Marques de; MORAIS, Ricardo Antônio Maia de. Decisões automatizadas nas relações de emprego: art. 20 da LGPD ante o silêncio da CLT. *O uso de dados pessoais e inteligência artificial na relação de trabalho: proteção, discriminação, violência e assédio digital*. Brasília: Ministério Público do Trabalho, 2022.

15. Ibidem.

16. LIMA, Taisa Maria Macena; SÁ, Maria de Fátima Freire de. Inteligência artificial e Lei Geral de Proteção de Dados Pessoais: o direito à explicação nas decisões automatizadas. *Revista Brasileira de Direito Civil – RBDCivil*. Belo Horizonte, v. 26, p. 233, 2020.

lêmicas têm cercado a interpretação da norma, inclusive no que consistiria uma decisão para os fins do GDPR e o que seria uma decisão tomada exclusivamente com base no tratamento automatizado, questionando-se que nível de participação humana afastaria a incidência da norma¹⁷. Como alternativa, o Grupo de Trabalho do Artigo 29 para a Proteção de Dados, órgão consultivo independente criado pela União Europeia para lidar com questões relacionadas à privacidade, fixou uma interpretação ampla quanto ao escopo da legislação. Nota-se:

[...] “decisões tomadas “exclusivamente com base” no tratamento automatizado são aquelas em que não há uma supervisão humana relevante. Assim, segundo a interpretação do grupo, o controlador não pode se eximir da incidência do artigo fabricando uma intervenção humana meramente simbólica; esta deve ser realizada “por alguém com autoridade e competência para alterar a decisão e que, no âmbito da análise, deverá tomar em consideração todos os dados pertinentes¹⁸.”

Por sua vez, diante da mesma situação, a autoridade de proteção de dados britânica indica que a regra em questão se refere a situações em que não há influência humana sobre o processo decisório¹⁹. Desta forma, um processo poderia ser considerado totalmente automatizado se um ser humano apenas inserisse os dados pessoais a serem processados, sendo a decisão tomada por uma máquina. Contudo, um processo não seria considerado totalmente automatizado se um ser humano avaliasse e interpretasse os resultados de uma decisão automatizada antes de aplicá-la a um indivíduo²⁰.

Ainda neste sentido, para Rony Vainzof e Andriei Gutierrez, as decisões abarcadas pelo art. 20 da Lei Geral de Proteção de Dados são aquelas que resultam apenas do processamento automático de dados, sem nenhuma intervenção humana. Como exemplificação, tem-se que é possível que o resultado

17. WIMMER, Miriam; DONEDA, Danilo. “Falhas de IA” e a intervenção humana em decisões automatizadas: parâmetros para a legitimação pela humanização. *Dossiê – Inteligência Artificial, Ética e Epistemologia*, vol.18, n.100. Brasília: Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, 2021.

18. WP29 – Grupo de Trabalho do Artigo 29 para a Proteção de Dados. Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679. Adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection_pt. Acesso em: set. 2021. In: WIMMER, Miriam; DONEDA, Danilo. “Falhas de IA” e a intervenção humana em decisões automatizadas: parâmetros para a legitimação pela humanização. *Dossiê – Inteligência Artificial, Ética e Epistemologia*, vol.18, n.100. Brasília: Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, 2021.

19. ICO – INFORMATION COMMISSIONER’S OFFICE. Detailed Guidance on Automated Decision-Making and Profiling (2018). Disponível em: <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling-1-1.pdf>. Acesso em: jan. 2025.

20. WIMMER, Miriam; DONEDA, Danilo. “Falhas de IA” e a intervenção humana em decisões automatizadas: parâmetros para a legitimação pela humanização. *Dossiê – Inteligência Artificial, Ética e Epistemologia*, vol.18, n.100. Brasília: Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, 2021.

seja interpretado pelo humano, mas ainda assim todo processo decisório é automatizado²¹. Em completude, Taisa Maria Macena de Lima e Maria de Fátima Freire de Sá evidenciam a timidez do texto normativo, manifestando-se no sentido de que não há como ignorar os processos decisórios complexos nos quais algumas fases são automatizadas e outras fases são implementadas com decisões puramente humanas, de forma que tais processos decisórios são merecedores de igual cobertura legal²².

Importa também mencionar que, para além deste aspecto, foi proposto o projeto de lei nº 4496/2019 para definir a expressão “decisão automatizada” na legislação, que também possui sua conceituação silente. Assim sendo, foi sugerido o seguinte conceito:

Decisão automatizada é o processo de escolha, de classificação, de aprovação ou rejeição, de atribuição de nota, medida, pontuação ou score, de cálculo de risco ou de probabilidade, ou outro semelhante, realizado pelo tratamento de dados pessoais utilizando regras, cálculos, instruções, algoritmos, análises estatísticas, inteligência artificial, aprendizado de máquina, ou outra técnica computacional²³.

Desta forma, evidencia-se uma carência de aperfeiçoamentos para dar ao comando legal a efetividade necessária, deixando dúvidas quanto à extensão do conceito e lacunas capazes de comprometer a proteção pretendida, possibilitando que agentes de tratamento se valham destas arestas para afastar a incidência normativa e, conseqüentemente, a estruturação de um processo apto a atender o direito de revisão dos titulares.

Neste sentido, a seguir, a presente pesquisa versará sobre a interpretação e a abrangência do art. 20 da Lei Geral de Proteção de Dados nas análises de compatibilidade de perfis através do uso de inteligência artificial nos processos de recrutamento e seleção, tendo em vista a complexidade do processo decisório deste ecossistema, envolvendo simultaneamente análise algorítmica e atuação humana.

21. VAINZOF, Rony; GUTIERREZ, Andriei. Transparência e revisão de decisões automatizadas. In: VAINZOF, Rony; GUTIERREZ, Andriei. *Inteligência Artificial (IA)*. São Paulo: Editora Revista dos Tribunais, 2021.

22. LIMA, Taisa Maria Macena; SÁ, Maria de Fátima Freire de. Inteligência artificial e Lei Geral de Proteção de Dados Pessoais: o direito à explicação nas decisões automatizadas. *Revista Brasileira de Direito Civil – RBDCivil*. Belo Horizonte, v. 26, p. 233, 2020.

23. LIMA, Lindamaria. PL 4496/2019 – Entendendo o conceito de decisão automatizada. Disponível em: <https://blog.tripla.com.br/decisao-automatizada/>. Acesso em: 15 jan. 2025.

4. Convergência entre algoritmos e decisão humana: zona cinzenta?

Nas seções supra, tem-se que o art. 20 da LGPD foi desenvolvido para proteger os titulares de dados de decisões tomadas exclusivamente por algoritmos. Contudo, conforme delimitado, uma zona cinzenta se revela ao restringir o direito à explicação, despertando algumas indagações: processos decisórios que forem resultados de uma atuação simultânea entre algoritmos e humanos serão alcançados pela previsão normativa? No ecossistema do recrutamento e seleção, se o ATS apenas classifica ou ranqueia candidatos, mas a decisão final é tomada por um recrutador humano, pode-se argumentar que a decisão não é única e exclusivamente automatizada, afastando a aplicabilidade do direito de revisão?

Neste sentido, à primeira vista e embasado isoladamente na letra fria da legislação, o dispositivo analisado pode sugerir descortinar a possibilidade de que o direito à revisão exista nestas situações. Contudo, faz-se imperioso interpretar a LGPD de modo sistemático e teleológico, uma vez que se trata de um microssistema completo protetivo de dados e, para esta interpretação alcançar a completude, é necessária uma visita aos princípios sob os quais o tratamento de dados deve ser realizado, conforme art. 6 da mesma legislação²⁴, a saber:

Como há direito ao tratamento de dados com transparência sobre a finalidade, adequação, necessidade e predomina a ideia do livre acesso, não faz sentido compreender que o titular de dados – empregado – não possua o direito de informações claras sobre as decisões automatizadas, inclusive as que contenham interferência humana. A transparência depende da informação, pois uma retroalimenta a outra.²⁵

Para além desta ótica, constata-se que embora a análise de compatibilidade de perfis *de per si* não implique isoladamente em uma decisão final, é inegável que imprime um impacto considerável no decurso do processo seletivo e na decisão humana. Afinal, trata-se de uma funcionalidade que logicamente foi criada para otimizar o tempo da pessoa recrutadora, atuando na diminuição do trabalho manual e na eliminação de tarefas repetitivas. Logo, logicamente,

24. ALMEIDA, Dayse Coelho de. *Lei Geral de Proteção de Dados e novos direitos do empregado na decisão automatizada*. Disponível em: <https://www.migalhas.com.br/depeso/356587/lgpd-e-novos-direitos-do-empregado-na-decisao-automatizada>. Acesso em: 19 jan. 2025.

25. Ibidem.

em uma situação em que o time de recrutamento possui um grande volume de currículos e faz uso de inteligência artificial para analisá-los, a atenção maior se volta para os candidatos que foram mapeados como um “alto *fit*” com a vaga, apresentaram um *score* elevado ou uma melhor colocação no *ranking*.

Portanto, faz-se importante considerar o risco de vieses humanos, como o viés de confirmação e o automatismo humano, em influenciar a atuação das pessoas recrutadoras frente aos resultados fornecidos pela inteligência artificial. Ou seja, ao visualizar uma classificação vantajosa, há uma tendência natural de confirmar essa avaliação inicial feita pela IA, buscando inconscientemente apenas elementos que reforcem a percepção positiva daquele candidato, em detrimento de uma análise mais crítica e isenta. Esse fenômeno, aliado ao automatismo – em que decisões humanas passam a ser tomadas de forma quase mecânica com base em sugestões automatizadas – pode reduzir a autonomia crítica dos profissionais de recrutamento e comprometer o processo seletivo.

De modo a corroborar com o contexto, manifestam-se Micaela Barros Barcelos Fernandes e Camila Helena Melchior no sentido de que a mera presença de uma pessoa humana na cadeia de etapas decisórias não é assecuratória de decisões justas e em conformidade com o ordenamento jurídico, de forma que esta pode ser apenas uma presença formal, mas não substancial. Ao mesmo passo, um processo decisório unicamente automatizado não necessariamente resulta em decisões injustas. Nota-se:

Embora se reconheça que, com a automatização os riscos de processamentos que levam a resultados indevidamente discriminatórios aumentam, eles não estão necessariamente vinculados a um processo de decisão unicamente automatizada. A pressuposição de que o problema de decisões que violam a normativa vigente e garantias de não discriminação decorrem somente da automatização, como parece ter sido a escolha estrutural da lei, pode resultar em situações injustas, mas aparentemente não questionáveis. Os intérpretes e os aplicadores da lei devem estar atentos a esta possibilidade.

Cabe, portanto, uma interpretação funcional do dispositivo, para que seja alcançado o objetivo do legislador, isto é, garantir ao titular de dados um tratamento não discriminatório e que respeite a privacidade e a autodeterminação do titular dos dados, como se depreende de outros dispositivos contidos na lei.²⁶

26. FERNANDES, Micaela Barros Barcelos; OLIVEIRA, Camila Helena Melchior Baptista. O artigo 20 da LGPD e os desafios interpretativos ao direito à revisão das decisões dos agentes de tratamento pelos titulares de dados. *Revista de Direito e as Novas Tecnologias*. Rio de Janeiro, vol. 8, p.4, 2020.

Reconhece-se que as abordagens mencionadas oferecem um equilíbrio interessante entre eficiência empresarial e proteção dos direitos dos candidatos, permitindo que a decisão final seja feita por um recrutador humano, o que ajuda a manter um controle ético maior sobre o processo e pode ser visto como uma forma de reduzir os vieses discriminatórios. Contudo, não deixam de apresentar desafios em termos de transparência e explicabilidade, de forma que os candidatos podem se sentir frustrados se não entenderem como foram classificados e o porquê do resultado da compatibilidade. Portanto, o candidato deve ter a oportunidade de questionar sua posição na avaliação realizada, e as plataformas ATS devem estar preparadas para fornecer explicações claras sobre os critérios usados no processo, sem, contudo, afetar o direito das empresas de garantirem seus segredos industriais e propriedade intelectual²⁷.

Dessa forma, torna-se relevante que as organizações estejam atentas inclusive às diretrizes internacionais de uso ético da IA, como as estabelecidas pela UNESCO e pela OCDE, especialmente no que diz respeito à explicabilidade. Neste contexto, tem-se pela OCDE que o Princípio em questão visa permitir que as pessoas afetadas pelo resultado de um sistema de IA entendam como ele foi alcançado, o que implica no fornecimento de informações fáceis de entender e que possam permitir que indivíduos afetados adversamente contestem o resultado, os fatores e a lógica que levaram a um resultado. Dessa forma, a explicabilidade deve ser adaptada ao contexto, pois, em alguns casos, exigir explicações pode comprometer a precisão, a segurança ou aumentar custos, afetando especialmente pequenas e médias empresas²⁸. No mesmo sentido, a UNESCO entende que embora sejam necessários esforços para aumentar a transparência e a explicabilidade dos sistemas de IA, para apoiar a governança democrática, o nível desses dois aspectos sempre deve ser adequado ao contexto e ao impacto, pois pode haver uma necessidade de equilíbrio entre transparência, explicabilidade e outros princípios, como privacidade, segurança e proteção²⁹.

A explicabilidade desses sistemas também se refere à compreensibilidade sobre a entrada, a saída e o funcionamento de cada bloco de construção dos algoritmos e como ele contribui para o resulta-

27. ALMEIDA, Dayse Coelho de. *Lei Geral de Proteção de Dados e novos direitos do empregado na decisão automatizada*. Disponível em: <https://www.migalhas.com.br/depeso/356587/lgpd-e-novos-direitos-do-empregado-na-decisao-automatizada>. Acesso em: 19 jan. 2025.

28. OCDE. Transparência e explicabilidade. Disponível em: <https://oecd.ai/en/dashboards/ai-principles/P7>. Acesso em: 16 abr. 2025.

29. UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. Paris: Organização das Nações Unidas para a Educação, a Ciência e a Cultura, 2022, p. 20.

do dos sistemas. Assim, a explicabilidade está estreitamente relacionada com a transparência, pois os resultados e os subprocessos que conduzem a resultados devem almejar serem compreensíveis e rastreáveis, conforme o contexto. Os atores de IA devem se comprometer a garantir que os algoritmos desenvolvidos sejam explicáveis. No caso de aplicativos de IA que afetam o usuário final de uma forma que não seja temporária, facilmente reversível ou de baixo risco, deve-se garantir que seja fornecida uma explicação significativa para qualquer decisão que resultou na ação tomada, para que o resultado seja considerado transparente. Transparência e explicabilidade estão intimamente relacionadas com medidas de responsabilidade e prestação de contas adequadas, assim como com a confiabilidade dos sistemas de IA³⁰.

Para tanto, faz-se necessário que uma política de transparência entre dados, parâmetros e padrões adotados pela IA sejam acessíveis. Neste prisma, um sistema inteligível, transparente ou compreensível é aquele que permite ao ser humano compreender o seu funcionamento de forma a esclarecer dúvidas específicas sobre como é que executa determinadas decisões ou previsões. Dessa forma, ao adotar uma postura proativa, as empresas podem não apenas garantir a conformidade, como também fortalecer sua reputação e atratividade como empregadoras, promovendo um ambiente de confiança e respeito mútuo no mercado.

Considerações finais

Em uma nova realidade corporativa, cada vez mais tecnológica, as plataformas digitais de recrutamento se tornaram a principal forma de recrutamento na maioria das empresas. Essas plataformas reduzem o tempo de recrutamento para o preenchimento de vagas e têm o desafio de fornecer mecanismos eficientes de seleção.³¹ Para atender a essa demanda, muitas plataformas digitais voltadas para o setor de *talent acquisition* passaram a integrar a inteligência artificial em suas funcionalidades, valendo-se de algoritmos para fazer a triagem e análise de perfis, de forma a identificar e destacar os candidatos que melhor se aderem aos requisitos da vaga divulgada, trazendo ganhos em relação a agilidade e redução de custos.

Contudo, esse avanço tecnológico também traz à tona questões éticas e legais, especialmente no que diz respeito à transparência, à privacidade dos

30. Ibidem.

31. FREIRE, Maurício Noris; CASTRO, Leandro. *e-Recruitment recommender systems: a systematic review*. London: Knowledge and Information Systems, 2020, p. 5.

dados e à possível perpetuação de vieses discriminatórios nos processos seletivos, vez que a inteligência artificial não apenas baseia suas decisões em grandes volumes de dados, como também aprende através de padrões que podem, inadvertidamente, reproduzir preconceitos sociais já existentes. Ante o exposto, fatores como gênero, raça, idade ou até mesmo localização podem ser indiretamente considerados nas análises, resultando na exclusão de candidatos de grupos minoritários e na manutenção de representações estereotipadas no ambiente corporativo – inclusive sem que a sociedade saiba disso, dada a falta de transparência dos modelos utilizados.

Desta forma, torna-se essencial recorrer a preceitos da LGPD, especialmente ao princípio da transparência e ao direito à revisão de decisões automatizadas, conferindo aos candidatos o direito de questionar decisões tomadas através de algoritmos que os afetem negativamente, como uma eventual exclusão de uma vaga ou uma classificação inferior no processo seletivo. Esse direito à revisão é essencial para garantir que os algoritmos operem de forma justa e ética, permitindo que os candidatos possam se proteger contra decisões discriminatórias ou arbitrárias.

Neste sentido, com base nos preceitos do art. 20 da Lei Geral de Proteção de Dados, as empresas e as plataformas que utilizam inteligência artificial para triar candidatos têm a responsabilidade de informar claramente os usuários sobre como os dados estão sendo processados, quais algoritmos são utilizados e como podem questionar decisões que considerem injustas ou discriminatórias. Contudo, ao limitar o direito à explicação apenas às decisões exclusivamente automatizadas, o texto normativo cria uma zona cinzenta, que desafia a aplicação plena da norma, principalmente nestes processos decisórios híbridos, nos quais a intervenção humana ainda é significativa.

A área de recrutamento e seleção ilustra bem a complexidade do cenário, vez que embora a decisão final, em muitos casos, seja tomada por um ser humano, a análise algorítmica exerce uma influência considerável no processo, o que levanta questões sobre a aplicabilidade do direito à revisão. A interpretação sistemática e teleológica da LGPD, aliada à observância dos princípios que regem o tratamento de dados, como transparência, adequação e necessidade, sugere que o titular dos dados, mesmo em contextos de decisão híbrida, deve ter o direito de compreender os critérios utilizados na análise automatizada e questionar os resultados obtidos.

Dessa forma, a imprecisão da linguagem jurídica impõe o estabelecimento de critérios interpretativos adicionais que permitam avaliar se, quando e

em que circunstâncias a intervenção humana seria necessária para legitimar a decisão adotada, dependendo de uma interpretação mais abrangente para lidar com a realidade.

Referências

ALBERTO, Leonardo de Andrade; YASUOKA, Renan Takeshi; PIERANTI, Octavio Penna. *O uso de inteligência artificial nos processos de recrutamento e seleção: reflexões introdutórias*. São Paulo: Simpósio dos Programas de Mestrado Profissional, 2021.

ALMEIDA, Dayse Coelho de. Lei Geral de Proteção de Dados e novos direitos do empregado na decisão automatizada. Disponível em: <https://www.migalhas.com.br/depeso/356587/lgpd-e-novos-direitos-do-empregado-na-decisao-automatizada>. Acesso em: 19 jan. 2025.

ARBEX, Gabriela. Estudo mapeia HR Techs do Brasil e aponta enorme potencial de crescimento. Disponível em: <https://forbes.com.br/forbes-tech/2020/06/exclusivo-estudo-mapeia-rh-techs-do-brasil-e-aponta-enorme-potencial-de-crescimento/>. Acesso em: 03 jan. 2025.

BRASIL. Lei 13.709/2018. *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: 19 jan. 2025.

CIPRIANO, Gael Santos; CERIBELI; Harrison Bachion; MACIEL, Gustavo Nunes; CAMPOS, Rita de Cássia Legal. Inteligência artificial nos processos de seleção de RH. *Revista Estudos de Administração e Sociedade*, n.2, v.6. Niterói: Universidade Federal Fluminense, 2021.

FERNANDES, Micaela Barros Barcelos; OLIVEIRA, Camila Helena Melchior Baptista. O artigo 20 da LGPD e os desafios interpretativos ao direito à revisão das decisões dos agentes de tratamento pelos titulares de dados. *Revista de Direito e as Novas Tecnologias*. Rio de Janeiro, vol. 8, p.4, 2020.

FREIRE, Maurício Noris; CASTRO, Leandro. *e-Recruitment recommender systems: a systematic review*. London: Knowledge and Information Systems, 2020.

ICO – INFORMATION COMMISSIONER’S OFFICE. Detailed Guidance on Automated Decision-Making and Profiling (2018). Disponível em: <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling-1-1.pdf>. Acesso em: 19 jan. 2025.

JUNQUEIRA, Thiago. *Discriminação: o desafio da inteligência artificial em processos seletivos*. Disponível em: <https://veja.abril.com.br/economia/discriminacao-o-desafio-da-inteligencia-artificial-em-processos-seletivos>. Acesso em: 05 jul. 2024.

LIMA, Francisco Gérson Marques de; MORAIS, Ricardo Antônio Maia de. Decisões automatizadas nas relações de emprego: art. 20 da LGPD ante o silêncio da CLT. O uso de dados pessoais e inteligência artificial na relação de trabalho: proteção, discriminação, violência e assédio digital. Brasília: Ministério Público do Trabalho, 2022.

LIMA, Lindamaria. PL 4496/2019 – Entendendo o conceito de decisão automatizada. Disponível em: <https://blog.tripla.com.br/decisao-automatizada/>. Acesso em: 15 jan. 2025.

LIMA, Taisa Maria Macena; SÁ, Maria de Fátima Freire. Inteligência Artificial e Lei Geral de Proteção de Dados Pessoais: o direito à explicação nas decisões automatizadas. *Revista Brasileira de Direito Civil*, v.26. Belo Horizonte: 2020.

OCDE. Transparência e explicabilidade. Disponível em: <https://oecd.ai/en/dashboards/ai-principles/P7>. Acesso em: 16 abr. 2025.

POISAT, Paul; MEY, Michelle R. Gestão eletrônica de recursos humanos: aprimorado ou fascinante? *Jornal de Gestão de Recursos Humanos*, n.5. África do Sul: Universidade Metropolitana Nelson Mandela, 2017.

SANKIEVICZ, Alexandre; PINHEIRO, Guilherme Pereira. Aspectos da proteção de dados nas relações de trabalho. In: DONEDA, Danilo... [et al.]. *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. Paris: Organização das Nações Unidas para a Educação, a Ciência e a Cultura, 2022, p. 20.

VAINZOF, Rony; GUTIERREZ, Andriei. Transparência e revisão de decisões automatizadas. In: VAINZOF, Rony; GUTIERREZ, Andriei. *Inteligência Artificial (IA)*. São Paulo: Editora Revista dos Tribunais, 2021.

WIMMER, Miriam; DONEDA, Danilo. “Falhas de IA” e a intervenção humana em decisões automatizadas: parâmetros para a legitimação pela humanização. Dossiê – Inteligência Artificial, Ética e Epistemologia, vol.18, n.100. Brasília: Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, 2021.

WP29 – Grupo de Trabalho do Artigo 29 para a Proteção de Dados. Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679. Adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection_pt. Acesso em: 19 jan. 2025.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

EIXO IV

Reconhecimento Facial, Segurança e Infância

AUTORES

Ana Carolina Gomes Rosa

Manuela Pereira Gomes

Maria Emilia Loth Machado

**Segurança biométrica: a
utilização de reconhecimento
facial para identificação
biométrica dos espectadores
em arenas esportivas e
o tratamento de dados
pessoais sensíveis à luz da Lei
Geral de Proteção de Dados**

MANUELA PEREIRA GOMES

Sumário: Introdução. 1. O reconhecimento facial e a Lei Geral do Esporte. 2. Lei Geral de Proteção de Dados: o dado biométrico como um dado pessoal sensível. 3. Os riscos da utilização de reconhecimento facial. Considerações finais. Referências.

Introdução

Este trabalho tem como objetivo analisar a compatibilidade da obrigação legal de uso de reconhecimento facial em arenas esportivas com capacidade para mais de vinte mil pessoas, prevista no art. 148 da Lei Geral do Esporte (Lei nº 14.597/2023), com os princípios e garantias previstos na Lei Geral de Proteção de Dados (Lei nº 13.709/2018). Atualmente, o uso de reconhecimento facial apresenta inúmeros riscos aos direitos à liberdade, igualdade e proteção de dados pessoais, urgindo a necessidade de um debate social a respeito das tecnologias de reconhecimento facial.

Os sistemas de reconhecimento facial estão presentes em vários setores da vida cotidiana ao ponto de um simples telefone celular possuir a opção de reconhecimento facial como forma de desbloqueio de tela. Antes a identificação biométrica facial era vista como uma tecnologia futurista apresentada em filmes de ação e ficção científica, mas com auxílio da inteligência artificial (IA) e a mineração de dados, os equipamentos de reconhecimento facial permitem que indivíduos sejam identificados em tempo real.

A contemporaneidade está sendo marcada pela ascensão da segurança biométrica, no qual os equipamentos biométricos apresentam resultados rápidos e precisos, revolucionando o modo de se prestar serviços de segurança em locais de acesso ao público. Nessa perspectiva, a obrigatoriedade da identificação biométrica dos espectadores em arenas esportivas com capacidade para mais de vinte mil pessoas, prevista no art. 148 da Lei Geral do Esporte, enquadra-se como uma das hipóteses de tratamento de dados pessoais sensíveis, visto que os dados biométricos são considerados dados pessoais sensíveis pelo art. 5º, II, da Lei Geral de Proteção de Dados.

Visando abordar a problemática dos riscos da implementação dos sistemas de reconhecimento facial para identificação dos espectadores em arenas esportivas, esse trabalho justifica-se diante o baixo acervo literário sobre o tema e o fato do parágrafo único do art. 148 da Lei Geral do Esporte, prevê que

1. Pós-graduanda em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio (ITS Rio), em parceria com a Universidade do Estado do Rio de Janeiro (UERJ) e o Centro de Estudos e Pesquisas no Ensino do Direito (CEPED). Advogada e Consultora Jurídica.

as arenas esportivas deverão se adequar a obrigatoriedade até 2025, exsurgindo a necessidade da exploração do tema no meio acadêmico e social.

Considerando o atual cenário que nenhuma lei brasileira disciplina a utilização da tecnologia de reconhecimento facial, nota-se que os problemas relacionados à utilização dessa tecnologia vão desde análise facial discriminatória até a vigilância dos cidadãos. Dessa forma, o presente trabalho partiu da necessidade de entender como a utilização do reconhecimento facial em arenas esportivas pode impactar direta ou indiretamente na realidade social do cidadão brasileiro.

A metodologia utilizada compreendeu uma pesquisa básica, de abordagem qualitativa e de caráter exploratório, a partir de uma revisão bibliográfica e legislativa, apresentando uma visão geral sobre a tecnologia de reconhecimento facial, identificação biométrica em arenas esportivas, dados biométricos, tratamento de dados pessoais sensíveis e os eventuais riscos do uso de reconhecimento facial.

O presente trabalho está estruturado em três seções. A primeira define o que seria a tecnologia de reconhecimento facial e o seu uso para o cumprimento da obrigatoriedade presente na Lei Geral do Esporte. A segunda seção aborda a análise do dado biométrico com um dado pessoal sensível e o uso de sistemas de reconhecimento facial para identificação biométrica dos espectadores em arenas esportivas como uma hipótese de tratamento de dados pessoais sensíveis. E, por fim, a terceira seção trata da abordagem dos riscos da utilização da tecnologia de reconhecimento facial.

1. O reconhecimento facial e a Lei Geral do Esporte

Na sociedade contemporânea, diversos aparelhos telefônicos estão sendo desbloqueados instantaneamente quando colocados em frente aos rostos de seus usuários; empresas averiguam o nível de satisfação de determinados produtos através da análise facial dos seus clientes ao efetuarem compras em uma de suas lojas físicas; e empresas de ônibus estão permitindo o acesso dos passageiros através do reconhecimento facial em catracas. Antes a utilização da tecnologia de reconhecimento facial era algo futurístico que só era visto em filmes de ação e ficção científica.

A ascensão da segurança biométrica contribuiu para a normalização da identificação biométrica facial. Os equipamentos biométricos funcionam através do mapeamento de impressões digitais, verificação de retina, reconhecimento de voz e facial. Eles permitem que através da métrica de características

físicas ou comportamentais que um indivíduo seja a identificação, autenticação e autorização de determinado indivíduo.

Como categoria da segurança biométrica, o mecanismo de reconhecimento facial funciona com base em processo de identificação automatizada de atributos faciais, que pode ocorrer em tempo real ou não. Para a melhor compreensão do reconhecimento facial, vale destacar que o reconhecimento é iniciado com a coleta da imagem da pessoa, esta imagem passa por um filtro que determinará se uma face humana ou não. Com a normalização, os rostos são classificados em padrões, e logo em seguida, os atributos físicos são remodelados em pontos de referência que serão utilizados para verificar a semelhança entre a imagem capturada e armazenada².

Como as demais tecnologias contemporâneas, o reconhecimento facial funciona com o auxílio da inteligência artificial (IA) e também aprende a diferenciar os rostos pelo *data mining* (mineração de dados). O resultado de reconhecimento facial é dado pelo treinamento de algoritmos que foram alimentados com uma grande quantidade de dados extraídos de diferentes rostos capturados, no qual o treinamento possibilita que a máquina detecte, classifique, verifique e identifique indivíduos específicos ou grupo de pessoas.

Nesta perspectiva, Stefano Rodotà, em sua obra intitulada “Transformações do corpo”, propõe que o corpo humano virou uma fonte para novas informações. Como objeto do *data mining*, o corpo humano se tornou em uma espécie de senha para identificação ou chave de acesso a serviços, fazendo que os dados biométricos não sejam utilizados somente para identificação, mas também como uma forma permanente de confirmação de identidade³. É possível verificar a transformação do corpo em uma senha para acesso em serviços pode ser exemplificada pela obrigatoriedade identificação biométrica facial por reconhecimento facial em arenas esportivas.

A transformação do corpo em uma senha para acesso a serviços pode ser exemplificada pela obrigatoriedade de identificação biométrica facial por reconhecimento facial em arenas esportivas, disposta na Lei nº 14.597/2023, que foi promulgada no dia 14 de junho de 2023, que instituindo a Lei Geral do Esporte (LGE).

2. OLIVEIRA, Bruno Bastos de; MALDONADO, Glesler Sales. *A necessária regulação do reconhecimento facial no Brasil dos riscos à intimidade e à privacidade*. RIOS-Revista Científica do Centro Universitário do Rio São Francisco. Bahia, v. 17, n. 35, p. 160-182, dez.2022. Disponível em: <http://www.publicacoes.unirios.edu.br/index.php/revistarios/article/view/730>. Acesso: 12 nov. 2024. p. 168.

3. RODOTÁ, Stefano. *Transformações do corpo*. Revista Trimestral de Direito Civil, Rio de Janeiro, v. 5, n. 19, p. 91-107, jul./set. 2004. p. 93.

A subseção II da Lei nº 14.597/2023, intitulada “Da segurança nas Arenas Esportivas e do Transporte Público”, presente na Seção II do Capítulo IV, destaca o direito à segurança nas arenas esportivas, prevendo que o espectador esportivo tem o direito à segurança durante a totalidade do evento esportivo até mesmo após a realização das provas e partidas (art. 146 da LGE). A lei inova ao trazer a obrigação legal de identificação biométrica dos espectadores em arenas esportivas com capacidade para mais de vinte mil pessoas, prevista em seu art. 148.

O controle e fiscalização do acesso do público deverá ser feito por uso de reconhecimento facial nas catracas para a identificação biométrica dos espectadores em arenas esportivas com capacidade para mais de vinte mil pessoas, devendo ser criadas centrais técnicas com a devida estrutura para o monitoramento do público presente e o cadastramento biométrico dos espectadores (art. 148, *caput*, da LGE). A identificação biométrica facial está sendo realizada através de sistemas de reconhecimento facial.

Figura como uma condição de acesso e permanência no recinto esportivo, a necessidade do espectador com mais de 16 anos se cadastrar no sistema de controle biométrico (art. 158, XII, da LGE). Caso descumpra esta condição, o espectador poderá ser impossibilitado de acessar a arena esportiva ou, até mesmo, ser afastado imediatamente do recinto esportivo (art. 158, parágrafo único, da LGE).

Levando em conta a entrada em vigor da Lei Geral do Esporte, dia 14 de junho de 2023, as arenas esportivas com capacidade para mais de vinte mil pessoas, terão até 2025 para cumprir a obrigatoriedade da identificação biométrica facial (art. 148, parágrafo único, da LGE). Alguns estádios de futebol estão cumprindo a obrigatoriedade por meio do uso de sistemas de reconhecimento facial em catracas. A implementação desta tecnologia em estádios de futebol, contribui para redução da prática do cambismo, auxiliou na responsabilização daqueles que cometeram ilícitos e reduziu o tempo de espera das filas que permitem o acesso ao estádio de futebol.

O Ministério do Esporte, pela Portaria nº 55 de 17 de agosto de 2023, listou os requisitos mínimos obrigatórios que devem constar nos laudos técnicos referentes às condições de segurança em estádios utilizados para competições esportivas. A portaria definiu como de “grande porte” os estádios com capacidade para mais de vinte mil pessoas e os clubes que utilizarem esses estádios de grande porte, deverão elaborar o Plano Completo de Segurança, que deve constar: o ponto de controle de acesso, os mecanismos de controle

de acesso que impeçam o ingresso de torcedores desautorizados ou objetos ilícitos no estádio, sendo o sistema de reconhecimento facial um mecanismo de controle e acesso⁴.

O uso de reconhecimento facial para identificação dos espectadores em arenas esportivas com capacidade para mais de vinte mil pessoas, deverá ser feito conforme os princípios e garantias previstos na Lei Geral de Proteção de Dados. O reconhecimento facial como categoria da segurança biométrica, funciona pelo tratamento de dados biométricos, considerados dados pessoais sensíveis à luz do art. 5º, II, da LGPD.

2. Lei Geral de Proteção de Dados: o dado biométrico como um dado pessoal sensível

A Lei nº 13.709/2018, popularmente conhecida como Lei Geral de Proteção de Dados (LGPD), foi publicada em 14 de agosto de 2018, entrando em vigor somente em agosto de 2020. A referida lei disciplina o tratamento de dados pessoais realizado por pessoa natural ou jurídica, visando a proteção de direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural (art.1º, *caput*, da LGPD).

O dado pessoal é objetivamente conceituado no art. 5º, I, da LGPD, como “informação relacionada a pessoa natural identificada ou identificável”. Já o art. 5º, II, da LGPD, define o dado pessoal que pode ser compreendido como um dado pessoal sensível⁵, sendo o dado biométrico definido como um dado pessoal sensível, mas a LGPD acaba não conceituando o que seria um dado biométrico.

Diante da ausência de conceituação legal, é necessário reportar ao Decreto nº 10.046/2019, que define os atributos biométricos no inciso II do art. 2º, como: “características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou íris dos olhos, o formato da face, a voz e a maneira de andar”.

Com o auxílio da definição de atributos biométricos dada pelo Decreto nº 10.046/19, é possível compreender que os dados biométricos podem ser extraídos de impressões digitais, íris e outros atributos físicos ou comportamen-

4. BRASIL. Ministério do Esporte. Gabinete da Ministra. Portaria nº 55, de 17 de agosto de 2023. Brasília, 2023.

5. “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”.

tais, possibilitando a identificação ou confirmação pessoal individualizada de uma pessoa natural através de um reconhecimento automatizado.

Quando o indivíduo é identificado biometricamente por um sistema reconhecimento facial, o resultado é obtido por meio de um reconhecimento automatizado que funciona através do tratamento de um dado pessoal sensível, o dado biométrico. Para Teffé, o dado pessoal sensível possui em seu núcleo um conteúdo que pode ser utilizado para reprodução de discriminações ilícitas ou abusivas, e essa delimitação como sensível, demarca a necessidade de uma proteção mais específica e essencial para a garantia dos direitos e liberdades fundamentais do titular, pois, esses dados sensíveis trazem em seu núcleo informações que tratadas inadequadamente ou vazadas poderão ensejar discriminações ilícitas ou abusivas, gerando risco à pessoa humana⁶.

Como a proteção dos dados pessoais está intimamente relacionada à observância do princípio da dignidade da pessoa humana, um dos fundamentos da República Federativa do Brasil (art. 1º, III, da CRFB/1988), e a promoção da igualdade em seu sentido material, o art. 7º da LGPD, trata as hipóteses do tratamento de dados pessoais e as hipóteses de tratamento de dados pessoais sensíveis estão exemplificadas no art. 11 da LGPD em virtude da relevância dos dados pessoais sensíveis para garantia de direitos e liberdades fundamentais.

A qualificação dos dados pessoais como sensíveis reforça a necessidade de uma proteção mais rigorosa dos dados pessoais sensíveis, pois esta qualificação dos dados pessoais denota que o tratamento inadequado desses dados poderão facilitar a exclusão e segregação. Assim, com o desenvolvimento tecnológico pautado no armazenamento e circulação de dados pessoais, a privacidade como autodeterminação informativa/existencial ganha maior destaque, de modo que novas formas de manifestação de proteção jurídica de pessoa humana, serão desenvolvidas como forma de resposta às ameaças de estigmas e discriminações tecnológicas⁷.

Vale destacar, que o rol das hipóteses de tratamento de dados pessoais sensíveis não é um rol taxativo, pois o art. 11, § 1º, da LGPD, autoriza que as hipóteses de tratamento de dados pessoais sensíveis sejam aplicadas em situações de tratamento de dados pessoais que revelem dados pessoais sensíveis e causem lesões ao seu titular. Ademais, no Enunciado nº 689 da IX Jornada de

6. TEFFÉ, Chiara Spadaccini de. *Dados pessoais sensíveis: qualificação, tratamento e boas práticas*. 1. ed. Indaiatuba, SP: Foco, 2022. E-book. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 15 out. 2024.

7. KONDER, Carlos Nelson. *O tratamento de dados sensíveis à luz da Lei 13. 709/2018*. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord). *A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 451.

Direito Civil do Conselho da Justiça Federal (CJF), foi firmado o entendimento que não há hierarquia entre os dispositivos de tratamento de dados pessoais e de tratamento de dados pessoais sensíveis.

A obrigação legal da identificação biométrica dos espectadores por uso reconhecimento facial em arenas esportivas com capacidade para mais de vinte mil pessoas, prevista no art. 148 da LGE, enquadra-se em uma das hipóteses do tratamentos dos dados pessoais sensíveis da LGPD, em que tratamento será feito sem o consentimento do titular, conforme a previsão do art. 11, II, “a”, da LGPD, em que o tratamento de dados pessoais sensíveis poderá ser realizado para o “cumprimento de obrigação legal ou regulatória pelo controlador”.

O tratamento de dados pessoais sensíveis para a identificação biométrica por uso do reconhecimento facial, também será legítima quando voltada para a proteção da vida ou incolumidade física (art. 11, II, “e”, da LGPD) ou voltada para prevenção à fraude e à segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (art. 11, II, “g”, da LGPD).

A identificação biométrica facial em arenas esportivas ascende a observância dos princípios da não discriminação (art. 6º, IX, da LGPD) e o da responsabilização e prestação de contas (art. 6º, X, da LGPD) durante as atividades de tratamento de dados pessoais. O princípio da não discriminação veda que o tratamento de dados pessoais seja realizado para fins discriminatórios ilícitos ou abusivos. Pelo princípio da responsabilização e prestação de contas, caberá aos responsáveis pelo controle e fiscalização do acesso do público nas arenas esportivas, demonstrar que adotaram as medidas eficazes, e que cumprem com as normas de proteção de dados pessoais.

Outro princípio que merece destaque, é o princípio da transparência que garante aos titulares de dados a prestação de informações claras, precisas e de fácil acesso referente a realização do tratamento, sendo resguardado os segredos comercial e industrial (arts. 6º, IV e 9º, II, da LGPD). Nesse viés, o art. 20 da LGPD garante ao titular de dados o direito à explicação que pode ser compreendido como a possibilidade do titular de dados poder solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, especialmente dos tratamentos automatizados de dados pessoais destinados à definição de perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (art. 20, *caput*, da LGPD).

Pelo § 1º do art. 20 da LGPD, quando solicitada a revisão das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais,

o controlador deverá disponibilizar informações claras e adequadas sobre os critérios e os procedimentos adotados para resultado do tratamento, salvo as informações de segredos comercial e industrial. Cabe a Autoridade Nacional de Proteção de Dados (ANPD), diante da não disponibilidade pela justificativa de segredos comercial e industrial, realizar auditoria para verificação de aspectos discriminatórios (art. 20, § 2º, da LGPD).

Vale destacar, que o § 3º do art. 20 da LGPD, previa a possibilidade da revisão humana das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais. O referido parágrafo foi objeto de veto presidencial pelas justificativas do parágrafo ser contrário ao interesse público e possibilidade de gerar o aumento de custo para as empresas de moda acarretar barreiras para as negociações empresariais.

Como o reconhecimento facial é uma categoria da tecnologia biométrica, o resultado das tecnologias biométricas são dados por processos automatizados que possibilitam a identificação de um indivíduo mediante aspectos físicos únicos ou comportamentais⁸. Nessa conjuntura, os espectadores identificados biometricamente em arenas esportivas, poderão solicitar a revisão das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, cabendo a autoridade nacional realizar auditorias para averiguar a ocorrência de equívocos e discriminações por parte do sistema de reconhecimento facial utilizado pelas arenas esportivas.

Os falsos positivos constituem os principais dilemas que cercam a utilização do reconhecimento facial. Embora haja a previsão do direito à explicação e da possibilidade da autoridade nacional realizar auditorias para verificação de discriminações ilícitas ou abusiva por parte decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, não houve um estudo de avaliação de impacto à proteção de dados pessoais durante o processo legislativo da Lei Geral do Esporte, sendo necessário um debate público voltado a criação de uma legislação específica ou protocolo nacional sobre a utilização de reconhecimento facial em ambientes de acesso ao público.

3. Os riscos da utilização de reconhecimento facial

Devido a importância do incentivo e promoção do progresso científico em uma sociedade, o art. 218, *caput*, da Constituição Federal de 1988, estabelece que: “O Estado promoverá e incentivará o desenvolvimento científico, a

8. CANEZIN, Pedro Henrique. *Perícia papiloscópica e reconhecimento facial*. Curitiba, PR: Intersaberes, 2023. E-book. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 11 out. 2024. p. 126.

pesquisa, a capacitação científica e tecnológica e a inovação”. Para que haja o incentivo ao progresso científico e tecnológico é necessário considerar a ocorrência de alguns riscos, fazendo com que à medida que novas tecnologias vão sendo desenvolvidas, surgem novos desafios para a proteção de direitos consagrados como fundamentais.

Como visto, o reconhecimento facial como uma tecnologia que se vale de processos automatizados para o seu funcionamento e a LGPD garante aos espectadores identificados biometricamente o direito de solicitarem a revisão das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, devendo ser observados os segredos comercial e industrial. Essa observância impulsiona o problema da opacidade da máquina que consiste no fato de alguns agentes desenvolvedores de tecnologias se aproveitarem da justificativa da observância dos segredos comercial e industrial para não disponibilizarem as fórmulas matemáticas ou métodos utilizados para produção e aperfeiçoamento da máquina, dificultando a investigação dos aspectos discriminatórios.

O tratamento automatizado impacta diretamente na dinâmica social, ao ponto da decisão automatizada está sendo utilizada para condenar ou inocentar réus, admitir ou rejeitar recursos e selecionar os currículos que prosseguiram na vaga de emprego⁹. Boa parte da população não sabe como uma decisão automatizada funciona, muito menos, como os seus dados biométricos estão sendo tratados para o resultado do seu reconhecimento facial.

Referente o monitoramento por imagem com a identificação biométrica dos espectadores em arenas esportivas com capacidade para mais de 20 mil pessoas, foi identificado pela Coordenação-Geral de Fiscalização (CGF) da Autoridade Nacional de Proteção de Dados, indícios de irregularidade do uso do sistema de reconhecimento facial. Os torcedores estão sendo expostos à captura massiva de seus dados pessoais, havendo pouca transparência sobre a circulação, tratamento e o ciclo de vida dos dados biométricos dos torcedores.

Em 18 de janeiro de 2025, a ANPD iniciou a fiscalização sobre o uso dos sistemas de reconhecimento facial na venda de ingressos e no acesso a estádios de 23 clubes de futebol. A fiscalização tem como objetivo avaliar o cumprimento de obrigações de transparência e a adequação do tratamento de dados biométricos de crianças e adolescentes¹⁰. Foi constatado que não foram

9. LINDOSO, Maria Cristine Branco. *Discriminação de gênero no tratamento autorizado de dados pessoais*. 1. ed. Rio de Janeiro: Processo, 2021. E-book. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 12 nov. 2024. p. 123.

10. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. ANPD fiscaliza uso de sistema de reconhecimento facial na venda de ingressos na entrada de estádios por 23 clubes de futebol. 18 de fevereiro de 2025. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-fiscaliza-uso-de-sistema-de-reconhecimento-facial-na-venda-de-ingressos-e-na-entrada-de-estadios-por-23-clubes-de-futebol>. Acesso em: 15 abr. 2025.

disponibilizados aos responsáveis legais menores de idade os mecanismos necessários para o asseguramento da devida assistência durante os procedimentos de cadastramento biométrico de adolescentes.

A CGF expediu como medida preventiva a necessidade dos clubes de futebol terem que publicar informações claras sobre os procedimentos de cadastramento e identificação biométrica de torcedores nas plataformas de venda de ingressos. Os clubes ainda deverão apresentar os Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) demonstrando os procedimentos de cadastramento e identificação biométrica de torcedores, também devendo justificar a forma que ocorre o tratamento de dados biométricos dos menores de idade em prol de atender o melhor interesse da criança e adolescente.

Tangenciando a ascensão da segurança biométrica, é inegável que esses equipamentos são excelentes para o controle e fiscalização de ambientes públicos e privados. Porém, é necessário observar que o reconhecimento facial é feito pelo auxílio da inteligência artificial que não apresenta exatidão em seus resultados. Os algoritmos de inteligência artificial não trabalham com mecanismos de exatidão durante o processo da identificação biométrica facial, mas operam com mecanismos de ponto de semelhança que é somando ao fato das máquinas não serem dotadas de sensibilidade humana, há a possibilidade da aprendizagens equivocadas por dados mal coletados ou mal interpretados¹¹, sendo necessário a reflexão social sobre o uso do reconhecimento facial na vida cotidiana, pois a ausência da exatidão enseja problemas de falsos positivos, ou seja, o equipamento identifica uma pessoa, que na verdade, era outra pessoa.

A máquina ao apresentar resultados discriminatórios, reflete os preconceitos existentes na sociedade, pois uma invenção reflete as ideias do seu desenvolvedor. Os sistemas de reconhecimento facial, assim como a maioria das tecnologias, são predominantemente desenvolvidas por homens brancos que treinam os algoritmos a partir de seus rostos brancos e masculinos, resultando nos resultados discriminatórios equivocados ou abusivos, pois não há um treinamento pautado na diversidade de atributos faciais.

Os sistemas de inteligência artificial estão sendo implementados em diversos setores ao redor mundo, ao ponto de muitos países já se valem do policiamento preditivo em que através de uma análise de dados disponíveis a polícia pode prever o local que um crime pode ocorrer. Entretanto, inúmeras previsões

11. TOMASEVICIUS FILHO, Eduardo. *Reconhecimento Facial e lesões aos direitos da personalidade*. In: BARBOSA, Mafalda Miranda, BRAGA NETTO, Felipe; SILVA, Michael César; FALEIROS JÚNIOR, José Luiz de Moura Faleiros (coord.). *Direito digital e inteligência artificial: diálogos entre Brasil e Europa*. Indaiatuba, SP: Foco, 2021.p. 136-137.

foram distorcidas, já que o sistema foi alimentado por dados programados por humanos que acabam contaminando os sistemas com seus preceitos¹².

No tocante a raça, existe uma gritante diferença entre a taxa de acerto no reconhecimento de pessoas, sendo os rostos de pessoas negras os mais afetados pelos falsos positivos. No campo da segurança pública o viés é agravado, evidenciando que os programadores contaminam os dados com seus preceitos fundados nas relações históricas de desigualdade e discriminação¹³. O resultado equivocado por parte do sistema de reconhecimento facial, fomenta o racismo estrutural, acarretando no aumento da imputação criminal de pessoas pretas. Há uma necessidade de se rever possibilidade legal da revisão humana das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, principalmente pelo fato do resultado da revisão funcionar como meio de prova contra as discriminações, já que o direito de defesa no processo penal figura como uma garantia constitucional (art. 5º, LV, da CRFB/1998), e todas as atividades de tratamento de dados pessoais deverão observar o princípio da não discriminação (art. 6º, IX, da LGPD).

O Departamento de Polícia de Nova Iorque utiliza a tecnologia de reconhecimento facial para o policiamento discriminatório em bairros não-brancos, como o Bronx e Brooklyn, no qual esses bairros são os mais vigiados por câmeras que fomentaram o aumento da revista e abordagem racista pela polícia nova-iorquina¹⁴. A identificação biométrica facial em arenas esportivas, é uma hipótese de tratamento de dados pessoais sensíveis que ocorre sem o consentimento do titular, abrindo margem para as empresas capturarem em tempo real uma quantidade massiva de rostos de forma indiscriminada, impulsionando atividades econômicas pautadas na vigilância do cidadão.

Com desenvolvimento cada vez mais sofisticado das formas de vigilância, emerge o que Shoshana Zuboff conceitua como “capitalismo de vigilância” que consiste em um novo estágio do capitalismo em que as experiências humanas figuram como matéria-prima que serão traduzidas em dados com-

12. FREIRE DE SÁ, M. de F.; MACENA DE LIMA, T. M. *Inteligência artificial e Lei Geral de Proteção de Dados: o direito à explicação nas decisões automatizadas*. Revista Brasileira de Direito Civil, [S. l.], v. 26, n. 04, p. 227, 2021. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/584>. Acesso em: 21 out. 2024. p. 231.

13. CEIA, Eleonora Mesquita; TEFFÉ, Chiara Spadaccini. *Reconhecimento Facial e segurança pública nas cidades: uma análise crítica na perspectiva das competências federativas e dos direitos fundamentais*. In: EDLER, Daniel Edler Duarte; CEIA, Eleonora Mesquita (org.). *Tecnologia, Segurança e Direitos: os usos de sistemas de reconhecimento facial no Brasil*. Rio de Janeiro: Konrad Adenauer Stiftung, 2022. E-book. Disponível em: <https://www.kas.de/pt/web/brasilien/einzeltitel/-/content/tecnologia-seguranca-e-direitos-1>. Acesso em: 23 nov. 2024. p. 208.

14. ANISTIA INTERNACIONAL.EUA: a tecnologia de reconhecimento facial reforça a abordagem e revista revista da polícia de nova york – nova pesquisa. 23 de fevereiro de 2022. Disponível em: <https://anistia.org.br/informe/eua-a-tecnologia-de-reconhecimento-facial-reforca-a-abordagem-e-revista-racista-da-policia-de-nova-york-nova-pesquisa/>. Acesso em: 12 abr. 2025.

portamentais¹⁵. Para Zuboff, alguns dados comportamentais são declarados como “superávit comportamental do proprietário” que quando manufaturados, transforma-se em “produtos de predição”, possibilitando que grandes grupos econômicos prevejam os comportamentos e desejos dos titulares dos dados comportamentais.

As experiências humanas figuram como uma matéria-prima gratuita que permite que seja traçado um perfil psicossocial de cada titular de dados, fazendo que esses produtos de predição fomentem um novo tipo de mercado intitulado como “mercados de comportamentos futuros”. O capitalismo de vigilância exprime que os processos automatizados não só conhecem o comportamento humano, mas também moldam o comportamento humano.

Com a popularização da identificação biométrica por reconhecimento facial, é notório a necessidade de reflexão a cerca da discriminação algorítmica e sua utilização para vigilância em massa que ameaça os direitos à privacidade, liberdade e igualdade, sendo necessário a criação de uma lei específica ou protocolo nacional que discipline a utilização de reconhecimento facial em ambientes de acesso ao público.

Vale destacar, que a Lei Geral de Proteção de Dados não pode ser aplicada quando o tratamento de dados pessoais forem realizados exclusivamente para segurança (art. 4º, III, “a”, da LGPD). Entretanto, o tratamento de dados pessoais dos torcedores em arenas esportivas é realizado para uma relação de consumo entre os torcedores e as entidades esportivas, e não para fins exclusivos de segurança pública ou atividades de investigação e repressão de infrações penais, no qual o tratamento deverá ser regido por uma legislação específica que preverá as médias proporcionais e estritamente necessárias ao atendimento do interesse público (art. 4º, § 1º, da LGPD), podendo a autoridade nacional emitir opiniões técnicas ou recomendações, solicitando aos responsáveis, relatórios de impacto à proteção de dados pessoais (art. 4º, § 3º, da LGPD).

Até o presente momento, nenhuma legislação específica foi criada para disciplinar tratamento de dados pessoais realizados exclusivamente para segurança, assim como, não há em vigência nenhuma lei que discipline a utilização do reconhecimento facial ou da inteligência artificial. Há projetos de leis que versam sobre utilização da inteligência artificial no país, como o Projeto de Lei do Senado 2338, de 2023, de autoria do Senador Rodrigo Pacheco (MG),

15. 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.

que dispõe sobre o uso da IA no Brasil, destacando o direito da não-discriminação e à correção de vieses discriminatórios diretos, indiretos, ilegais ou abusivos; além de garantir o direito de contestar as decisões e de solicitar intervenção humana.

O texto final aprovado, em seu art. 5º prevê os direitos dos afetados pelos sistemas de inteligência artificial, sendo eles: “I – direito à informação quanto às suas interações com sistemas de IA, de forma acessível, gratuita e de fácil compreensão, inclusive sobre caráter automatizado da interação, exceto nos casos em que se trate de sistemas de IA dedicados única e exclusivamente à cibersegurança e à ciberdefesa, conforme regulamento”; “II – direito à privacidade e à proteção de dados pessoais, em especial os direitos dos titulares de dados nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e da legislação pertinente” ; “III – direito à não discriminação ilícita ou abusiva e à correção de vieses discriminatórios ilegais ou abusivos, sejam eles diretos ou indiretos.”¹⁶.

Diante da eventual ausência legal, a responsabilização será feita conforme o art. 149 da LGE, que dispõe que a responsabilidade pela segurança do espectador recai diretamente ao responsável pela realização esportiva e de seus dirigentes, sem prejuízo da aplicação das regras de responsabilidade do Código de Defesa do Consumidor. Assim, o responsável pela realização esportiva e seus dirigentes serão responsabilizados com base no art. 42 da LGPD pelos excessos do sistema de reconhecimento facial implantado, podendo recair as sanções previstas no art. 52 da LGPD.

Considerações finais

O trabalho desenvolvido observou o dilema da utilização da tecnologia do reconhecimento facial através do art. 148 da LGE, que prevê obrigatoriedade do monitoramento por imagem das catracas e com identificação biométrica dos espectadores nas arenas esportivas com capacidade para mais de 20 mil pessoas. Essa identificação biométrica em arenas esportivas dos espectadores é uma hipótese legítima para o tratamento de dados pessoais sensíveis, enquadrando-se na hipótese prevista no art. 11, II, “a”, da LGPD.

Todavia, não houve um estudo de impacto regulatório ou de proteção de dados durante o processo legislativo da Lei Geral do Esporte e com a vigência

16. SENADO FEDERAL. Projeto de Lei 2338, de 2023, do Sen. Rodrigo Pacheco. Dispõe sobre o desenvolvimento, fomento e uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2868197&filename=PL%202338/2023. Acesso em: 18 abr. 2025.

da lei, os direitos à privacidade, liberdade e igualdade estão correndo risco de serem violados pela falta de exatidão apresentada pela tecnologia de reconhecimento facial, afetando os grupos vulneráveis, pois os sistemas de inteligência artificial são alimentados por dados programados por humanos que acabam contaminando os sistemas.

Os objetivos deste estudo foram alcançados, visto que foi possível conceituar o reconhecimento facial, ressaltar o reconhecimento facial como uma tecnologia biométrica, analisar o dado biométrico como um dado pessoal sensível à luz da LGPD e abordar os riscos da identificação biométrica por reconhecimento facial. Logo, é necessário um debate multissetorial com a participação da sociedade civil, visando a criação de uma lei que discipline a utilização de sistemas de reconhecimento facial no país, especialmente que haja a previsão da possibilidade de avaliação de impacto à proteção de dados pessoais que será feita pela ANPD para que esta tecnologia seja utilizada em prol da segurança pública.

Caso o espectador se sinta lesado pelo resultado de sua identificação biométrica, o art. 20 da LGPD, garante o direito do titular de solicitar a revisão de decisões tomadas por tratamento automatizado de dados pessoais, devendo o controlador ceder informações claras e precisas sobre os critérios e procedimentos. Caso essas informações não sejam oferecidas com base na justificativa de segredos comercial e industrial, cabendo a ANPD realizar auditorias para a análise de aspectos discriminatórios em tratamentos automatizados.

Diante da ausência legal que discipline o uso reconhecimento facial no país, o art. 149 da LGE, dispõe que o responsável pela realização do evento esportivo e de seus dirigentes serão responsabilizados pelas eventuais análises equivocadas ou que deflagram discriminações ilícitas ou abusivas, ocorrendo a responsabilização com base nos art. 42 da LGPD, podendo recair as sanções administrativas do art. 52 da LGPD.

Com isso, foi possível constatar que o monitoramento por imagem das catracas e com identificação biométrica por reconhecimento facial em arenas esportivas com capacidade para mais de vinte mil pessoas, traz benefícios referentes a agilidade na investigação de crimes cometidos em ambientes esportivos e redução das filas de acesso ao local do evento esportivo, mas ao mesmo tempo põem em risco à própria segurança do espectador. Assim, pode-se compreender que o estudo contribui para demarcar a necessidade de uma regulação que discipline o uso da tecnologia de reconhecimento facial no país, prevendo que o reconhecimento facial seja utilizado de modo que não viole os direitos consagrados como fundamentais, cabendo a ANPD realizar

avaliações de impacto à proteção de dados pessoais, principalmente quando o mecanismo for utilizado no campo da segurança pública.

Diante de tais considerações, conclui-se que o reconhecimento facial é uma tecnologia biométrica que identifica o indivíduo através de processos automatizados. Assim, ao cumprir a obrigatoriedade do monitoramento por imagem das catracas e com identificação biométrica dos espectadores em arenas esportivas, o responsável pela realização esportiva e seus dirigentes deverão respeitar os princípios e garantias previstos na legislação de proteção de dados, pois tecnologia de reconhecimento facial pode apresentar resultados equivocados ou discriminatórios que violam direitos caros à sociedade.

Referências

ANISTIA INTERNACIONAL. EUA: a tecnologia de reconhecimento facial reforça a abordagem e revista revista da polícia de nova york –nova pesquisa. 23 de fevereiro de 2022. Disponível em: <https://anistia.org.br/informe/eua-a-tecnologia-de-reconhecimento-facial-reforca-a-abordagem-e-revista-racista-da-policia-de-nova-york-nova-pesquisa/>. Acesso em: 12 abr. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. ANPD fiscaliza uso de sistema de reconhecimento facial na venda de ingressos na entrada de estádios por 23 clubes de futebol. 18 de fevereiro de 2025. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-fiscaliza-uso-de-sistema-de-reconhecimento-facial-na-venda-de-ingressos-e-na-entrada-de-estadios-por-23-clubes-de-futebol>. Acesso em: 15 abr. 2025.

BRASIL. Conselho Federal. IX Jornada de Direito Civil: enunciados aprovados. Comemoração dos 20 anos da Lei nº 10.406/2022 e da instituição da Jornada de Direito Civil. Brasília: Conselho da Justiça Federal, Centro de Estudos Judiciários, 2022. 56 p. Disponível em: <https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf>. Acesso: 10 nov. 2024.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 05 nov. 2024.

BRASIL. Decreto nº 10.046, de 09 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm. Acesso em: 12 nov. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Institui a Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 05 nov. 2024.

BRASIL. Lei nº 14.597, de 14 de junho de 2023. Institui a Lei Geral do Esporte (LGE). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/L14597.htm. Acesso em: 05 nov. 2024.

BRASIL. Ministério do Esporte. Gabinete da Ministra. Portaria nº 55, de 17 de agosto de 2023. Brasília, 2023.

- CANEZIN, Pedro Henrique. *Perícia papiloscópica e reconhecimento facial*. Curitiba, PR: Intersaberes, 2023. E-book. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 11 out. 2024.
- CEIA, Eleonora Mesquita; TEFFÉ, Chiara Spadaccini. *Reconhecimento Facial e segurança pública nas cidades: uma análise crítica na perspectiva das competências federativas e dos direitos fundamentais*. In: EDLER, Daniel Edler Duarte; CEIA, Eleonora Mesquita (org.). Tecnologia, Segurança e Direitos: os usos de sistemas de reconhecimento facial no Brasil. Rio de Janeiro: Konrad Adenauer Stiftung, 2022. E-book. Disponível em: <https://www.kas.de/pt/web/brasilien/einzeltitel/-/content/tecnologia-seguranca-e-direitos-1>. Acesso em: 23 nov. 2024.
- FREIRE DE SÁ, M. de F.; MACENA DE LIMA, T. M. *Inteligência artificial e Lei Geral de Proteção de Dados: o direito à explicação nas decisões automatizadas*. Revista Brasileira de Direito Civil, [S. l.], v. 26, n. 04, p. 227, 2021. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/584>. Acesso em: 21 out. 2024.
- KONDER, Carlos Nelson. *O tratamento de dados sensíveis à luz da Lei 13. 709/2018*. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord). A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2019.
- LINDOSO, Maria Cristine Branco. *Discriminação de gênero no tratamento autorizado de dados pessoais*. 1. ed. Rio de Janeiro: Processo, 2021. E-book. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 12 nov. 2024.
- OLIVEIRA, Bruno Bastos de; MALDONADO, Glesler Sales. *A necessária regulação do reconhecimento facial no Brasil diante dos riscos à intimidade e à privacidade*. RIOS – Revista Científica do Centro Universitário do Rio São Francisco. Bahia, v. 17, n. 35, p. 160-182, dez. 2022. Disponível em: <http://www.publicacoes.unirios.edu.br/index.php/revistarios/article/view/730>. Acesso em: 12 nov. 2024.
- RODOTÀ, Stefano. *Transformações do corpo*. Revista Trimestral de Direito Civil, Rio de Janeiro, v. 5, n. 19, p. 91-107, jul./set. 2004.
- SENADO FEDERAL. Projeto de Lei 2338, de 2023, do Sen. Rodrigo Pacheco. Dispõe sobre o desenvolvimento, fomento e uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mos-trarintegra?codteor=2868197&filename=PL%202338/2023. Acesso em: 18 abr. 2025.
- TEFFÉ, Chiara Spadaccini de. *Dados pessoais sensíveis: qualificação, tratamento e boas práticas*. 1. ed. Indaiatuba, SP: Foco, 2022. E-book. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 15 out. 2024.
- TOMASEVICIUS FILHO, Eduardo. *Reconhecimento Facial e lesões aos direitos da personalidade*. In: BARBOSA, Mafalda Miranda, BRAGA NETTO, Felipe; SILVA, Michael César; FALEIROS JÚNIOR, José Luiz de Moura Faleiros (coord.). Direito digital e inteligência artificial: diálogos entre Brasil e Europa. Indaiatuba, SP: Foco, 2021.
- 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.

Reconhecimento facial nas escolas públicas brasileiras: sistema de segurança ou risco à privacidade?

ANA CAROLINA GOMES ROSA

Sumário: Introdução; 1 panorama geral da nova tecnologia: definindo o reconhecimento facial e entendendo a sua funcionalidade; 2 aspecto brasileiro na temática; 2.1 Como as leis brasileiras abordam a temática da proteção das crianças e dos adolescentes combinada com o reconhecimento facial; 2.2 O uso do reconhecimento facial nas escolas públicas brasileiras; 2.3 Seria a tecnologia de reconhecimento facial a mais adequada para lidar com os problemas das escolas públicas brasileiras? Considerações finais; Referências.

Introdução

A educação é um tema importantíssimo: é dever do Estado garantir que tal direito se cumpra, e a Constituição Federal de 1988 faz seu papel de tornar esse dever público². Sem fazer distinção de raça, cor, credo, etc., a Lei Maior declara que devem ser atendidas as demandas de busca por uma educação de qualidade.

Outro tema que não escapa aos olhos da população em geral, é a tecnologia. Atualmente, o acesso aos meios tecnológicos está tão intenso, e numa rapidez impressionante, que não se faz distinção de idade: todos estão se conectando, desde o mais novo ao mais velho.

Tecnologias como a do reconhecimento facial, por exemplo, têm auxiliado pessoas a desbloquearem o celular, entrarem no aplicativo do banco, confirmarem sua identidade no aeroporto, entrarem num estabelecimento, e até responderem à chamada na sala de aula.

O reconhecimento facial nas escolas públicas brasileiras tem sido comum por diversas razões, como garantir a segurança, otimizar o tempo gasto com atividades que a inteligência artificial poderia desempenhar, garantir uma diminuição de erros em que humanos podem incorrer, etc.³

Com uma ferramenta tão poderosa, é fundamental discutir os aspectos éticos que tais funcionalidades trazem como principais preocupações, visto que fatores – como os vieses da própria inteligência artificial por trás do servi-

1. Advogada com experiência em Proteção de Dados e Inteligência Artificial. Graduada em Direito pela Universidade Federal do Rio de Janeiro. Pós-Graduada em Direito Digital pelo ITS em parceria com a UERJ. Colaboradora do LABIDD (Laboratório de Inovação e Direitos Digitais da UFBA).

2. BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal, 2016. 496 p. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf. Acesso em: 9 dez. 2024.

3. TAVARES, C.; SIMÃO, B., MARTINS, F.; SANTOS, B., ARAÚJO, A.. “Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras”. São Paulo: *InternetLab*, 2023.

ço prestado – podem fazer com que ocorram situações de preconceitos, discriminações, injustiças, entre outros⁴.

Por fim, entendendo que a adoção dessas tecnologias traz situações tanto benéficas quanto maléficas, é essencial debater se tal recurso é o melhor a ser explorado pelos docentes ou se os prejuízos aos jovens estudantes serão maiores do que os benefícios trazidos.

Dessa forma, considerando o quão importante e atual é o tema, o presente trabalho se propõe a responder à seguinte pergunta: o uso de reconhecimento facial nas escolas públicas brasileiras está em conformidade com os direitos fundamentais das crianças? Consequentemente, será possível discutir a temática apresentada e entender se é viável desenharmos um modelo ideal, que seja capaz de lidar com as problemáticas que a tecnologia pode apresentar, para que, então, seja encarado somente o resultado proveitoso que ela tem a oferecer.

1. Panorama geral da nova tecnologia: definindo o reconhecimento facial e entendendo a sua funcionalidade

À medida em que as relações humanas aumentam e as diferentes tecnologias progridem, é preciso pensar em aprimorar técnicas de segurança que sejam capazes de lidar com os diferentes tipos de golpes existentes⁵. Dessa forma, recorrer à tecnologia de análise de características biológicas mostra-se como uma opção eficaz na tentativa de solucionar tal problema⁶.

A utilização de dados biométricos como forma de identificação ou verificação de um indivíduo vem se tornando uma prática cada vez mais comum, seja na seara privada ou na pública⁷. Esses dados podem estar relacionados à impressão digital, ao padrão de comportamento ou até mesmo ao gênero de uma pessoa⁸. Essa ferramenta como uma possibilidade cresce à medida que a tecnologia se mostra mais avançada⁹, substituindo métodos tradicionais, por

4. ANDREJEVIC, Mark; SELWYN, Neil. Facial recognition technology in schools: Critical questions and concerns. *Learning, Media and Technology*, v. 45, n. 2, p. 115-128, 2020.

5. CANUTO, Anne Magaly de Paula. Ética no Uso de Dados Biométricos: Histeria ou Uma Preocupação Coerente?. *Computação Brasil*, n. 47, p. 36-39, 2022.

6. *Ibid.*

7. TEFFÉ, Chiara Spadaccini de. Dados Biométricos: Uma Análise Crítica Acerca de Seu Tratamento e Aplicações. In: *Direitos fundamentais e novas tecnologias: homenagem ao professor Danilo Doneda/organizadores Ricardo Villas Bôas Cueva et al.* 1.ed – Rio de Janeiro: GZ, 2024.

8. WENDEHORST, Christiane; DULLER, Yannic. Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces. *European Parliament*, 2021.

9. ANDREJEVIC, Mark; SELWYN, Neil. Facial recognition technology in schools: Critical questions and concerns. *Learning, Media and Technology*, v. 45, n. 2, p. 115-128, 2020.

exemplo, como cartões de crédito/débito e senhas, na busca por uma opção mais eficiente e segura¹⁰.

A Lei Geral de Proteção de Dados Pessoais (LGPD)¹¹, no seu art. 5º, inciso II¹², classifica o dado biométrico como sendo de caráter sensível, reconhecendo, portanto, que o seu tratamento poderia acarretar a discriminação do titular do dado, e, por isso, sua proteção deve ser feita de forma ampla¹³.

Os dados biométricos podem ser coletados, entre outros, através do processo de reconhecimento facial, que é utilizado para identificar ou confirmar pessoas através da tecnologia, com o auxílio de vídeos, fotos ou até mesmo filmagens em tempo real¹⁴.

Esses sistemas buscam analisar a forma do rosto de cada pessoa (a distância dos olhos, a posição do nariz, o formato da boca etc.), entendendo que a natureza de cada rosto será diferente¹⁵. Apesar desse tipo de tecnologia ser menos preciso que outros métodos biométricos (por exemplo, esse mecanismo não funciona com qualidade em ambientes com pouca luminosidade), ele permite que a inspeção se dê de forma online¹⁶.

Para que um sistema como esse funcione, existem três importantes etapas que devem ser observadas e alcançadas: “captura e tratamento de imagem (1), detecção (2) e reconhecimento (3) dos rostos humanos”¹⁷.

Alinhado com essa diretriz, a Autoridade Nacional de Proteção de Dados (ANPD)¹⁸ define quatro parâmetros para a tecnologia de biometria atrelada ao reconhecimento facial, como sendo a detecção–tentativa de localização dos rostos apresentados em fotos e vídeos–, a identificação–entendendo se é possível reconhecer o indivíduo–, verificação–após o reconhecimento inicial, há a busca da pessoa no banco de dados do sistema–e classificação–alocar o indivíduo com base em seus perfis característicos, como raça, etnia, suas emoções, idade, etc.

No reconhecimento facial utilizado para verificar pessoas, a pergunta para a qual o sistema pretende emitir uma resposta, é: esse rosto que se apresenta tem

10. CANUTO, *op. cit.*

11. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados (LGPD)*.

12. “Art. 5º Para os fins desta Lei, considera-se: 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”

13. TEFFÉ, *op. cit.*

14. SULLIVAN, E. Facial recognition technology: verification vs. Identification. *Montana Legislative Services Division*, 2021.

15. ANDREJEVIC, Mark; SELWYN, Neil. Facial recognition technology in schools: Critical questions and concerns. *Learning, Media and Technology*, v. 45, n. 2, p. 115-128, 2020.

16. *Ibid.*

17. ALMEIDA, Luiz Felipe de Oliveira *et al.* Sistema de chamada escolar com reconhecimento facial utilizando opencv. *Revista de Ubiquidade*, v. 5, n. 2, p. 1-16, 2022, p. 2.

18. CEBRIAN, Fabiana S. P. Faraco *et al.* biometria e reconhecimento facial. Brasília: *Radar Tecnológico*, n. 2, 2024.

relação com o rosto esperado?¹⁹ É o que a máquina busca entender quando uma professora tira foto da turma, na busca por executar a chamada, por exemplo.

O setor da educação é uma das principais apostas para a aplicação desse tipo de tecnologia, considerando, principalmente, fatores como a responsabilidade de criação de disciplina na sala de aula e a crescente normalização do monitoramento de crianças e adolescentes em nome da segurança²⁰.

Entendendo que a internet pode ser acessada através do celular, é importante destacar que a pesquisa TIC Kids Online Brasil 2023²¹, produzido pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), registrou que cerca de 38% dos usuários de internet, que estão na faixa de idade entre 9 e 17 anos, acessaram a internet por meio de um aparelho celular apenas, além de identificar que as crianças e adolescentes que têm acesso a esse tipo de recurso têm habilidades digitais consideráveis.

Por conta da Covid-19, muitas escolas adotaram o “ensino virtual” como sua prática cotidiana²². Para que os professores tivessem um maior controle sobre os alunos, principalmente quando os estudantes estivessem realizando alguma prova, alguns colégios optaram por contratar sistemas de monitoramento, que utilizam inteligência artificial, capazes de detectar os movimentos dos estudantes através do computador²³.

Segundo estudo do InternetLab²⁴, que mapeou a política de reconhecimento facial de algumas escolas públicas no Brasil, pelo menos 10 estados brasileiros, de todas as regiões do país, implementaram tecnologias de reconhecimento facial em escolas públicas. No estado de Tocantins, por exemplo, a implementação da política de reconhecimento facial está em fase de testes e pretende se estender a todas as escolas da rede estadual²⁵. Em algumas escolas dos estados de Minas Gerais, Pernambuco e Goiás, o novo recurso já foi implementado, apesar de algumas unidades de ensino relatarem que a ferramenta precisa de ajustes técnicos para se interligar ao sistema da própria escola²⁶.

19. BUOLAMWINI, Joy. *Unmasking AI: My mission is to protect what is human in a world of machines*. Random House, New York. 2023.

20. ANDREJEVIC e SELWYN, *op. cit.*

21. CETIC. Pesquisa sobre o Uso da Internet por Crianças e Adolescentes no Brasil: *TIC Kids Online Brasil 2023* [livro eletrônico]. 1ª ed., São Paulo, 2024. Disponível em: https://cetic.br/media/docs/publicacoes/2/20241104103339/tic_kids_online_2023_livro_eletronico.pdf. Acesso em: 17 abr. de 2025.

22. BROWN, Lydia X.Z. *How Automated Test Proctoring Software Discriminates Against Disabled Students*. Washington, D.C.: Center for Democracy & Technology, 2020. Disponível em: <https://cdt.org/insights/how-automated-test-proctoring-software-discriminates-against-disabled-students/>. Acesso em: 10 dez. de 2024.

23. *Ibid.*

24. TAVARES, C.; SIMÃO, B., MARTINS, F.; SANTOS, B., ARAÚJO, A.. “Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras”. São Paulo: InternetLab, 2023.

25. *Ibid.*

26. *Ibid.*

Sob a ótica da administração pública, entende-se que há uma controvérsia no que tange à legalidade do uso dessa nova tecnologia, visto que o entendimento da proteção de dados pessoais como direito fundamental está em conexão direta com a natureza sensível desses dados que são coletados, requerendo uma maior atenção às regras e aos princípios aplicados²⁷.

Em razão da tecnologia de caráter invasivo e com potencial de redução de direitos fundamentais, apenas contar com os textos da Constituição ou da LGPD, que tratam esse assunto de forma geral, não é o suficiente²⁸.

2. Aspecto brasileiro na temática

2.1 Como as leis brasileiras abordam a temática da proteção das crianças e dos adolescentes combinada com o reconhecimento facial

Quando uma decisão diz respeito a crianças, de um modo geral, deve-se considerar, principalmente, o seu melhor interesse, levando em conta a norma em si, e também o que se relaciona a ela (por exemplo, questões relacionadas à interpretação desse dispositivo)²⁹. O Estatuto da Criança e do Adolescente (ECA)³⁰ foi aprovado em 1990 e dispõe sobre diversos direitos da criança e do adolescente, incluindo, mas não se limitando, a sua proteção, sua liberdade e sua dignidade, que podem ser traduzidas, dentre outros, como uma vida sem discriminação, preservando sua imagem e privacidade³¹.

Essa é uma interpretação que também pode ser compreendida através do artigo 14, LGPD³². Além disso, o parágrafo 6º³³ desse mesmo artigo deixa evidente a preocupação com o tratamento de dados pessoais de crianças e adolescentes quando elucida que as informações sobre o referido tratamento devem ser disponibilizadas de forma simples e de fácil acesso tanto aos responsáveis pela criança, quanto às próprias crianças, que devem entender a situação como um todo.

27. REIS, Carolina; ALMEIDA, Eduarda; DA SILVA, Felipe; DOURADO, Fernando. Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil. Brasília: Laboratório de Políticas Públicas e Internet, 2021.

28. *Ibid.*

29. TAVARES, C.; SIMÃO, B., MARTINS, F.; SANTOS, B., ARAÚJO, A.. “Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras”. São Paulo: InternetLab, 2023.

30. BRASIL. Lei Federal n. 8069, de 13 de julho de 1990. *Estatuto da Criança e do Adolescente (ECA)*.

31. TAVARES, SIMÃO, MARTINS, SANTOS e ARAÚJO, *op cit.*

32. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados (LGPD)*.

33. “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. § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.”

Essa proteção se inspira no texto da Constituição da República Federativa do Brasil de 1988 (CF), no seu artigo 227³⁴, que designa, entre outros, o direito à vida, à educação e à dignidade da criança e do adolescente como sendo um dever não só da família desse indivíduo, mas também da sociedade como um todo e do próprio Estado.

Além disso, a Constituição defende, em seu artigo 5º³⁵, que as pessoas são iguais perante a lei, e que a elas é garantido o direito à vida, à segurança, à liberdade etc., além de garantir também, em seu inciso LXXIX³⁶, nos meios digitais ou não, a proteção dos dados pessoais dos indivíduos.

O Projeto de Lei nº 2392/2022³⁷, que busca tratar sobre as tecnologias de reconhecimento facial nas esferas público e privada, propõe que um relatório de impacto seja feito antes que os dados biométricos, obtidos através de sistemas de reconhecimento facial, sejam utilizados, havendo, ainda, justificativas para seu uso e a impossibilidade de utilização de outro tipo de tecnologia que não demande tais dados.

Além disso, focando no setor público, o Projeto de Lei informa que a tecnologia de reconhecimento facial não deve ser o único mecanismo que permita usufruir serviços públicos, e que deverão ser disponibilizadas outras formas de acessos, já prevendo um possível não reconhecimento³⁸.

No entanto, o Projeto de Lei não impõe critérios claros para avaliar a proporcionalidade e a necessidade dos usos dessas tecnologias, seguindo as diretrizes dos incisos presentes no art. 6º, LGPD. Por exemplo, seria importante esclarecer pontos como: os riscos atrelados ao sistema estariam justificados pelos seus ganhos, considerando o melhor para as crianças e adolescentes? Os dados coletados seriam estritamente necessários à prática desejada?

Sistemas de Inteligência Artificial baseados em algoritmos podem ter vieses discriminatórios em relação à raça e gênero, por exemplo³⁹. Isso implica dizer que o uso de algoritmos de reconhecimento facial nas escolas pode amplificar esses vieses, resultando em erros desproporcionais direcionados a crianças

34. BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal, 2016. 496 p. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf. Acesso em: 15 dez. 2024.

35. *Ibid.*

36. Art. 5º, LXXIX, CF/88: “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.”

37. BRASIL. Projeto de Lei nº 2392, de 31 de agosto de 2022. Dispõe sobre o uso de tecnologias de reconhecimento facial nos setores público e privado. *Câmara dos Deputados*, Brasília, DF, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2205672&filename=PL%202392/2022. Acesso em: 15 dez. 2024.

38. *Ibid.*

39. BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: Intersectional accuracy disparities in commercial gender classification. In: Conference on fairness, accountability and transparency. *PMLR*, 81:1–15, 2018.

de grupos diversos (como raciais, de gênero, e até socioeconômicos), violando diretamente o princípio da não-discriminação, presente no art. 6º, IX, LGPD.

O fato de que, até o momento, não existe uma legislação específica para tratar do uso de reconhecimento facial nas escolas, não significa dizer que a sua utilização é legalizada, principalmente se levarmos em consideração a importância e a seriedade com as quais a educação brasileira deve ser tratada⁴⁰.

Conforme relatório publicado pela ANPD⁴¹, o uso dessas novas tecnologias de biometria nas escolas tem gerado preocupação, visto que, para além do tema tratar dados sensíveis, é um assunto que esbarra em grupos de titulares mais vulneráveis—crianças e adolescentes—e que exige um olhar mais atento, além da concordância com o princípio do melhor interesse—presente na LGPD e abordado anteriormente neste trabalho.

Além da legalidade, a segurança também é um fator importante a ser considerado no desenvolvimento e no uso de tecnologias de reconhecimento facial quando lidamos, principalmente, com dados biométricos⁴².

Entendendo que um vazamento de dados já seria preocupante o bastante, quando abordamos essa temática no âmbito dos dados biométricos, isso se torna ainda mais crucial. Uma vez que aconteça o roubo desses dados, por exemplo, entendendo que não são só senhas comuns, mas características das pessoas, a reposição desse tipo de dado se torna impossível, e sua recuperação, muito difícil⁴³.

2.2 O uso do reconhecimento facial nas escolas públicas brasileiras

A tecnologia nos centros educacionais vêm sendo utilizada de diversas formas e com diferentes finalidades, como parte de um modelo de ampliação de técnicas de segurança modernas e digitalizadas⁴⁴.

O aprendizado virtual é um exemplo de aplicação e demanda, em que o sistema de reconhecimento facial é empregado como controle do acesso ao conteúdo online, confirmando que o aluno está presente na aula, e que dessa forma ele permaneceu durante toda a atividade educacional⁴⁵.

40. TAVARES, C.; SIMÃO, B., MARTINS, F. ; SANTOS, B., ARAÚJO, A.. “Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras”. São Paulo: *InternetLab*, 2023.

41. CEBRIAN, Fabiana S. P. Faraco *et al.* biometria e reconhecimento facial. Brasília: *Radar Tecnológico*, n. 2, 2024.

42. CANUTO, Anne Magaly de Paula. Ética no Uso de Dados Biométricos: Histeria ou Uma Preocupação Coerente?. *Computação Brasil*, n. 47, p. 36-39, 2022.

43. *Ibid.*

44. TAVARES, C.; SIMÃO, B., MARTINS, F. ; SANTOS, B., ARAÚJO, A.. “Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras”. São Paulo: *InternetLab*, 2023.

45. ANDREJEVIC, Mark; SELWYN, Neil. Facial recognition technology in schools: Critical questions and concerns. *Learning, Media and Technology*, v. 45, n. 2, p. 115-128, 2020.

Também existe um interesse constante nas tecnologias de reconhecimento facial nas escolas para que elas sirvam de indicadores de engajamento e aprendizado dos alunos⁴⁶. Para isso, a câmera detecta não só os rostos dos estudantes, mas também é capaz de dizer sobre suas emoções, e esse resultado se torna um indicativo para entender se aquele aluno está interessado na aula, se ele está aprendendo, se ele está frustrado com a matéria etc.⁴⁷

Essa questão impacta a vida, principalmente, dos estudantes, e ainda pode ter limitações no campo técnico, que devem ser estudadas com atenção. Por exemplo, Lisa Feldman Barrett⁴⁸ descreve que o principal erro desse monitoramento é pensar que existe um padrão universal para analisar expressões faciais, enquanto que, na verdade, essas expressões variam tanto de aspectos geográficos e culturais, quanto de contextos nos quais esses estudantes estão inseridos no momento da captação da imagem.

A política de reconhecimento facial vem sendo implementada nas escolas públicas brasileiras com as finalidades de, principalmente, evitar evasão escolar, ter um mecanismo mais eficiente de gestão das escolas e garantir a segurança daqueles que circulam nesse ambiente⁴⁹.

No estudo produzido pelo InternetLab, os pesquisadores elucidam que nas escolas públicas dos municípios de Fortaleza, Potirendaba, Rio de Janeiro, Morrinhos, Mata de São João e Goiânia, o reconhecimento facial seria uma forma de evitar evasão escolar, visto que presenças e faltas estariam documentadas, então seria quase impossível buscar uma alteração nesse cenário, já que muitos pais no final do ano tentam realizar acordos com os professores, uma vez que seus filhos não alcançaram a frequência necessária⁵⁰.

Ao que tange à otimização da gestão escolar, os municípios pesquisados justificaram o uso de tecnologia de reconhecimento facial com argumentos de que a ferramenta seria uma modernização na forma de realizar as chamadas de faltas, economizando o tempo dos professores, garantindo que os pais fossem avisados caso seus filhos não fossem à escola⁵¹.

Além disso, também seria um mecanismo útil no momento da criação de relatórios atualizados com os principais motivos para as ausências registradas: o município de Morrinhos, em Goiás, por exemplo, conta com um apli-

46. *Ibid.*

47. *Ibid.*

48. 2021, apud ISRAEL *et al.*, 2023, p. 32.

49. TAVARES, SIMÃO, MARTINS, SANTOS e ARAÚJO, *op cit.*

50. *Ibid.*

51. *Ibid.*

cativo que, a partir do registro de frequência, avisa sobre avaliações, tarefas realizadas pelo estudante e dias de reunião⁵².

Por último, para os municípios de Mata de São João, Itanhaém, Potirendaba, Porto Alegre, Fortaleza, Águas Lindas, Betim e Xaxim, as políticas de reconhecimento facial são justificadas pelo viés da segurança (dos alunos, dos funcionários, e até da própria escola): as tecnologias são utilizadas para assegurar que os alunos estejam no colégio e não saiam sem autorização, para evitar a entrada de pessoas não autorizadas, e para proteger o próprio patrimônio escolar de depredação de materiais, por exemplo⁵³.

Independente do motivo, deve-se levar em consideração se essa vigilância é de fato necessária ou se é mais um mecanismo de invasão da privacidade desses alunos, justificada, também, por uma preocupação à segurança.

2.3 Seria a tecnologia de reconhecimento facial a mais adequada para lidar com os problemas das escolas públicas brasileiras?

Preocupações éticas com os dados biométricos são um ponto de consideração para a sociedade democrática: de um lado, há situações em que será preciso priorizar a segurança do indivíduo, enquanto, do outro lado, pesam-se a privacidade e a autonomia dessa pessoa⁵⁴.

Além disso, esse tipo de tecnologia, assim como muitos outros, também pode apresentar erros ao tentar executar uma tarefa. Parecer ser inteligente não significa ser funcional: muitos sistemas de reconhecimento facial podem apresentar o chamado “falso positivo”, quando detectam uma face que não está presente, ou então o “falso negativo”, quando não reconhecem um rosto que se apresenta⁵⁵.

Outro fator importante é a base de dados desse sistema, que determina o viés com o qual a inteligência artificial em questão foi/está sendo treinada, podendo gerar reconhecimentos faciais equivocados (ou o não reconhecimento, em diversos casos) de grupos que possuem etnias e cores de pele específicas, por exemplo⁵⁶.

52. *Ibid.*

53. *Ibid.*

54. SMITH, Marcus; MILLER, Seumas. The ethical application of biometric facial recognition technology. *Ai & Society*, v. 37, n. 1, p. 167-175, 2022.

55. BUOLAMWINI, Joy. *Unmasking AI: My mission to protect what is human in a world of machines*. Random House, 2024.

56. ANDREJEVIC, Mark; SELWYN, Neil. Facial recognition technology in schools: Critical questions and concerns. *Learning, Media and Technology*, v. 45, n. 2, p. 115-128, 2020.

Essa discussão é ainda mais relevante se pensarmos no ambiente escolar, em que os titulares de dados são, principalmente, crianças e adolescentes. Como já citado anteriormente, o risco de vazamento desses dados existe e deve ser levado em consideração quando se busca entender os benefícios e os malefícios da tecnologia de reconhecimento facial nos ambientes de ensino.

As tecnologias de reconhecimento facial tendem a exacerbar (e não mitigar) tendências autoritárias na estrutura escolar em que são implementadas: num ambiente assim, alunos comecem a se comportar de maneira diferente (não necessariamente boa ou má), apenas com medo de que a inteligência artificial possa captar algo equivocado, fazendo com que esse seja o novo normal⁵⁷.

Ademais, essa prática recai sobre a necessidade de automação das funções. Uma base de dados automatizada processa inúmeras decisões também automatizadas: isso significa dizer que têm-se cada vez menos humanos no topo da decisão, impedindo, por exemplo, que professores possam reconhecer as necessidades e os comportamentos dos seus próprios alunos, visto que suas interações são mais reduzidas⁵⁸.

Há uma grande preocupação com vieses racistas no reconhecimento facial de emoções, visto que as máquinas tendem a associar sentimentos negativos a pessoas pretas com muito mais frequência do que a pessoas brancas, interpretando, dessa forma, essas emoções de modo distinto dependendo da cor da pele do aluno⁵⁹.

Tendo em vista os problemas apresentados, e suas justificativas, é de certo se questionar se a tecnologia de reconhecimento facial é a mais adequada para lidar com tais situações. Além de entender se a política de privacidade dessas ferramentas nas escolas abrange todos os riscos, de forma clara e inequívoca, e se os pais estão cientes de que tipos de dados os seus filhos estão compartilhando.

De acordo com uma professora da UNB, entrevistada pelos pesquisadores do InternetLab, há situações mais complicadas no ambiente escolar, como escassez de professores, infraestrutura ruim, falta de energia, deslocamento e

57. *Ibid.*

58. *Ibid.*

59. ISRAEL, C. B. et al. Reconhecimento Facial nas Escolas Públicas do Paraná: Relatório 2023. Coordenação Carolina Batista Israel, Rodrigo Firmino. Curitiba: UFPR, 142p, 2023.

trânsito etc., que deveriam ser prioridade, e que não serão solucionados com a tecnologia de reconhecimento facial⁶⁰.

Com a chamada realizada por meio do reconhecimento facial, por exemplo, o tempo gasto pelo professor ainda é alto e o verdadeiro problema de superlotação das salas ainda não é resolvido⁶¹.

Além disso, é possível observar que não há iniciativa para possíveis mudanças na formação dos docentes, introduzindo as novas tecnologias, ou seja, há esforço para justificar a usabilidade desses sistemas, mas não há o mesmo empenho em estudar e aprimorar o ecossistema onde as ferramentas serão inseridas⁶².

Stark⁶³ afirma que implementar essas novas tecnologias no ambiente escolar é como trocar uma atividade que apresenta um risco enorme por um ganho relativamente baixo. As escolas não devem ser um lugar onde as crianças têm um risco de serem potencialmente discriminadas, transformando esse no novo normal dos ambientes escolares⁶⁴.

Israel et al.⁶⁵ nos informa que tecnologias como essas devem carregar uma preocupação ainda maior, visto o tamanho da desproporcionalidade entre os objetivos benéficos que se pretende atender e os potenciais impactos que podem gerar, principalmente se pensarmos que o propositor dessa tentativa é o próprio Estado.

Para que esse tipo de tecnologia possa ser usada, é preciso seguir certas diretrizes, a fim de mitigar os riscos já tratados neste trabalho. Devido aos impactos que pode trazer à população, é preciso que a tecnologia seja alvo de debate público, explicando com detalhes o contexto, os tipos de dados coletados, suas justificativas, e o que mais de informação a tecnologia demandar⁶⁶.

Além disso, seria importante a realização de estudos de impacto regulatório, demandando ação do Estado para o problema em voga, além de se avaliar a possibilidade de haver consentimento informado nas escolas ou modelos de accountability no setor público.

60. TAVARES, C.; SIMÃO, B., MARTINS, F. ; SANTOS, B., ARAÚJO, A.. “Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras”. São Paulo: *InternetLab*, 2023.

61. *Ibid.*

62. *Ibid.*

63. 2019, apud ANDREJEVIC e SELWYN, 2020, p. 126.

64. *Ibid.*

65. ISRAEL, C. B. et al. Reconhecimento Facial nas Escolas Públicas do Paraná: Relatório 2023. Coordenação Carolina Batista Israel, Rodrigo Firmino. Curitiba: *UFPR*, 142p, 2023.

66. *Ibid.*

Pensando em quem terá acesso a esses dados, é necessário que se pense na criação de credenciais para quem pode acessar o sistema, além da maneira como esse acesso se dará, a forma de armazenamento, além de criptografia de ponta para os métodos de autenticação e o banco de dados onde os dados dos alunos estarão armazenados⁶⁷.

Muitos são os desafios a serem enfrentados na seara da educação combinada à tecnologia. Os limites dessas ferramentas ainda são indefinidos, e sua adequabilidade ainda é desproporcional ao que se propõe, tendo, assim, desequilíbrio entre os riscos e seus benefícios⁶⁸.

É preciso escutar mais pais, professores, alunos, com o ouvido atento ao que esses, que estão na linha de frente do problema, tem a dizer sobre uma ferramenta tão poderosa, capaz de mudar as dinâmicas escolares há muito conhecidas.

Considerações finais

A tecnologia entrou em esferas públicas, como a educação, e vem prometendo ser uma solução para problemas que as escolas públicas brasileiras vêm enfrentando. No entanto, é sabido que questões estruturais não podem ser consertadas apenas com o advento de mecanismos de inteligência artificial, como, por exemplo, o reconhecimento facial.

Até o momento, não temos uma lei específica para tratar esse assunto, mas podemos recorrer a textos constitucionais e infraconstitucionais, que já lidam com os titulares de dados que estão na ponta desse tema: as crianças e adolescentes, que devem ter seus direitos levados em consideração, muito por conta do cuidado extra que se deve ter quando seus dados são coletados, armazenados, compartilhados etc.

Como se buscou demonstrar neste trabalho, a tecnologia de reconhecimento facial já saiu da seara do pensamento e está em fase de testes em diversas escolas públicas espalhadas pelo Brasil. Logo, pretende-se pensar se os direitos desses jovens estão sendo atendidos e, ainda, se essa seria a melhor solução para os problemas que se busca enfrentar.

Para além de problemas como falhas no reconhecimento e má luminosidade, que podem atrapalhar a captação da imagem, esse sistema está suscetível a cometimento de diferentes formas de preconceito. Dados de crianças e

67. TAVARES, C.; SIMÃO, B., MARTINS, F. ; SANTOS, B., ARAÚJO, A.. Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras. São Paulo: *InternetLab*, 2023.

68. *Ibid.*

adolescentes vazados também devem ser um dos cerne dessa preocupação, visto que nesse tipo de tecnologia não é possível trocar o objeto que garante o acesso.

Sendo assim, conclui-se que a tecnologia de reconhecimento facial nas escolas públicas brasileiras não se demonstra como sendo a mais indicada para resolver os problemas apresentados durante o decorrer do trabalho, considerando os malefícios que a ferramenta também traz. Neste sentido, é fundamental que a ANPD atue como autoridade fiscalizadora e oriente esse entendimento na prática dessas atividades, tendo maior transparência, e aplicando as respectivas sanções, quando cabíveis.

É preciso que haja: (i) um estudo mais aprofundado sobre o sistema; (ii) conversas com pais e professores; (iii) uma política de privacidade que abarque os riscos de forma objetiva; (iv) a criação de marco normativo específico para uso de biometria na educação; (v) a inclusão da formação docente em ética digital e direitos de proteção de dados; (vi) a suspensão temporária da tecnologia até regulamentação adequada; e (vii) políticas públicas criadas e realizadas por humanos, que visem melhorar os aspectos estruturais da educação.

Dessa forma, será possível avançar e, quem sabe, somente então, utilizar a tecnologia a favor dos estudantes do Brasil.

Referências

ALMEIDA, Luiz Felipe de Oliveira et al. Sistema de chamada escolar com reconhecimento facial utilizando opencv. *Revista de Ubiquidade*, v. 5, n. 2, p. 1-16, 2022.

ANDREJEVIC, Mark; SELWYN, Neil. Facial recognition technology in schools: Critical questions and concerns. *Learning, Media and Technology*, v. 45, n. 2, p. 115-128, 2020.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal, 2016. 496 p. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf. Acesso em: 15 dez. 2024.

BRASIL. Lei Federal n. 8069, de 13 de julho de 1990. *Estatuto da Criança e do Adolescente (ECA)*.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados (LGPD)*.

BRASIL. Projeto de Lei nº 2392, de 31 de agosto de 2022. Dispõe sobre o uso de tecnologias de reconhecimento facial nos setores público e privado. *Câmara dos Deputados*, Brasília, DF, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2205672&-filename=PL%202392/2022. Acesso em: 15 dez. 2024.

BROWN, Lydia X.Z. *How Automated Test Proctoring Software Discriminates Against Disabled Students*. Washington, D.C.: Center for Democracy & Technology, 2020. Disponível em: <https://>

cdt.org/insights/how-automated-test-proctoring-software-discriminates-against-disabled-students/. Acesso em: 10 dez. de 2024.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: Intersectional accuracy disparities in commercial gender classification. *In: Conference on fairness, accountability and transparency. PMLR*, 81:1-15, 2018.

BUOLAMWINI, Joy. Unmasking AI: My mission is to protect what is human in a world of machines. *Randon House*, New York. 2023.

CANUTO, Anne Magaly de Paula. Ética no Uso de Dados Biométricos: Histeria ou Uma Preocupação Coerente?. *Computação Brasil*, n. 47, p. 36-39, 2022.

CEBRIAN, Fabiana S. P. Faraco et al. biometria e reconhecimento facial. Brasília: *Radar Tecnológico*, n. 2, 2024.

CETIC. Pesquisa sobre o Uso da Internet por Crianças e Adolescentes no Brasil: *TIC Kids Online Brasil 2023* [livro eletrônico]. 1ª ed., São Paulo, 2024. Disponível em: https://cetic.br/media/docs/publicacoes/2/20241104103339/tic_kids_online_2023_livro_eletronico.pdf. Acesso em: 17 abr. de 2025.

ISRAEL, C. B. et al. Reconhecimento Facial nas Escolas Públicas do Paraná: Relatório 2023. Coordenação Carolina Batista Israel, Rodrigo Firmino. Curitiba: *UFPR*, 142p, 2023.

REIS, Carolina; ALMEIDA, Eduarda; DA SILVA, Felipe; DOURADO, Fernando. Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil. Brasília: *Laboratório de Políticas Públicas e Internet*, 2021.

SMITH, Marcus; MILLER, Seumas. The ethical application of biometric facial recognition technology. *Ai & Society*, v. 37, n. 1, p. 167-175, 2022.

SULLIVAN, E. Facial recognition technology: verification vs. Identification. *Montana Legislative Services Division*, 2021.

TAVARES, C.; SIMÃO, B., MARTINS, F. ; SANTOS, B., ARAÚJO, A.. “Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras”. São Paulo: *InternetLab*, 2023.

TEFFÉ, Chiara Spadaccini de. Dados Biométricos: Uma Análise Crítica Acerca de Seu Tratamento e Aplicações. *In: Direitos fundamentais e novas tecnologias: homenagem ao professor Danilo Doneda/organizadores Ricardo Villas Bôas Cueva et al.* 1.ed – Rio de Janeiro: *GZ*, 2024.

WENDEHORST, Christiane; DULLER, Yannic. Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces. *European Parliament*, 2021.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

15

**Segurança patrimonial
da criança e adolescente
que executam trabalho de
teor artístico: análise do
projeto de lei nº 3916/2023 e
apensos e a observância ao
influenciador digital mirim**

MARIA EMILIA LOTH MACHADO

Sumário: Introdução. 1. O trabalho infantil artístico e a gerência patrimonial exercida pelos responsáveis legais pela criança e adolescente. 2. A inclusão do papel de influenciador digital mirim como trabalho de teor artístico. 3. Proteção ao patrimônio do influenciador digital mirim – ocorrência nos sistemas jurídicos estrangeiros em oposição ao sistema jurídico brasileiro. 4. Proposições legislativas acerca da segurança patrimonial da criança e adolescente que exercem trabalho de teor artístico. Considerações finais. Referências.

Introdução

O presente trabalho pretende verificar quais os mecanismos legais atualmente disponíveis para salvaguardar a segurança patrimonial de influenciadores digitais mirins (crianças e adolescentes) e analisar propostas de lei que versam sobre o assunto, todas ensejadas pelo caso “Larissa Manoela”. A esse respeito, cumpre ressaltar que o caso é utilizado no presente estudo como parâmetro não somente por ter sido amplamente citado por alguns dos projetos de lei sobre o assunto, mas também com o objetivo de servir de gatilho para reflexão jurídica sistêmica. Além disso, busca-se analisar se tais projetos proporcionam segurança jurídica e patrimonial suficiente a esses influenciadores digitais, se preveem mecanismos para garanti-la e se as soluções propostas são inovadoras. Dessa forma, pretende-se chamar atenção a uma nova modalidade de trabalho infantil artístico que tem se desenvolvido com rapidez e que não pode passar despercebido pelo legislador e pelos fiscais da lei, eis que também envolve o melhor interesse da criança, ainda que seja em ambiente digital.

O caso “Larissa Manoela” gerou ampla repercussão nacional no segundo semestre de 2023, quando foi anunciado que a atriz Larissa Manoela, já maior de idade, mas que havia construído uma carreira artística desde a infância, havia rompido com os pais por divergências irreconciliáveis na administração de seu patrimônio. O que ensejou o rompimento foi a descoberta de que a atriz possuía apenas 2% das cotas da sociedade empresarial que os pais estruturaram quando ela ainda era menor de idade para gerir o patrimônio acumulado através do seu trabalho, sendo os 98% das cotas restantes pertencentes aos próprios pais. Eles foram responsáveis por negociações e contratos de trabalho da atriz durante toda sua trajetória profissional, até o momento do desentendimento descrito.

1. Advogada formada pela UFRRJ. Especialista em Contratos pela PUC-RIO e pós-graduanda em Direito Digital pelo ITS-Rio/ UERJ. Pesquisadora de Direito Internacional Privado no Núcleo de Estudos e Pesquisa em Direito Internacional – NEPEDI UERJ.

O caso chama a atenção pela potencial complexidade da discussão jurídica e pela ausência de dispositivos legais que limitem claramente a ingerência dos responsáveis pelo patrimônio acumulado pelo artista mirim. No entanto, um aspecto pouco observado do assunto é que um novo tipo de trabalho infantil artístico vem se desenvolvendo e ganhando força recentemente, gerando também quantias expressivas para essas crianças e adolescentes: o de influenciador digital mirim. Se atores e modelos mirins, profissões de teor artístico mais comuns, já são atingidos por essa insegurança jurídica quanto à administração de seu patrimônio, os influenciadores digitais mirins ainda enfrentam o desafio de terem seu trabalho pouco reconhecido como de teor artístico pelo simples fator da novidade, inclusive pela legislação.

A segurança patrimonial de artistas mirins já é pauta consolidada em outros países, como Estados Unidos, e atualmente tem sido discutida também em relação aos influenciadores digitais mirins. No Brasil, o movimento é similar, tendo sido recentemente motivado pelo caso descrito acima. Foram propostos alguns projetos de leis com base na temática, e serão eles o ponto focal do trabalho, de forma a analisar a segurança financeira por eles oferecida e a atenção dada também a esta nova figura de trabalho artístico performada por menores de idade.

A hipótese inicial é que nenhum dos projetos consegue abraçar todas as questões já existentes nesse âmbito, tais como limitação de movimentações financeiras, de remuneração aos responsáveis legais do menor e sanções para aqueles que depredarem o patrimônio gerado por esse trabalho.

O método utilizado no trabalho foi o de revisão legislativa e bibliográfica, utilizando-se majoritariamente dos projetos de lei que versam sobre o assunto, leis já publicadas relacionadas, livros, artigos publicados em periódicos e textos de lei com o mesmo propósito em vigor nos Estados Unidos e na França. Foram guardadas as devidas proporções quanto a comparação de legislações estrangeiras em relação à brasileira, eis que é necessário levar em conta não somente as diferenças entre os sistemas jurídicos destes três países, mas também as diferentes formas como cada um desses Estados exerce seu poder nesse âmbito.

Já em relação ao referencial teórico, tiveram destaque na presente pesquisa os projetos de lei de número 3916/2023, 3917/2023, 3918/2023, 3919/2023, 3938/2023, 3960/2023, 4053/2023 e 4990/2023. Da mesma forma, foram referências importantes sobre o assunto a tese “O que você vai ser antes de crescer? Youtubers, Infância e Celebridade”, de Renata Tomaz; os artigos “Co-

leção Comentário Geral nº 25 na Prática: Orientações para a defesa das crianças e dos adolescentes no ambiente digital”, de autoria do Instituto Alana e do Ministério Público de São Paulo; “Sharenting Comercial: os direitos de crianças e adolescentes em face da superexposição virtual com fins econômicos e a figura do influenciador digital mirim”, de Julya Naara Mayer Wisniewski; e “Sharenting e os desafios da regulamentação: uma análise no Brasil e em França”, de Doris Ghilardi e Gabriela Pinheiro Santos.

O artigo foi dividido em quatro tópicos, de forma a introduzir o tema e seu contexto até a apresentação e análise do problema. O primeiro tópico introduz o tema da gerência patrimonial dos responsáveis legais pela criança ou adolescente que exerce trabalho artístico, o segundo tópico aprecia a classificação do influenciador digital mirim como trabalho de teor artístico, o terceiro tópico menciona brevemente duas alternativas legislativas estrangeiras para proteção patrimonial de menores, em comparação aos dispositivos legais atuais na legislação brasileira, e por fim, o quarto tópico analisa propostas de lei que visam aumentar a proteção patrimonial do menor que exerce trabalhos de teor artístico, incluindo os influenciadores digitais mirins.

Por fim, cumprida a análise de todos os projetos de lei e considerando também a bibliografia reunida, é possível responder às duas perguntas de pesquisa, qual sejam: os projetos de lei analisados no âmbito do presente trabalho proporcionam segurança jurídica e patrimonial suficiente a influenciadores digitais menores de idade? Há previsão de mecanismos para garanti-la e se as soluções propostas são inovadoras?

1. O trabalho infantil artístico e a gerência patrimonial exercida pelos responsáveis legais pela criança e adolescente

O panorama legislativo brasileiro sobre trabalho infantil funciona plenamente, embora não seja simplificado. A única hipótese admitida para a modalidade consiste no trabalho infantil de caráter artístico, com base na Convenção nº 138 da Organização Internacional do Trabalho (OIT), a qual foi ratificada pelo Decreto nº 4134/2002, revogado pelo Decreto 10.088/2019, o qual unificou todos os atos normativos que dispõem sobre promulgação de convenções e recomendações da OIT.

Embora existam diversos dispositivos legais que conversem entre si sobre o tema e sejam costumeiramente interpretadas em conjunto, não há legislação específica para definir, delimitar e regulamentar o trabalho infantil de caráter artístico. Essa modalidade de trabalho escapa à previsão do artigo 7º,

XXXIII da Constituição Federal, o qual prevê a “proibição de trabalho noturno, perigoso ou insalubre a menores de dezoito e de qualquer trabalho a menores de dezesseis anos, salvo na condição de aprendiz, a partir de quatorze anos”. Isso acontece inclusive no quesito idade mínima de trabalho (quatorze anos), eis que as autorizações necessárias são dadas caso a caso, mesmo a menores de quatorze anos, visando preservar o direito à liberdade de expressão artística previsto pelo artigo 5º, IX do mesmo diploma, o qual prevê que “é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença”.

A liberdade de expressão artística foi introduzida em nosso ordenamento a partir da previsão feita pela Convenção nº 138 da OIT, que prevê a participação de crianças em representações artísticas mediante a concessão de licenças individuais, as quais limitam número de horas e estabelecem as condições em que tal trabalho é permitido. Nesse sentido, o ECA, em seu artigo 149, elenca critérios que devem ser apreciados pela autoridade judiciária para concessão de tal licença (alvará), como a existência de instalações adequadas e o tipo de frequência habitual ao local, dentre outros.

Os diplomas acima citados cobrem uma gama de detalhes envolvidos no trabalho infantil artístico, e de fato a sua interpretação conjunta permite maior controle acerca de como esse trabalho ocorre, privilegiando sempre o bem-estar infantil. Ainda assim, nenhuma dessas leis ou recomendações foi específica o suficiente no que tange à segurança financeira das crianças que exercem esse tipo de trabalho, exigindo-se a esses casos uma interpretação conjunta também do Código Civil, o qual dispõe acerca do usufruto e administração dos bens de filhos menores em seus artigos 1689 a 1693. Em relação a tais artigos, importante frisar especialmente o disposto nos incisos II dos artigos 1689 e 1693, que dispõem:

Art. 1.689. O pai e a mãe, enquanto no exercício do poder familiar:

I – são usufrutuários dos bens dos filhos;

II – têm a administração dos bens dos filhos menores sob sua autoridade. (grifos nossos)

Art. 1.693. Excluem-se do usufruto e da administração dos pais:

(...)

II – os valores auferidos pelo filho maior de dezesseis anos, no exercício de atividade profissional e os bens com tais recursos adquiridos; (grifos nossos)

(...)

Ou seja, no caso de crianças que exerçam trabalho de caráter artístico, cabe primeiramente aos pais a administração e usufruto de seus bens até os dezesesseis anos. No entanto, não há qualquer disposição acerca de temas como a reserva e administração desses valores, penalidades para a má administração de tal patrimônio ou previsões acerca da fiscalização de tal administração. Sobre o tema, o STJ já se manifestou acerca da possibilidade de ajuizamento de pedido de prestação de contas de filhos contra os pais responsáveis pela administração de seus bens², mas é cabível reflexão acerca de alternativas mais eficazes que ajam de forma preventiva a um possível abuso financeiro que pode ser praticado pelos administradores de tais bens.

2. A inclusão do papel de influenciador digital mirim como trabalho de teor artístico

O tema tem ganhado novos contornos com o surgimento e consolidação da figura do influenciador digital mirim, tendo em vista que os avanços tecnológicos recentes propiciam cada vez mais a presença de crianças e adolescentes no ambiente online, seja de forma passiva (como expectadores) ou de maneira ativa (como atores).

Ainda não há reconhecimento formal acerca do enquadramento do trabalho do influenciador mirim como trabalho artístico, mas já é possível encontrar interpretações favoráveis a este enquadramento. Em estudo orientado por Eloísa Machado de Almeida e Vivianne Ferreira, sugere-se a interpretação do artigo 2º da Lei nº 6.533/1978 em conjunto com o artigo 15, parágrafo 1º do Comentário 21 do Comitê de Direitos Econômicos Sociais e Culturais da ONU, os quais dispõem sobre as características essenciais de um artista, de uma obra de caráter cultural e do direito de as pessoas participarem na vida cultural³. Analisando tais critérios, de acordo com os autores, “pode-se cogitar que a atividade de ‘influencer mirim’ pode ser equivalente a ‘trabalho artístico’”⁴.

Já o Ministério Público do Estado de São Paulo considera outros critérios para configurar a atividade do influenciador mirim como forma de trabalho infantil artístico. Tais critérios seriam o da monetização (seja através de par-

2. STJ. *Suspeita de abuso na administração de bens autoriza filho a exigir prestação de contas dos pais*. Brasília, DF: STJ, 2018. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2018/2018-03-21_06-51_Suspeita-de-abuso-na-administracao-dos-bens-autoriza-filho-a-exigir-prestacao-de-contas-dos-pais.aspx. Acesso em: 04 de jan. de 2025.

3. ALMEIDA, E. M. de; FERREIRA, V. (org.). *Influencers mirins – um estudo sobre trabalho infantil nas redes sociais*. São Paulo, SP: FGV, 2024. Disponível em: https://direitosp.fgv.br/sites/default/files/arquivos/policy-paper_0.pdf. Acesso em: 04 de jan. de 2025.

4. Ibidem, p. 18.

cerias com empresas para divulgação de produtos e serviços ou através de monetização de conteúdo oferecida pela própria plataforma digital); o da habitualidade (é considerado sinal de profissionalização de produção e orientação do conteúdo às expectativas externas quando a sua publicação ocorre em dias e horários fixos); a orientação da produção a expectativas externas em si (conteúdo que não está pautado pelos interesses e desejos da própria criança, mas sim por interesses comerciais); e a profissionalização (consistente no investimento de recursos materiais nas atividades da criança influenciadora)⁵. Presentes tais critérios, os autores concluem que é necessária a intervenção pela autoridade judiciária “para que sejam evitados abusos e violações de direitos da criança influenciadora”⁶.

Superada tal questão e considerando que o influenciador digital mirim exerce um trabalho artístico, ainda remanesce a ausência de especificidade na legislação quanto a segurança financeira dessas crianças, e se tal especificidade de fato seria necessária.

3. Proteção ao patrimônio do influenciador digital mirim – ocorrência nos sistemas jurídicos estrangeiros em oposição ao sistema jurídico brasileiro

Há exemplos de legislações recentes em países como França e Estados Unidos, que se aprofundaram um pouco mais na questão econômica não só das crianças que exercem trabalhos artísticos mais tradicionais, como na atuação ou como modelos, mas também das crianças que atuam como influenciadores digitais em diversas plataformas online.

Na França, a Lei n° 1266 de 2020 determina em seu artigo 3° que, se a renda derivada de um conteúdo publicado online ultrapassar determinada quantia dentro de determinado período, o excedente deve ser depositado integralmente em um fundo na “Caixa de Depósitos e Consignações”, o qual será gerenciado por tal órgão até que a criança atinja a maioridade ou se emancipe⁷. A regra para o pagamento de publicidades veiculadas através do influenciador digital mirim também é o depósito da remuneração no mesmo dito fundo, sendo

5. Ministério Público do Estado de São Paulo. *Comentário Geral n° 25 na Prática: Orientações para a defesa das crianças e dos adolescentes no ambiente digital*. São Paulo, SP: Ministério Público do Estado de São Paulo, 2023. Disponível em: https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/BibliotecaDigital/Publicacoes_MP/Todas_publicacoes/Comentario-geral-n.25-na-pratica_orientacoes-para-a-defesa-das-criancas_2023.pdf. Acesso em 04 de jan. de 2025.

6. Ibid., p. 34.

7. França. Loi n° 2020-1266 du 19 octobre 2020. Visant à encadrer l'exploitation commerciale de l'image d'enfants de moins de seize ans sur les plateformes en ligne (1). *JORF* n°0255 du 20 octobre 2020. Texte n° 1. Disponível em: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042439054>. Acesso em 05 de jan. de 2025.

que a disposição de parcela desse pagamento aos responsáveis pela criança é a exceção. Em tal exceção, a porção a ser disponibilizada aos responsáveis ainda é determinada por autoridade competente. Por fim, é previsto o pagamento de multa no valor de 3.750 (três mil, setecentos e cinquenta) euros aos responsáveis pelo pagamento de publicidades que deixarem de observar a lei, especialmente a questão referente ao depósito de valores em fundo específico na “Caixa de Depósitos”.

Nos Estados Unidos, especificamente na Califórnia, a “Lei Coogan” (Coogan’s Law ou Coogan Act), já existente desde 1939 para proteger os interesses de crianças que exerçam trabalhos artísticos, determina que ao menos quinze por cento do pagamento recebido pelo trabalho de uma criança deve ser depositado diretamente pelo pagador em uma conta específica, popularmente conhecida como “Coogan Trust Account”⁸. Posteriormente, em 1999, os legisladores deram mais um passo para fortalecer a segurança financeira das crianças que exercem trabalhos artísticos e são protegidas por essa lei, declarando que a totalidade de seus recebimentos pertence somente a elas, e não apenas os quinze por cento depositados nas contas “Coogan”. Os pais ou responsáveis podem usar os oitenta e cinco por cento dos valores disponíveis para os cuidados da criança, seja comprando uma casa, pagando suas despesas ou separando para si um salário por gerenciar a carreira da criança, mas ainda assim, todos os valores recebidos pertencem apenas à criança⁹.

Recentemente, em setembro de 2024, foram feitas emendas à Lei Coogan, quais sejam, a SB 764 (Padilla) e a AB 1880 (Alanis). A primeira, originada no senado (portanto, “Senate Bill”), estabeleceu proteções legais e financeiras para menores que participem de conteúdo online monetizado, determinando que seus pais ou guardiões legais depositem determinada quantia em fundos específicos. A segunda, originada na câmara estadual (denominada “Assembly Bill”), torna a Lei Coogan aplicável a menores que trabalhem como criadores de conteúdo em plataformas e redes sociais online¹⁰. Dessa forma, a proteção à criança que trabalha no meio artístico e de entretenimento abraçou mais um

8. Estados Unidos, Estado da Califórnia. *Family Code – FAM. §6752(b)(1)*. DIVISION. 11, PART 3, CHAPTER 3. Contracts in Art, Entertainment, and Professional Sports [6750 – 6753]. Estado da Califórnia, 2020. Disponível em: https://leginfo.ca.gov/faces/codes_displaySection.xhtml?sectionNum=6752.&nodeTreePath=13.5.3&lawCode=FAM. Acesso em 05 de jan. de 2025.

9. REARDON, J. New Kidfluencers on the Block: The Need to Update California’s Coogan Law to Ensure Adequate Protection for Child Influencers, 73 *Case W. Rsrv. L. Rev.* 165 (2022). Disponível em: <https://scholarlycommons.law.case.edu/caselrev/vol73/iss1/6>. Acesso em 05 de jan. de 2025. P. 172.

10. GOVERNOR GAVIN NEWSOM. *Governor Newsom joins Demi Lovato to sign legislation to protect the financial security of child influencers*. California: Governor Gavin Newsom, 2024. Disponível em: <https://www.gov.ca.gov/2024/09/26/governor-newsom-joins-demi-lovato-to-sign-legislation-to-protect-the-financial-security-of-child-influencers/>. Acesso em 07 de jan. de 2025.

espectro desse trabalho, principalmente no que diz respeito ao aspecto da sua administração financeira.

No Brasil, em virtude do caso da atriz Larissa Manoela, foram propostos alguns projetos de lei visando a proteção patrimonial de crianças e adolescentes que desenvolvam trabalho cultural, artístico ou esportivo. O primeiro projeto proposto sobre o tema foi o de nº 3916/2023, ao qual foram apensados os projetos de números 3917/2023, 3918/2023, 3919/2023, 3938/2023, 3960/2023, 4053/2023 e 4990/2023.

Enquanto alguns desses projetos criam leis para regulamentar as atuais lacunas do tema, outros visam aumentar a proteção patrimonial desses trabalhadores através de alteração na legislação já em vigor, mais especificamente o Código Civil e o Estatuto da Criança e do Adolescente. Os projetos que propõem essas alterações são os de números 3917, 3938, 3960, 4990 (para alterar o Código Civil, incluindo novos artigos ou parágrafos em artigos já existentes) e 4053 (que se propõe a alterar o ECA no mesmo sentido). Os de número 3916, 3918 e 3919 se propõem a criar uma nova lei para dispor unicamente sobre temas desse assunto.

Todos os projetos contêm boas sugestões, podendo ser considerados complementares uns aos outros, eis que não vislumbram todas as principais questões que permeiam o debate acerca do gerenciamento e utilização das remunerações recebidas pelo trabalho de artistas mirins. Nesse sentido, cita-se que os projetos de lei de número 3916/23, 3918/23 e 4990/23 citam expressamente o trabalho exercido pelos menores de 18 anos em plataformas digitais, redes sociais e na internet em geral, demonstrando que esses menores também constituem um ponto de atenção no tema. Considerando que o projeto de lei principal e seus apensos são sucintos, é oportuna a análise, ainda que breve, de cada um deles.

4. Proposições legislativas acerca da segurança patrimonial da criança e adolescente que exercem trabalho de teor artístico

No que diz respeito ao Projeto de Lei nº 3916/23, ele é um dos poucos que menciona o trabalho artístico de crianças e adolescentes na internet, em atenção à quantidade cada vez maior de influenciadores digitais mirins no Brasil. Procura-se garantir a formalidade do gerenciamento de carreira do artista mirim e o direito de acesso à informação por parte da criança e do adolescente, formalizando questões sobre a abertura de CNPJ (artigo 2º do PL) e determinando a manutenção de registros financeiros que devem se encontrar disponíveis para auditoria (artigos 5 e 6º do PL).

Merecem destaque os artigos 7º a 9º de tal projeto, abaixo transcritos:

Art. 7º Qualquer investimento robusto, gasto significativo ou transação financeira que afete de maneira importante o patrimônio da criança ou adolescente requererão pareceres dos profissionais técnicos adequados, como empresários, investidores, contadores e advogados, que indiquem a viabilidade dos negócios ou empreendimentos e a proteção dos interesses dos menores.

Art. 8º **A movimentação do patrimônio obtido pelo trabalho cultural, artístico ou esportivo de criança ou adolescente deverá, excepcionando o art. 7º, limitar-se a 30% do valor total, podendo este montante ser utilizado para cobrir despesas imediatas relacionadas à carreira e bem-estar dos interessados no desempenho da atividade econômica correspondente.**

Art. 9º Com a exceção do mencionado no art. 7º, **qualquer alteração, movimentação ou investimento relacionados aos 70% do patrimônio, reservados para a criança ou adolescente, só poderão ser realizados por estes com o atingimento da maioridade**, os quais passarão a ter pleno controle sobre seus patrimônios.

Acerta o artigo 8º ao limitar o montante que poderá ser movimentado com fins de remunerar os responsáveis pelo gerenciamento da carreira do artista mirim e também com fins de manter o padrão de vida tanto da criança ou adolescente trabalhador, quanto de sua família. Ao limitar a movimentação do patrimônio nesta porcentagem e prevendo essas duas hipóteses, o projeto se mantém coerente também ao seu próprio artigo 4º, que determina a inexigibilidade de contribuição financeira das crianças para os rendimentos pessoais ou projeto de vida de seus responsáveis legais. Ao mesmo tempo, havendo a necessidade de investimento ou gasto que ultrapasse tal patamar, estes não se tornam proibitivos, eis que o artigo 7º prevê tal hipótese sob a condição de que tal investimento ou gasto de grande porte seja feito com o apoio de pareceres dos profissionais técnicos adequados.

Tais artigos possuem boa convergência com os artigos 1689 e 1693 do Código Civil, também já citados, eis que, mesmo após o adolescente completar 16 anos, a movimentação de seu patrimônio continuará limitada aos 30% do valor total. Assim, mantém-se os demais 70% do patrimônio disponíveis para serem utilizados apenas pelo artista mirim, quando este completar a maioridade e atingir a plena capacidade civil para fazer melhor uso de sua reserva financeira.

O projeto de lei também prevê sanções para os responsáveis que deixarem de seguir as determinações ali impostas, estabelecendo cinco penalida-

des diferentes. Este, inclusive, é o único momento em que se menciona o dano à imagem, conforme o texto abaixo:

Art. 10 As violações aos dispositivos desta lei sujeitam os infratores às seguintes sanções, que podem ser cumuladas ou não:

(...)

V – Reparação de danos aos menores, por culpa ou dolo, provado o dano, dispensada a prova deste em se tratando de dano moral ou a imagem.

Tal artigo também está coerente em relação ao artigo 17 do Estatuto da Criança e do Adolescente, o qual prevê a inviolabilidade da imagem à criança.

Digno de observação que um dos Projetos de Lei atrelados ao de nº 3916, mais especificamente o de nº 4053, propõe alterar este mesmo artigo do ECA de forma a incluir a inviolabilidade da integridade patrimonial da criança e do adolescente. Tal proposta também sugere inclusões no ECA para determinar que os pais, usufrutuários e administradores dos bens de menores prestem contas judicialmente acerca dos valores recebidos em nome do menor. Ela prevê também duas inclusões aos artigos 24 e 129 do Estatuto, que descrevem que será devido o ressarcimento do dano caso haja abuso dos bens dos filhos por parte dos usufrutuários ou administradores.

A proposta de número 3917 por sua vez, embora sugira mera alteração no Código Civil e deixe de abordar questões relevantes levantadas pela 3916, também aborda assuntos importantes. Tal projeto exige que o Ministério Público se manifeste quando um menor de idade for incluído como sócio em sociedade empresária e que seja obrigatória a inclusão de cláusula revisional condicionada à maioria dos filhos em todos os contratos firmados no exercício do poder familiar, incluindo efeitos suspensivos do negócio jurídico. Outra proposta que caminha no mesmo sentido é a de número 3938, que também sugere a inclusão de dois incisos no artigo 1634 do Código Civil. A primeira adição prevê a obrigação de o responsável manter, no mínimo, 60% do patrimônio total do menor. A segunda, estabelece a divisão no mínimo igualitária dos percentuais de participação em sociedades, empresas ou empreendimentos nos quais sejam acionistas.

Seria interessante, no caso da inserção desse segundo inciso que versa sobre percentuais de participação em sociedades, que o legislador descrevesse pormenorizadamente se a divisão igualitária dos percentuais de participação em sociedades seria entre a criança e os responsáveis legais ou se seria apenas entre os responsáveis legais, excluindo a criança da sociedade, eis que

o caput do artigo referenciado se refere a “ambos os pais, qualquer que seja a sua situação conjugal”.

A proposta 3918 é bastante semelhante à de número 3916, incluindo a consideração a respeito das crianças que exercem atividade artística através de plataformas digitais. Em relação às limitações financeiras, exige a criação de conta específica para se manter ao menos 30% de toda a remuneração auferida pela criança através da atividade artística.

A proposta de número 3960 é a terceira que propõe a alteração do Código Civil de modo a incluir dois parágrafos ao artigo 1691. O primeiro deles cuida em limitar a remuneração dos pais, tutores ou empresários envolvidos na administração da carreira artística do menor que exerça trabalho na área, dando direito máximo a 10% anuais de todos os valores arrecadados. O outro parágrafo incluído diz respeito ao acompanhamento periódico das atividades desenvolvidas pelos menores envolvidos em atividade artística pelo Conselho Tutelar da região. No entanto, essa função já é exercida pelo Ministério Público estadual e do trabalho, motivo pelo qual tal adição pode parecer redundante. Tendo em vista que o objetivo principal do projeto de lei é “regulamentar percentual máximo relativo à administração do patrimônio dos filhos menores”, a inclusão apenas da limitação de remuneração dos responsáveis do menor parece fazer mais sentido.

Por fim, a proposta de número 4990, através da inclusão de um artigo de número 1693-A ao Código Civil, sugere a exclusão total da possibilidade dos pais ou responsáveis pelo menor envolvido em atividade artística serem usufrutuários de bens decorrentes da atividade exercida. Tal restrição parece demasiado rigorosa, eis que há casos concretos, como o da própria Larissa Manoela, o padrão de vida da família evoluiu demasiadamente devido às atividades artísticas praticadas pela atriz desde a tenra idade. Privar os pais de usufruírem dos bens dos filhos menores implicaria em privar o próprio menor de usufruir dos bens que seu trabalho lhe possibilitou adquirir, restringindo qualquer possibilidade de o menor ter uma melhora na qualidade de vida. Embora tal restrição fosse preservar o patrimônio adquirido através do trabalho artístico em sua integralidade, ela não parece atender totalmente ao melhor interesse da criança e do adolescente.

De forma a possibilitar melhor visualização sobre os mecanismos constantes nas propostas acima descritas, inclui-se a tabela abaixo com um breve resumo sobre os tópicos destacados nos parágrafos anteriores:

Projeto de Lei	Principais Mecanismos	Vantagens	Lacunas
3916/23	• Pretende estabelecer diretrizes para a proteção patrimonial de crianças e adolescentes que desenvolvam trabalho cultural, artístico ou esportivo; • Determina que os responsáveis envolvidos no trabalho devem se registrar na receita através de CNPJ; • Crianças e adolescentes têm direito a receber orientação empresarial, jurídica e contábil-financeira independente; • Auditorias regulares e fiscalização pelo MP das receitas geradas pela criança; • Investimentos e gastos significativos requerem pareceres profissionais técnicos que indiquem a viabilidade dos negócios e proteção dos interesses dos menores; • Movimentação do patrimônio da criança deve ser limitada a 30% do valor total, podendo esse montante ser usado pra cobrir despesas imediatas de carreira e bem-estar. Só a criança ou adolescente pode movimentar os 70% após maioria; • Previsão de sanções aos violadores da lei.	• Menciona o trabalho artístico de crianças e adolescentes na internet; • Limita movimentações no patrimônio financeiro; • Prevê sanções aos que não seguirem os parâmetros estabelecidos; • Mantém bom diálogo com outras leis já existentes, como o Código Civil e o ECA.	
3917/23	• Propõe que o Ministério Público se manifeste sempre que um menor de idade for incluído em sociedade empresária; • Institui que seja obrigatória a inclusão de cláusula revisional em contratos condicionada à maioria do trabalhador artístico mirim.	• Proporciona aumento da observância do órgão fiscalizador em relações jurídicas que envolvam menores de idade • Zela pelo patrimônio do trabalhador artístico mirim ao determinar a criação da clausula revisional em contratos firmados dentro do exercício do poder familiar	• Propõe alteração simples no Código Civil; • Deixa de abordar outros pontos importantes, como limitação na movimentação de patrimônio financeiro e estabelecimento de penalidades para o uso indiscriminado da renda gerada pelo trabalho artístico do menor de idade.

Projeto de Lei	Principais Mecanismos	Vantagens	Lacunas
3918/23	• Exige a criação de conta de renda fixa para o menor, onde será depositado 30% de todo o rendimento da atividade artística-cultural por ele exercida; • Determina que tal conta só será movimentada mediante autorização judicial até que o menor complete sua maioridade; • Determina que a autoridade judicial acompanhará a cada ano ou sempre que solicitada nova autorização para o trabalho artístico infantil.	• Menciona trabalho artístico exercido em plataformas digitais; • Delimita porcentagem do patrimônio a ser reservada e como ela será cuidada; • Determina maior fiscalização judicial sobre o patrimônio do menor; • Cria lei focada apenas no assunto.	• Acompanhamento da autoridade judicial é mal descrito, poderia ter sido mais bem delimitado.
3919/23	• Define parâmetros para gestão patrimonial do menor, como prestação de contas e investimentos que visem a conservação do patrimônio, proibindo que o gestor adquira bens, dispor de bens ou constituir-se cessionário de crédito ou de direito contra o menor. • Prevê penalidades ao gestor que contribua negativamente ao patrimônio do menor, como ressarcimento e imputação do crime previsto no artigo 168, §1, II do Código Penal (apropriação indébita com aumento de pena por ter recebido a coisa na qualidade de tutor).	• Limita movimentações no patrimônio financeiro; • Prevê sanções aos que não seguirem os parâmetros estabelecidos;	• Fala pouco sobre fiscalização da autoridade judiciária; • Não menciona menores que trabalham com plataformas digitais.
3938/23	• Impõe a reserva e manutenção de no mínimo 60% do patrimônio total do menor; • Estabelece divisão no mínimo igualitária dos percentuais de participação em sociedades, empresas ou empreendimentos nos quais sejam acionistas	• Prevê limitação aos gastos do patrimônio do menor; • Regulamenta acerca da participação do menor em sociedades vinculadas a seu trabalho artístico.	• Muito raso, propõe alteração de somente um artigo do Código Civil através da inclusão de dois incisos; • Não deixa clara a existência da possibilidade de o menor ter maior participação em sociedades, empresas ou empreendimentos nos quais for acionista; • Não menciona menores que trabalham com plataformas digitais

Projeto de Lei	Principais Mecanismos	Vantagens	Lacunas
3960/23	• Limita a remuneração de pais, tutores ou empresários a no máximo 10% anuais de todos os valores arrecadados em função da atividade cultural, artística ou esportiva realizada pelo menor	• Limita remuneração de responsáveis	• Não menciona menores que trabalham com plataformas digitais • Inclui inciso desnecessário sobre o acompanhamento de crianças e adolescentes pelo Conselho Tutelar.
4053/23	• Institui a prestação de contas judicial por pais, usufrutuários e administradores de bens dos filhos; • Prevê possibilidade de proposição de ação de ressarcimento de danos contra pais que eventualmente percam ou tenham suspenso seu poder familiar por abuso de direito como usufrutuário e administrador de bens dos filhos	• Prevê prestação de contas pelos responsáveis/usufrutuários do patrimônio do menor; • Prevê penalidades para os que realizam mal uso do patrimônio	• Se propõe apenas a modificar o ECA • Não estabelece periodicidade sobre prestação de contas e a condiciona somente a suspeita de abuso de poder
4990/23	• Proíbe que pais sejam usufrutuários do patrimônio gerado pela atividade artística exercida pelo menor	• Reconhece menores que trabalham com plataformas digitais • Proíbe que os pais usufruam do patrimônio gerado pelo menor, garantindo maior proteção à infância	• Não impõe deveres de prestação de contas, não fornece diretrizes sobre manutenção do patrimônio e não prevê penalidades para o uso inadequado deste patrimônio.

Atualmente, o projeto principal foi anexado ao PL de número 3914/2023 que visa tipificar o crime de violência patrimonial contra crianças e adolescentes. Este último, por sua vez, foi aprovado pela Câmara dos Deputados e aguarda avaliação do Senado.

Foi possível observar que alguns dos projetos se debruçaram sobre os exemplos trazidos anteriormente, possivelmente das leis francesa e americana, de forma a limitar o uso da remuneração paga pelo trabalho artístico do menor e a destinar a maior parte desses ganhos a uma conta que só pudesse ser movimentada quando o menor atingisse sua maioridade.

A análise de todas as leis supracitadas, como o Estatuto da Criança e do Adolescente e o Código Civil em suas disposições sobre o assunto, permitem observar que a gestão e segurança patrimoniais de crianças e adolescentes

que exercem trabalho de teor artístico são ainda pouco observadas. Ainda menos atenção é dada aos menores que exercem esse trabalho como influenciadores digitais, tendo em vista a novidade da própria figura de influenciador como forma de trabalho. No entanto, se a atividade artística é de livre expressão também às crianças e adolescentes, e se tal expressão é passível de monetização, é importante que tanto o legislador, quanto os responsáveis pela correta execução e fiscalização da lei, olhem com mais atenção para essa nova forma de trabalho. Somente dessa forma será possível garantir não só a liberdade de expressão a esses menores, como também toda a segurança e proteção a eles devida.

Ainda que as propostas prevejam boas limitações aos gastos do patrimônio construído pelo menor através de seu trabalho, inclusive no aspecto de fiscalização, elas se mostram falhas na inserção do influenciador digital mirim como agente a ser observado pelos órgãos fiscalizadores no contexto da execução de um trabalho artístico. Não parece razoável aceitar que a lei automaticamente o protege por citá-lo em seu preâmbulo ou em seus primeiros artigos, que definem a quem aquelas disposições de destinam. Isso porque antes de fechar contratos de publicidade e receber uma remuneração por visualizações das plataformas em que atua, os menores que pretendem exercer esse tipo de trabalho precisam se expor e publicar material com certa periodicidade.

Dessa forma, seria interessante criar um critério que definisse a partir de qual momento a criança ou adolescente estaria de fato exercendo o ofício de influenciador digital, para que se pudesse determinar um momento a partir do qual seu patrimônio deve passar a ser protegido e suas condições de trabalho, verificadas pelos agentes competentes. Um bom parâmetro a ser utilizado poderia ser o sugerido pelo Ministério Público do Estado de São Paulo, que dentre outros critérios, consideram principalmente a monetização do conteúdo e sua profissionalização¹¹.

Considerações Finais

Os projetos de lei analisados demonstram que casos de muita repercussão pública continuam a ter grande impacto no sistema legislativo, eis que vários deles pretendem criar uma nova lei que seria popularmente conhecida por “Lei Larissa Manoela”, assim como as leis “Maria da Penha” e “Carolina

11. São Paulo, ref. 4.

Dieckmann”. Assim como nesses outros casos famosos, o que ensejou a criação desses projetos de lei foi a proteção esparsa a aspectos específicos de relações jurídicas, como a segurança patrimonial de crianças e adolescentes que exercem trabalho de teor artístico.

No entanto, as tentativas de suprir tais lacunas evidenciam a ausência de planejamento do legislador, que embalado pelo clamor público, pode tender a tentar abraçar muitas frentes ao mesmo tempo, o que evidentemente tira a eficácia de seus projetos de lei. As propostas de lei ora analisadas se preocupam com a segurança patrimonial do menor envolvido em trabalhos de teor artístico, e até mencionam os influenciadores digitais mirins, mas falha em destinar a eles maior observância e fiscalização de suas condições de trabalho. Por conseguirem aferir lucro através das próprias plataformas de redes sociais, de dentro de suas próprias residências, eles não passam pelo crivo do judiciário antes de começar a maioria de seus trabalhos, como é o caso de atores e atrizes mirins, que necessitam de um alvará específico para cada trabalho do qual participarão.

Ainda assim, as proposições de lei analisadas podem observar esses atores de maneira satisfatória, eis que a imposição de limitação ao uso de seus ganhos com as plataformas digitais pode garantir uma segurança financeira à sua maioria, e que o próprio influenciador digital decida, efetivamente, como investir e fazer uso geral de seu patrimônio.

Desta forma, é possível concluir que o atual arcabouço legal disponível deixa diversas lacunas no que diz respeito à segurança patrimonial de crianças e adolescentes que reúnem patrimônio através de um trabalho de teor artístico, permitindo que seus pais ou responsáveis legais dilapidem seus ganhos com relativa facilidade sob o pretexto de serem usufrutuários desses bens, assim como sob o pretexto de gerenciar a carreira artística do menor. As propostas de lei que surgiram com o objetivo de preencher tais lacunas, provavelmente baseadas também em iniciativas de outros países que testemunharam problemas semelhantes ao da atriz Larissa Manoela, como nos Estados Unidos, apresentam boas inovações e soluções para problemas específicos. São dignos de nota positiva a limitação ao uso de quantias a título de gerenciamento de carreira e pagamento de despesas do menor, assim como a destinação de grande parte dos valores ganhos pelos trabalhos para uma conta que só poderá ser utilizada pelo menor, na ocasião do atingimento de sua maioria. Essas soluções atendem também o influenciador digital mirim no sentido de garantir sua segurança patrimonial e financeira, mas é possível notar que o legislador

não se atentou em sugerir muitos mecanismos que garantam a eficácia dessas soluções. Nesse sentido, destaca-se o artigo 10 do Projeto de Lei nº 3916/23. Tal projeto foi apensado, recentemente, ao PL de número 3914/2023 que visa tipificar o crime de violência patrimonial contra crianças e adolescentes. O PL 3914/2023 foi aprovado pela Câmara em março de 2025, seguindo para avaliação do Senado, agora junto aos demais Projetos ora citados.

No entanto, verifica-se que o legislador ainda não possui dimensão acerca do trabalho exercido pelo influenciador digital mirim, que embora também seja um trabalho de teor artístico, pode facilmente consumir o tempo de um menor inadequadamente, impedindo que ele usufrua de direitos e garantias básicos em prol de um trabalho que exige alto dispêndio de horas, mas com altas possibilidades de grande remuneração. Dado que foram feitas propostas para melhor regulação da proteção patrimonial de crianças artistas, incluindo aquelas que atuam através do ambiente digital, teria sido oportuno regular também a partir de qual momento os fiscais da lei devem observar mais de perto os influenciadores digitais mirins, assim como a partir de quando seus pais ou responsáveis devem manter registro financeiro de suas atividades e administrar formalmente os bens adquiridos por esse trabalho, de forma que eles possam ser verificados pela autoridade competente.

Tais regulamentações poderiam, inclusive, dar origem a um marco normativo específico para influenciadores digitais mirins, tendo como base os pilares do reconhecimento legal da atividade, a proteção patrimonial de tais influenciadores e a proteção da imagem e do tempo da criança. Para atingir tais objetivos, tal diploma também poderia recomendar campanhas educativas para pais, responsáveis e plataformas digitais, como parte de uma solução não exclusivamente jurídica, mas que também visa dar maior efetividade a tal regulamentação.

Referências

ALMEIDA, E. M. de; FERREIRA, V. (org.). *Influencers mirins – um estudo sobre trabalho infantil nas redes sociais*. São Paulo, SP: FGV, 2024. Disponível em: https://direitosp.fgv.br/sites/default/files/arquivos/policy-paper_0.pdf. Acesso em: 04 de jan. de 2025.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Senado Federal, 2016. 496 p. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 03 jan. 2025.

_____. Decreto nº 4134/2002 – Promulga a Convenção nº 138 e a Recomendação nº 146 da Organização Internacional do Trabalho (OIT) sobre Idade Mínima de Admissão ao Emprego. *Diário*

Oficial da República Federativa do Brasil, Brasília, DF, 18 fev. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/2002/d4134.htm. Acesso em 04 jan. 2025.

_____. Decreto nº 10088/2019 – Consolida atos normativos editados pelo Poder Executivo Federal que dispõem sobre a promulgação de convenções e recomendações da Organização Internacional do Trabalho – OIT ratificadas pela República Federativa do Brasil. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 06 de nov. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10088.htm#art6. Acesso em 04 jan. 2025.

_____. Lei nº 8069/1990 – Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 16 jul. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm#art266. Acesso em 06 jan. 2025.

_____. Lei nº 10406/2002 – Institui o Código Civil. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm#art2044. Acesso em 04 jan. 2025.

_____. *Projeto de Lei nº 3916/2023 – Estabelece diretrizes para a proteção patrimonial de crianças e adolescentes que desenvolvam trabalho cultural, artístico ou esportivo*. Brasília, DF: Câmara dos deputados, 2023. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2379223>. Acesso em 06 jan. 2025.

_____. *Projeto de Lei nº 3917/2023 – Altera a Lei nº 10406 de 10 de janeiro de 2002 (Código Civil) para tratar da administração de bens dos filhos menores*. Brasília, DF: Câmara dos deputados, 2023. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2379237>. Acesso em 06 jan. 2025.

_____. *Projeto de Lei nº 3918/2023 – Dispõe e regula ganhos financeiros de crianças que trabalham com audiovisual, artistas mirins, para a proteção do patrimônio e investimentos futuros*. Brasília, DF: Câmara dos deputados, 2023. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2379366>. Acesso em 06 jan. 2025.

_____. *Projeto de Lei nº 3919/2023 – Cria a “Lei Larissa Manoela” para regulamentar a gestão do patrimônio de menores que exerçam atividade artística*. Brasília, DF: Câmara dos deputados, 2023. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2379382>. Acesso em 06 jan. 2025.

_____. *Projeto de Lei nº 3938/2023 – Altera a Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), visando a Preservação do Patrimônio dos Menores de Idade (LEI LARISSA MANOELA)*. Brasília, DF: Câmara dos deputados, 2023. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2379949>. Acesso em 06 jan. 2025.

_____. *Projeto de Lei nº 3960/2023 – Altera a Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil) objetivando regulamentar percentual máximo relativo à administração do patrimônio dos filhos menores*. Brasília, DF: Câmara dos deputados, 2023. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2380252>. Acesso em 06 jan. 2025.

_____. *Projeto de Lei nº 4053/2023 – Altera a Lei n. 8.069, de 13 de julho de 1990 – Estatuto da Criança e do Adolescente, para dispor sobre a gestão do patrimônio e a transparência no usufruto e administração dos bens dos filhos menores*. Brasília, DF: Câmara dos deputados, 2023. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2381449>. Acesso em 06 jan. 2025.

----- *Projeto de Lei nº 4990/2023 – Acrescenta o art. 1.693A ao Código Civil – Lei nº 10.406, de 10 de janeiro de 2002*. Brasília, DF: Câmara dos deputados, 2023. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2395819>. Acesso em 06 jan. 2025.

ESTADOS UNIDOS, Estado da Califórnia. *Family Code – FAM. §6752(b)(1)*. DIVISION. 11, PART 3, CHAPTER 3. Contracts in Art, Entertainment, and Professional Sports [6750 – 6753]. Estado da Califórnia, 2020. Disponível em: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=6752.&nodeTreePath=13.5.3&lawCode=FAM. Acesso em 05 jan. 2025.

FRANÇA. Loi nº 2020-1266 du 19 octobre 2020. Visant à encadrer l'exploitation commerciale de l'image d'enfants de moins de seize ans sur les plateformes en ligne (1). *JORF* nº 0255 du 20 octobre 2020 Texte nº 1. Disponível em: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042439054>. Acesso em 05 de jan. de 2025.

GHILARDI, D.; SANTOS, G. P. Sharenting e os desafios da regulamentação: Uma análise no Brasil e em França. *Revista Jurídica Luso-Brasileira*, Ano 9 (2023), nº 5, p. 567-601.

GOVERNOR GAVIN NEWSOM. *Governor Newsom joins Demi Lovato to sign legislation to protect the financial security of child influencers*. California: Governor Gavin Newson, 2024. Disponível em: <https://www.gov.ca.gov/2024/09/26/governor-newsom-joins-demi-lovato-to-sign-legislation-to-protect-the-financial-security-of-child-influencers/>. Acesso em 07 jan. 2025.

REARDON, J. *New Kidfluencers on the Block: The Need to Update California's Coogan Law to Ensure Adequate Protection for Child Influencers*, 73 *Case W. Rsrv. L. Rev.* 165 (2022). Disponível em: <https://scholarlycommons.law.case.edu/caselrev/vol73/iss1/6>. Acesso em 05 jan. 2025.

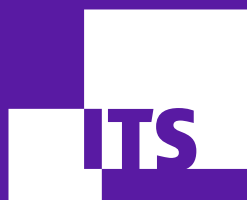
SÃO PAULO. Ministério Público do Estado de São Paulo. *Comentário Geral nº 25 na Prática: Orientações para a defesa das crianças e dos adolescentes no ambiente digital*. São Paulo, SP: Ministério Público do Estado de São Paulo, 2023. Disponível em: https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/BibliotecaDigital/Publicacoes_MP/Todas_publicacoes/Comentario-geral-n.25-na-pratica_orientacoes-para-a-defesa-das-criancas_2023.pdf. Acesso em 04 de jan. de 2025.

SILVA, F. de O. *Influenciadores digitais mirins: os riscos advindos da exposição nas redes sociais e as possíveis violações aos direitos da criança e do adolescente*. 2023. 114 p. Trabalho de Conclusão de Curso (Pós-graduação Lato Sensu) Escola da Magistratura do Estado do Rio de Janeiro, Rio de Janeiro, 2023.

SILVA, A. R. B. da; VIANA, E. B. D.; JULIÃO, I. L. A.; FARIAS, L. J. S. Os aspectos do trabalho infantil brasileiro na plataforma Youtube. *Revista Ibero-Americana de Humanidades, Ciências e Educação*. São Paulo, v.9.n.11. nov.2023. P. 1098-1118.

STJ. *Suspeita de abuso na administração de bens autoriza filho a exigir prestação de contas dos pais*. Brasília, DF: STJ, 2018. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2018/2018-03-21_06-51_Suspeita-de-abuso-na-administracao-dos-bens-autoriza-filho-a-exigir-prestacao-de-contas-dos-pais.aspx. Acesso em: 04 de jan. de 2025.

TOMAZ, R. *O que você vai ser antes de crescer? Youtubers, Infância e Celebridade*. 2017, 232 p. Tese de doutorado (Doutorado em Comunicação e Cultura). Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2017.



Acesse nossas redes



itsrio.org

Este livro foi composto nas fontes Termina,
FreightSans Pro e Public Sans e lançado pelo Instituto
de Tecnologia e Sociedade, em junho de 2025.