

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

Inteligência Artificial e Sociedade Conectada

COORDENAÇÃO
Sérgio Branco
Chiara de Teffé

PUBLICAÇÃO
janeiro/2025



DIREITO
UERJ

CEPED

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

Inteligência Artificial e Sociedade Conectada

COORDENAÇÃO
Sérgio Branco
Chiara de Teffé

PUBLICAÇÃO
janeiro/2025



COORDENAÇÃO:

Sérgio Branco e Chiara de Teffé

PROJETO GRÁFICO, CAPA E DIAGRAMAÇÃO:

Leandro Collares e Mariana Bertoluci

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)**

Inteligência artificial e sociedade conectada
[livro eletrônico] / coordenação Sérgio Branco,
Chiara de Teffé. -- 1. ed. -- Rio de Janeiro :
ITS - Instituto de Tecnologia E Sociedade,
2025. -- (Diálogos da pós-graduação em direito
digital)
PDF

Vários autores.
Bibliografia.
ISBN 978-85-5596-010-9

1. Direito digital 2. Inteligência artificial -
Direito 3. Proteção de dados pessoais 4. Proteção
de dados - Legislação - Brasil 5. Sociedade da
informação - Aspectos jurídicos I. Branco, Sérgio.
II. Teffé, Chiara de. III. Série.

24-243711

CDU-34:004.8

Índices para catálogo sistemático:

1. Inteligência artificial e direito 34:004.8

Aline Grazielle Benitez - Bibliotecária - CRB-1/3129

COMO CITAR:

BRANCO, Sérgio; TEFFÉ, Chiara Spadaccini de (Coords.). *Inteligência artificial e sociedade conectada*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2025. 368p.

INSTITUTO DE TECNOLOGIA E SOCIEDADE:

itsrio.org | @itsriodejaneiro | midias@itsrio.org



A obra Inteligência Artificial e Sociedade Conectada 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

Bárbara Gomes D'Ascensão

Carolina Freitas Gomide de Araujo

Cláudio Mendes da Silva

Daniel Santiago Diniz

Elmano Rodrigues Pinheiro Filho

Giovana Sant'Anna

Henrique Segolin Molina

Lígia Maria de Souza Lopes Reis

Luís Henrique de Menezes Acioly

Luisa Amélia

Maíra Lima de Souza

Maria Fernanda Longato Maturana

Matheus Mantuani

Nina Ramalho Pinheiro

Rodrigo Santana dos Santos

Taís Bigarella Lemos

Victor Chame Alvim

Vinicius Azevedo Coelho

APRESENTAÇÃO

Em um cenário de inovação acelerada, em que a Inteligência Artificial e as tecnologias digitais vêm impactando as relações humanas e institucionais, o livro *Inteligência Artificial e Sociedade Conectada* visa contribuir com as discussões legais, sociais e tecnológicas dessa nova era.

Dividido em três eixos temáticos, a obra conta com análises de diversos autores especializados, todos estudantes da pós-graduação *lato sensu* em Direito Digital do ITS Rio em parceria com a UERJ e o CEPED, que buscam desvendar os complexos aspectos da regulação da inteligência artificial, da proteção de dados e da estruturação das cidades inteligentes. Esse livro se revela uma leitura imprescindível para estudiosos, profissionais e todos aqueles interessados nos impactos profundos da inteligência artificial em uma sociedade cada vez mais conectada.

O primeiro eixo, dedicado à Inteligência Artificial, oferece uma abordagem ampla sobre aspectos regulatórios aplicados à IA, especialmente no contexto brasileiro. Questões como a definição de uma autoridade regulatória para a IA, treinamento de IA via web scraping e originalidade das criações de IA destacam a importância de se definir limites e responsabilidades para essa tecnologia. Temas importantes como o racismo e a discriminação algorítmica ganham espaço em discussões detalhadas que abordam desde a justiça social até a urgência de regulamentações que promovam uma IA justa e responsável. Por fim, a obra explora o campo emergente dos neurodireitos e suas implicações, sinalizando o impacto direto da IA em direitos fundamentais.

No segundo eixo, Cidades Inteligentes e Novas Tecnologias, os autores analisam as implicações das tecnologias nas chamadas cidades inteligentes e nas regulamentações que surgem para acompanhá-las. Questões como a necropolítica e a proteção de dados nas cidades inteligentes são abordadas, fornecendo uma perspectiva crítica sobre como essas inovações afetam os direitos fundamentais. As discussões sobre o sandbox regulatório em âmbito municipal e o papel do Banco Central na regulação de fintechs de pagamento trazem ao leitor uma visão prática dos avanços e das complexidades que a tecnologia impõe sobre a segurança jurídica e a governança pública. Em um olhar sobre a tecnologia blockchain, uma perspectiva de gênero é introduzida, estimulando uma reflexão sobre a inclusão em um campo em rápido desenvolvimento.

APRESENTAÇÃO

O terceiro eixo, Proteção de Dados e Segurança Digital, oferece uma análise regulatória voltada ao fortalecimento da cibersegurança e da proteção de dados pessoais diante das ameaças que permeiam o ambiente virtual. Um destaque é a discussão sobre a cibersegurança infantil, que explora a necessidade de políticas específicas para garantir a segurança de crianças e adolescentes na internet, em um cenário cada vez mais conectado. O eixo se encerra com uma análise das bases legais para a coleta de dados na área da saúde, enfatizando a importância de um sistema que respeite a privacidade e valorize a diversidade, promovendo uma abordagem ética e inclusiva para proteger informações sensíveis.

Inteligência Artificial e Sociedade Conectada é uma obra que combina rigor acadêmico com uma visão inovadora sobre os desafios contemporâneos das tecnologias digitais. Com reflexões que transcendem fronteiras e disciplinas, este livro é um recurso valioso para compreender como a sociedade pode avançar de forma ética, inclusiva e informada na era digital.

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 voltadas 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, 02 de dezembro de 2024.

OS COORDENADORES

OS COORDENADORES

Chiara de Teffé

Doutora e mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ), tendo sido aprovada com distinção, louvor e recomendação para publicação. Graduada em Direito pela Universidade Federal do Rio de Janeiro (UFRJ), quando foi bolsista de iniciação científica do CNPq e da FAPERJ. 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 de Direito Civil e Direito Digital na faculdade de Direito do IBMEC. Leciona em cursos específicos de pós-graduação e extensão do CEPED-UERJ, da PUC-Rio, da EMERJ e do ITS Rio. Membro da Comissão de Proteção de Dados e Privacidade da OAB/RJ. Membro da Comissão de Direito Civil do Conselho Seccional do Rio de Janeiro da OAB (2022/2024). 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. Atua como advogada em áreas do Direito Civil e do Direito Digital e como consultora em proteção de dados pessoais. 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".

Sérgio Branco

Cofundador e diretor do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio). Doutor e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (Uerj). Pesquisador convidado do Centre de Recherche en Droit Publique da Universidade de Montreal. Visiting Research Fellow em Sciences Po entre 2023 e 2024. 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). Sócio do escritório de advocacia Rennó Penteado Sampaio.

SUMÁRIO

EIXO I

INTELIGÊNCIA ARTIFICIAL

13

Regulação da inteligência artificial: reflexões sobre a definição de uma autoridade competente no Brasil

ELMANO RODRIGUES PINHEIRO FILHO

35

Inteligência Artificial e Proteção de Dados Pessoais: reflexões sobre a base legal adequada para fundamentar o treinamento via web scraping

MATHEUS MANTUANI

56

Racismo Algorítmico: Os Desafios da Inteligência Artificial e a Justiça Social no Contexto Digital

BÁRBARA GOMES D'ASCENÇÃO

72

Coleta de Dados Pessoais para o Treinamento de Inteligência Artificial Generativa: Um Desafio para a Proteção de Dados e a Privacidade

RODRIGO SANTANA DOS SANTOS

94

Classificação de danos decorrentes de incidentes de IA

VINICIUS AZEVEDO COELHO

113

PL 2.338/2023: um estudo sobre as disposições de direitos autorais

NINA RAMALHO PINHEIRO

133

Originalidade Algorítmica: há originalidade nos outputs da inteligência artificial generativa?

TAÍS BIGARELLA LEMOS

SUMÁRIO

151

Os desafios envoltos a utilização e regulamentação da inteligência artificial diante da discriminação algorítmica

MARIA FERNANDA LONGATO MATURANA

169

Uma análise crítica acerca da algoritmização discriminatória no âmbito do direito penal

LUISA AMÉLIA LINO

190

Entre Cérebro e Computador: Diálogos sobre Neurodireitos e Inteligência Artificial

HENRIQUE SEGOLIN MOLINA

EIXO II

CIDADES INTELIGENTES E NOVAS TECNOLOGIAS

212

Cidades Inteligentes e Necropolítica: A proteção de dados e os direitos fundamentais na Era Digital

CLÁUDIO MENDES DA SILVA

230

Implementação de cidades inteligentes e sandbox regulatório: Desafios e oportunidades na lei de inovação de Juiz de Fora

DANIEL SANTIAGO DINIZ

251

Da Segurança Jurídica à Segurança Técnica: Temas Decodificadores do Avanço Tecnológico no Registro Eletrônico de Imóveis

LUÍS HENRIQUE DE MENEZES ACIOLY

273

O papel do Banco Central do Brasil na regulação das fintechs de pagamento

VICTOR CHAME ALVIM

SUMÁRIO

287

Blockchain como substantivo feminino: uma análise de gênero quanto ao uso em ascensão da tecnologia blockchain

CAROLINA FREITAS GOMIDE DE ARAUJO

EIXO III

PROTEÇÃO DE DADOS E SEGURANÇA DIGITAL

304

Risco e Cibersegurança no Brasil: uma análise regulatória visando a proteção de dados

GIOVANA SANT'ANNA

326

Ciberinfância e cibersegurança social: em busca de aprimoramento da proteção de crianças e adolescentes na internet

LÍGIA MARIA DE SOUZA LOPES REIS

346

As bases legais no sistema de coleta de informação sobre a diversidade na Saúde e na Saúde Digital

MAÍRA LIMA DE SOUZA

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

EIXO I

Inteligência Artificial

AUTORES

Bárbara Gomes D'Ascensão

Elmano Rodrigues Pinheiro Filho

Henrique Segolin Molina

Luisa Amélia

Maria Fernanda Longato Maturana

Matheus Mantuani

Nina Ramalho Pinheiro

Rodrigo Santana dos Santos

Taís Bigarella Lemos

Vinicius Azevedo Coelho

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

1

Regulação da inteligência artificial: reflexões sobre a definição de uma autoridade competente no Brasil

ELMANO RODRIGUES PINHEIRO FILHO

Sumário: Introdução. 1. Regulação de tecnologias digitais emergentes. 2. Regulação da inteligência artificial. 2.1. Abordagens regulatórias na União Europeia, nos Estados Unidos e no Reino Unido. 2.2. Propostas de regulação estatal para a IA no Brasil. 3. Reflexões sobre a definição de uma autoridade competente para a regulação de inteligência artificial no Brasil. Considerações finais. Referências.

Introdução

A regulação é tema central em muitas discussões contemporâneas sobre políticas públicas. Após a crise econômica de 2008 e a pandemia de COVID-19, poucos discordariam da importância da regulação para o bom funcionamento das modernas economias de mercado². No entanto, nem sempre o papel da regulação foi compreendido, reconhecido ou desejado, especialmente quando se trata de tecnologias digitais emergentes, como foi o caso da internet.

Na “Declaração de Independência do Ciberespaço”, John Perry Barlow, renomado ativista dos direitos na internet, defendeu a ideia de que a rede deveria ser tratada como um novo mundo, sem regras, e livre dos abusos autoritários dos governos.

Contrariamente a essa visão utópica, a internet é vista, hoje, como um prolongamento do “mundo real”. Com a difusão das redes em todas as áreas da sociedade – política, econômica, social e cultural –, as discussões passaram a reconhecer a regulação como essencial, visando coibir comportamentos indesejados, como a concentração de mercados pelas plataformas digitais, e promover usos positivos, como o acesso a conteúdos digitais com respeito aos direitos autorais.

O debate sobre a regulação das tecnologias digitais emergentes, a exemplo do que aconteceu com a internet, alcançou um novo nível nos últimos anos, marcando uma espécie de perda de inocência em relação às discussões dos anos 1990 e 2000. Enquanto no período anterior predominava a argumenta-

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. LODGE, Martin; WEGRICH, Kai. O enraizamento da Regulação de Qualidade: fazer as perguntas difíceis é a resposta. In: PROENÇA, Jadir Dias; COSTA, Patrícia Vieira da; MONTAGNER, Paula (Coord). *Desafios da regulação no Brasil*. Brasília: ENAP, 2009. p. 17.

ção contra qualquer forma de regulação, com uma perspectiva utópica dos benefícios que a inovação tecnológica sem controle poderia trazer, nos últimos vinte anos observa-se uma visão muito mais cética e pessimista sobre o tema³, reconhecendo-se a necessidade do estabelecimento de um quadro legal específico que minimize seus eventuais efeitos nocivos. Não obstante, tal regulação tem sido construída numa perspectiva adaptativa, fundamentada na experiência e na prática, de modo que possa ser eficaz e relevante, a exemplo do que já fora pensado para a regulação da internet⁴.

O propósito deste trabalho é explorar uma das mais significativas tecnologias digitais emergentes: a inteligência artificial. No entanto, não se pretende esgotar completamente o tema, pois, dada a complexidade do assunto, uma análise minuciosa de todos os aspectos envolvidos ultrapassaria os limites estabelecidos para o trabalho. O objetivo é examinar aspectos específicos da regulação da inteligência artificial.

O objetivo geral deste trabalho é avaliar diferentes modelos de regulação da inteligência artificial que vêm sendo implementados. De forma específica, busca-se: compreender as especificidades da regulação de tecnologias digitais e os possíveis impactos de sua implementação; verificar as diferentes abordagens e estruturas regulatórias relativas à inteligência artificial na União Europeia, nos Estados Unidos e no Reino Unido; avaliar a proposta de regulação da inteligência artificial no Brasil; investigar como o Projeto de Lei nº 2.338, de 2023, trata da questão da definição de uma autoridade competente para a regulação da inteligência artificial.

A relevância da temática se deve ao fato de que as tecnologias digitais emergentes, que transformam relações pessoais e patrimoniais, criando e aperfeiçoando produtos, serviços e atividades, procedimentos e práticas, em vários setores econômicos e em relação a muitos aspectos da sociedade, também acarretam novos riscos e amplificam os já existentes. O uso da inteligência artificial, por exemplo, na produção ou manipulação de conteúdo com o intuito de disseminar fatos notoriamente falsos ou descontextualizados, pode potencialmente prejudicar o equilíbrio e a integridade dos processos eleitorais, justificando, assim, alguma forma de regulação. Para a análise, será adotada a metodologia de revisão bibliográfica.

3. 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. 266-267.

4. LESSIG, Lawrence. *The Law of the Horse: What Cyber Law Might Teach*. Harvard Law Review, Harvard, v. 113, p. 501-546, dez. 1999. Disponível em: <https://cyber.harvard.edu/works/lessig/finalhls.pdf>. Acesso em: 1 out. 2024.

Assim sendo, o presente artigo será dividido em quatro capítulos. No capítulo 1, serão apresentadas considerações sobre a teoria da regulação e os desafios para a regulação de tecnologias digitais emergentes, a exemplo da inteligência artificial. No capítulo 2, dividido em duas seções, será examinada a evolução da regulação da inteligência artificial no mundo, apresentando-se algumas abordagens já realizadas, e o debate sobre a regulação da inteligência artificial no Brasil. No capítulo 3, será feita uma reflexão sobre a definição de uma autoridade competente para a regulação da inteligência artificial no País, apresentando-se vantagens e desvantagens da adoção de diferentes modelos e sob a coordenação de diferentes entidades. Ao término, serão apresentadas as considerações finais do trabalho, destacando-se as principais constatações e fornecendo-se sugestões para futuras pesquisas a serem realizadas.

1. Regulação de tecnologias digitais emergentes

As tecnologias digitais estão revolucionando quase todos os setores da economia, introduzindo produtos e serviços inovadores, favorecendo novos modelos de negócios e transformando a maneira como os países promovem e usufruem do desenvolvimento socioeconômico. As tecnologias digitais possibilitam conectar cidadãos a serviços e oportunidades, ajudando a construir um futuro mais inclusivo e próspero. No entanto, para garantir que os mercados operem eficazmente e atendam satisfatoriamente às necessidades e expectativas da sociedade, é essencial que essa transformação seja acompanhada por políticas públicas e um ambiente regulatório adequados, que promovam a competição justa, protejam os consumidores e incentivem a inovação responsável⁵.

A digitalização das sociedades e economias está gerando quantidade sem precedentes de dados, impulsionada pela crescente e rápida conectividade entre pessoas e dispositivos. Tecnologias emergentes (como o 5G) estão facilitando o engajamento em atividades digitais, enquanto plataformas de mídia social e conteúdo gerado por usuários incentivam essa interação. Simultaneamente, mais dispositivos estão se tornando “inteligentes”, conectando-se à internet para trocar informações. Como resultado do explosivo crescimento de dados, surgiram novas tecnologias que filtram e analisam grandes conjuntos de dados, descritas em termos amplos como inteligência artificial e *big data*⁶.

5. UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES; BANCO MUNDIAL. *Digital Regulation Handbook*. Genebra, 2020. Disponível em: <http://handle.itu.int/11.1002/pub/81630556-en>. Acesso em: 22 jul. 2024.

6. *Ibidem*, p. 142.

Essas inovações tecnológicas estão desafiando os reguladores a revisar suas estratégias para promover uma competição justa e proteger os consumidores. Além dos desafios técnicos, essas tecnologias levantam questões legais, éticas e macroeconômicas. Bancos centrais, agências de proteção ao consumidor, comissões de competição e reguladores do setor de Tecnologia da Informação e Comunicação (TIC) estão trabalhando para avaliar o impacto dessas mudanças em suas respectivas áreas de responsabilidade. Isso pode envolver a necessidade de redesenhar as funções de diversos reguladores⁷.

No que diz respeito aos reguladores que supervisionam o setor de TIC, e que estão diretamente envolvidos com as tecnologias digitais emergentes, o *Digital Regulation Handbook*, publicado pela UIT e pelo Banco Mundial, identifica três modelos principais de estrutura institucional: regulador específico do setor, regulador multissetorial e regulador convergente. Segundo o estudo, tradicionalmente, os reguladores com foco exclusivo eram comuns para a regulação das telecomunicações. Porém, atualmente, tais reguladores são menos frequentes em comparação aos convergentes ou multissetoriais.

Assim, pode-se afirmar que a era digital mudou profundamente os papéis dos reguladores e formuladores de políticas públicas. Embora as áreas tradicionais de responsabilidade e a estrutura institucional dos reguladores possam ainda permanecer relevantes no ambiente digital, a regulamentação precisa se tornar mais flexível e adaptável. As competências dos reguladores também podem necessitar de ajustes para abranger as novas realidades digitais⁸.

Contudo, essas novas áreas nem sempre se encaixam claramente nas estruturas regulatórias existentes e muitos países vêm discutindo se seus reguladores tradicionais teriam a autoridade necessária para lidar com as tecnologias digitais emergentes. Embora essas discussões estejam em estágios iniciais, a análise, geralmente, compreende avaliar se seria necessário um novo órgão regulador dedicado exclusivamente a questões digitais, se seria necessário expandir as competências de um regulador existente ou se o modelo mais adequado seria um regulador de TIC atuando em conjunto com outras autoridades governamentais responsáveis por áreas como proteção ao consumidor, privacidade e segurança cibernética⁹.

7. *Ibidem*, p. 142.

8. SCHOLZE, Simone Henriqueta Cossetin; VIEIRA, Vania Lucia Ribeiro; AGUIAR, Alexandre Kehrig Veronese. *Estudo sobre modelo regulatório pró-inovação*. 2024. p. 41.

9. UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES; BANCO MUNDIAL. *Digital Regulation Handbook*. Genebra, 2020. p. 8. Disponível em: <http://handle.itu.int/11.1002/pub/81630556-en>. Acesso em: 22 jul. 2024.

2. Regulação da inteligência artificial

Para se discutir a regulação da inteligência artificial é fundamental esclarecer o que se entende por inteligência artificial (IA). As definições variam de acordo com a área de conhecimento utilizada para explicá-la e levam em conta a sua transdisciplinaridade e complexidade dos seus sistemas, algoritmos e aplicações¹⁰. Dado o rápido avanço tecnológico, o conceito de inteligência artificial também tem sido constantemente atualizado e ajustado para refletir as mudanças mais recentes.

Nesse contexto, reconhecendo que o conceito está sujeito a revisões, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) define inteligência artificial como um sistema baseado em máquina que, para objetivos explícitos ou implícitos, infere, a partir dos dados que recebe, como gerar resultados como previsões, conteúdo, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais. Diferentes sistemas de IA variam em seus níveis de autonomia e adaptabilidade após a implementação¹¹.

Conforme sua conceituação, a inteligência artificial é uma tecnologia digital emergente que tem o potencial de transformar diversos aspectos da vida e da sociedade, incluindo o bem-estar humano, o crescimento econômico inclusivo, o desenvolvimento sustentável, a inovação e a proteção dos direitos humanos e das liberdades fundamentais. No entanto, também apresenta riscos consideráveis para a população e a sociedade, podendo ameaçar esses direitos e liberdades essenciais. Um desses riscos é a propagação de vieses e de discriminação, em que IA pode tomar decisões discriminatórias. Outros riscos normalmente associados ao uso da IA são: violação de privacidade; cibersegurança; uso para fins maliciosos, como fraudes e ilícitos; obtenção de informações que possam causar riscos à integridade de pessoas; desinformação e manipulação de informação; danos ou prejuízos causados por consequências não intencionais¹².

Esses riscos associados à tecnologia têm levado a uma crescente demanda por uma regulação jurídica da inteligência artificial. Existem diversas abordagens para essa regulação, incluindo a criação de leis específicas para a IA,

10. DE OLIVEIRA, Thais Figueira. Uma autoridade reguladora para a inteligência artificial no Brasil. 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. 756-757.

11. ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. *Recommendation of the Council on Artificial Intelligence*. Paris, 2024. p. 7. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. Acesso em: 26 jul. 2024.

12. BRASIL. Tribunal de Contas da União. *Acórdão nº 616/2024*. Plenário. Relator: Ministro Aroldo Cedraz. Sessão de 03/04/2024. Brasília, TCU, 2024. p. 6. Disponível em: <https://pesquisa.apps.tcu.gov.br/redireciona/processo/3363820233>. Acesso em: 22 jul. 2024.

a adoção de legislações que promovam a inovação ou, até mesmo, a decisão de não regulamentar, com a justificativa de que as regulamentações atuais já seriam suficientes¹³.

Dada a natureza dinâmica e em rápida evolução da área, a regulação enfrenta o desafio de antecipar cenários futuros que podem ou não se concretizar. Uma regulamentação excessiva pode inibir o avanço tecnológico e reduzir a competitividade internacional dos setores produtivos. Assim, um dos principais desafios é encontrar um equilíbrio entre proteger os direitos individuais e coletivos e permitir a inovação e o desenvolvimento do mercado¹⁴. Nesse ambiente, as abordagens de regulação que estão sendo empregadas podem ser categorizadas em diversos tipos¹⁵, destacando-se três principais: a regulação baseada em princípios, a baseada em riscos e a baseada em direitos.

A regulação baseada em princípios direciona o desenvolvimento e a utilização de sistemas de inteligência artificial (IA) ao estabelecer premissas gerais e diretrizes éticas, sem a necessidade de especificar um conjunto rígido de direitos e obrigações desde o início. Esses princípios orientam o desenvolvimento e uso de sistemas de IA por meio de processos éticos, responsáveis, centrados no ser humano e respeitadores dos direitos humanos¹⁶.

Por sua vez, a regulação baseada em riscos concentra-se na identificação e gestão dos riscos associados ao desenvolvimento e uso de sistemas de inteligência artificial. Essa abordagem visa adaptar as obrigações ou requisitos da regulamentação com base no nível de risco apresentado por diferentes tipos de sistemas de IA¹⁷. Diferente da regulação baseada em princípios, que é mais flexível e orientada por valores gerais, a regulação baseada em riscos adota um método mais estruturado e específico. Ela classifica os sistemas de IA conforme seus níveis de risco e define padrões rigorosos de governança com base na gravidade dos riscos identificados. Essa abordagem visa assegurar que as medidas de controle e regulamentação sejam proporcionais ao risco apresentado por cada aplicação de IA¹⁸.

13. *Ibidem*, p. 7-8.

14. *Ibidem*, p. 8.

15. ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA. *Consultation Paper on AI Regulation: Emerging Approaches Across the World*. Paris, 2024. p. 20. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000390979>. Acesso em: 1 out. 2024.

16. *Ibidem*, p. 21.

17. *Ibidem*, p. 35.

18. BRASIL. Tribunal de Contas da União. *Acórdão nº 616/2024*. Plenário. Relator: Ministro Aroldo Cedraz. Sessão de 03/04/2024. Brasília, TCU, 2024, p. 8. Disponível em: <https://pesquisa.apps.tcu.gov.br/redireciona/processo/3363820233>. Acesso em: 22 jul. 2024.

Finalmente, a regulação baseada em direitos enfatiza a proteção dos direitos humanos e fundamentais no contexto dos sistemas de inteligência artificial. Essa abordagem define antecipadamente um conjunto específico de direitos e obrigações que devem ser respeitados no desenvolvimento e uso de IA, priorizando a salvaguarda dos direitos dos usuários. Embora essa abordagem ofereça um conjunto claro de normas e proteções, ela pode enfrentar desafios significativos, especialmente devido à sua natureza detalhada e completa, que pode não acompanhar a velocidade e flexibilidade do mercado de IA. Em contraste com outras abordagens, que podem ser mais adaptativas ou orientadas por princípios gerais, a regulação baseada em direitos pode implicar maiores dificuldades para a inovação e o avanço tecnológico, à medida que busca equilibrar a proteção dos direitos individuais com a necessidade de flexibilidade no desenvolvimento tecnológico¹⁹.

Na perspectiva internacionalista, as políticas normativas e regulatórias em matéria de inteligência artificial podem, ainda, ser sistematizadas em três abordagens de intervenção do direito: diálogos multilaterais e regionais (especialmente pelas organizações internacionais como as Nações Unidas e a União Europeia); estratégias nacionais (com a adoção de políticas governamentais com vistas a estimular a inteligência artificial nos ambientes domésticos); e padrões transnacionais de regulação (como princípios, códigos de conduta, diretrizes e recomendações de atores não estatais)²⁰.

Para uma análise mais detalhada dessas abordagens regulatórias, na próxima seção serão exploradas as iniciativas de regulação 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

Diversos países estão atualmente desenvolvendo estruturas regulatórias para integrar a inteligência artificial em seus sistemas jurídicos. Globalmente, observa-se uma tendência comum nas abordagens governamentais e jurisdicionais, que visa não apenas aproveitar os benefícios dos sistemas de IA para a sociedade, a indústria e o setor público, mas também equilibrar

19. *Ibidem*, p. 8.

20. POLIDO, Fabrício Bertini Pasquot. Novas perspectivas para regulação da inteligência artificial: diálogos entre as políticas domésticas e os processos legais transnacionais. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Coord). *Inteligência artificial e direito: ética, regulação e responsabilidade*. 2. ed. rev. atual. e aum. São Paulo: Thomson Reuters Brasil, 2020. p. 180.

essas vantagens com as preocupações éticas e legais associadas à sua implementação²¹.

A União Europeia, em virtude de sua experiência com proteção de dados pessoais, o que levou à edição do Regulamento Geral sobre a Proteção de Dados (GDPR), modelo regulatório sobre o tema, realizou, no que respeita à inteligência artificial, um esforço contínuo para desenvolver um sistema abrangente que garanta uma tecnologia segura e ética. Em 2018, a Comissão Europeia criou um grupo específico para tratar do tema da IA, marcando o início dos trabalhos de regulação. Em 2021, foi publicada a proposta para uma regulamentação legal sobre IA, que, após discussões extensas, recebeu a posição de negociação do Parlamento Europeu em junho de 2023 e um acordo final em dezembro do mesmo ano, e que ficou conhecida como *Artificial Intelligence Act (EU AI Act)*²².

O *EU AI Act* adota uma abordagem baseada em riscos, classificando os sistemas de IA em diferentes categorias de risco, como inaceitável, elevado, limitado e mínimo. Esta abordagem não apenas estabelece requisitos legais rigorosos para sistemas de alto risco, abordando aspectos como governança de dados, transparência e segurança, mas também inclui um ambiente regulatório experimental (*sandbox* regulatório²³). Essa estratégia visa garantir que a regulamentação seja adaptável e equilibrada, incentivando a inovação ao mesmo tempo em que protege os direitos dos usuários e a segurança²⁴.

Para implementar o *EU AI Act*, cada Estado-Membro da UE deve designar ou criar uma autoridade nacional responsável pela avaliação e fiscalização da conformidade com a legislação. Além disso, o projeto prevê a criação do *European Artificial Intelligence Board*, um comitê destinado a aconselhar e auxiliar as autoridades nacionais na aplicação das normas. No entanto, emendas recentes sugerem a necessidade de uma agência centralizada com personalidade jurídica própria, financiamento e pessoal, para coordenar e harmonizar as ações entre os Estados-Membros e evitar a fragmentação do mercado. Essa proposta busca assegurar uma regulação mais uniforme e eficaz, alinhando

21. DE OLIVEIRA, Thais Figueira. Uma autoridade reguladora para a inteligência artificial no Brasil. 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. 762.

22. BRASIL. Tribunal de Contas da União. *Acórdão nº 616/2024*. Plenário. Relator: Ministro Aroldo Cedraz. Sessão de 03/04/2024. Brasília, TCU, 2024, p. 8. Disponível em: <https://pesquisa.apps.tcu.gov.br/redireciona/processo/3363820233>. Acesso em: 22 jul. 2024.

23. O *sandbox* permite uma experimentação mais flexível com novos produtos e serviços, enquanto mantém a supervisão regulatória. Essa estratégia visa garantir que a regulamentação seja adaptável e equilibrada, incentivando a inovação ao mesmo tempo em que protege os direitos dos usuários e a segurança.

24. *Ibidem*, p. 8.

as decisões nacionais e promovendo um ecossistema de IA confiável e coeso em toda a União Europeia²⁵.

Por sua vez, a regulação da IA nos Estados Unidos está em um estágio inicial, refletindo uma abordagem ainda em desenvolvimento para lidar com a rápida evolução dessa tecnologia. Em outubro de 2022, o país lançou o *Blueprint for AI Bill of Rights*, um documento técnico destinado a orientar o desenvolvimento de políticas que protejam os direitos civis e promovam valores democráticos, mas que ainda não se constitui em uma legislação formal²⁶. Esse documento serve como um guia de princípios para o governo americano, focando em evitar a sobrecarga regulatória e manter a liderança dos Estados Unidos no setor de IA²⁷. Recentemente, em outubro de 2023, o presidente Joe Biden emitiu uma ordem executiva²⁸ que estabelece novos padrões de segurança e proteção, abordando preocupações como privacidade e equidade, e incentivando a inovação e a pesquisa no setor²⁹.

Nos Estados Unidos, a recente estrutura de regulação adota uma abordagem setorial, caracterizada pela corregulação, conduzida por meio da atuação de agências reguladoras federais, dos governos estaduais e locais. Nessa estrutura, os órgãos federais são responsáveis por emitir diretrizes baseadas em princípios e deixam a implementação para o setor privado. A *Federal Trade Commission (FTC)*, por exemplo, publicou diretrizes que destacam a importância de sistemas de IA serem transparentes, explicáveis, justos e responsáveis. O *Department of Defence (DoD)* adotou princípios éticos para IA aplicáveis a funções de combate e não-combate, focando em responsabilidade, equidade, rastreabilidade, confiabilidade e governabilidade. Além disso, a *Food and Drug Administration (FDA)* introduziu um plano de ação para software de IA como dispositivo médico, buscando avaliar e monitorar tais softwares ao longo de seu ciclo de vida³⁰.

25. DE OLIVEIRA, Thaís Figueira. Uma autoridade reguladora para a inteligência artificial no Brasil. 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. 764.

26. MELO, Ana Karolina Acris; SOUZA, Géssica Cardoso; VASCO, Amanda Corrêa; REIS, Bruno Salomon. *Regulação da Inteligência Artificial: benchmarking de países selecionados*. Brasília: Escola Nacional de Administração Pública, 2022. p. 18. Disponível em: <https://repositorio.enap.gov.br/handle/1/7419>. Acesso em: 1 out. 2024.

27. O texto não apresenta uma nova lei ou política regulatória do governo dos Estados Unidos. Trata-se de uma declaração de princípios, baseada em cinco premissas fundamentais para proteger o público na era da inteligência artificial: 1. Os sistemas automatizados devem ser seguros e eficazes; 2. Os usuários devem ser protegidos contra discriminação algorítmica, garantindo o uso equitativo; 3. As pessoas devem ter controle sobre o uso de seus dados, evitando práticas abusivas; 4. É fundamental que os usuários entendam como e por que um sistema de IA tomou determinada decisão; 5. As pessoas devem ter a opção de recusar decisões de IA e solicitar uma avaliação humana em caso de erro ou contestação.

28. *Executive Order*, equiparada a um Decreto da Presidência da República no Brasil.

29. NAZARENO, Claudio. *Regulação da inteligência artificial: experiências internacionais e desafios para o Brasil*. Brasília: Câmara dos Deputados, Consultoria Legislativa, 2024. p. 15. Disponível em: <https://bd.camara.leg.br/bd/handle/bdcamara/41741>. Acesso em: 1 out. 2024.

30. BELLI, Luca; CURZI, Yasmin; GASPAR, Walter B. *AI Regulation in Brazil: Advancements, flows, and need to learn from the data protection experience*. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, v. 48, p. 3-4.

Além das diretrizes e ordens executivas, nos Estados Unidos, foram aprovadas diversas propostas legislativas que tratam de inteligência artificial. Entre elas, o *Algorithmic Accountability Act* e o *Consumer Online Privacy Rights Act*, que visam criar regulamentações específicas para decisões automatizadas e privacidade online. O *Good AI Act* de 2022 propõe a criação de um “Grupo de Trabalho sobre Higiene da Inteligência Artificial”, enquanto o *Advancing American AI Act* busca regular o uso de IA por agências governamentais. No entanto, até o momento, não houve avanços significativos na adoção dessas propostas, e não existe uma legislação federal abrangente sobre IA no país³¹.

No que se refere ao Reino Unido, em 2023, o governo publicou o documento técnico *A pro-innovation approach to AI regulation*, refletindo uma estratégia distinta para a regulamentação da inteligência artificial. Por meio de uma abordagem flexível e iterativa³², o Reino Unido busca equilibrar a promoção da inovação com a gestão dos riscos associados à tecnologia. Ao invés de estabelecer uma regulação rígida e imediata, o modelo britânico é projetado para evoluir com o tempo, permitindo ajustes contínuos com base no progresso dos estudos e no amadurecimento do setor. Essa estratégia é orientada por princípios e premissas que se adaptam às necessidades específicas de diferentes áreas da economia, preferindo regular o uso da IA em vez da tecnologia em si³³.

Dessa forma, busca-se uma regulação que seja predominantemente setorial e ajustada conforme os ciclos rápidos de inovação e desenvolvimento da tecnologia. Neste caso, a função central da autoridade regulatória não é regular diretamente todos os aspectos da IA, mas sim gerenciar o processo por meio de monitoramento, avaliação e retroalimentação. A autoridade é responsável ainda por apoiar a implementação dos princípios regulatórios, gerenciar riscos intersetoriais, promover inovação, e garantir a interoperabilidade com modelos regulatórios internacionais³⁴.

Além de abordagem regulatória flexível, o governo do Reino Unido também publicou um padrão de transparência algorítmica, acompanhado de um modelo e diretrizes para apoiar o setor público na adoção desse padrão. Essa iniciativa reflete o compromisso do Reino Unido em estabelecer práticas cla-

31. RÁDI, V. Gábor. *Comparative Analysis of the AI Regulation of the EU, US and China from a Privacy Perspective*. 2023 46th MIPRO ICT and Electronics Convention (MIPRO), Opatija, Croatia, 2023, p. 1446.

32. Nessa abordagem, a regulação é elaborada à medida que os estudos avançam, o setor amadurece e os riscos são identificados, permitindo uma adaptação mais eficaz em um campo que requer ciclos rápidos de iteração e desenvolvimento.

33. BRASIL. Tribunal de Contas da União. *Acórdão nº 616/2024*. Plenário. Relator: Ministro Aroldo Cedraz. Sessão de 03/04/2024. Brasília, TCU, 2024, p. 9. Disponível em: <https://pesquisa.apps.tcu.gov.br/redireciona/processo/3363820233>. Acesso em: 22 jul. 2024.

34. *Ibidem*, p. 9.

ras e responsáveis na utilização de sistemas baseados em algoritmos, visando aumentar a transparência e a responsabilidade no setor público³⁵.

Além do Reino Unido, diversos países estão adotando uma abordagem setorial para a regulação da inteligência artificial^{36,37}. Esses países visam integrar a regulamentação de IA aos sistemas legais existentes, garantindo que os princípios de responsabilidade e confiabilidade sejam cumpridos de maneira eficaz dentro das áreas específicas de atuação de suas respectivas autoridades³⁸.

2.2 Propostas de regulação estatal para a IA no Brasil

A trajetória da inteligência artificial no Brasil tem sido marcada por esforços estratégicos e legislativos significativos, refletindo a crescente importância desta tecnologia para o desenvolvimento nacional. A Estratégia Brasileira de Inteligência Artificial (EBIA), instituída pela Portaria MCTI nº 4.617/2021 e atualizada pela Portaria nº 4.979/2021, surge como um marco inicial importante³⁹. Desenvolvida com base nas diretrizes da OCDE, a EBIA visa promover o crescimento inclusivo, a transparência, e a segurança na implementação da IA no país⁴⁰. No entanto, a execução da EBIA tem enfrentado desafios, como a falta de um cronograma detalhado e a definição de responsabilidades claras, aspectos que têm sido criticados por analistas e especialistas da área⁴¹.

Os objetivos da EBIA incluem a promoção de investimentos em pesquisa e inovação, a formação de profissionais especializados, e a facilitação da cooperação entre setores públicos e privados. Apesar de seu papel fundamental, a estratégia tem sido alvo de críticas pela falta de um plano detalhado e pela ausência de uma autoridade reguladora dedicada à IA. A implementação tem sido lenta, exacerbada pela mudança de governo em 2023, e a revisão da es-

35. BELLI, Luca; CURZI, Yasmin; GASPAR, Walter B. *AI Regulation in Brazil: Advancements, flows, and need to learn from the data protection experience*. Computer Law & Security Review: The International Journal of Technology Law and Practice, v. 48, p. 4.

36. IAPP. IAPP Research and Insights, 2023. *International Definitions of Artificial Intelligence*. Disponível em: <https://iapp.org/resources/article/international-definitions-of-ai/>. Acesso em: 2 out. 2024.

37. WHITE & CASE. White & Case, 2024. *AI Watch: Global regulatory tracker*. Disponível em: <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker>. Acesso em: 31 jul. 2024.

38. DE OLIVEIRA, Thaís Figueira. Uma autoridade reguladora para a inteligência artificial no Brasil. 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. 766-767.

39. Informações sobre os avanços das tecnologias habilitadoras da IA, e que possibilitam análises sobre sua adoção e os seus principais impactos sobre a sociedade, podem ser obtidas no Observatório Brasileiro de Inteligência Artificial, acessível em: <https://obia.nic.br/s/home>.

40. BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. *Estratégia Brasileira de Inteligência Artificial – EBIA*. Brasília, MCTIC, 2021, p. 17. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ia_estrategia_diagramacao_4-979_2021.pdf. Acesso em: 26 jul. 2024.

41. DE OLIVEIRA, Thaís Figueira. Uma autoridade reguladora para a inteligência artificial no Brasil. 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. 759-760.

estratégia pode incorporar novos eixos e temas, como a cibersegurança e uma abordagem mais robusta para a segurança pública⁴².

No Congresso Nacional, o debate sobre a regulação da IA tem avançado por meio de diversos Projetos de Lei (PL). O PL nº 21, de 2020, aprovado pela Câmara dos Deputados e atualmente em tramitação no Senado, estabeleceu o marco inicial para a regulação da IA, mas foi criticado por seu caráter genérico e falta de profundidade. Este projeto buscou criar diretrizes básicas e princípios para a utilização de IA, mas não abordou de forma suficiente questões como privacidade, ética, e a criação de uma autoridade⁴³.

Esse projeto foi unificado a outros para tramitação conjunta. Com o intuito de elaborar um texto legislativo altamente técnico e avançado, foi criada uma Comissão de Juristas destinada a subsidiar a elaboração de minuta de substitutivo. Com base em todo o material analisado, a Comissão de Juristas apresentou seu relatório final, juntamente com um anteprojeto de lei para regulamentação da inteligência artificial. Nesse contexto, foi elaborado o Projeto de Lei nº 2.338, de 2023, que se fundamentou nas conclusões da referida Comissão e buscou conciliar, na legislação, a proteção dos direitos e liberdades fundamentais, a valorização do trabalho e da dignidade da pessoa humana, e a promoção da inovação tecnológica representada pela inteligência artificial⁴⁴.

O PL nº 2.338/2023 representou uma tentativa mais estruturada de regulamentar a inteligência artificial no Brasil, adotando uma abordagem baseada em riscos, similar à proposta da União Europeia, e estabelecendo medidas rigorosas para sistemas de alto risco. Ao dispor sobre a fiscalização da inteligência artificial, o projeto determinou que o Poder Executivo designasse autoridade para zelar pelo cumprimento das normas estabelecidas, sem definir se este órgão seria algum já existente na estrutura da Administração Pública Federal ou um novo órgão a ser posteriormente criado.

O substitutivo ao PL nº 2.338/2023, apresentado pelo Senador Eduardo Gomes em junho de 2024, reflete as recentes discussões sobre o tema da inteligência artificial, destacando a necessidade de uma governança multissetorial, enfatizando a transparência, a responsabilidade, e a proteção dos direitos

42. BRASIL. Tribunal de Contas da União. *Acórdão nº 616/2024*. Plenário. Relator: Ministro Aroldo Cedraz. Sessão de 03/04/2024. Brasília, TCU, 2024, p. 7. Disponível em: <https://pesquisa.apps.tcu.gov.br/redireciona/processo/3363820233>. Acesso em: 22 jul. 2024.

43. DE OLIVEIRA, Thaís Figueira. Uma autoridade reguladora para a inteligência artificial no Brasil. 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. 761.

44. BRASIL. Senado Federal. Projeto de Lei nº 2338, de 3 de maio de 2023. *Dispõe sobre o uso da Inteligência Artificial*. Brasília: Senado Federal, 2023. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 22 jul. 2024.

humanos. O texto prevê a criação de uma base de dados pública sobre IA de alto risco e a responsabilidade civil dos agentes de IA, bem como mecanismos de comunicação de incidentes e supervisão da conformidade. Esses aspectos demonstram um avanço em relação às propostas anteriores, buscando equilibrar a proteção dos direitos com a promoção da inovação. No que diz respeito à autoridade competente, o substitutivo ao PL nº 2.338/2023 prevê a designação de um sistema de fiscalização e supervisão que contempla:

- criação do Sistema Nacional de Regulação e Governança de Inteligência Artificial (SIA), que valoriza as competências regulatórias das autoridades setoriais;
- designação da Autoridade Nacional de Proteção de Dados (ANPD) como autoridade competente para coordenar o SIA, que também terá por missão reduzir a assimetria regulatória face aos diversos usos intensos de sistemas de IAs em setores não regulados.

3. Reflexões sobre a definição de uma autoridade competente para a regulação de inteligência artificial no Brasil

As autoridades reguladoras têm a finalidade de regular, organizar, controlar e fiscalizar assuntos específicos e podem variar em estrutura, abordagem, objetivos e escopo. Podem ser estabelecidas dentro da Administração Pública Direta ou Indireta, ou podem funcionar como entidades independentes ou organizações privadas com responsabilidades de interesse público⁴⁵. No exercício de uma reflexão sobre uma autoridade competente para a regulação de inteligência artificial no Brasil, a questão pode ser avaliada, fundamentalmente, sob as perspectivas de definição de um modelo de estrutura institucional a ser empregado e de um órgão a ser utilizado como autoridade central desse modelo.

Como exposto em seções anteriores, as propostas de uma autoridade competente para regular tecnologias digitais emergentes, a exemplo da IA, têm seguido três diferentes modelos: regulador específico do setor, regulador multissetorial e regulador convergente.

O modelo de regulador específico de inteligência artificial, empregado na Espanha, por exemplo, com a criação da *Agencia Española de Supervisión*

45. DE OLIVEIRA, Thaís Figueira. Uma autoridade reguladora para a inteligência artificial no Brasil. 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. 770.

de la Inteligencia Artificial (AESIA), tem como vantagem a possibilidade de desenho de uma autoridade com as características necessárias para enfrentar desafios éticos e de direitos humanos levantados pelo desenvolvimento, implantação e uso da IA. Há entendimentos de que, dada a complexidade do tema, uma autoridade regulatória precisaria integrar diversas *expertises* e conhecimentos multidisciplinares, inclusive jurídicos e técnicos, além de possuir uma capacidade regulatória e normativa abrangente⁴⁶. Por outro lado, a criação de um órgão com tamanha competência e características pode demandar um alto investimento por parte do Poder Público. Além disso, ainda não há suficientes informações sobre a efetividade de aplicação desse modelo em outras partes do mundo.

Por sua vez, o modelo de regulador multissetorial, empregado, por exemplo, na Jamaica (*Office of Utilities Regulation*, que supervisiona os setores de telecomunicações, energia, água e transporte), tem como vantagem o aproveitamento da estrutura institucional existente para a regulação de um novo setor, com sinergias administrativas e economias de escala na melhoria de processos. Contudo, no caso brasileiro, não há órgãos com essa característica habilitados à função de regular a IA, tendo em vista que os existentes, a exemplo do Conselho Administrativo de Defesa Econômica (CADE), tratam de aspectos muito específicos da regulação (no caso, a defesa da concorrência).

Já a criação ou fusão de autoridades existentes em um regulador convergente, englobando áreas conexas de TIC (como telecomunicações e proteção de dados), apresenta as mesmas vantagens do modelo anterior, com o benefício de aumento do grau de especialização, o que torna a autoridade mais apta a responder de maneira ágil e coordenada a desafios emergentes na área de inteligência artificial⁴⁷. Exemplo dessa abordagem é a China, com a Administração do Ciberespaço da China⁴⁸. No Brasil, tal abordagem é particularmente delicada em razão das necessárias intervenções do Poder Legislativo no Executivo⁴⁹.

46. DATA PRIVACY BRASIL. Data Privacy Brasil, 2023. *IA no Brasil: quem será responsável pela regulamentação?*. Disponível em: <https://www.dataprivacybr.org/documentos/ia-no-brasil-quem-sera-responsavel-pela-regulamentacao/?idProject=2331>. Acesso em: 2 out. 2024.

47. BRASIL. Autoridade Nacional de Proteção de Dados. *Nota Técnica nº 16/2023/CGTP/ANPD*. Brasília, ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf. Acesso em: 30 jul. 2024.

48. STANFORD UNIVERSITY. DigiChina, 2022. *Behind the Facade of China's Cyber Super-Regulator*. Disponível em <https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/>. Acesso em: 2 out. 2024.

49. Exemplo de controvérsia foi a edição da Lei Geral de Proteção de Dados Pessoais (LGPD), em que os dispositivos propostos pelo Legislativo e que tratavam da estruturação da Autoridade Nacional de Proteção de Dados (ANPD) foram vetados pelo Presidente da República, por incorrerem em alegada inconstitucionalidade do processo legislativo, por afronta ao artigo 61, § 1º, II, 'e', cumulado com o artigo 37, XIX da Constituição. Maiores informações sobre a reserva de iniciativa em: REZENDE, R. M. de. *A Insustentável Incerteza no Dever-Ser: reserva de iniciativa de leis, jurisprudência oscilante e a criação de fundos orçamentários*. Brasília: Núcleo de Estudos e Pesquisas/CONLEG/Senado, Abril/2017 (Texto para Discussão nº 231). Disponível em: <http://senado.leg.br/estudos>. Acesso em: 3 out. 2024.

Avaliando-se as vantagens e desvantagens desses três modelos, e considerando o ordenamento jurídico brasileiro e o contexto em que se insere, além da transdisciplinaridade e complexidade dos sistemas de IA, uma abordagem híbrida parece ser a mais adequada para sua regulamentação no Brasil, com a utilização de uma autoridade convergente como coordenador de um sistema regulatório, associada a agências reguladoras de setores específicos já existentes, a exemplo do que deve ser realizado na França com a Comissão Nacional de Informática e Liberdades (CNIL). Isso se justifica pelo fato de que as autoridades setoriais, com sua experiência e especialização, estão melhor posicionadas para lidar com questões relacionadas ao desenvolvimento e à aplicação de sistemas de IA em áreas como saúde, transportes e recursos naturais, por exemplo⁵⁰. Tal alternativa vai ao encontro do que fora proposto no substitutivo ao PL nº 2.338/2023, apresentado pelo Senador Eduardo Gomes e, atualmente, em discussão no Congresso Nacional.

Nessa perspectiva, a escolha do órgão regulador central recai, naturalmente, em uma das duas principais agências relacionadas à regulação de TIC no Brasil: a Agência Nacional de Telecomunicações (Anatel) e a Autoridade Nacional de Proteção de Dados (ANPD).

Criada pela Lei Geral de Telecomunicações (Lei nº 9.472, de 16 de julho de 1997), a Anatel foi a primeira agência reguladora a ser instalada no Brasil, em 5 de novembro de 1997. A Anatel 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.

Com sede em Brasília, a Anatel realiza as atividades de fiscalização e mantém contato mais próximo com a sociedade por meio de unidades em todas as capitais brasileiras. Seu quadro de pessoal, segundo informações de março de 2024⁵¹, totaliza 1.343 (mil trezentos e quarenta e três) servidores, dos quais 96,87% são de seus quadros próprios, 2,68% são requisitados de outros ór-

50. DE OLIVEIRA, Thaís Figueira. Uma autoridade reguladora para a inteligência artificial no Brasil. 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. 772.

51. BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. *Boletim da Administração Direta, Autárquica e Fundacional*. Brasília, MGI, 2024, p. 165. Disponível em: <https://www.gov.br/gestao/pt-br/central-de-conteudo/publicacoes/boletins/boletins-da-administracao-direta>. Acesso em: 30 jul. 2024.

gãos da administração pública e 0,45% não têm vínculo com o serviço público, ocupando cargos de livre nomeação e exoneração.

Por sua vez, a ANPD foi criada pela Medida Provisória nº 869, de 2018, convertida na Lei nº 13.853, de 8 de julho de 2019, que alterou a Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018), e passou a funcionar efetivamente com a nomeação de seu primeiro Diretor-Presidente, em 5 de novembro de 2020. A ANPD, a exemplo da Anatel, é uma autarquia de natureza especial vinculada ao Ministério da Justiça e Segurança Pública, possuindo, conseqüentemente, autonomia técnico-decisória e patrimônio próprio. A ANPD é o órgão central de interpretação da Lei Geral de Proteção de Dados, cabendo a ela estabelecer normas e diretrizes para a sua implementação, buscando zelar pela garantia do direito de todos os brasileiros terem seus dados pessoais devidamente protegidos.

Com sede em Brasília, mas sem unidades descentralizadas, a ANPD não possui quadro de servidores próprio. Para formar seu quadro de pessoal, contou com a requisição de 120 (cento e vinte) servidores de outros órgãos. Contando com o pessoal da limpeza, secretariado, recepção e estagiários, a agência tem ao todo 152 (cento e cinquenta e duas) pessoas, das quais apenas 10 (dez) trabalhando com fiscalização ou tratamento de incidentes de segurança, segundo informações de dezembro de 2023⁵².

Pelo exposto, tomando-se como referência as atuais competências da Anatel no que respeita às telecomunicações, entende-se que essa agência já possui experiência na realização de atividades semelhantes às que deverão ser realizadas pela autoridade competente de IA, a exemplo da acreditação, certificação e fiscalização⁵³. Em que pese uma aparente falta de sinergia entre os setores, o desenvolvimento das soluções e dos sistemas de inteligência artificial baseia-se em uma imensa massa de dados em constante fluxo, cujo acesso só é possível por meio de uma infraestrutura de conectividade robusta, estável, ampla e resiliente, composta por múltiplas redes de acesso e transporte de dados⁵⁴. Além disso, caso o PL nº 2.768, de 2022, venha a

52. CÂMARA DOS DEPUTADOS. Agência Câmara de Notícias, 2023. *Presidente da ANPD pede concurso para agência; divisão de fiscalização tem apenas 5 funcionários*. Disponível em: <https://www.camara.leg.br/noticias/1014383-presidente-da-anpd-pede-concurso-para-agencia-divisao-de-fiscalizacao-tem-apenas-5-funcionarios>. Acesso em: 31 jul. 2024.

53. BRASIL. Agência Nacional de Telecomunicações. *Informe nº 27/2024/ARI*. Brasília, Anatel, 2024. Disponível em: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46lzCFD-26Q9Xx5QNDbqbJNRZm5SUvRZmQf9kFzb6NVVMeEFdPgHerLaOe9k3Jw_0wiL8oZeTeLc2rSt0jscq85OhSwCRK5T4Bs-fXOKEQg. Acesso em: 30 jul. 2024.

54. BRASIL. Agência Nacional de Telecomunicações. *IA – Inteligência Artificial: Visão Institucional de Futuro*. Brasília, Anatel, 2024. Disponível em: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46lzCFD26Q9Xx5QNDbqYiHvsTCI8r6V00ltjrypit3yX4N4bkPXcoJgxuzJCUPSMamOo4UK2mN71rPT-Gc_Cr76yKk1yu0Ggxy4v3MR80F. Acesso em: 30 jul. 2024.

ser aprovado nos seus atuais termos, a Agência teria seu campo de atuação ampliado em relação às tecnologias digitais emergentes. Assim, o emprego dessa agência como órgão central da regulação da IA se mostra adequado, levando-se em conta sua estrutura consolidada, presença regional e quadro de pessoal.

Por outro lado, a ANPD já se destaca como uma entidade de referência na proteção de dados pessoais e na garantia da privacidade dos cidadãos. A IA, com suas capacidades de processamento e análise de grandes volumes de dados, está diretamente alinhada às competências da ANPD^{55, 56, 57}, fato reconhecido no substitutivo ao PL nº 2.338/2023⁵⁸. Essa interseção entre IA e proteção de dados centraliza a governança da IA nas questões técnicas e operacionais, com ênfase contínua na proteção dos direitos fundamentais e na segurança dos dados pessoais. Além disso, permite a formação de um corpo técnico especializado em ambas as áreas, otimizando a aplicação de recursos públicos e evitando a fragmentação regulatória e a sobreposição de competências entre diferentes órgãos⁵⁹. Contudo, por ser um órgão recente e em formação, e por não dispor de um quadro de pessoal próprio nem uma atuação descentralizada, as alterações em suas competências poderiam ter impactos em sua estrutura e orçamentos, o que se traduziria em comprometimento de seus resultados.

Considerações finais

Por meio deste estudo, foi possível compreender as especificidades da regulação de tecnologias digitais e os possíveis impactos de sua implementação, bem como entender as diferentes abordagens e estruturas regulatórias relativas à inteligência artificial.

Os estudos também possibilitaram um melhor entendimento da trajetória da inteligência artificial no Brasil, que reflete um esforço contínuo para alinhar

55. BRASIL. Autoridade Nacional de Proteção de Dados. *Análise preliminar do Projeto de Lei nº 2338/2023, que dispõe sobre o uso da Inteligência Artificial*. Brasília, ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anali-sepreliminar-do-pl-2338_2023-formatado-ascom.pdf. Acesso em: 3 out. 2024.

56. BRASIL. Autoridade Nacional de Proteção de Dados. *Nota Técnica nº 16/2023/CGTP/ANPD*. Brasília, ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf. Acesso em: 30 jul. 2024.

57. BRASIL. Autoridade Nacional de Proteção de Dados. *PL 2338 – SUBSTITUTIVO – COMISSÃO ESPECIAL CONTRIBUIÇÕES DA ANPD – MAIO - 2024*. Brasília, ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-apresenta-propostas-de-alteracao-do-substitutivo-ao-pl-2338-sobre-inteligencia-artificial/Versao_final_07.05.24_PL_2338_Substitutivo_Comissao_Especial_Propostas_ANPD1.pdf. Acesso em: 3 out. 2024.

58. BRASIL. Senado Federal. *Projeto de Lei nº 2338, de 3 de maio de 2023. Dispõe sobre o uso da Inteligência Artificial*. Brasília: Senado Federal, 2023. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 22 jul. 2024.

59. BRASIL. Autoridade Nacional de Proteção de Dados. *Nota Técnica nº 16/2023/CGTP/ANPD*. Brasília, ANPD, 2023. p. 6. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf. Acesso em: 30 jul. 2024.

o País com as melhores práticas internacionais, promovendo um desenvolvimento tecnológico responsável e inovador. Embora a EBIA e projetos de lei, como o PL nº 2.338/2023, representem avanços significativos, a implementação efetiva e a criação de estruturas regulatórias dedicadas serão fundamentais para garantir que o Brasil aproveite plenamente o potencial da IA. Isso deve ser feito ao mesmo tempo em que se deva proteger os direitos dos cidadãos e promover um ambiente de inovação seguro e ético.

Ainda assim, apesar das propostas avançadas, o Brasil enfrenta desafios na implementação eficaz dessas estratégias e regulamentações. A questão de criar uma autoridade reguladora especializada ou utilizar a estrutura regulatória existente permanece em aberto. Uma autoridade dedicada poderia desempenhar um papel crucial na aplicação e fiscalização das leis de IA, bem como na definição de melhores práticas e auditorias.

Independentemente do sistema de regulação escolhido e à luz do modelo de administração pública organizado na Constituição Federal de 1988, é essencial que a autoridade seja estabelecida como uma autarquia de natureza especial, com autonomia técnica e decisória, além de contar com patrimônio e pessoal próprios. A experiência com a implementação de agências reguladoras no Brasil indica que a autoridade regulatória de inteligência artificial deve incorporar, em seu processo decisório, práticas como consultas e audiências públicas, interação com as partes interessadas e adoção de mecanismos colaborativos e baseados em evidências. Além disso, a autoridade deve dispor de um órgão consultivo cuja principal função seja assegurar a participação ativa de diversos grupos e setores da sociedade nas decisões relacionadas à IA, tanto na formulação e execução de políticas públicas quanto na atuação da autoridade central.

Diante do exposto, sugere-se para futuras pesquisas a serem realizadas a avaliação da eficácia da EBIA na prática, analisando como tem sido aplicada e quais foram seus impactos até o momento, bem como a análise de políticas regulatórias em outras jurisdições, de modo a identificar fatores de sucesso ou fracasso e implicações para a regulação de inteligência artificial no Brasil.

Conforme inicialmente anunciado, constatou-se a complexidade da questão da inteligência artificial em nosso tempo. Evidenciou-se, também, a urgência e a inevitabilidade de enfrentamento do tema e a necessidade de definição de sua regulamentação para que a sociedade brasileira se coloque à altura dos desafios que a IA representa.

Referências

BELLI, Luca; CURZI, Yasmin; GASPAR, Walter B. *AI Regulation in Brazil: Advancements, flows, and need to learn from the data protection experience*. Computer Law & Security Review: The International Journal of Technology Law and Practice, v. 48, p. 105767, 2023. Disponível em: <https://doi.org/10.1016/j.clsr.2022.105767>. Acesso em: 23 jul. 2024.

BELLI, Luca; ZINGALES, Nicolo. *Data protection and artificial intelligence inequalities and regulations in Latin America*. Computer Law & Security Review: The International Journal of Technology Law and Practice, v. 47, p. 105761, 2022. Disponível em: <https://doi.org/10.1016/j.clsr.2022.105761>. Acesso em: 24 jul. 2024.

BRASIL. Agência Nacional de Telecomunicações. *Informe nº 27/2024/ARI*. Brasília, Anatel, 2024. Disponível em: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqbJNRZm5SUvRZ-mQf9kFzb6NVVMeEFdPgHerLaOe9k3Jw_0wiL8oZeTeLc2rSt0jscq85OhSwCRK5T4BsfXOKE-Qg. Acesso em: 30 jul. 2024.

BRASIL. Agência Nacional de Telecomunicações. *IA – Inteligência Artificial: Visão Institucional de Futuro*. Brasília, Anatel, 2024. Disponível em: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx-5QNDbqYiHvsTCI8r6V00ltjrypit3yX4N4bkPXcoJgxuzJCUPSMamOo4UK2mN71rPTGc-Cr76yKk1yu0Ggxy4v3MR80F. Acesso em: 30 jul. 2024.

BRASIL. Autoridade Nacional de Proteção de Dados. *Análise preliminar do Projeto de Lei nº 2338/2023, que dispõe sobre o uso da Inteligência Artificial*. Brasília, ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/analisepreliminar-do-pl-2338_2023-formatado-ascom.pdf. Acesso em: 3 out. 2024.

BRASIL. Autoridade Nacional de Proteção de Dados. *Nota Técnica nº 16/2023/CGTP/ANPD*. Brasília, ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf. Acesso em: 30 jul. 2024.

BRASIL. Autoridade Nacional de Proteção de Dados. *PL 2338 – SUBSTITUTIVO – COMISSÃO ESPECIAL CONTRIBUIÇÕES DA ANPD – MAIO – 2024*. Brasília, ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-apresenta-propostas-de-alteracao-do-substituto-ao-pl-2338-sobre-inteligencia-artificial/Versao_final_07.05.24_PL_2338_Substituto_Comissao_Especial_Propostas_ANPD1.pdf. Acesso em: 3 out. 2024.

BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. *Estratégia Brasileira de Inteligência Artificial – EBIA*. Brasília, MCTIC, 2021. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ia_estrategia_diagramacao_4-979_2021.pdf. Acesso em: 26 jul. 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. *Boletim da Administração Direta, Autárquica e Fundacional*. Brasília, MGI, 2024. Disponível em: <https://www.gov.br/gestao/pt-br/central-de-conteudo/publicacoes/boletins/boletins-da-administracao-direta>. Acesso em: 30 jul. 2024.

BRASIL. Senado Federal. *Projeto de Lei nº 2338, de 3 de maio de 2023. Dispõe sobre o uso da Inteligência Artificial*. Brasília: Senado Federal, 2023. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 22 jul. 2024.

BRASIL. Tribunal de Contas da União. *Acórdão nº 616/2024*. Plenário. Relator: Ministro Aroldo Cedraz. Sessão de 03/04/2024. Brasília, TCU, 2024. Disponível em: <https://pesquisa.apps.tcu.gov.br/redireciona/processo/3363820233>. Acesso em: 22 jul. 2024.

CÂMARA DOS DEPUTADOS. Agência Câmara de Notícias, 2023. *Presidente da ANPD pede concurso para agência; divisão de fiscalização tem apenas 5 funcionários*. Disponível em: <https://www.camara.leg.br/noticias/1014383-presidente-da-anpd-pede-concurso-para-agencia-divisao-de-fiscalizacao-tem-apenas-5-funcionarios>. Acesso em: 31 jul. 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.

DATA PRIVACY BRASIL. Data Privacy Brasil, 2023. *IA no Brasil: quem será responsável pela regulamentação?*. Disponível em: <https://www.dataprivacybr.org/documentos/ia-no-brasil-quem-sera-responsavel-pela-regulamentacao/?idProject=2331>. Acesso em: 2 out. 2024.

DELOITTE. Deloitte Insights, 2018. *The Future of Regulation: Principles for Regulating Emerging Technologies*. Disponível em: <https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation/regulating-emerging-technology.html>. Acesso em: 31 jul. 2024.

FRAZÃO, Ana; MULHOLLAND, Caitlin (Coord). *Inteligência artificial e direito: ética, regulação e responsabilidade*. 2. ed. rev. atual. e aum. São Paulo: Thomson Reuters Brasil, 2020. 736 p. ISBN 978-65-5614-221-0.

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

HARTMANN, Ivar A. (Coord). *Policy Paper: Regulação de Inteligência Artificial no Brasil*. Rio de Janeiro: FGV Direito Rio, 2020. 39 p. Disponível em: <https://diretorio.fgv.br/conhecimento/policy-paper-regulacao-de-inteligencia-artificial-no-brasil>. Acesso em: 1 out. 2024.

IAPP. IAPP Research and Insights, 2023. *International Definitions of Artificial Intelligence*. Disponível em: <https://iapp.org/resources/article/international-definitions-of-ai/>. Acesso em: 2 out. 2024.

KLARIĆ, Mirko. *Regulation of AI Technology Implementation in Public Administration*. 2024 47th MIPRO ICT and Electronics Convention (MIPRO), Opatija, Croatia, 2024, p. 1450-14564. Disponível em: <https://doi.org/10.1109/MIPRO60963.2024.10569836>. Acesso em: 24 jul. 2024.

LESSIG, Lawrence. *The Law of the Horse: What Cyber Law Might Teach*. Harvard Law Review, Harvard, v. 113, p. 501-546, dez. 1999. Disponível em: <https://cyber.harvard.edu/works/lessig/finalhls.pdf>. Acesso em: 1 out. 2024.

MELO, Ana Karolina Acris; SOUZA, Géssica Cardoso; VASCO, Amanda Corrêa; REIS, Bruno Salomon. *Regulação da Inteligência Artificial: benchmarking de países selecionados*. Brasília: Escola Nacional de Administração Pública, 2022. 35 p. Disponível em: <https://repositorio.enap.gov.br/handle/1/7419>. Acesso em: 1 out. 2024.

NAZARENO, Claudio. *Regulação da inteligência artificial: experiências internacionais e desafios para o Brasil*. Brasília: Câmara dos Deputados, Consultoria Legislativa, 2024. 32 p. Disponível em: <https://bd.camara.leg.br/bd/handle/bdcamara/41741>. Acesso em: 1 out. 2024.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA. *Consultation Paper on AI Regulation: Emerging Approaches Across the World*. Paris, 2024. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000390979>. Acesso em: 1 out. 2024.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. *Recommendation of the Council on Artificial Intelligence*. Paris, 2024. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. Acesso em: 26 jul. 2024.

PROENÇA, Jadir Dias; COSTA, Patrícia Vieira da; MONTAGNER, Paula (Coord). *Desafios da regulação no Brasil*. Brasília: ENAP, 2009. 342 p. ISBN 978-85-256-0062-2.

RÁDI, V. Gábor. *Comparative Analysis of the AI Regulation of the EU, US and China from a Privacy Perspective*. 2023 46th MIPRO ICT and Electronics Convention (MIPRO), Opatija, Croatia, 2023, p. 1446-1451. Disponível em: <https://doi.org/10.23919/MIPRO57284.2023.10159864>. Acesso em: 24 jul. 2024.

RAJAGOPAL, Manikandan; SIVASAKTHIVEL, Ramkumar; RAMAR, Gobinath; ANIFA, Mansurali; KARUPPASAMY, Sathesh Kumar. *A Conceptual Framework for AI Governance in Public Administration – A Smart Governance Perspective*. 2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Kirtipur, Nepal, 2023, p. 488-495. Disponível em: <https://doi.org/10.1109/I-SMAC58438.2023.10290366>. Acesso em: 24 jul. 2024.

REZENDE, R. M. de. *A Insustentável Incerteza no Dever-Ser: reserva de iniciativa de leis, jurisprudência oscilante e a criação de fundos orçamentários*. Brasília: Núcleo de Estudos e Pesquisas/CONLEG/Senado, Abril/2017 (Texto para Discussão nº 231. Disponível em: www.senado.leg.br/estudos. Acesso em: 3 out. 2024.

ROQUETE, Felipe Leitão Valadares. *Inteligência artificial, valores e incerteza: um problema insolúvel para a regulação?*. Revista Internet & Sociedade, v. 2, n. 2, p. 150-154, dez. 2021. Disponível em: <https://revista.internetlab.org.br/wp-content/uploads/2022/03/Inteligencia-artificial-valores-e-incerteza-um-problema-insolavel-para-a-regulacao.pdf>. Acesso em: 1 out. 2024.

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).

STANFORD UNIVERSITY. DigiChina, 2022. *Behind the Facade of China's Cyber Super-Regulator*. Disponível em <https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/>. Acesso em: 2 out. 2024.

THE ECONOMIST. The Economist, 2023. *The world wants to regulate AI, but does not quite know how*. Disponível em: <https://www.economist.com/business/2023/10/24/the-world-wants-to-regulate-ai-but-does-not-quite-know-how>. Acesso em: 31 jul. 2024.

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES; BANCO MUNDIAL. *Digital Regulation Handbook*. Genebra, 2020. Disponível em: <http://handle.itu.int/11.1002/pub/81630556-en>. Acesso em: 22 jul. 2024.

WEBER, Rolf. Artificial Intelligence: A Theoretical Analysis of Regulatory Models. In: BELLI, Luca; GASPAR, Walter B. (Coord). *The Quest for AI Sovereignty, Transparency and Accountability: Official Outcome of the UN IGF Data and Artificial Intelligence Governance Coalition*. Rio de Janeiro: FGV Direito Rio, 2023. p. 71-83.

WHITE & CASE. White & Case, 2024. *AI Watch: Global regulatory tracker*. Disponível em: <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker>. Acesso em: 31 jul. 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

2

**Inteligência Artificial e
Proteção de Dados Pessoais:
reflexões sobre a base legal
adequada para fundamentar
o treinamento via web
scraping**

MATHEUS MANTUANI

Sumário: Introdução. 1. Raspagem de Informações *Online* em Tempos de *Big Data*. 2. Compatibilização da Proteção de Dados com o *Web Scraping*. 3. Em Busca da Hipótese Legal Aplicável ao Treinamento de IA. Considerações Finais. Referências.

Introdução

Em 1956, dez cientistas se reuniram na Faculdade de Dartmouth, em New Hampshire, Estados Unidos, para a realização de um estudo sobre inteligência artificial (“IA”), o qual partia da hipótese de que aspectos de aprendizagem e outras características da mente humana poderiam, a princípio, ser precisamente descritos de modo que uma máquina fosse capaz de simulá-los.²

Passados quase setenta anos da inauguração de tal campo de pesquisa, nota-se como sistemas de IA³ prosseguiram historicamente de acordo com esse ideal de usos probabilísticos baseados em informações, a fim de chegar-se a determinados resultados,⁴ cada vez mais complexos.⁵ Isso porque a área da computação definiu por pressuposto aqueles sistemas como máquinas que manipulavam números, de sorte que tudo poderia ser codificado matematicamente,⁶ por meio de algoritmos – operações que ofereciam um caminho para as máquinas processarem dados e automatizarem decisões.⁷

1. Advogado. Pós-Graduando em Direito Digital pela UERJ. Graduado em Direito pela UERJ. Atua na área de tecnologia e propriedade intelectual em Rennó Penteado Sampaio Advogados, desde 2021. Atuou como Editor Técnico e Coordenador da Revista da Faculdade de Direito da UERJ. Estagiou no Tribunal de Justiça do Estado do Rio de Janeiro e na Defensoria Pública do Estado do Rio de Janeiro. Foi Diretor do Centro Acadêmico Luiz Carpenter e Representante Discente no Conselho Departamental, Departamento de Direito do Estado e Departamento de Teorias e Fundamentos do Direito da Faculdade de Direito da UERJ. Atuou como pesquisador e monitor bolsista na UERJ. Autor de artigos publicados em periódicos científicos e em capítulos de livros.

2. MCCARTHY, John *et alii*. *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*. EUA, New Hampshire: Dartmouth College, 1955.

3. O conceito exato de sistema de IA permanece em disputa, mas para os fins da presente pesquisa será adotada a noção prevista no Regulamento da Inteligência Artificial, recentemente aprovado na União Europeia: “um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais”. UE. *Artificial Intelligence Act. Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence*. União Europeia: Parlamento Europeu, 2024, artigo 3.º, n.º 1.

4. BOSTROM, Nick. *Superinteligência: caminhos, perigos e estratégias para um novo mundo*. Tradução: Aurélio Monteiro, Clemente Penna, Fabiana Monteiro e Patrícia Geremias. Rio de Janeiro: Darkside, 2018.

5. BARROSO, Luís Roberto; MELLO, Patrícia Perrone Campos. *Inteligência artificial: promessas, riscos e regulação. Algo de novo debaixo do sol*. Revista Direito e Práxis. Rio de Janeiro, 2024. No prelo.

6. NEWELL, Allen. *Intellectual Issues in the History of Artificial Intelligence*. IN: MACHLUP, Fritz; MANSFIELD, Una (Eds.). *The Study of Information: interdisciplinary messages*. EUA, Nova Iorque: Wiley, 1983, pp. 187-294.

7. BAROCAS, Solon; SELBST, Andrew. *Big Data's Disparate Impact*. California Law Review. EUA, Califórnia, v. 104, n. 3, pp. 671-732, jun., 2016.

Dentre as informações que poderiam ser utilizadas para treinar e desenvolver os sistemas de IA, os dados pessoais⁸ disponíveis na Internet⁹ têm ganhado especial atenção em um cenário de *Big Data*, termo empregado para descrever o “combustível” que faria as máquinas funcionarem,¹⁰ a matéria-prima necessária para o processamento dos sistemas.¹¹ Como salienta Gustavo Tepedino, “a cada dia uma infinidade de dados é extraída, de forma incalculável, por agentes econômicos”,¹² conjuntura a qual permite que as máquinas se tornem mais “inteligentes” – no sentido de aprenderem e melhorarem os seus sistemas com base nos dados pessoais coletados.¹³

Uma das técnicas comumente utilizadas nesses contextos é a raspagem de dados (*data scraping*) – extração automatizada que visa coletar grandes quantidades de informações para a sua estruturação em um banco de dados,¹⁴ com o intuito de garantir-se análises e usos posteriores.¹⁵ Todavia, a raspagem de informações na Internet (*web scraping*) sofre críticas orientadas por uma perspectiva de proteção de dados pessoais,¹⁶ tendo em vista que legislações específicas na matéria tendem a impor restrições à coleta e ao tratamento¹⁷

8. Dado pessoal pode ser definido, à luz do artigo 5º, I, da Lei Geral de Proteção de Dados Pessoais (Lei Federal n.º 13.709/2018), como a informação relacionada à pessoa natural identificada ou identificável. BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)*. Brasília: Congresso Nacional, 2018.

9. Internet é definida pelo artigo 5º, I, do Marco Civil da Internet (“MCI”), como o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes. *Idem. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil*. Brasília: Congresso Nacional, 2014.

10. “O Big Data é fundamental para o uso e o desenvolvimento de algoritmos e inteligência artificial (‘IA’). Os algoritmos e a IA são as máquinas; o Big Data é o combustível que faz as máquinas funcionarem. Assim como o petróleo fazia as máquinas e fábricas funcionarem na Era Industrial, o Big Data faz as máquinas relevantes funcionarem na Sociedade Algorítmica.” [Tradução nossa]. BALKIN, Jack. *Free Speech in the Algorithmic Society: big data, private governance, and new school speech regulation*. University of California, Davis, Law Review. EUA, Califórnia, v. 51, n. 615, pp. 1.149-1.210, set., 2017, p. 1.154.

11. ZUBOFF, Shoshana. *A Era do Capitalismo de Vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução: George Schlesinger. São Paulo: Intrínseca, 2019.

12. TEPEDINO, Gustavo. *As tecnologias e a renovação do Direito Civil*. OAB/RJ, Rio de Janeiro, 12 de junho de 2019.

13. SURBLYTÈ, Gintarè. *Data as a Digital Resource*. Max Planck Institute for Innovation & Competition Research Paper n. 16-12. Alemanha, Baviera, out., 2016, p. 29

14. Banco de dados, de acordo com o artigo 5º, IV, da Lei Geral de Proteção de Dados Pessoais, refere-se ao conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico. BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018, locus citatum*.

15. AARONSON, Susan Ariel. *Data Dysphoria: the governance challenge posed by Large Language Models*. Institute for International Economic Policy Working Paper n. 2023-07. EUA, Washington, DC., ago., 2023.

16. Recentemente, a Autoridade Nacional de Proteção de Dados brasileira (“ANPD”) determinou a suspensão cautelar do tratamento de dados pessoais para treinamento da IA da empresa Meta Platforms, Inc., por considerar ilegal, em um juízo de verossimilhança, a “ampla, geral e indiscriminada coleta de todas as informações disponíveis e compartilhadas por usuários nas plataformas” daquela empresa. BRASIL. *Voto n.º 11/2024/DIR-MW/CD*. Brasília: Autoridade Nacional de Proteção de Dados, 2024, p. 11.

17. Na legislação brasileira, consoante artigo 5º, X, da Lei Geral de Proteção de Dados Pessoais, o termo técnico tratamento engloba toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. *Idem. Lei n.º 13.709, de 14 de agosto de 2018, locus citatum*.

posterior desses dados disponíveis *online*,¹⁸ como se observa nas atividades voltadas ao treinamento de sistemas de IA.

Nessa linha, a presente pesquisa tem por objetivo central identificar em que medida a Lei Geral de Proteção de Dados Pessoais do Brasil (Lei Federal n.º 13.709/2018, “LGPD”) limita o *web scraping* para fins de treinamento de sistemas de IA, por força da necessidade de fundamentar a coleta de informações *online* em uma das hipóteses previstas na legislação – as chamadas bases legais. A partir de pesquisas de bibliografia e da revisão direta em fontes da literatura especializada, os capítulos do artigo apresentam a ascensão do *scraping* na Internet e no contexto de *Big Data*, o seu entrelaço com a legislação de proteção de dados pessoais e os desafios de identificar-se uma hipótese legal que permita o treinamento de IA via raspagem *online*. Em considerações finais, observa-se o papel substancial da Autoridade Nacional de Proteção de Dados brasileira (“ANPD”),¹⁹ enquanto intérprete da LGPD, no balanceamento entre a proteção dos interesses e direitos fundamentais dos titulares, e no privilégio ao desenvolvimento tecnológico do país, em igual atenção ao princípio da liberdade dos modelos de negócios promovidos na Internet.

1. Raspagem de Informações Online em Tempos de Big Data

O *web scraping* costuma facilitar processos analíticos por meio de IA, a partir de uma linguagem de códigos,²⁰ por meio de etapas-chave, as quais envolvem, por exemplo, a inserção de informações e do URL (“Uniform Resource Locator”), termo que compreende a “indicação específica” de uma página na Internet,²¹ no *script* (roteiro) da raspagem, para que se extraiam os dados e conteúdos solicitados pelo programador, ato que ocorre geralmente por meio de planilhas ou arquivos de texto.²²

Essa espécie de mineração de dados constitui um pressuposto para o modelo de negócios de variadas empresas de tecnologia. A coleta de informações disponíveis *online* configura, na contemporaneidade, a estruturação necessá-

18. Um exemplo de limitação do *web scraping* é o artigo 7º, § 7º, da Lei Geral de Proteção de Dados Pessoais, de acordo com o qual o tratamento posterior de dados pessoais públicos ou tornados manifestamente públicos pelo titular poderá ser realizado para novas finalidades, apenas se observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos naquela Lei. *Ibidem*.

19. A ANPD é, à luz do artigo 5º, XIX, da LGPD, o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei em todo o território nacional. *Ibidem*.

20. A linguagem de programação Python é um exemplo de facilitador nesses processos. Confira-se ASHRAF, Rasha. *Scraping EDGAR with Python*. Journal of Education for Business. Reino Unido, Londres, v. 92, n. 4, pp. 179-185, mai., 2017.

21. SOUZA, Carlos Affonso; LEMOS, Ronaldo. *Marco Civil da Internet: construção e aplicação*. Juiz de Fora: Editar, 2016, p. 125.

22. TALIAFERRO, Jocelyn; HEDADJI, Fatima; DULING, Emma. *Web Scraping as a Data Collection Strategy: the perils and pitfalls*. Social Sciences & Humanities Open. Holanda, Amsterdã. No prelo.

ria para a criação e agregação de valor, extraído a partir da raspagem: a prática já foi utilizada, a título de exemplo, para o monitoramento de preços de concorrentes e para a integração e comparação de preços de produtos, o que fortaleceu a judicialização na área e a contestação dessas operações.²³ Há notícia, inclusive, do emprego da raspagem de dados na Internet para atividades de *spam*, golpes cibernéticos, fraudes, ataques de negação de serviço, vendas de imagens faciais a órgãos de segurança pública e manipulação de eleições.²⁴

Ao mesmo tempo, o *scraping* de informações em larga escala na Internet tornou-se igualmente fundamental para o treinamento de certos modelos de IA, como a inteligência artificial generativa²⁵ ou sistemas de propósito geral.²⁶ Fala-se aqui, aliás, não apenas do *web scraping* de dados pessoais, mas também do conteúdo de livros,²⁷ notícias e artigos jornalísticos –quadro que evoca discussões e impedimentos adicionais relacionados a direitos autorais e direitos conexos.²⁸ A raspagem se torna, portanto, um método “conveniente”, embora criticado, para a obtenção de matérias-primas para o desenvolvimento dos sistemas de IA.²⁹

A construção de obstáculos via propriedade intelectual para o treinamento desses modelos pode corresponder a um desafio relevante aos desenvolvedores de sistemas.³⁰ Afinal, o modelo de negócios que tem prevalecido com o *web scraping* é o da alimentação da IA com quantidades consideráveis de informação, facilitada por progressos tecnológicos recentes, a fim de que os modelos fundamentem e formem os seus padrões de decisão apoiados nos

23. Para uma análise de casos judiciais que envolveram empresas como Amazon, Walmart, eBay, LinkedIn, Ticketmaster e Southwest Airlines, confira-se GOODYEAR, Michael. *Circumscribing the Spider: Trademark Law and the edge of data scraping*. Kansas Law Review. EUA, Kansas, v. 70, n. 2, pp. 295-328, dez., 2021.

24. PARKS, Andrew. *Unfair Collection: reclaiming control of publicly available personal information from internet data scrapers*. Michigan Law Review. EUA, Michigan, v. 120, n. 5, pp. 913-945, mar., 2022.

25. A IA generativa foi definida, no artigo 4º, IV, da última versão do Projeto de Lei brasileiro n.º 2.338, de 2023, como um modelo de IA especificamente destinado a gerar ou modificar significativamente, com diferentes graus de autonomia, textos, imagens, áudios, vídeos ou códigos de *software*. BRASIL. *Projeto de Lei n.º 2.338, de 2023. Dispõe sobre o desenvolvimento, fomento, uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana*. Brasília: Congresso Nacional, 2024.

26. O Regulamento da Inteligência Artificial europeu define sistemas de propósito geral como modelos de IA, inclusive treinados com uma grande quantidade de dados a partir de autossupervisão em escala, que apresentam uma generalidade significativa e são capazes de executar de forma competente uma vasta gama de tarefas distintas, independentemente da forma como são colocados no mercado, e que podem ser integrados em uma variedade de sistemas ou aplicações, com exceção de modelos utilizados como protótipos antes da circulação no mercado. UE. *Artificial Intelligence Act, locus citatum*, artigo 3.º, n.º 63.

27. O GLOBO. *Escritores Processam OpenAI por Uso de Obras para Treinar ChatGPT sem Autorização*. O Globo, Rio de Janeiro, 20 de jul. de 2023.

28. GRYNBAUM, Michael; MAC, Ryan. *The Times Sues OpenAI and Microsoft Over A.I. Use of Copyrighted Work*. The New York Times. EUA, Nova Iorque, 27 de dez. de 2023.

29. AMARIKWA, Melany. *Internet Openness at Risk: generative AI's impact on data scraping*. Richmond Journal of Law & Technology. EUA, Virgínia, v. 30, n. 3, pp. 533-589, mai., 2024, p. 538.

30. DELACROIX, Sylvie. *Sustainable Data Rivers? Critical AI*. EUA, Carolina do Norte, 2024. No prelo.

dados acessados, motivo pelo qual se afirma que “qualquer algoritmo só é tão bom quanto os dados que lhe servem como base”.³¹

Para além de uma preocupação com direitos autorais, todavia, o treinamento de sistemas de IA procede com frequência da coleta de dados pessoais em larga escala na Internet,³² o que inaugura um debate e análise complementares, com restrições próprias à raspagem em território nacional, visto que a LGPD assegura a toda pessoa natural a titularidade de seus dados pessoais e a garantia dos direitos fundamentais de liberdade, de intimidade e de privacidade.³³

2. Compatibilização da Proteção de Dados com o Web Scraping

A proteção de dados pessoais tem sido descrita, há anos, como um direito fundamental,³⁴ antes mesmo de sua inclusão expressa na Constituição.³⁵ Buscava-se, com tal definição, um equilíbrio face a outros direitos afins – como à privacidade, à informação e à transparência –, além de uma definição que concomitantemente privilegiasse uma inserção dos dados pessoais no mercado, sem que essas informações fossem atreladas a meros bens jurídicos de propriedade de seus titulares.³⁶⁻³⁷ É certo que os dados pessoais podem ser convertidos em informações valiosas para atividades econômicas, de modo que seria razoável considerar o advento da LGPD como um reforço à autode-

31. DONEDA, Danilo *et alia*. *Considerações Iniciais sobre Inteligência Artificial, Ética e Autonomia Pessoal*. Pensar. Fortaleza, v. 23, n. 4, pp. 1-17, out./dez., 2018, p. 5.

32. A literatura argumenta que embora dados pessoais sejam tornados públicos pelo titular *online*, deve haver uma razoabilidade na coleta e no tratamento dessas informações. Confira-se PARKS, Andrew. *Unfair Collection: reclaiming control of publicly available personal information from internet data scrapers*, *locus citatum*.

33. BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018, locus citatum*, artigo 17. Para uma análise crítica do artigo 17 da LGPD, confira-se FRAZÃO, Ana. *Direitos Básicos dos Titulares de Dados Pessoais*. Revista do Advogado, v. 39, n. 144, pp. 33-46, nov., 2019.

34. “No qualitativo *fundamentais* acha-se a indicação de que se trata de situações jurídicas sem as quais a pessoa humana não se realiza, não convive e, às vezes, nem mesmo sobrevive”. SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. São Paulo: Malheiros, 2005, p. 178.

35. BRASIL. Emenda Constitucional n.º 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília: Congresso Nacional, 2022.

36. Titular é a pessoa natural a quem se referem os dados pessoais, consoante artigo 5º, V, da LGPD. *Idem*. *Lei n.º 13.709, de 14 de agosto de 2018, locus citatum*. Quanto ao termo adotado pela legislação, importa acentuar que o “uso do termo ‘titular’, embora criticado por parte da doutrina (que identifica na referência à titularidade uma remissão à ótica proprietária, de todo inadequada em matérias que dizem respeito diretamente à pessoa humana), parece ainda oportuno, tendo em vista a necessidade de identificar com clareza os sujeitos a que se refere a lei.” SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. *Tutela da Pessoa Humana na Lei Geral de Proteção de Dados Pessoais: entre a atribuição de direitos e a enunciação de remédios*. Pensar. Fortaleza, v. 24, n. 3, pp. 1-22, jul./set., 2019, p. 8.

37. DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais: elementos da formação da Lei Geral de Proteção de Dados*. São Paulo: Thomson Reuters, 2020.

terminação informativa³⁸ e um contraponto ao “varejo”³⁹ de dados autorregulado pelos agentes de tratamento em si.⁴⁰

Assim, a legislação de proteção de dados pessoais brasileira estabelece um ambiente de proatividade,⁴¹ para que os controladores⁴² “intensifiquem os cuidados no desenvolver de suas atividades.”⁴³ Os modelos de negócio na Internet que envolvem o tratamento de dados pessoais e IA precisam, por conseguinte, conciliar-se junto às disposições legais da LGPD,⁴⁴ em um compasso criativo que inclua também, por parte do Estado regulador, a garantia da liberdade de iniciativa para as atividades econômicas desenvolvidas *online*.⁴⁵⁻⁴⁶ Essa não é uma tarefa trivial e Carlos Affonso Souza registra um dos tantos percalços relativos ao equilíbrio entre proteção de dados e desenvolvimento de sistemas de IA:

A LGPD diz que todos os titulares de dados têm direito a solicitar a retificação e o apagamento de seus dados pessoais detidos por uma empresa.[⁴⁷] Mas o que acontece quando esse dado pessoal já foi usado para treinar um modelo que alicerça um sistema de IA generativa? Uma vez treinado o modelo, a empresa pode até apagar o dado pessoal arquivado em seus sistemas, mas o resultado desse treinamento pode aparecer na forma pela qual o modelo é utilizado nas mais diferentes aplicações. Não existem, até o momento, formas viáveis de se destreinar um modelo sem implicar em custos, gasto de energia e mão de obra desproporcionais.⁴⁸

38. A autodeterminação informativa pode ser descrita como um “direito de manter o controle sobre as próprias informações”. RODOTÀ, Stefano. *A Vida na Sociedade de Vigilância: a privacidade hoje*. Tradução: Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008, p. 92.

39. BIONI, Bruno. *Proteção de Dados Pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019, p. 48.

40. FRAZÃO, Ana. *Fundamentos da Proteção de Dados Pessoais – noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters, 2023, pp. 21-50.

41. MORAES, Maria Celina Bodin de. *LGPD: um novo regime de responsabilização civil dito proativo*. *Civilistica.com*. Rio de Janeiro, v. 8, n. 3, pp. 1-6, dez., 2019.

42. O controlador é, na acepção do artigo 5º, VI, da LGPD, a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018, locus citatum*.

43. MONTEIRO FILHO, Carlos Edison do Rêgo. *Tutela dos Dados Pessoais e sua Efetividade no Ordenamento Jurídico Brasileiro: direito de acesso, reparação e prevenção de danos*. *Revista de Direito da Responsabilidade*. Portugal, Coimbra, v. 3, pp. 298-315, mar., 2021, p. 314.

44. TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. *A Utilização Econômica de Rastreadores e Identificadores On-Line de Dados Pessoais*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters, 2023, pp. 585-604.

45. Destaca-se que a disciplina do uso da Internet no Brasil abrange um equilíbrio principiológico entre, *exempli gratia*, a proteção dos dados pessoais e a liberdade dos modelos de negócios promovidos na Internet. BRASIL. *Lei n.º 12.965, de 23 de abril de 2014, locus citatum*, artigo 3º, III e VIII.

46. Parcela da literatura afirma, *exempli gratia*, que “não se admite presunção de que uma determinada maneira ou modelo para a exploração de uma área da atividade econômica na Internet é vedada.” SOUZA, Carlos Affonso; LEMOS, Ronaldo. *Marco Civil da Internet: construção e aplicação, locus citatum*, p. 48.

47. O artigo 18, III e IV, da LGPD, prevê como direitos do titular dos dados pessoais a requisição da correção de dados incompletos, inexatos ou desatualizados, bem como da anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na legislação. BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018, locus citatum*.

48. SOUZA, Carlos Affonso. *Meta x ANPD: separar espaços da IA e dos dados pessoais não será nada fácil*. *Universo Online*, São Paulo, 04 de jul. de 2024.

Somado a isso, um dos princípios previstos na LGPD com impacto direto no treinamento de sistemas de IA é o da transparência:⁴⁹ a garantia de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento.⁵⁰ Logo, a despeito da importância econômica do uso automatizado de dados pessoais,⁵¹ é inviável que os controladores simplesmente não indiquem aos titulares informações a respeito do desenvolvimento dessas atividades.⁵²

Porém, a complexidade das associações e correlações operadas no decorrer da alimentação da IA, as quais podem tornar-se até mesmo inesperadas,⁵³ traduz um outro desafio no sentido de como apontar atividades inicialmente desconhecidas ou mal compreendidas pelos próprios controladores.⁵⁴⁻⁵⁵ Tal cenário enseja riscos para potenciais violações adicionais aos princípios da finalidade⁵⁶ e da adequação.⁵⁷ Conseqüentemente, o criticado mistério⁵⁸ do funcionamento das operações tem aberto o caminho para debates sobre auditorias algorítmicas que objetivem desvendar decisões equivocadas ou imprecisas, discriminações ilícitas ou abusivas e da-

49. Presente igualmente na legislação europeia, a autoridade espanhola de proteção de dados (“AEPD”) orienta que a transparência deve permitir aos titulares ciência do impacto associado ao uso de soluções de IA, de modo que o controlador teria de apresentar informações acerca da eficiência, recursos e limitações dos sistemas. Isso inclui, aliás, indicação específica ao titular se o uso de seus dados pessoais para o treinamento da IA possibilitará sua reidentificação posterior pelos modelos desenvolvidos. ESPANHA. *Adecuación al RGPD de Tratamientos que Incorporan Inteligencia Artificial – una introducción*. Espanha, Madri: Agencia Española de Protección de Datos, 2020.

50. BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018, locus citatum*, artigo 6º, VI.

51. Vale ressaltar que “o processamento de informações e dados por meio de algoritmos pode ser um meio de simplificar decisões econômicas, aumentar a eficiência e personalizar a produção, bem como ampliar as possibilidades de monetização de serviços digitais a partir da personalização do conteúdo e do marketing digital.” DONEDA, Danilo *et alia*. *Considerações Iniciais sobre Inteligência Artificial, Ética e Autonomia Pessoal, locus citatum*, p. 4.

52. Afinal, sem mencionada transparência o titular não poderia requerer os direitos previstos na LGPD ao controlador, uma vez que nem ao menos saberia da existência do tratamento de seus dados pessoais. Parte da literatura, contudo, acredita que a confiança na transparência e em um modelo de autodeterminação informativa em matéria de IA seria insuficiente para a contenção de danos relativos a sistemas que representam riscos à pessoa humana. Confira-se SOLOVE, Daniel; HARTZOG, Woodrow. *Kafka in the Age of AI and the Futility of Privacy as Control*. Boston University Law Review. EUA, Massachusetts, v. 104, n. 4, pp. 1.021-1.042, mai., 2024.

53. SOUZA, Carlos Affonso; PERRONE, Christian; MAGRANI, Eduardo. *O Direito à Explicação entre a Experiência e a sua Positivização na LGPD*. IN: MENDES, Laura Schertel *et alii* (Coords.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021, pp. 243-270.

54. A LGPD obriga, *exempli gratia*, que o agente de tratamento apresente informação a respeito da finalidade específica da atividade com dados pessoais. Caso o consentimento seja a base legal aplicável, aliás, será possível revogá-lo, na hipótese de o titular discordar da nova finalidade. BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018, locus citatum*, artigo 9º, I e § 2º.

55. “Essa complexidade evidencia ainda mais as limitações dos atuais direitos de privacidade na abordagem de implicações mais amplas relacionadas ao uso de dados e à tomada de decisões com base em algoritmos. Até mesmo os especialistas têm dificuldade para entender por que os algoritmos geram determinados resultados.” [Tradução nossa]. SOLOVE, Daniel. *Artificial Intelligence and Privacy*. Florida Law Review. EUA, Flórida, v. 77, n. 1, jan., 2025. No prelo.

56. “[R]ealização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”. BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018, opere citato*, artigo 6º, I.

57. “[C]ompatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento”. *Ibidem*, artigo 6º, II.

58. PASQUALE, Frank. *The Black Box Society: the secret algorithms that control money and information*. EUA, Massachusetts: Harvard University Press, 2015.

nos ao titular.⁵⁹⁻⁶⁰ Por outro lado, a noção de uma definição prévia dos propósitos do tratamento foi descrita como uma “ideia antiga” e que poderia opor-se ao potencial de os sistemas de IA identificarem novas finalidades, inclusive benéficas aos titulares.⁶¹

As técnicas de raspagem, empregadas por desenvolvedores para a coleta de informações na Internet, ademais, provam-se um outro componente na discussão do limiar entre IA e proteção de dados pessoais: para alguns, o fato de informações dos titulares encontrarem-se publicamente disponíveis *online* não deve configurar uma “brecha” para a condução da coleta, do uso compartilhado e demais atividades de tratamento sem a devida transparência e para propósitos meramente comerciais.⁶² Ao contrário, a ausência de informações específicas, concisas, compreensíveis e facilmente acessíveis⁶³ sobre o *scraping* tem como resultado o impedimento de o titular exercer seus direitos de oposição à operação.⁶⁴

Assim, o Comitê Europeu para a Proteção de Dados (“EDPB”) indica que a raspagem de informações apresenta riscos peculiares para os direitos e para as liberdades fundamentais das pessoas naturais,⁶⁵ e a Autoridade Europeia para a Proteção de Dados (“EDPS”) argumenta que o *web scraping* voltado para fins de treinamento de IA pode estar em desconformidade com os princípios de proteção de dados pessoais.⁶⁶

Contudo, uma potencial incompatibilidade não significa que a raspagem deva passar por uma “proibição categórica”, dificultando o treinamento da IA,

59. MITTELSTADT, Brent *et alia*. *The Ethics of Algorithms: mapping the debate*. Big Data & Society. EUA, Califórnia, v. 3, n. 2, jul./dez., 2016.

60. A LGPD, inclusive, prevê que a ANPD poderá realizar auditoria para a verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais, observado o segredo comercial e industrial, caso o controlador não forneça – quando solicitado – informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para determinada decisão automatizada. BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018, locus citatum*, artigo 20, § 2º. Para uma compreensão pormenorizada do significado de tratamento automatizado de dados pessoais, confira-se VERONESE, Alexandre. *Os Direitos de Explicação e de Oposição diante das Decisões Totalmente Automatizadas: comparando o RGPD da União Europeia com a LGPD brasileira*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters, 2023, pp. 377-408.

61. HILDEBRANDT, Mireille. *Esclavos de los macrodatos. ¿O no?* Revista de Internet, Derecho y Política. Espanha, Barcelona, v. 17, pp. 7-44, nov., 2013, p. 19.

62. PARKS, Andrew. *Unfair Collection: reclaiming control of publicly available personal information from internet data scrapers, locus citatum*, p. 922.

63. Orientações da autoridade francesa de proteção de dados (“CNIL”). FRANÇA. *La Réutilisation des Données Publiquement Accessibles En Ligne à des Fins de Démarchage Commercial*. França, Paris: Commission Nationale de l’Informatique et des Libertés, 2020.

64. A autoridade de proteção de dados polonesa (“UODO”) aplicou esse entendimento ao multar a empresa Bisnode por não informar diretamente os titulares acerca de suas práticas de raspagem de dados. Sob o argumento de que a notificação pessoa a pessoa envolveria “esforços desproporcionais”, o agente de tratamento havia apenas mencionado a operação em sua política de privacidade – o que foi considerado insuficiente pelo regulador no caso concreto. POLÔNIA. *NSA Przyznał Rację UODO ws. Decyzji dotyczącej Pierwszej Kary Nałożonej przez Organ Nadzorczy*. Polônia, Varsóvia: Urząd Ochrony Danych Osobowych, 2023.

65. UE. *Report of the work undertaken by the ChatGPT Taskforce*. União Europeia: European Data Protection Board, 2024.

66. *Idem*. *Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems*. União Europeia: European Data Protection Supervisor, 2024.

embora haja aqui uma necessidade de aplicar proporcionalmente os requisitos legais de proteção de dados, para que eles também não percam o seu sentido, caso não se vislumbre uma reconciliação entre os dois campos.⁶⁷ Logo, enquanto o impedimento da raspagem traria um custo considerável aos desenvolvedores, visto que funções básicas de busca e de recuperação de informação “dependem” do *web scraping*,⁶⁸ é certo que o direito fundamental à proteção de dados deve igualmente ser levado a sério e não pode ser tido como um mero empecilho às atividades econômicas dos agentes de tratamento.

Em conclusão, nota-se que as legislações de proteção de dados parecem, no limite, conflitar em certa medida com operações de IA contextualizadas em um marco de *Big Data*,⁶⁹ o que corre o risco de inibir a inovação e novos benefícios tecnológicos à sociedade,⁷⁰ ao passo em que os Estados-nação intensificam a competição estratégica e a flexibilização do intervencionismo para privilegiar o desenvolvimento em matéria de IA.⁷¹

O Brasil tem optado, entretanto, por praticamente espelhar a moldura regulatória mais protetiva da Europa,⁷²⁻⁷³ de forma que se pretende manter a plena aplicabilidade da LGPD ao treinamento de IA via *web scraping*.⁷⁴ Vale destacar, ainda, que a legislação de proteção de dados brasileira apenas autoriza o tratamento posterior de dados pessoais públicos ou tornados manifestamente públicos por seu titular quando garantidos propósitos legítimos e específicos para a nova atividade e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos na LGPD.⁷⁵

67. SOLOVE, Daniel; HARTZOG, Woodrow. *The Great Scrape: the clash between scraping and privacy*, p. 5. No prelo.

68. “A proibição da raspagem teria um grande custo financeiro e social, visto que muitas funções básicas da Internet e da IA, relativas a busca e recuperação de informação, dependem do *scraping*. A raspagem pode ser uma ferramenta valiosa para capacitar as pessoas, promover a concorrência e responsabilizar o setor e o governo por suas próprias práticas relacionadas a dados.” [Tradução nossa]. *Ibidem*, p. 52.

69. ZARSKY, Tal. *Incompatible: the GDPR in the age of Big Data*. Seton Hall Law Review. EUA, Nova Jérsei, v. 47, n. 4, pp. 995-1.020, ago., 2017.

70. Carlos Affonso Souza, Christian Perrone e Eduardo Magrani sustentam que “a proibição do uso de mecanismos que automatizam decisões ou mesmo inteligência artificial, *machine learning* e afins, seria o mesmo que condenar os humanos ao uso de cavalos depois da invenção do motor a combustão.” SOUZA, Carlos Affonso; PERRONE, Christian; MAGRANI, Eduardo. *O Direito à Explicação entre a Experiência e a sua Positivização na LGPD*, locus citatum, p. 246.

71. Para um mapeamento das diferentes propostas regulatórias sobre IA, não restritas à legislação europeia, confira-se ITS. *Como Regular a Inteligência Artificial?* Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2024.

72. UE. *Artificial Intelligence Act*, locus citatum.

73. Para uma compreensão sobre as influências da legislação europeia ao redor do mundo, confira-se BRADFORD, Anu. *The Brussels Effect: how the European Union rules the world*. Reino Unido, Oxford: Oxford University Press, 2020.

74. De acordo com o artigo 30, III, do Projeto de Lei brasileiro n.º 2.338, de 2023, o desenvolvedor de um sistema de IA de propósito geral deve, antes de disponibilizar no mercado para fins comerciais, apenas processar e incorporar conjuntos de dados coletados e tratados em conformidade com as exigências legais, sujeitos a uma adequada governança de dados, em especial de acordo com a LGPD. Além disso, o artigo 61, § 3º, do Projeto, determina que a atividade de mineração de textos e dados que envolva dados pessoais estará sujeita às disposições da LGPD. BRASIL. *Projeto de Lei n.º 2.338, de 2023*, locus citatum. De maneira similar, a regulação europeia indica que a concepção, o desenvolvimento e a utilização de sistemas de IA que envolvam dados pessoais continuam adstritos à legislação que rege a proteção dessas informações. UE. *Artificial Intelligence Act*, locus citatum, considerando 10 e artigo 2.º, n.º 7.

75. BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018*, locus citatum, artigo 7º, § 7º.

O caminho que parece trilhar o país certamente privilegia o direito fundamental à proteção de dados pessoais, no que se refere ao desenvolvimento de sistemas que tenham por matéria-prima essas informações – embora ainda não haja consenso acerca da escolha regulatória adequada para a salvaguarda “quanto aos problemas que a IA pode trazer.”⁷⁶ De todo modo, o cenário atual conflui para um alicerce legislativo centralizado na pessoa humana,⁷⁷ ao mesmo tempo em que empresas de tecnologia sustentam determinadas práticas econômicas na raspagem de dados *online*, o que torna a continuidade do *scraping* um verdadeiro “enigma”.⁷⁸

A fim de melhor delinear os contornos e os desafios da viabilização da raspagem na Internet, o próximo capítulo da pesquisa investiga as possibilidades de fundamentação do *web scraping* em uma das hipóteses legais previstas na LGPD, tendo em vista que os agentes de tratamento precisam selecionar uma das bases contidas na legislação enquanto uma condição para iniciarem qualquer operação com dados pessoais,⁷⁹ inclusive a coleta para o treinamento de sistemas de IA.

3. Em Busca da Hipótese Legal Aplicável ao Treinamento de IA

A seleção de uma hipótese autorizativa é um dos “requisitos” dispostos na LGPD para garantir a licitude de uma atividade de tratamento com dados pessoais.⁸⁰ Na prática, o controlador deve avaliar a finalidade e o contexto específicos para os quais busca operar as informações, a fim de compatibilizá-los com um dos enunciados normativos descritos na legislação.⁸¹ No Brasil, aliás, cabe ressaltar que inexistente hierarquia entre as bases, “por estarem todas elas horizontalmente elencadas” na LGPD.⁸²

Todavia, há uma segmentação entre as hipóteses que avalizam o tratamento de dados pessoais sensíveis⁸³ (artigo 11, LGPD) e não sensíveis (artigo

76. LEMOS, Ronaldo. *O que o Brasil Quer da Inteligência Artificial?* Folha de São Paulo, São Paulo, 07 de abr. de 2024.

77. BRASIL. Projeto de Lei n.º 2.338, de 2023, *locus citatum*, artigo 2º, I.

78. SOBEL, Benjamin. *A New Common Law of Web Scraping*. Lewis & Clark Law Review. EUA, Idaho, v. 25, n. 1, pp. 147-207, mar., 2021, p. 150.

79. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. *Tratamento de Dados Pessoais na LGPD: estudo sobre as bases legais*. *Civilitica.com*. Rio de Janeiro, v. 9, n. 1, pp. 1-38, mai., 2020.

80. SOUZA, Carlos Affonso; VIOLA, Mario; PADRÃO, Vinicius. *Considerações Iniciais sobre os Interesses Legítimos do Controlador na Lei Geral de Proteção de Dados Pessoais*. *Direito Público*. Brasília, v. 16, n. 90, pp. 109-131, dez., 2019, p. 110.

81. REINO UNIDO. *A Guide to Lawful Basis*. Reino Unido, Wilmslow: Information Commissioner’s Office, 2022.

82. BIONI, Bruno. *Proteção de Dados Pessoais: a função e os limites do consentimento*, *locus citatum*, p. 188.

83. São considerados dados pessoais sensíveis, consoante artigo 5º, II, da LGPD, dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural. BRASIL. Lei n.º 13.709, de 14 de agosto de 2018, *locus citatum*.

7º, LGPD), visto que os primeiros compõem uma categoria especial protegida pela Lei, a qual estabelece mecanismos mais rígidos para autorizar atividades dos controladores com aquelas informações, em face de uma potencial utilização indevida para discriminações ilícitas ou abusivas e demais sortes de violações aos direitos da pessoa humana.⁸⁴

Aqui, uma primeira concepção cabível é a argumentação segundo a qual a coleta de dados pessoais via *web scraping* para fins de treinamento de sistemas de IA não tem por finalidade e objetivo⁸⁵ a operação de informações sensíveis ou a causação de danos aos titulares, mas tão somente a garantia, na lógica de *Big Data*, dos insumos necessários para alimentar os sistemas. O EDPB afirma, nessa linha, que o simples fato de um agente de tratamento conduzir uma atividade em larga escala não significa automaticamente que exista um propósito de inferir⁸⁶ dados sensíveis, na hipótese de essas informações serem também coletadas durante a operação.⁸⁷ Ainda nesse contexto de *scraping* na Internet, pode-se afirmar que dificilmente seria viável conduzir uma análise pormenorizada de cada informação tratada, a fim de detectar-se a presença de dados sensíveis no conjunto raspado.⁸⁸

Por outro lado, é igualmente possível sustentar que o tratamento por raspagem para treinar sistemas de IA deve fundamentar-se em uma base mais protetiva, caso haja a coleta de dados pessoais sensíveis ao longo do *scraping*, independentemente da finalidade e do potencial de dano da atividade.⁸⁹ A autoridade francesa de proteção de dados (“CNIL”) salienta, porém, que se o controlador implementar medidas para excluir automaticamente a coleta de

84. TEFFÉ, Chiara Spadaccini de. *Dados Pessoais Sensíveis: qualificação, tratamento e boas práticas*. Indaiatuba: Foco, 2022. A mesma autora também argumenta que: “[c]omo a inteligência artificial tem sido frequentemente usada para a tomada de decisões, a vida das pessoas fica cada vez mais vulnerável a tratamentos discriminatórios ilícitos ou abusivos, como em situações que envolvem análise de probabilidade de cometimento de crimes, tutela da saúde, concessão de crédito e participação em processos seletivos de emprego, por exemplo.” *Idem*. *A Categoria Especial de Dados Sensíveis: fundamentos e contornos*. IN: SCHREIBER, Anderson; MONTEIRO FILHO, Carlos Edison do Rêgo; OLIVA, Milena Donato (Orgs.). *Problemas de Direito Civil*. Rio de Janeiro: Forense, 2021, pp. 97-123, p 105.

85. Para uma visão dos potenciais usos de IA com o propósito de coletar ou inferir dados pessoais sensíveis, confira-se ARTICLE 19. *Privacy and Freedom of Expression in the Age of Artificial Intelligence*. Reino Unido, Londres: Article 19, 2018.

86. O artigo 11, § 1º, da LGPD, prevê que a proteção particular aos dados sensíveis é aplicável a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular. BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018, locus citatum*.

87. UE. *Guidelines 8/2020 on the Targeting of Social Media Users*. União Europeia: European Data Protection Board, 2021. O raciocínio parece semelhante ao empregado pela literatura na descrição da captação, via circuito fechado de televisão (“CFTV”), da imagem de uma pessoa vestida com trajes religiosos: como as câmeras são utilizadas para garantir a segurança do ambiente, sem a coleta de dados biométricos ou para identificar a convicção religiosa das pessoas, não faria sentido impor a fundamentação do tratamento em uma base mais protetiva vinculada a dados sensíveis. Confira-se NGUYEN, Alexander. *Videoüberwachung in Sensitiven Bereichen*. *Datenschutz und Datensicherheit*. Alemanha, Bonn, v. 35, n. 10, pp. 715-717, out., 2011.

88. UE. *Report of the work undertaken by the ChatGPT Taskforce, locus citatum*.

89. Nesse cenário, reitera-se, seria imprescindível identificar uma hipótese legal específica mais restritiva antes de prosseguir com o tratamento. Confira-se REINO UNIDO. *Guidance on AI and Data Protection*. Reino Unido, Wilmslow: Information Commissioner’s Office, 2023. Cabe observar, ainda, que a legislação europeia autoriza atividades com dados sensíveis voltadas a “assegurar a detecção e a correção” de vieses relativos aos sistemas de IA, observados requisitos adicionais para garantir a proteção dos titulares. UE. *Artificial Intelligence Act, locus citatum*, artigo 10.º, n.º 5.

dados sensíveis pela raspagem, operações incidentais e residuais com essas informações, não amparadas por base mais restritiva, deixariam de ser ilícitas nesses casos.⁹⁰

No contexto nacional, dentre as principais hipóteses contidas na LGPD e relacionadas ao tratamento de dados não sensíveis para o treinamento de sistemas de IA, com propósitos comerciais e via *web scraping*, destacam-se somente o consentimento e o legítimo interesse.⁹¹ De forma mais restritiva, apenas o consentimento específico e destacado, em tese, poderia fundamentar a raspagem *online* para o treinamento comercial de IA com dados pessoais sensíveis.⁹² Isso porque a finalidade específica de aprimorar os sistemas não parece se confundir com a execução de um eventual contrato entre o *scraper* e o titular, tampouco com a análise creditícia porventura conduzida por um *bureau* para a proteção do crédito em si – outras hipóteses que poderiam ser apresentadas pelo agente de tratamento a fim de sustentar-se a atividade de raspagem, mas que exigiriam um maior esforço argumentativo nessa direção, por estarem relacionadas a casos exclusivos e pouco usuais.⁹³

Ao mesmo tempo, a própria base legal de consentimento, a qual consiste no fornecimento, pelo titular, de manifestação livre, informada e inequívoca, pela qual concorda com o tratamento de seus dados pessoais para uma finalidade determinada,⁹⁴ enfrenta desafios no quadro sob análise, uma vez que – como supramencionado – o titular pode não compreender os propósitos de determinadas operações “opacas” conduzidas para o treinamento da IA,⁹⁵⁻⁹⁶ tampouco revogar a sua autorização e solicitar a exclusão de dados que já alimentaram

90. FRANÇA. *IA: assurer que le traitement est licite – définir une base légale*. França, Paris: Commission Nationale de l'Informatique et des Libertés, 2024.

91. BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018, locus citatum*, artigo 7º, I e IX.

92. *Ibidem*, artigo 11, I.

93. Para uma análise da base legal de execução de contrato e de exercício regular de direitos em contrato, confira-se PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. *Compliance Digital e LGPD*. São Paulo: Thomson Reuters, 2021. Para uma visão específica sobre proteção do crédito e LGPD, confira-se OLIVA, Milena Donato; VIÉGAS, Franciso de Assis. *Tratamento de Dados para a Concessão de Crédito*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters, 2023, pp. 547-584.

94. BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018, locus citatum*, artigo 5º, XII. Para uma análise pormenorizada da hipótese legal de consentimento, confira-se TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. *O Consentimento na Circulação de Dados Pessoais*. *Revista Brasileira de Direito Civil*. Belo Horizonte, v. 25, n. 3, pp. 83-116, nov., 2020; e BIONI, Bruno. *Proteção de Dados Pessoais: a função e os limites do consentimento, locus citatum*.

95. MITROU, Lilian. *Data Protection, Artificial Intelligence and Cognitive Services: is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?* Social Science Research Network. EUA, Nova Iorque, pp. 1-90, jun., 2019, p. 70; e REINO UNIDO. *Guidance on AI and Data Protection, locus citatum*.

96. Tal preocupação é ainda mais relevante quando se fala em consentimento para o tratamento de dados sensíveis, uma vez que a manifestação nesses casos precisa ser específica. De acordo com a literatura, “[e]specífico deve ser compreendido como um consentimento manifestado em relação a propósitos concretos e claramente determinados pelo controlador e antes do tratamento dos dados, havendo também aqui, e com mais ênfase, as obrigações de granularidade.” TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. *Tratamento de Dados Pessoais na LGPD: estudo sobre as bases legais, locus citatum*, p. 34.

os sistemas,⁹⁷ em prejuízo aos requisitos de consentimento livre, informado e inequívoco. Além disso, obter um consentimento individual de cada titular parece inviável e um esforço custosamente desproporcional à luz das atividades de *web scraping*, as quais envolvem a coleta em larga escala de dados pessoais.⁹⁸

Restaria, portanto, somente a hipótese legal de interesse legítimo do controlador, inaplicável ao tratamento de dados pessoais sensíveis, e descrita pela autoridade holandesa de proteção de dados (“AP”), posto que criticamente, como a única base adequada à raspagem *online*.⁹⁹ O legítimo interesse é a “hipótese autorizativa concebida justamente para dar cabo de situações em que a busca pelo consentimento do titular poderia se transformar até mesmo em um óbice para a exploração regular de dados pessoais”:¹⁰⁰ a sua correta utilização “proporciona e incrementa novos modelos de negócios e diversas estratégias comerciais”.¹⁰¹ Todavia, essa base legal precisa ser ponderada caso a caso em face dos direitos e liberdades fundamentais do titular,¹⁰² suscetível, ainda, a fiscalização pela Autoridade Nacional, a qual já apresentou modelo de teste para o controlador balancear os interesses do tratamento com eventuais impactos indesejados, os quais devem ser lidos em conformidade com a LGPD.¹⁰³ Isso significa que atividades puramente econômicas dos agentes de tratamento precisam ser funcionalizadas, em privilégio à pessoa humana e à proteção de seus dados pessoais.¹⁰⁴

Enfim, no tocante ao tratamento de dados para o treinamento de sistemas via *web scraping*, a hipótese do interesse legítimo figura como uma solução flexível para fundamentar a operação, na medida em que permite o equilíbrio entre benefícios comerciais e sociais da IA e os direitos e interesses dos titulares.¹⁰⁵ Não obstante, é importante que o controlador adote concretamente medidas

97. REINO UNIDO. *How to Use AI and Personal Data Appropriately and Lawfully*. Reino Unido, Wilmslow: Information Commissioner’s Office, 2022; e SOUZA, Carlos Affonso. *Meta x ANPD: separar espaços da IA e dos dados pessoais não será nada fácil*, locus citatum.

98. SOLOVE, Daniel. *Artificial Intelligence and Privacy*, locus citatum; SOLOVE, Daniel; HARTZOG, Woodrow. *The Great Scrape: the clash between scraping and privacy*, locus citatum; e NOVELLI, Claudio et alii. *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*. ArXiv Working Paper n. 2401.07348. EUA, Nova Iorque, mar., 2024.

99. HOLANDA. *Handreiking Scraping door Particulieren en Private Organisaties*. Países Baixos, Haia: Autoriteit Persoonsgegevens, 2024.

100. SOUZA, Carlos Affonso; VIOLA, Mario; PADRÃO, Vinicius. *Considerações Iniciais sobre os Interesses Legítimos do Controlador na Lei Geral de Proteção de Dados Pessoais*. Direito Público. Brasília, v. 16, n. 90, pp. 109-131, dez., 2019, p. 110.

101. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. *Tratamento de Dados Pessoais na LGPD: estudo sobre as bases legais*, locus citatum, p. 19.

102. BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018*, locus citatum, artigos 7º, IX, e 10.

103. BRASIL. *Hipóteses Legais de Tratamento de Dados Pessoais – legítimo interesse*. Brasília: Autoridade Nacional de Proteção de Dados, 2024.

104. BUCAR, Daniel; VIOLA, Mario. *Tratamento de Dados Pessoais por “Legítimo Interesse do Controlador”: primeiras questões e apontamentos*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters, 2023, pp. 453-472.

105. REINO UNIDO. *Big Data, Artificial Intelligence, Machine Learning and Data Protection*. Reino Unido, Wilmslow: Information Commissioner’s Office, 2017, p. 34.

robustas de segurança e de mitigação de riscos¹⁰⁶ – como a pseudonimização, a seleção de critérios para coletar apenas informações necessárias ao treinamento,¹⁰⁷ e a implementação de mecanismos de oposição à atividade (“*opt-out*”)¹⁰⁸ –, além de providenciar informações transparentes e constantemente atualizadas a respeito do tratamento,¹⁰⁹ sem o que a referida base legal igualmente restará inadequada e em desarmonia com a LGPD, com as orientações da ANPD¹¹⁰ e com as melhores práticas em matéria de privacidade e proteção de dados pessoais.

Considerações Finais

O presente artigo buscou identificar a base legal mais apropriada para fundamentar o treinamento de sistemas de IA com dados pessoais, por meio de práticas de *web scraping*. A partir de uma análise da raspagem informacional na era do *Big Data*, pontuou-se como a LGPD inaugurou um cenário notável de privilégio à pessoa humana, de modo que atividades econômicas dos controladores passaram a ser consideradas *vis-à-vis* aos diversos requisitos e obrigações presentes na legislação de regência. Nessa complexa conjuntura, cabe à ANPD deliberar em caráter terminativo sobre a interpretação da LGPD, ao mesmo tempo em que equilibra práticas de raspagem *online* com a proteção de dados pessoais, e ao passo em que também se posiciona como a autoridade competente para coordenar o Sistema Nacional de Regulação e Governança de Inteligência Artificial. Esse é um trabalho desafiador e que exigirá especial atenção da Autoridade, a qual já contempla o *web scraping* e IA em seu mapa de temas prioritários e agenda regulatória.

Vale ressaltar, por último, que a seleção de hipótese legal adequada a uma atividade de tratamento não garante, por si só, a conformidade da operação com a LGPD, razão pela qual é importante que os controladores continuem a implementar boas práticas para resguardar os direitos do titular e os princí-

106. ESPANHA. *Adecuación al RGPD de Tratamientos que Incorporan Inteligencia Artificial – una introducción*, locus citatum.

107. FRANÇA. *IA: assurer que le traitement est licite – définir une base légale*, locus citatum. A pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. Ademais, o princípio da necessidade (artigo 6º, III, LGPD) merece reforço quando do tratamento fundamentado em interesse legítimo. BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018*, locus citatum, artigos 10, § 1º, e 13, § 4º.

108. REINO UNIDO. *Big Data, Artificial Intelligence, Machine Learning and Data Protection*, locus citatum, p. 34.

109. ITÁLIA. *ChatGPT: Garante privacy, limitazione provvisoria sospesa se OpenAI adotterà le misure richieste*. Itália, Roma: Garante per la Protezione dei Dati Personali, 2023. A LGPD também determina que o controlador adote medidas para garantir a transparência do tratamento de dados baseado em interesse legítimo. BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018*, locus citatum, artigos 10, § 2º.

110. A Autoridade também recomenda a comprovação da legítima expectativa dos titulares com o tratamento, a disponibilização de mecanismos para o exercício de direitos, o respeito ao princípio da necessidade, a elaboração de teste de balanceamento em três fases, bem como maior atenção quanto ao tratamento de dados de crianças e adolescentes. BRASIL. *Hipóteses Legais de Tratamento de Dados Pessoais – legítimo interesse*, locus citatum.

pios e fundamentos previstos na Lei. Somente com uma cooperação entre os agentes regulados e a ANPD é que será possível assegurar a liberdade dos modelos de negócios promovidos na Internet, em um equilíbrio criativo com a proteção da privacidade e dos dados pessoais no Brasil, rumo ao desenvolvimento, fomento, uso ético e responsável da IA, com base na centralidade da pessoa humana.

Referências

AARONSON, Susan Ariel. *Data Dysphoria: the governance challenge posed by Large Language Models*. Institute for International Economic Policy Working Paper n. 2023-07. EUA, Washington, DC., ago., 2023.

AMARIKWA, Melany. *Internet Openness at Risk: generative AI's impact on data scraping*. Richmond Journal of Law & Technology. EUA, Virgínia, v. 30, n. 3, pp. 533-589, mai., 2024.

ARTICLE 19. *Privacy and Freedom of Expression in the Age of Artificial Intelligence*. Reino Unido, Londres: Article 19, 2018.

ASHRAF, Rasha. *Scraping EDGAR with Python*. Journal of Education for Business. Reino Unido, Londres, v. 92, n. 4, pp. 179-185, mai., 2017.

BALKIN, Jack. *Free Speech in the Algorithmic Society: big data, private governance, and new school speech regulation*. University of California, Davis, Law Review. EUA, Califórnia, v. 51, n. 615, pp. 1,149-1.210, set., 2017.

BAROCAS, Solon; SELBST, Andrew. *Big Data's Disparate Impact*. California Law Review. EUA, Califórnia, v. 104, n. 3, pp. 671-732, jun., 2016.

BARROSO, Luís Roberto; MELLO, Patrícia Perrone Campos. *Inteligência artificial: promessas, riscos e regulação. Algo de novo debaixo do sol*. Revista Direito e Práxis. Rio de Janeiro, 2024. No prelo.

BIONI, Bruno. *Proteção de Dados Pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019.

BOSTROM, Nick. *Superinteligência: caminhos, perigos e estratégias para um novo mundo*. Tradução: Aurélio Monteiro, Clemente Penna, Fabiana Monteiro e Patrícia Geremias. Rio de Janeiro: Darkside, 2018.

BRADFORD, Anu. *The Brussels Effect: how the European Union rules the world*. Reino Unido, Oxford: Oxford University Press, 2020.

BRASIL. *Emenda Constitucional n.º 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais*. Brasília: Congresso Nacional, 2022.

BRASIL. *Hipóteses Legais de Tratamento de Dados Pessoais – legítimo interesse*. Brasília: Autoridade Nacional de Proteção de Dados, 2024.

BRASIL. *Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil*. Brasília: Congresso Nacional, 2014.

BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)*. Brasília: Congresso Nacional, 2018.

BRASIL. *Projeto de Lei n.º 2.338, de 2023. Dispõe sobre o desenvolvimento, fomento, uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana*. Brasília: Congresso Nacional, 2024.

BRASIL. *Voto n.º 11/2024/DIR-MW/CD*. Brasília: Autoridade Nacional de Proteção de Dados, 2024.

BUCAR, Daniel; VIOLA, Mario. *Tratamento de Dados Pessoais por “Legítimo Interesse do Controlador”: primeiras questões e apontamentos*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters, 2023, pp. 453-472.

DELACROIX, Sylvie. *Sustainable Data Rivers? Critical AI*. EUA, Carolina do Norte, 2024. No prelo.

DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais: elementos da formação da Lei Geral de Proteção de Dados*. São Paulo: Thomson Reuters, 2020.

DONEDA, Danilo; MENDES, Laura Schertel; SOUZA, Carlos Affonso Pereira de; ANDRADE, Norberto. *Considerações Iniciais sobre Inteligência Artificial, Ética e Autonomia Pessoal*. Pensar. Fortaleza, v. 23, n. 4, pp. 1-17, out./dez., 2018.

ESPAÑA. *Adecuación al RGPD de Tratamientos que Incorporan Inteligencia Artificial – una introducción*. Espanha, Madri: Agencia Española de Protección de Datos, 2020.

FRANÇA. *IA: assurer que le traitement est licite – définir une base légale*. França, Paris: Commission Nationale de l’Informatique et des Libertés, 2024.

FRANÇA. *La Réutilisation des Données Publiquement Accessibles En Ligne à des Fins de Démarchage Commercial*. França, Paris: Commission Nationale de l’Informatique et des Libertés, 2020.

FRAZÃO, Ana. *Direitos Básicos dos Titulares de Dados Pessoais*. Revista do Advogado, v. 39, n. 144, pp. 33-46, nov., 2019.

FRAZÃO, Ana. *Fundamentos da Proteção de Dados Pessoais – noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters, 2023, pp. 21-50.

GOODYEAR, Michael. *Circumscribing the Spider: Trademark Law and the edge of data scraping*. Kansas Law Review. EUA, Kansas, v. 70, n. 2, pp. 295-328, dez., 2021.

GRYNBAUM, Michael; MAC, Ryan. *The Times Sues OpenAI and Microsoft Over A.I. Use of Copyrighted Work*. The New York Times. EUA, Nova Iorque, 27 de dez. de 2023.

HILDEBRANDT, Mireille. *Esclavos de los macrodatos. ¿O no?* Revista de Internet, Derecho y Política. Espanha, Barcelona, v. 17, pp. 7-44, nov., 2013.

HOLANDA. *Handreiking Scraping door Particulieren en Private Organisaties*. Países Baixos, Haia: Autoriteit Persoonsgegevens, 2024.

ITÁLIA. *ChatGPT: Garante privacy, limitazione provvisoria sospesa se OpenAI adotterà le misure richieste*. Itália, Roma: Garante per la Protezione dei Dati Personali, 2023.

ITS. *Como Regular a Inteligência Artificial?* Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2024.

LEMOS, Ronaldo. *O que o Brasil Quer da Inteligência Artificial?* Folha de São Paulo, São Paulo, 07 de abr. de 2024.

MCCARTHY, John; MINSKY, Marvin; ROCHESTER, Nathaniel; SHANNON, Claude. *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*. EUA, New Hampshire: Dartmouth College, 1955.

MITROU, Lilian. *Data Protection, Artificial Intelligence and Cognitive Services: is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?* Social Science Research Network. EUA, Nova Iorque, pp. 1-90, jun., 2019, p. 70.

MITTELSTADT, Brent; ALLO, Patrick; TADDEO, Mariarosaria; WACHTER, Sandra; FLORIDI, Luciano. *The Ethics of Algorithms: mapping the debate*. Big Data & Society. EUA, Califórnia, v. 3, n. 2, jul./dez., 2016.

MONTEIRO FILHO, Carlos Edison do Rêgo. *Tutela dos Dados Pessoais e sua Efetividade no Ordenamento Jurídico Brasileiro: direito de acesso, reparação e prevenção de danos*. Revista de Direito da Responsabilidade. Portugal, Coimbra, v. 3, pp. 298-315, mar., 2021.

MORAES, Maria Celina Bodin de. *LGPD: um novo regime de responsabilização civil dito proativo*. Civilistica.com. Rio de Janeiro, v. 8, n. 3, pp. 1-6, dez., 2019.

NEWELL, Allen. *Intellectual Issues in the History of Artificial Intelligence*. IN: MACHLUP, Fritz; MANSFIELD, Una (Eds.). *The Study of Information: interdisciplinary messages*. EUA, Nova Iorque: Wiley, 1983, pp. 187-294.

NGUYEN, Alexander. *Videoüberwachung in Sensitiven Bereichen*. Datenschutz und Datensicherheit. Alemanha, Bonn, v. 35, n. 10, pp. 715-717, out., 2011.

NOVELLI, Claudio; CASOLARI, Federico; HACKER, Philipp; SPEDICATO, Giorgio; FLORIDI, Luciano. *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*. ArXiv Working Paper n. 2401.07348. EUA, Nova Iorque, mar., 2024.

O GLOBO. *Escritores Processam OpenAI por Uso de Obras para Treinar ChatGPT sem Autorização*. O Globo, Rio de Janeiro, 20 de jul. de 2023.

OLIVA, Milena Donato; VIÉGAS, Franciso de Assis. *Tratamento de Dados para a Concessão de Crédito*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *Lei Geral de Prote-*

ção de Dados Pessoais e suas Repercussões no Direito Brasileiro. São Paulo: Thomson Reuters, 2023, pp. 547-584.

PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. *Compliance Digital e LGPD*. São Paulo: Thomson Reuters, 2021.

PARKS, Andrew. *Unfair Collection: reclaiming control of publicly available personal information from internet data scrapers*. Michigan Law Review. EUA, Michigan, v. 120, n. 5, pp. 913-945, mar., 2022.

PASQUALE, Frank. *The Black Box Society: the secret algorithms that control money and information*. EUA, Massachusetts: Harvard University Press, 2015.

POLÔNIA. *NSA Przyznał Rację UODO ws. Decyzji dotyczącej Pierwszej Kary Nałożonej przez Organ Nadzorczy*. Polônia, Varsóvia: Urząd Ochrony Danych Osobowych, 2023.

REINO UNIDO. *A Guide to Lawful Basis*. Reino Unido, Wilmslow: Information Commissioner's Office, 2022.

REINO UNIDO. *Guidance on AI and Data Protection*. Reino Unido, Wilmslow: Information Commissioner's Office, 2023.

REINO UNIDO. *Big Data, Artificial Intelligence, Machine Learning and Data Protection*. Reino Unido, Wilmslow: Information Commissioner's Office, 2017.

REINO UNIDO. *How to Use AI and Personal Data Appropriately and Lawfully*. Reino Unido, Wilmslow: Information Commissioner's Office, 2022.

RODOTÀ, Stefano. *A Vida na Sociedade de Vigilância: a privacidade hoje*. Tradução: Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008.

SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. São Paulo: Malheiros, 2005.

SOBEL, Benjamin. *A New Common Law of Web Scraping*. Lewis & Clark Law Review. EUA, Idaho, v. 25, n. 1, pp. 147-207, mar., 2021

SOLOVE, Daniel. *Artificial Intelligence and Privacy*. Florida Law Review. EUA, Flórida, v. 77, n. 1, jan., 2025. No prelo.

SOLOVE, Daniel; HARTZOG, Woodrow. *The Great Scrape: the clash between scraping and privacy*. No prelo.

SOLOVE, Daniel; HARTZOG, Woodrow. *Kafka in the Age of AI and the Futility of Privacy as Control*. Boston University Law Review. EUA, Massachusetts, v. 104, n. 4, pp. 1.021-1.042, mai., 2024.

SOUZA, Carlos Affonso. *Meta x ANPD: separar espaços da IA e dos dados pessoais não será nada fácil*. Universo Online, São Paulo, 04 de jul. de 2024.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. *Marco Civil da Internet: construção e aplicação*. Juiz de Fora: Editar, 2016.

SOUZA, Carlos Affonso; PERRONE, Christian; MAGRANI, Eduardo. *O Direito à Explicação entre a Experiência e a sua Positivção na LGPD*. IN: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo; RODRIGUES JR., Otavio; BIONI, Bruno (Coords.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021, pp. 243-270.

SOUZA, Carlos Affonso; VIOLA, Mario; PADRÃO, Vinicius. *Considerações Iniciais sobre os Interesses Legítimos do Controlador na Lei Geral de Proteção de Dados Pessoais*. *Direito Público*. Brasília, v. 16, n. 90, pp. 109-131, dez., 2019.

SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. *Tutela da Pessoa Humana na Lei Geral de Proteção de Dados Pessoais: entre a atribuição de direitos e a enunciação de remédios*. *Pensar*. Fortaleza, v. 24, n. 3, pp. 1-22, jul./set., 2019.

SURBLYTĒ, Gintarė. *Data as a Digital Resource*. Max Planck Institute for Innovation & Competition Research Paper n. 16-12. Alemanha, Baviera, out., 2016.

TALIAFERRO, Jocelyn; HEDADJI, Fatima; DULING, Emma. *Web Scraping as a Data Collection Strategy: the perils and pitfalls*. *Social Sciences & Humanities Open*. Holanda, Amsterdã. No prelo.

TEFFÉ, Chiara Spadaccini de. *A Categoria Especial de Dados Sensíveis: fundamentos e contornos*. IN: SCHREIBER, Anderson; MONTEIRO FILHO, Carlos Edison do Rêgo; OLIVA, Milena Donato (Orgs.). *Problemas de Direito Civil*. Rio de Janeiro: Forense, 2021, pp. 97-123.

TEFFÉ, Chiara Spadaccini de. *Dados Pessoais Sensíveis: qualificação, tratamento e boas práticas*. Indaiatuba: Foco, 2022.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. *Tratamento de Dados Pessoais na LGPD: estudo sobre as bases legais*. *Civilitica.com*. Rio de Janeiro, v. 9, n. 1, pp. 1-38, mai., 2020.

TEPEDINO, Gustavo. *As tecnologias e a renovação do Direito Civil*. OAB/RJ, Rio de Janeiro, 12 de junho de 2019.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. *O Consentimento na Circulação de Dados Pessoais*. *Revista Brasileira de Direito Civil*. Belo Horizonte, v. 25, n. 3, pp. 83-116, nov., 2020.

TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. *A Utilização Econômica de Rastreadores e Identificadores On-Line de Dados Pessoais*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters, 2023, pp. 585-604.

UE. *Artificial Intelligence Act. Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence*. União Europeia: Parlamento Europeu, 2024.

UE. *Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems*. União Europeia: European Data Protection Supervisor, 2024.

UE. *Guidelines 8/2020 on the Targeting of Social Media Users*. União Europeia: European Data Protection Board, 2021.

UE. *Report of the work undertaken by the ChatGPT Taskforce*. União Europeia: European Data Protection Board, 2024.

VERONESE, Alexandre. *Os Direitos de Explicação e de Oposição diante das Decisões Totalmente Automatizadas: comparando o RGPD da União Europeia com a LGPD brasileira*. IN: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters, 2023, pp. 377-408.

ZARSKY, Tal. *Incompatible: the GDPR in the age of Big Data*. *Seton Hall Law Review*. EUA, Nova Jérsei, v. 47, n. 4, pp. 995-1.020, ago., 2017.

ZUBOFF, Shoshana. *A Era do Capitalismo de Vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução: George Schlesinger. São Paulo: Intrínseca, 2019.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

3

Racismo Algorítmico: Os Desafios da Inteligência Artificial e a Justiça Social no Contexto Digital

BÁRBARA GOMES D'ASCENÇÃO

Sumário: Introdução. 1. Capitalismo de Dados e Desigualdades. 2. Racismo Algorítmico na Segurança Pública e no Mercado de Trabalho. 3. Colonialismo de Dados e Cultura; 4. Transparência, Ética Algorítmica e Políticas Públicas. Considerações finais. Referências.

Introdução

A inteligência artificial (IA) tem se tornado uma presença constante e transformadora em diversos setores da sociedade moderna, desde assistentes virtuais até sistemas complexos de tomada de decisão em áreas críticas como saúde, segurança pública e mercado de trabalho. Exemplos notáveis incluem o uso de IA para diagnóstico médico e sistemas de vigilância preditiva utilizados por forças policiais em diversas cidades. Embora a IA ofereça inúmeras vantagens, ela também traz consigo desafios significativos, especialmente no que diz respeito à justiça social e à equidade. Um dos problemas mais prementes é o racismo algorítmico, em que algoritmos refletem e reforçam desigualdades raciais presentes na sociedade. Conforme destaca Noble², “os algoritmos têm o poder de perpetuar vieses históricos e estruturais sob a aparência de neutralidade técnica”.

O racismo é uma construção social que permeia diversas esferas da vida e a tecnologia, desenvolvida por sujeitos sociais, não está imune a essas influências. A tecnologia, apesar de sua aparência neutra, pode perpetuar lógicas dominantes e hegemônicas. A questão central que este artigo se propõe a abordar é: de que maneira os algoritmos utilizados em diferentes esferas sociais contribuem para o reforço do racismo estrutural? Esse questionamento é crucial, pois, conforme Silva³, “os sistemas de IA não são meras ferramentas técnicas, mas reproduções dos valores e preconceitos de suas sociedades de origem”.

A relevância do estudo reside na necessidade de uma compreensão crítica, ética e política dos sistemas de IA. As decisões tomadas por esses sistemas afetam diretamente a vida de milhões de pessoas, especialmente as pertencentes a grupos minoritários. Entender e mitigar o racismo algorítmico é crucial para promover uma sociedade mais justa e equitativa. Como Zuboff⁴

1. D'ASCENÇÃO, Bárbara Gomes. Currículo disponível em: <https://www.linkedin.com/in/b%C3%A1rbara-dascencao/>.

2. NOBLE, Safiya Umoja. *Algoritmos da Opressão: como o Google fomenta e lucra com o racismo*. Santo André: Editora Rua do Sabão, 2021. p. 34.

3. SILVA, Tarcízio da. *Racismo Algorítmico: Inteligência Artificial e Discriminação nas Redes Digitais*. São Paulo: Edições Sesc SP, 2022. p. 45.

4. ZUBOFF, Shoshana. *The Age of Surveillance Capitalism*. New York: PublicAffairs, 2018. p. 102.

argumenta, “o capitalismo de vigilância aprofunda desigualdades ao monetizar dados pessoais, frequentemente reforçando preconceitos existentes”.

1. Capitalismo de Dados e Desigualdades

O modelo capitalista vigente tem exacerbado desigualdades existentes ao se basear na extração e comercialização de grandes volumes de dados. Zuboff⁵ define o “capitalismo de vigilância” como a lógica econômica que utiliza dados pessoais para prever e modificar o comportamento humano em prol do lucro. Segundo Van Dijck⁶, o processo de “dataficação” transforma comportamentos e práticas sociais em dados quantificáveis, os quais são frequentemente utilizados sem consideração pelos vieses subjacentes.

A coleta de dados pessoais ocorre em várias plataformas digitais, incluindo redes sociais, mecanismos de busca e serviços online. Esses dados são utilizados para criar perfis detalhados de usuários, permitindo que empresas e governos tomem decisões baseadas em informações pessoais. O problema é que esses dados muitas vezes carregam consigo preconceitos históricos e estruturais. Por exemplo, dados de localização podem refletir segregações racial e socioeconômica nas cidades, perpetuando desigualdades existentes⁷.

A coleta de dados, portanto, não é um processo neutro, mas sim carregado de significados e preconceitos que podem ser utilizados para discriminar e marginalizar ainda mais certos grupos.

Os dados utilizados para treinar sistemas de IA frequentemente carregam preconceitos históricos. Esses sistemas, quando aplicados em áreas como segurança pública, saúde e mercado de trabalho, podem perpetuar e até amplificar desigualdades raciais. O’Neil⁸ afirma que “os algoritmos não são imparciais; eles refletem as prioridades e preconceitos de seus criadores e os dados que os alimentam”. Por exemplo, um estudo de Noble⁹ revelou que as buscas no Google por nomes tradicionalmente afro-americanos retornavam anúncios relacionados a antecedentes criminais mais frequentemente do que para no-

5. ZUBOFF, Shoshana. *The Age of Surveillance Capitalism*. New York: PublicAffairs, 2018.

6. VAN DIJCK, José. *Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology*. *Surveillance & Society*, 2014. p. 198.

7. NOBLE, Safiya Umoja. *Algoritmos da Opressão: como o Google fomenta e lucra com o racismo*. Santo André: Editora Rua do Sabão, 2021. p. 43.

8. O’NEIL, Cathy. *Algoritmos de Destruição em Massa: como o big data aumenta a desigualdade e ameaça à democracia*. Santo André: Editora Rua do Sabão, 2020. p. 56.

9. NOBLE, Safiya Umoja. *Algoritmos da Opressão: como o Google fomenta e lucra com o racismo*. Santo André: Editora Rua do Sabão, 2021.

mes tradicionalmente brancos, demonstrando como preconceitos históricos são integrados nos dados que alimentam esses sistemas.

Ademais, o uso de dados para a tomada de decisões pode levar a práticas discriminatórias. Em um estudo conduzido por Pasquale¹⁰, foi demonstrado que algoritmos de crédito tendem a negar empréstimos a indivíduos de minorias raciais em uma taxa desproporcional. Esses algoritmos, treinados em dados históricos de crédito, refletem os preconceitos e discriminações passadas, perpetuando a exclusão financeira dessas comunidades. A falta de transparência sobre como os dados são coletados, processados e utilizados também exacerba o problema, dificultando a identificação e correção de vieses.

O capitalismo de vigilância, como descrito por Zuboff¹¹ não apenas explora dados pessoais para lucro, mas também contribui para a construção de um sistema social onde a desigualdade é institucionalizada através da tecnologia. Este modelo econômico prioriza a maximização do lucro sobre a equidade e justiça, resultando em um ciclo vicioso onde os marginalizados continuam a ser desfavorecidos. A falta de regulação e a opacidade das práticas de coleta e uso de dados tornam difícil para os indivíduos compreenderem e contestarem as decisões tomadas pelos algoritmos.

Para entender melhor como o capitalismo de dados perpetua desigualdades, é importante analisar a interseção entre tecnologia, sociedade e economia. O modelo capitalista vigente utiliza a tecnologia não apenas como uma ferramenta de eficiência, mas como um mecanismo de controle social e econômico. A “dataficação” das práticas sociais transforma aspectos da vida cotidiana em mercadoria, que é então utilizada para prever e influenciar comportamentos de consumo, reforçando padrões de discriminação e exclusão. Zuboff¹² argumenta que esse modelo cria uma nova forma de poder, onde aqueles que controlam os dados têm a capacidade de moldar a realidade social de maneiras que perpetuam a desigualdade.

A análise crítica de Gomes¹³ sobre o colonialismo de dados evidencia que o controle e a manipulação dos dados são formas modernas de colonialismo, em que o poder e a exploração não se dão mais pelo controle territorial, mas pelo controle dos dados. Gomes argumenta que “o colonialismo de dados perpetua a exploração e a marginalização das populações já vulnerabilizadas, ao

10. PASQUALE, Frank. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge: Harvard University Press, 2015. p. 97.

11. ZUBOFF, Shoshana. *The Age of Surveillance Capitalism*. New York: PublicAffairs, 2018. p. 124.

12. ZUBOFF, Shoshana. *The Age of Surveillance Capitalism*. New York: PublicAffairs, 2018. p. 132.

13. GOMES, Bárbara. *Crimes Cibernéticos e Cultura: Uma Análise do Colonialismo de Dados e Suas Implicações*. TCC. 2023. p. 25.

mesmo tempo que consolida o poder das grandes corporações tecnológicas”. Esta perspectiva crítica complementa a análise de Zuboff¹⁴ ao destacar como as estruturas de poder histórico e colonial são reproduzidas e reforçadas no ambiente digital.

Gomes¹⁵ também destaca que as práticas de extração de dados são frequentemente realizadas sem o consentimento explícito dos indivíduos, o que reforça a assimetria de poder entre os coletadores de dados e os sujeitos dos dados. Isso resulta em uma forma de colonização onde os dados são extraídos e utilizados de maneiras que beneficiam principalmente as corporações tecnológicas e os governos, em detrimento das populações mais vulneráveis.

2. Racismo Algorítmico na Segurança Pública e no Mercado de Trabalho

No Sergipe, durante uma partida de futebol do Campeonato Sergipano de Futebol, o sistema de reconhecimento facial causou a detenção de uma pessoa inocente, por conta de falso positivo, gerando constrangimento e medo ao cidadão que foi detido incorretamente¹⁶. Este incidente evidencia como a tecnologia pode reforçar preconceitos existentes, transformando-se em uma ferramenta de opressão em vez de justiça. Os sistemas de reconhecimento facial, amplamente utilizados por forças de segurança, demonstram como a aplicação não crítica de IA pode resultar em práticas discriminatórias que exacerbam a marginalização de grupos vulneráveis.

Sistemas de segurança pública frequentemente utilizam algoritmos que associam negritude e pobreza à criminalidade, resultando em um aumento das taxas de encarceramento e violência contra minorias. De acordo com Silva¹⁷, “os sistemas de vigilância algorítmica perpetuam a criminalização de corpos negros, reforçando o racismo estrutural através de práticas automatizadas”. Esses algoritmos, desenvolvidos com base em dados históricos de policiamento, frequentemente incorporam e amplificam preconceitos, resultando em práticas de vigilância e controle que desproporcionalmente afetam comunidades negras.

14. ZUBOFF, Shoshana. *The Age of Surveillance Capitalism*. New York: PublicAffairs, 2018.

15. GOMES, Bárbara. *Crimes Cibernéticos e Cultura: Uma Análise do Colonialismo de Dados e Suas Implicações*. TCC. 2023. p. 23.

16. G1. ‘Medo, frustrado e constrangido’, diz homem detido por engano em estádio após erro do sistema de reconhecimento facial. *Fantástico*, 21 abr. 2024. Disponível em: <https://g1.globo.com/fantastico/noticia/2024/04/21/medo-frustrado-e-constrangido-diz-homem-detido-por-engano-em-estadio-apos-erro-do-sistema-de-reconhecimento-facial.ghtml>. Acesso em: 18 out. 2024.

17. SILVA, Tarcizio da. *Racismo Algorítmico: Inteligência Artificial e Discriminação nas Redes Digitais*. São Paulo: Edições Sesc SP, 2022. p. 102.

Estudos mostram que sistemas de reconhecimento facial têm maior probabilidade de erro ao identificar indivíduos de determinadas etnias. O estudo *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* revelou, por meio da comparação de 189 algoritmos de 99 desenvolvedores diferentes, que a maioria dos algoritmos apresentava variações de precisão com base em fatores demográficos, gerando uma taxa mais alta de falsos positivos para rostos asiáticos e afro-americanos em comparação com rostos caucasianos, chegando a ser 10 a 100 vezes maior dependendo do algoritmo¹⁸. Esses erros não são meramente técnicos; eles têm implicações profundas, como a criminalização injusta de indivíduos e a perpetuação de estereótipos raciais. Bezerra e Costa¹⁹ destacam que “os algoritmos de reconhecimento facial frequentemente falham ao identificar corretamente pessoas de pele mais escura, exacerbando práticas de vigilância discriminatória”.

A aplicação de algoritmos no mercado de trabalho também revela desigualdades profundas. Algoritmos utilizados por empresas para seleção de candidatos muitas vezes desfavorecem minorias raciais. Noble²⁰ observa que esses algoritmos podem refletir os preconceitos dos programadores e os dados históricos utilizados para treiná-los. O estudo *Are Emily and Greg More Employable than Lakisha and Jamal? A Field Experiment on Labor Market Discrimination* da Universidade de Washington mostrou que os sistemas de IA utilizados para triagem de currículos tendem a rejeitar nomes que soam afro-americanos, mesmo quando todas as outras qualificações são iguais²¹. Esta prática não apenas exclui candidatos qualificados, mas também perpetua a segregação racial no mercado de trabalho, demonstrando como os algoritmos podem reforçar barreiras sociais e econômicas.

Além de tudo, a falta de diversidade nas equipes de desenvolvimento de IA pode exacerbar esses problemas. Desenvolvedores de IA frequentemente não representam a diversidade da população que suas tecnologias irão impactar, o que pode levar a um ciclo de feedback onde preconceitos são inadvertidamente codificados nos algoritmos. Benjamin²² argumenta que “a inclusão de

18. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. NIST Interagency/Internal Report (NISTIR) - 8280. 2019. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>. Acesso em: 18 out. 2024.

19. BEZERRA, Arthur Coelho; COSTA, Camila Mattos da. Pele negra algoritmos brancos: informação e racismo nas redes sociotécnicas. *Liinc em Revista*, v. 18, n. 2, 2022. p. 89.

20. NOBLE, Safiya Umoja. *Algoritmos da Opressão: como o Google fomenta e lucra com o racismo*. Santo André: Editora Rua do Sabão, 2021. p. 92.

21. BERTRAND, Marianne; MULLAINATHAN, Sendhil. *Are Emily and Greg More Employable than Lakisha and Jamal? A Field Experiment on Labor Market Discrimination*. National Bureau of Economic Research, Working Paper 9873, 2003. Disponível em: https://www.nber.org/system/files/working_papers/w9873/w9873.pdf. Acesso em: 18 out. 2024.

22. BENJAMIN, Ruha. *Race After Technology: Abolitionist Tools for the New Jim Code*. Medford, MA: Polity, 2019. p. 88.

diversas vozes no desenvolvimento de algoritmos é crucial para criar sistemas mais justos e equitativos”. Isso significa que a diversidade deve ser uma consideração central não apenas nos dados, mas também nas equipes que desenvolvem e implementam esses sistemas.

A interação entre racismo algorítmico e práticas de segurança pública e emprego revela como as tecnologias, quando não supervisionadas e reguladas adequadamente, podem reforçar estruturas de poder desiguais. A tecnologia, que deveria servir como uma ferramenta para a justiça e equidade, muitas vezes acaba perpetuando as mesmas desigualdades que prometia resolver. A falta de diversidade e a presença de vieses nos dados e nas equipes de desenvolvimento são fatores cruciais que contribuem para essa perpetuação.

Gomes²³ oferece uma análise aprofundada das implicações do racismo algorítmico no contexto dos crimes cibernéticos e da segurança pública. Gomes²⁴ destaca casos específicos em que sistemas de vigilância preditiva têm levado a intervenções policiais desproporcionais em bairros predominantemente negros, exacerbando a desconfiança e o conflito entre essas comunidades e as forças de segurança.

Também discutido como a falta de transparência e a dificuldade em acessar os critérios usados pelos algoritmos de vigilância criam um ambiente onde os abusos podem ocorrer sem fiscalização adequada. Este ponto é crucial para entender como a tecnologia pode ser usada tanto para o bem quanto para o mal, dependendo de como é implementada e regulamentada.

3. Colonialismo de Dados e Cultura

O conceito de *colonialismo de dados*, conforme discutido por Zuboff²⁵, refere-se ao controle e exploração de dados de populações marginalizadas por corporações tecnológicas e governos, sem o consentimento ou benefício adequado dessas populações. Este processo perpetua desigualdades e marginaliza ainda mais os grupos já vulneráveis, criando um novo tipo de colonialismo no ambiente digital.

Couldry e Mejias²⁶ definem *colonialismo de dados* como “uma nova fase do capitalismo, onde a extração de dados é a principal forma de acumulação de

23. ZUBOFF, Shoshana. *The Age of Surveillance Capitalism*. New York: PublicAffairs, 2018.

24. GOMES, Bárbara. *Crimes Cibernéticos e Cultura: Uma Análise do Colonialismo de Dados e Suas Implicações*. TCC. 2023

25. GOMES, Bárbara. *Crimes Cibernéticos e Cultura: Uma Análise do Colonialismo de Dados e Suas Implicações*. TCC. 2023.

26. COULDRY, Nick; MEJIAS, Ulises A. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford: Stanford University Press, 2019. p. 336.

capital”. Eles argumentam que essa prática reflete e amplia as desigualdades globais, com empresas de tecnologia dos países desenvolvidos extraíndo dados de usuários de países em desenvolvimento para seus próprios benefícios econômicos. Esta dinâmica cria uma relação de dependência e exploração, onde as populações dos países em desenvolvimento são reduzidas a meros fornecedores de dados.

Além disso, Thatcher, O’Sullivan e Mahmoudi²⁷ destacam que o *colonialismo de dados* envolve a “produção de conhecimento a partir de dados extraídos, que são frequentemente utilizados para controlar e governar as populações de forma não transparente”. Eles argumentam que a produção de conhecimento a partir de dados extraídos muitas vezes ignora os contextos sociais e culturais dos quais esses dados são retirados, resultando em políticas e práticas que perpetuam a marginalização e a exclusão.

Um exemplo claro de *colonialismo de dados* pode ser visto na utilização de dados coletados por empresas de redes sociais para influenciar eleições e moldar a opinião pública. O escândalo Cambridge Analytica, em que dados de milhões de usuários do Facebook foram utilizados sem consentimento para influenciar a eleição presidencial dos EUA em 2016, destaca como os dados podem ser explorados para fins políticos e econômicos²⁸. Esse caso ilustra as implicações do *colonialismo de dados*, em que a extração de dados é utilizada para manipular processos democráticos, reforçando o poder das elites sobre as massas.

As implicações culturais do *colonialismo de dados* são profundas. Gomes²⁹ discute como a apropriação e exploração de dados podem levar à perda de controle cultural e à erosão da autonomia das comunidades. A autora destaca que “a coleta e utilização de dados sem o envolvimento adequado das comunidades pode resultar na distorção e descontextualização de práticas culturais, contribuindo para a alienação e desvalorização dessas culturas”. Este proces-

27. THATCHER, Jim; O’SULLIVAN, David; MAHMOUDI, Dillon. *Data colonialism through accumulation by dispossession: New metaphors for understanding the societal impacts of Big Data*. Environment and Planning D: Society and Space, 2016. p. 991.

28. O escândalo Cambridge Analytica, exposto em 2018, envolveu o uso indevido de dados de milhões de usuários do Facebook. A empresa Cambridge Analytica utilizou um aplicativo chamado *thisisyourdigitallife*, que coletava dados pessoais sob o pretexto de um teste de personalidade para fins acadêmicos. No entanto, esses dados foram compartilhados com a Cambridge Analytica e usados para criar perfis psicológicos detalhados, com o objetivo de influenciar eleitores durante a campanha presidencial dos EUA em 2016 e outras campanhas ao redor do mundo. A Federal Trade Commission (FTC) dos EUA processou a empresa e seus executivos por práticas enganosas, resultando em sanções significativas e levantando questões sobre privacidade e o uso ético de dados.

FTC - Federal Trade Commission. Cambridge Analytica, LLC, In the Matter of. Federal Trade Commission, 24 jul. 2019. Disponível em: <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer>. Acesso em: 15 out. 2024.

29. GOMES, Bárbara. *Crimes Cibernéticos e Cultura: Uma Análise do Colonialismo de Dados e Suas Implicações*. TCC. 2023. p. 23.

so não apenas perpetua desigualdades, mas também ameaça a integridade e a continuidade das culturas marginalizadas.

Para mais, o *colonialismo de dados* tem impactos significativos na autodestruição das comunidades. Ao serem reduzidas a fontes de dados, as comunidades perdem a capacidade de definir suas próprias narrativas e destinos. Como afirma Couldry e Mejias³⁰, “o colonialismo de dados mina a capacidade das populações de exercer controle sobre suas próprias vidas, substituindo formas de governança local por sistemas de gestão algorítmica”.

Para mitigar os efeitos do *colonialismo de dados*, é essencial desenvolver políticas públicas que protejam os direitos das populações marginalizadas e garantam uma distribuição equitativa dos benefícios da economia de dados. Esta abordagem participativa é fundamental para mitigar os efeitos negativos do *colonialismo de dados* e promover a justiça social no ambiente digital.

Couldry e Mejias³¹ defendem a criação de políticas de soberania de dados, em que as comunidades têm controle sobre seus próprios dados e podem decidir como eles são utilizados. Eles argumentam que “a soberania de dados é uma resposta crítica ao *colonialismo de dados*, permitindo que as comunidades recuperem o controle sobre seus recursos digitais”.

A implementação de regulamentos robustos que protejam a privacidade e garantam o consentimento informado é outro passo crucial. A Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia são exemplos de legislações que visam proteger os direitos dos indivíduos em relação aos seus dados pessoais. Essas leis estabelecem padrões para a coleta, armazenamento e uso de dados, promovendo transparência e responsabilidade.

Desse modo, é importante promover uma alfabetização digital crítica que permita às populações compreender e questionar as dinâmicas de poder no ambiente digital. Gomes³² levanta que a educação digital deve incluir uma compreensão crítica das implicações sociais e políticas da coleta e uso de dados, capacitando os indivíduos a resistir às formas de exploração digital. A educação é uma ferramenta poderosa para capacitar indivíduos e comunidades a exercerem controle sobre seus dados e resistirem às práticas de *colonialismo de dados*.

30. COULDRY, Nick; MEJIAS, Ulises A. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford: Stanford University Press, 2019. p. 341.

31. COULDRY, Nick; MEJIAS, Ulises A. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford: Stanford University Press, 2019. p. 342.

32. GOMES, Bárbara. *Crimes Cibernéticos e Cultura: Uma Análise do Colonialismo de Dados e Suas Implicações*. TCC. 2023. p. 34.

4. Transparência, Ética Algorítmica e Políticas Públicas

A opacidade dos algoritmos e a falta de transparência nas decisões tomadas por esses sistemas levantam questões éticas significativas. Pasquale³³ argumenta que “a caixa-preta dos algoritmos esconde vieses e preconceitos que têm consequências reais e prejudiciais para grupos marginalizados”. É essencial desenvolver uma ética algorítmica que promova transparência, responsabilidade e equidade. Capurro³⁴ sugere que é necessário entender o contexto cultural e histórico no qual os algoritmos são desenvolvidos para mitigar seus efeitos discriminatórios. Noble³⁵ também ressalta que “a resistência ao racismo algorítmico deve envolver tanto a crítica das tecnologias quanto a transformação dos sistemas sociais que as produzem”.

Para mitigar esses problemas, é fundamental que governos e instituições desenvolvam políticas públicas que regulem o uso de IA garantindo que esses sistemas sejam auditáveis e responsáveis. Yeshimabeit e Traub³⁶ propõem que “a regulação da IA deve incluir mecanismos de transparência e responsabilidade para evitar a perpetuação de desigualdades raciais”. Silva³⁷ argumenta que avaliações de impacto em direitos humanos devem ser um pré-requisito para a adoção de sistemas algorítmicos, enfatizando que “a transparência e a prestação de contas são essenciais para garantir a equidade nos processos algorítmicos”.

A implementação de auditorias regulares para identificar e corrigir vieses é uma das soluções propostas. O’Neil³⁸ sugere que “auditorias independentes são necessárias para garantir que os algoritmos não estejam reforçando preconceitos e desigualdades”. A prática de auditoria deve ser incorporada como uma norma nos processos de desenvolvimento e implementação de algoritmos, permitindo que vieses sejam detectados e corrigidos antes de causar danos significativos.

Para além disso, é crucial criar algoritmos que sejam treinados com dados diversificados e representativos. Benjamin³⁹ destaca que “a inclusão de diver-

33. PASQUALE, Frank. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge: Harvard University Press, 2015. p. 128.

34. CAPURRO, Rafael. *Enculturating Algorithms*. In: *Proceedings of the International Conference: Artificial Intelligence & Regulation*. LUISS Rome, 2019. p. 94.

35. NOBLE, Safiya Umoja. *Algoritmos da Opressão: como o Google fomenta e lucra com o racismo*. Santo André: Editora Rua do Sabão, 2021. p. 111.

36. YESHIMABEIT, M.; TRAUB, A. *Data capitalism and Algorithmic Racism*. Paper Knowledge: Toward a Media History of Documents, 2021. p. 75.

37. SILVA, Tarcízio da. *Racismo Algorítmico: Inteligência Artificial e Discriminação nas Redes Digitais*. São Paulo: Edições Sesc SP, 2022. p. 137.

38. O’NEIL, Cathy. *Algoritmos de Destruição em Massa: como o big data aumenta a desigualdade e ameaça à democracia*. Santo André: Editora Rua do Sabão, 2020. p. 143.

39. BENJAMIN, Ruha. *Race After Technology: Abolitionist Tools for the New Jim Code*. Medford, MA: Polity, 2019. p. 88.

sas vozes no desenvolvimento de algoritmos é crucial para criar sistemas mais justos e equitativos”. Além disso, Pasquale⁴⁰ defende que “os dados utilizados para treinar algoritmos devem ser cuidadosamente selecionados para evitar a reprodução de vieses históricos”. A diversidade de dados e a inclusão de perspectivas variadas são essenciais para desenvolver algoritmos que sirvam a toda a sociedade de maneira justa.

Aumentar a conscientização sobre os riscos e impactos da IA na sociedade é outro passo essencial. Capurro⁴¹ enfatiza a importância de uma alfabetização digital que inclua a compreensão crítica dos algoritmos e suas implicações sociais. Noble⁴² argumenta que “a educação sobre os impactos da IA deve ser parte integrante dos currículos acadêmicos para preparar as futuras gerações para lidar com as questões éticas e sociais dessas tecnologias”. A educação é uma ferramenta poderosa para capacitar indivíduos a questionarem e entenderem melhor a influência dos algoritmos em suas vidas diárias. Esse processo educacional não apenas constrói sujeitos críticos, mas também os capacita a utilizar a tecnologia em benefício próprio e para o bem social.

Gomes⁴³ sugere que a implementação de políticas públicas eficazes deve incluir a participação ativa das comunidades afetadas pelos algoritmos. É crucial que as políticas devem ser desenvolvidas com a inclusão das vozes das comunidades marginalizadas, garantindo que suas preocupações e necessidades sejam consideradas no desenvolvimento e implementação de sistemas de IA. Esta abordagem participativa é fundamental para criar políticas que não apenas mitiguem os efeitos negativos dos algoritmos, mas também promovam justiça e equidade.

Dessa forma, a IA pode ser utilizada para promover a justiça social, desenvolvendo tecnologias que contribuam para a redução das desigualdades e o empoderamento de comunidades marginalizadas. Noble⁴⁴ sugere que “as tecnologias de IA devem ser desenhadas com uma perspectiva de justiça social, considerando as necessidades e experiências de grupos historicamente

40. PASQUALE, Frank. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge: Harvard University Press, 2015. p. 151.

41. CAPURRO, Rafael. *Enculturating Algorithms*. In: *Proceedings of the International Conference: Artificial Intelligence & Regulation*. LUISS Rome, 2019. p. 101.

42. NOBLE, Safiya Umoja. *Algoritmos da Opressão: como o Google fomenta e lucra com o racismo*. Santo André: Editora Rua do Sabão, 2021. p. 135.

43. GOMES, Bárbara. *Crimes Cibernéticos e Cultura: Uma Análise do Colonialismo de Dados e Suas Implicações*. TCC. 2023. p. 28.

44. NOBLE, Safiya Umoja. *Algoritmos da Opressão: como o Google fomenta e lucra com o racismo*. Santo André: Editora Rua do Sabão, 2021. p. 149.

marginalizados”. Capurro⁴⁵ ressalta a necessidade de uma abordagem ética e responsável na implementação dessas tecnologias, afirmando que “a justiça social deve ser um princípio orientador no desenvolvimento e uso da IA”.

A falta de transparência nos sistemas algorítmicos pode resultar em decisões enviesadas e injustas que afetam negativamente grupos marginalizados. Um estudo apresentado na conferência NeurIPS em 2023, intitulado *Reevaluating COMPAS: Base Rate Tracking and Racial Bias*, analisou as falhas do COMPAS, mostrando desvios significativos e levantando preocupações sobre a presença de vieses raciais no sistema.⁴⁶

Para mitigar esses problemas, é essencial que os sistemas algorítmicos sejam transparentes e auditáveis. Isso significa que as organizações que utilizam esses sistemas devem ser capazes de explicar como os algoritmos funcionam e quais dados são utilizados para treinar e operar esses modelos. Diakopoulos⁴⁷ sugere que “a auditabilidade é uma ferramenta crucial para garantir que os algoritmos funcionem de forma justa e equitativa”. Ele argumenta que a auditabilidade permite que terceiros examinem e verifiquem a justiça e a precisão das decisões algorítmicas.

Além disso, é fundamental que haja um desenvolvimento ético dos algoritmos. Isso inclui a implementação de práticas que garantam a diversidade nos dados de treinamento e nas equipes de desenvolvimento. Binns⁴⁸ enfatiza a importância de “adotar uma abordagem ética no desenvolvimento de IA, que inclua a consideração de valores como justiça, responsabilidade e transparência”. Ele argumenta que os desenvolvedores devem estar cientes dos impactos sociais e éticos de suas criações e tomar medidas proativas para mitigar os riscos.

Um exemplo concreto de regulamentação de IA é o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia⁴⁹. O GDPR estabelece diretrizes rigorosas sobre como os dados pessoais devem ser coletados, armazenados e utilizados, garantindo que os indivíduos tenham controle sobre seus dados. Uma das disposições do GDPR, conforme o Artigo 22, exige que

45. CAPURRO, Rafael. *Enculturating Algorithms*. In: *Proceedings of the International Conference: Artificial Intelligence & Regulation*. LUISS Rome, 2019. p. 110.

46. CRESPO, Victor; RANDO, Javier; EVA, Benjamin; KESWANI, Vijay; SINNOTT-ARMSTRONG, Walter. *Reevaluating COMPAS: Base Rate Tracking and Racial Bias*. *NeurIPS*, 2023. Disponível em: NeurIPS Conference. Acesso em: 13 out. 2024.

47. DIAKOPOULOS, Nicholas. *Accountability in algorithmic decision making*. *Communications of the ACM*, v. 59, n. 2, 2016. p. 59.

48. BINNS, Reuben. *Fairness in Machine Learning: Lessons from Political Philosophy*. *Proceedings of the Conference on Fairness, Accountability, and Transparency (FAT)*, 2018, pp. 149-159. Disponível em: <https://proceedings.mlr.press/v81/binns18a.html>. Acesso em: 20 out. 2024.

49. UNIÃO EUROPEIA. Regulamento Geral sobre a Proteção de Dados (GDPR), Artigo 22. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>. Acesso em: 11 out. 2024.

as decisões automatizadas que afetam significativamente os indivíduos sejam explicáveis, permitindo que as pessoas entendam como essas decisões são tomadas e contestem-nas se necessário.

Outro exemplo é a Lei Geral de Proteção de Dados (LGPD)⁵⁰ no Brasil, que visa proteger os direitos de privacidade dos cidadãos brasileiros e regulamentar a coleta, armazenamento e uso de dados pessoais. A LGPD estabelece diversas bases legais para o tratamento de dados, sendo o consentimento explícito uma delas, mas também inclui bases como a execução de contratos, cumprimento de obrigações legais e legítimo interesse do controlador, entre outras. Além disso, a lei exige que as organizações implementem medidas para garantir a segurança e a privacidade dos dados pessoais tratados.

Além das regulamentações, iniciativas de autorregulação também têm sido propostas. Por exemplo, a Partnership on AI, uma coalizão de empresas de tecnologia, acadêmicos e organizações da sociedade civil, desenvolveu diretrizes para o desenvolvimento ético de IA incluindo princípios de transparência e responsabilidade. Essa coalizão trabalha para promover práticas de IA que respeitem os direitos humanos e promovam a justiça social.⁵¹

A implementação de auditorias independentes também é uma prática recomendada para garantir a transparência e a justiça dos algoritmos. O'Neil⁵² sugere que “auditorias independentes são necessárias para garantir que os algoritmos não estejam reforçando preconceitos e desigualdades”. Essas auditorias devem ser conduzidas por entidades independentes que possam avaliar objetivamente a equidade e a eficácia dos sistemas algorítmicos.

Considerações Finais

É possível analisar que, embora os algoritmos e sistemas de IA tenham potencial para beneficiar a sociedade, é crucial abordar e mitigar os vieses raciais incorporados nesses sistemas. A promoção de uma ética algorítmica é fundamental para garantir que a tecnologia avance de forma equitativa e justa. O reconhecimento e a transparência sobre os vieses algorítmicos são pas-

50. BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 out. 2024.

51. PARTNERSHIP ON AI. *Tenets of Partnership on AI*. Partnership on AI, 2018. Disponível em: <https://partnershiponai.org>. Acesso em: 20 set. 2024.

52. O'NEIL, Cathy. *Algoritmos de Destruição em Massa: como o big data aumenta a desigualdade e ameaça à democracia*. Santo André: Editora Rua do Sabão, 2020. p. 143.

so essenciais para a construção de uma sociedade mais justa⁵³. A luta contra o racismo algorítmico não é apenas uma questão técnica, mas uma batalha pela equidade e justiça em um mundo cada vez mais digitalizado.

Com isso, a necessidade de políticas públicas robustas e a implementação de auditorias regulares são medidas essenciais para garantir que os sistemas de IA não perpetuem injustiças. A inclusão de dados diversificados e a conscientização sobre os impactos da IA são passos fundamentais para criar um ambiente tecnológico que sirva a todos de maneira justa. Especialistas na área argumentam que combater o racismo algorítmico faz parte de uma luta maior pela justiça social e pelos direitos humanos no contexto digital.

Além disso, a promoção de uma alfabetização digital que permita a compreensão crítica dos algoritmos e suas implicações sociais é crucial para capacitar indivíduos a questionarem e entenderem melhor a influência dos algoritmos em suas vidas. A educação deve preparar as futuras gerações para lidar com as questões éticas e sociais dessas tecnologias, promovendo uma sociedade mais consciente e equitativa. Há consenso de que a educação sobre os impactos da IA deve ser parte integrante dos currículos acadêmicos para preparar as futuras gerações para esses desafios.

Portanto, a justiça social deve ser um princípio orientador no desenvolvimento e uso da IA. As tecnologias de IA devem ser desenhadas com uma perspectiva de justiça social, considerando as necessidades e experiências de grupos historicamente marginalizados. Dessa forma, é possível mitigar os efeitos negativos do racismo algorítmico e promover uma sociedade mais justa e inclusiva.

Referências

BENJAMIN, Ruha. *Race After Technology: Abolitionist Tools for the New Jim Code*. Medford, MA: Polity, 2019.

BERTRAND, Marianne; MULLAINATHAN, Sendhil. Are Emily and Greg More Employable than Lakisha and Jamal? A Field Experiment on Labor Market Discrimination. *National Bureau of Economic Research*, Working Paper 9873, 2003. Disponível em: https://www.nber.org/system/files/working_papers/w9873/w9873.pdf. Acesso em: 18 out. 2024.

BEZERRA, Arthur Coelho; COSTA, Camila Mattos da. Pele negra algoritmos brancos: informação e racismo nas redes sociotécnicas. *Liinc em Revista*, v. 18, n. 2, 2022.

53. SILVA, Tarcizio da. *Racismo Algorítmico: Inteligência Artificial e Discriminação nas Redes Digitais*. São Paulo: Edições Sesc SP, 2022.

BINNS, Reuben. Fairness in Machine Learning: Lessons from Political Philosophy. *Proceedings of the Conference on Fairness, Accountability, and Transparency (FAT)*, 2018. Disponível em: <https://proceedings.mlr.press/v81/binns18a.html>. Acesso em: 20 out. 2024.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 out. 2024.

COULDRY, Nick; MEJIAS, Ulises A. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford: Stanford University Press, 2019.

CRESPO, Victor; RANDO, Javier; EVA, Benjamin; KESWANI, Vijay; SINNOTT-ARMSTRONG, Walter. Reevaluating COMPAS: Base Rate Tracking and Racial Bias. *NeurIPS*, 2023. Disponível em: NeurIPS Conference. Acesso em: 13 out. 2024.

DIAKOPOULOS, Nicholas. Accountability in algorithmic decision making. *Communications of the ACM*, v. 59, n. 2, 2016.

FTC – Federal Trade Commission. Cambridge Analytica, LLC, In the Matter of. *Federal Trade Commission*, 24 jul. 2019. Disponível em: <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer>. Acesso em: 15 out. 2024.

G1. ‘Medo, frustrado e constrangido’, diz homem detido por engano em estádio após erro do sistema de reconhecimento facial. *Fantástico*, 21 abr. 2024. Disponível em: <https://g1.globo.com/fantastico/noticia/2024/04/21/medo-frustrado-e-constrangido-diz-homem-detido-por-engano-em-estadio-apos-erro-do-sistema-de-reconhecimento-facial.ghtml>. Acesso em: 18 out. 2024.

GOMES, Bárbara. *Crimes Cibernéticos e Cultura: Uma Análise do Colonialismo de Dados e Suas Implicações*. TCC. 2023.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. NIST Interagency/Internal Report (NISTIR) – 8280, 2019. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>. Acesso em: 18 out. 2024.

NOBLE, Safiya Umoja. *Algoritmos da Opressão: como o Google fomenta e lucra com o racismo*. Santo André: Editora Rua do Sabão, 2021.

O’NEIL, Cathy. *Algoritmos de Destruição em Massa: como o big data aumenta a desigualdade e ameaça à democracia*. Santo André: Editora Rua do Sabão, 2020.

PARTNERSHIP ON AI. Tenets of Partnership on AI. *Partnership on AI*, 2018. Disponível em: <https://partnershiponai.org>. Acesso em: 20 set. 2024.

PASQUALE, Frank. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge: Harvard University Press, 2015.

SILVA, Tarcízio da. *Racismo Algorítmico: Inteligência Artificial e Discriminação nas Redes Digitais*. São Paulo: Edições Sesc SP, 2022.

THATCHER, Jim; O'SULLIVAN, David; MAHMOUDI, Dillon. Data colonialism through accumulation by dispossession: New metaphors for understanding the societal impacts of Big Data. *Environment and Planning D: Society and Space*, v. 34, n. 6, 2016.

UNIÃO EUROPEIA. Regulamento Geral sobre a Proteção de Dados (GDPR), Artigo 22. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>. Acesso em: 11 out. 2024.

VAN DIJCK, José. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, v. 12, n. 2, 2014.

ZUBOFF, Shoshana. *The Age of Surveillance Capitalism*. New York: PublicAffairs, 2018.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

4

**Coleta de Dados Pessoais
para o Treinamento de
Inteligência Artificial
Generativa: Um Desafio para
a Proteção de Dados e a
Privacidade**

RODRIGO SANTANA DOS SANTOS

Sumário: Introdução. 1. Principais Conceitos. 1.1 Aprendizado de Máquina no Contexto da IA Generativa. 1.2 Extração de Dados na Internet (Raspagem de Dados). 1.3 Privacidade e Proteção de Dados e IA no Brasil. 2. Boas Práticas Internacionais sobre IA, Privacidade e Governança de Dados. 2.1 Organização para a Cooperação e o Desenvolvimento Econômico. 2.2 Diretrizes da União Europeia para uma IA Confiável. 3. Análise dos Estudos de Caso. 3.1 Extração de dados da internet por meio de raspagem de dados. 3.2 Coleta de dados do Meta para o treinamento da IA. 3.3 Possíveis Soluções Regulatórias. Considerações Finais. Referências.

Introdução

A regulação é uma arte que busca o equilíbrio entre a tutela de um serviço, uma atividade ou um direito com a promoção do ambiente regulado que promova novas tecnologias e modelos de negócio para o desenvolvimento socioeconômico do país. No ambiente digital, mostra-se de grande relevância a avaliação de modelos que busquem esse equilíbrio, dado o dinamismo do desenvolvimento tecnológico e a necessidade de confiança nas relações comerciais, econômicas e sociais em tal ambiente.

Nesse sentido, a Lei Geral de Proteção de Dados (LGPD) dispõe e cria importante marco regulatório para a atividade de tratamento de dados pessoais com objetivo de proteger os direitos fundamentais de proteção de dados e privacidade.

A Inteligência Artificial (IA), considerando suas inovações tecnológicas disruptivas, apresenta grandes desafios na construção do arcabouço regulatório que equilibre a proteção dos direitos fundamentais com a inovação e os potenciais benefícios que a IA pode proporcionar.

Um dos principais desafios é garantir a proteção de dados e a privacidade durante o treinamento da IA generativa, diante da necessidade de coleta excessiva de dados, inclusive pessoais. É inegável o potencial de oportunidades com o avanço desse segmento de IA, como por exemplo, no aprimoramento da escrita científica e criativa,² educação e aprendizagem,³ acessibilidade e

1. Atualmente é Coordenador-Geral de Normatização da Autoridade Nacional de Proteção de Dados (ANPD). Servidor público da carreira de Especialista em Regulação – Área Tecnológica com atuação na área de regulamentação de serviços de telecomunicações e de proteção de dados pessoais. Possui mestrado em Engenharia Elétrica na UNB. Pós-graduado em Direito Digital pelo ITS Rio/UERJ. É membro da Comissão de Estudos 20 da União Internacional de Telecomunicações (UIT) - Internet das Coisas, Comunidades e Cidades Inteligentes.

2. SPRINGER NATURE. Tools such as ChatGPT threaten transparent science; here are our ground rules for their use. *Nature*. 2023. 613 p. Disponível em: doi: <https://doi.org/10.1038/d41586-023-00191-1>. Acesso em: 02 de ago. 2024.

3. SAÚDE, Sandra; BARROS, João Paulo; ALMEIDA, Inês. Impacts of Generative Artificial Intelligence in Higher Education: Research Trends and Students' Perceptions. *Social Sciences*. 2024, 13, 410 p. Disponível em: <https://doi.org/10.3390/socsci13080410>. Acesso em: 27 de jul. 2024.

inclusão, redução da desigualdade econômica social,⁴ bem como na saúde e medicina.⁵

Diante disso, o presente artigo busca identificar os principais problemas e desafios envolvidos na coleta excessiva de dados pessoais para treinamento de IAs, considerando as técnicas de extração de dados da internet, como a raspagem de dados, e o movimento percebido por parte das chamadas Big Techs de alterar suas políticas de privacidade para coletar dados pessoais massivos de usuários, visando realizar o treinamento de IAs generativas.

O artigo está dividido em uma parte teórica, que engloba: principais conceitos, no qual são apresentados conceitos técnicos e legais, boas práticas interacionais sobre IA, privacidade e governança de dados e uma parte de estudos de casos de extração de dados da internet por meio de raspagem de dados e outro de coleta de dados do Meta para o treinamento da IA, com identificação de possíveis soluções regulatórias.

1. Principais Conceitos

1.1 Aprendizado de Máquina no Contexto da IA Generativa

O aprendizado de máquina representa um subcampo da IA focado no desenvolvimento de algoritmos que permitem que as máquinas aprendam a partir de dados e façam previsões ou decisões sem serem explicitamente programadas para cada tarefa específica.⁶ Pode ser definido ainda como método computacional usando experiências para aprimorar a performance ou fazer previsões mais acuradas.⁷

Dentre os diversos tipos de aprendizado de máquina, o aprendizado profundo (*deep learning*) é um subcampo que se concentra em algoritmos inspirados na arquitetura cerebral, ou seja, uma rede neural profunda e são utilizados para aprendizados na IA generativa.

Os algoritmos de aprendizado profundo são usados para várias aplicações, dentre as quais destaca-se: reconhecimento facial, classificação de imagens, detecção de objetos, conversão de fala para texto, assistentes virtuais, diag-

4. CARPRARO, Valerio, et al. The impact of generative artificial intelligence on socioeconomic inequalities and policy making. *Pnax Nexus*. 2024, 3, 191 p. Disponível em: <https://doi.org/10.1093/pnasnexus/pgae191>. Acesso em: 29 de jul. 2024.

5. ZHANG, Peng; BOULOS, Maged N.Kamel. Generative AI in Medicine and Healthcare: Promises, Opportunities and Challenges. *Future Internet*. 2023, 15, 286 p. Disponível em: <https://doi.org/10.3390/fi15090286>. Acesso em: 01 de ago. 2024.

6. MITCHELL, Tom. *Machine Learning*. 1997. McGraw-Hill.

7. MOHRI, M; Rostamizadeh, A; Talwalkar, A. *Foundations of Machine Learning*. Second Edition. MIT Press. 2018.

nóstico de doenças, análise de imagens médicas, condução autônoma e sistemas de navegação.

Nesse sentido, o modelo de aprendizado profundo necessita de grande volume de dados para treinar de forma eficaz os diversos parâmetros constituídos na rede neural e obviamente obter resultados mais precisos e corretos.⁸

1.2 Extração de Dados na Internet (Raspagem de Dados)

A extração de dados na Internet, também conhecida como raspagem, pode ser compreendida como a prática automatizada de extrair grandes quantidades de dados publicados em sites da internet. Esta extração é feita por meio de software que envia solicitações a páginas web, coleta e analisa o conteúdo dessas páginas, e extrai informações específicas de interesse. A extração permite a coleta rápida e econômica de dados, muitas vezes sem o consentimento ou conhecimento dos proprietários dos dados ou dos próprios indivíduos a quem os dados pertencem.⁹

O termo geral “raspagem de dados” se refere a qualquer momento em que “um programa de computador extrai dados de saída gerada de outro programa”. Mais especificamente, raspagem é a “recuperação de conteúdo postado na World Wide Web por meio do uso de um programa diferente de um navegador da web ou uma interface de programação de aplicativos (API)”. A extração “é usada para transformar dados não estruturados na web em dados estruturados que podem ser armazenados e analisados em um banco de dados local central ou planilha”.⁹

A raspagem de dados da internet é um método que possibilita a obtenção de uma enorme quantidade de dados com custo relativamente baixo. Esse cenário é ideal para atender as demandas do aprendizado de máquinas de IA, como aprendizado profundo, que precisam de elevada quantidade de dados.

Um dos casos mais notórios de raspagem para IA foi realizado pela *Clearview AI*, uma empresa iniciante que raspou mais de três bilhões de imagens para desenvolver um sistema de reconhecimento facial.⁹

Outro caso foi apresentado recentemente pela *Human Rights Watch*, organização internacional de direitos humanos, não-governamental, sem fins lucrativos, que analisou 0,0001% do banco de dados da LAION-5B, que possui 5,85 bilhões de imagens e legendas contidas no conjunto de dados, utilizadas

8. GOODFELLOW, I., Bengio, Y., & Courville, A. *Deep Learning*. MIT Press. 2016.

9. SOLOVE, Daniel J; HARTZOG, Woodrow. The Great Scrape: The Clash Between Scraping and Privacy. *SSRN*. 2024. Disponível em: <http://dx.doi.org/10.2139/ssrn.4884485>. Acesso em: 02 de ago. 2024.

para fazer treinamento de IA.¹⁰ Nesta investigação foram encontradas fotos de crianças de 10 estados brasileiros.¹¹

Muitos casos de raspagem de dados foram judicializados, como, por exemplo, o caso da hiQ Labs e o LinkedIn nos Estados Unidos.¹² A hiQ é uma pequena empresa de análise de dados que utilizava *bots* automatizados para coletar informações de perfis públicos do LinkedIn. O LinkedIn usou meios legais para impedir essa coleta, no entanto, a hiQ Labs abriu um processo contra o LinkedIn, buscando uma liminar contra essa limitação, que foi concedida. O LinkedIn apelou e foi confirmada a liminar preliminar do tribunal distrital, impedindo o LinkedIn de negar à hiQ Labs o acesso aos perfis públicos dos membros do LinkedIn. No entanto, após novo recurso em outro tribunal, foi considerado que a hiQ violou os termos de uso do LinkedIn e houve um acordo.¹²

Existem diversos casos judiciais nas cortes norte-americanas de empresas detentoras de plataformas que têm as informações de seus usuários raspadas. Nessa verdadeira guerra de raspagem de dados, várias empresas alegam que tal conduta entraria em conflito com legislações de proteção da privacidade e dos dados pessoais, mas, na verdade, em alguns casos estão buscando tutelar dados que acreditam ser seus ou protegendo seu site e seus próprios interesses comerciais. Em última análise, a privacidade e a segurança do usuário acabam sendo invocadas quando se alinham com os interesses corporativos.¹²

Por outro lado, percebe-se o surgimento de um novo mercado de raspagem de dados.¹² Por exemplo, a Open AI fez negócios com a Associated Press e a Axel Springer, empresa controladora da Político e da Business Insider, para conseguir dados, inclusive com envolvimento de dados pessoais.¹³

1.3 Privacidade e Proteção de Dados e IA no Brasil

A Lei Geral de Proteção de Dados (LGPD) é um marco regulatório que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

10. HUMAN RIGHTS WATCH. Brasil: *Fotos de crianças são usadas indevidamente para alimentar IA*. 2024. Disponível em: <https://www.hrw.org/pt/news/2024/06/10/brazil-childrens-personal-photos-misused-power-ai-tools>. Acesso em: 02 de ago. 2024.

11. UNIÃO EUROPEIA. *Artificial Intelligence Act*. 2024. Disponível em: <https://artificialintelligenceact.eu/ai-act-explorer/>. Acesso em: 03 de ago. 2024.

12. SOLOVE, Daniel J; HARTZOG, Woodrow. *The Great Scrape: The Clash Between Scraping and Privacy*. SSRN. 2024. Disponível em: <http://dx.doi.org/10.2139/ssrn.4884485>. Acesso em: 02 de ago. 2024.

13. SOLOVE, Daniel J; HARTZOG, Woodrow. *The Great Scrape: The Clash Between Scraping and Privacy*. SSRN. 2024. Disponível em: <http://dx.doi.org/10.2139/ssrn.4884485>. Acesso em: 02 de ago. 2024. Apud BARRADI, Thomas, *OpenAI Offering Media Outlets as Little as \$1M to Use News Articles for AI Models*, *New York Post*. 2024.

Nesse sentido, observa-se que a aplicação da lei estabeleceu um marco regulatório do tratamento de dados pessoais, independentemente do meio, físico ou digital, ou da tecnologia utilizada, como por exemplo, blockchain, IA.

Cabe ainda ressaltar que o art. 3º da LGPD dispõe que a lei se aplica caso: i) a operação de tratamento seja realizada no território nacional, ii) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional ou iii) os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional.

Assim, conclui-se que a LGPD é aplicável quando ocorrer o tratamento de dados pessoais, mesmo que por meio da IA, nos termos do art. 3º da lei.

Nesse diapasão, devem ser observados os princípios, os direitos e as garantias previstas na lei, destacando-se para o contexto de IA os princípios da finalidade, necessidade, não discriminação, transparência e responsabilização e prestação de contas.

Todo tratamento de dados pessoais deve ocorrer com base em alguma hipótese legal prevista nos art. 7 e 11 da LGPD, não havendo hierarquia entre elas. Cabe ressaltar que aos dados pessoais sensíveis previstos na lei e aos tratamentos que revelem esses tipos de dados existem maiores restrições na legislação, não se podendo aplicar a hipótese legal do legítimo interesse.

Outro destaque na LGPD relacionado à IA está previsto no art. 20. Está previsto nesse artigo o direito de revisão das decisões tomadas unicamente com base no tratamento automatizado quando afetar o interesse do titular. Já no §1º dispõe sobre o direito de informação sobre os critérios e procedimentos utilizados para a decisão utilizada, também conhecido como direito à explicação.

O artigo tem relação direta com sistemas de IA, mas alguns pontos precisam ser objeto de regulamentação ou interpretação por parte da ANPD. Destaca-se os parâmetros para considerar uma “tomada de decisão unicamente com base no tratamento automatizado”. Nesse caso, é interessante definir o nível de intervenção humana seria possível ocorrer para ser considerado tratamento automatizado. Outro destaque seria quais os critérios para determinar quando um interesse está sendo efetivamente afetado.

Nesse aspecto, para além do art. 20 da LGPD, um ponto tem demonstrado preocupação por parte das autoridades e academias e diz respeito à relação entre a coleta excessiva de dados pessoais para o treinamento de sistemas de IA e a privacidade.

Em relação a essa coleta de dados pessoais, existem aspectos legais que precisam ser observados, como, por exemplo, a observância dos princípios supracitados, hipóteses legais para o tratamento e obrigações previstas na LGPD.

Destaca-se também a provável limitação dos direitos dos titulares previstos na LGPD, como acesso, correção, anonimização, bloqueio, eliminação e explicação que serão mais bem discutidos à frente. Além disso, a autodeterminação informativa é um pilar fundamental da LGPD para atuação do titular.

Ademais, destaca-se que a política de proteção de dados e privacidade é um instrumento de boas práticas previsto no art. 50 da LGPD. O supracitado artigo dispõe que controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Dispõe ainda no § 2º que o controlador ou operador demonstre o comprometimento em adotar as políticas internas que assegurem o cumprimento de normas e boas práticas relativas à proteção de dados pessoais, bem como estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade.

Nesse sentido, pode-se considerar a política como um instrumento interno de governança dotado de diretrizes e medidas em relação ao tratamento de dados desde a coleta até a eliminação dos dados. Esse conjunto de regras é endereçado aos funcionários ou entidades, públicas e privadas, que se relacionem com o controlador ou operador.

Outro documento relevante é o aviso de privacidade, cujo objetivo é dar transparência ao tratamento de dados pessoais para a sociedade em geral, principalmente ao titular de dados. A LGPD não fez previsão expressa desse instrumento de governança, mas existem diversas experiências internacionais sobre o tema.

Nesse sentido, considerando as regras de boas práticas e de governança, previstas no art. 50 da LGPD, é necessário a adoção, por parte do controlador, de processos e políticas internas que assegurem o cumprimento, de

forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais. A título de exemplo, a autoridade de proteção do Reino Unido (*Information Commissioner's Office – ICO*) publicou material orientativo sobre como fornecer a informação de privacidade aos titulares de dados.¹⁴

2. Boas Práticas sobre IA, Privacidade e Governança de Dados

Existem várias regras e boas práticas internacionais que abordam a governança dos dados, inclusive durante o procedimento de treinamento de sistemas de IA. Essas práticas são essenciais para garantir que os modelos sejam treinados de maneira ética, eficiente e segura. A seguir serão apresentadas duas boas práticas relevantes.

2.1 Organização para a Cooperação e o Desenvolvimento Econômico

A Organização para a Cooperação e o Desenvolvimento Econômico (OCDE)¹⁵ publicou documento que analisa a interseção entre privacidade e inteligência artificial, principalmente a IA generativa, que necessita de enormes volumes de dados para o aprendizado¹⁶. Essa análise foi realizada com base nos princípios orientadores incluídos nas Diretrizes de Privacidade da OCDE de 1980, atualizadas em 2013, e na Recomendação da OCDE sobre IA de 2019 (chamada “Recomendação da OCDE sobre IA”), atualizada em 2024.

Esta análise conclui que, apesar dos desafios, os desenvolvimentos inovadores, tecnológicos e regulatórios da IA são principalmente compatíveis com, e podem até reforçar, as regras de privacidade e proteção de dados pessoais.

O documento aponta possibilidades de semelhanças e divergências nos princípios de IA e privacidade.

Princípio 1.1: *Crescimento inclusivo, desenvolvimento sustentável e bem-estar.* O documento aponta alguns positivos benefícios sociais, como a melhoria na saúde e no combate às mudanças climáticas e na economia, como a redução de custos na produção de produtos e serviços por meio de IA. Entretanto,

14. ICO. What methods can we use to provide privacy information? Disponível em: <https://ico.org.uk/for-organisations/uk-g-dpr-guidance-and-resources/individual-rights/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/>. Acesso em: 03 de ago. 2024.

15. Organização para a Cooperação e o Desenvolvimento Econômico (OCDE). Organização econômica intergovernamental com 38 países membros, fundada em 1961 para estimular o progresso econômico e o comércio mundial.

16. OCDE. AI, *Data Governance and Privacy*. 2024. Disponível em: https://www.oecd.org/en/publications/ai-data-governance-and-privacy_2476b1a4-en.html. Acesso em: 04 de ago. 2024.

uma maior precisão dos sistemas pode gerar conflito com direitos de privacidade e de proteção de dados, pois são necessárias maiores quantidades de dados para o treinamento. O documento destaca que autoridades de proteção de dados e tribunais têm lidado com esses conflitos há muitos anos, aplicando mecanismos constitucionais para resolver conflitos entre direitos e interesses concorrentes em casos específicos, por exemplo, a aplicação do “teste de balanceamento” para identificar a proporcionalidade entre privacidade e sistemas de IA.

Princípio 1.2: *Respeito pelo Estado de direito, pelos direitos humanos e pelos valores democráticos, incluindo justiça e privacidade.* Esse princípio pode ser dividido em três categorias: preconceito e discriminação; privacidade e governança de dados; e direitos humanos e valores democráticos. A IA generativa, conforme desenvolvida, implantada e usada atualmente, na ausência de limites de proteção, amplia esses riscos devido à escala e ao escopo massivos da aplicação de tais sistemas e seus dados de treinamento de entrada durante sua fase de treinamento.

Princípio 1.3: *Transparência e explicabilidade.* O documento descreve que a transparência se baseia na divulgação responsável para garantir que as pessoas estejam cientes de que a IA está sendo usada em uma previsão, recomendação, decisão ou em uma interação (por exemplo, um *chatbot*). Destaca que divulgações importantes, como conscientizar as pessoas de que estão lidando com IA ou que seus dados pessoais estão sendo usados, são um objetivo comum da IA e da regulamentação de privacidade e vêm sendo cada vez mais discutidas no contexto da IA generativa, em que os *chatbots* surgiram como aplicações muito populares em todos os setores.

Sobre a explicabilidade e interpretabilidade, o documento aponta que estão presentes em discussões políticas tanto na comunidade de IA quanto na comunidade de privacidade. A complexidade e a natureza frequentemente de “caixa preta” dos sistemas de IA derivados de aprendizado de máquina, e particularmente modelos de IA generativos, tornam essas questões cada vez mais urgentes.

Princípio 1.4: *Robustez, segurança e proteção.* Esse princípio trata de medidas de segurança e proteção em relação ao tratamento de dados que devem ser adotadas.

Aborda que esse princípio converge amplamente com o princípio de segurança de dados nas Diretrizes de Privacidade da OCDE: “Os dados pessoais devem ser protegidos por salvaguardas de segurança razoáveis contra riscos

como perda ou acesso não autorizado, destruição, uso, modificação ou divulgação de dados”.¹⁷ O documento aponta que modelos robustos de aprendizado de máquina tradicionalmente precisam de grandes conjuntos de dados representativos para seu treinamento. Isso pode entrar em conflito com o princípio de minimização de dados¹⁸. Entretanto, algumas salvaguardas, como as Privacy Enhancing Technologies ((PETs) – podem ajudar a reduzir a lacuna entre o desenvolvimento de modelos de IA seguros e a proteção dos direitos de privacidade dos indivíduos.

Princípio 1.5: *Accountability*. O documento dispõe que tanto as comunidades de privacidade quanto as comunidades de IA desenvolveram abordagens para responsabilização e gerenciamento de riscos. Destaca trabalhos da OCDE sobre classificação de IA¹⁹ e responsabilização,²⁰ que fornecem uma estrutura detalhada e robusta para identificar riscos, partes interessadas relevantes e medidas de mitigação para sistemas de IA com base no ciclo de vida do sistema de IA.

2.2 Diretrizes da União Europeia para uma IA Confiável

A União Europeia publicou diretrizes para considerar uma IA de confiança. Uma IA de confiança, segundo o documento, seria composta por três elementos, que deveriam ser observadas ao longo de todo o ciclo de vida do sistema: a) ser legal, cumprindo toda a legislação e regulamentação aplicáveis; b) ser ética, garantindo a observância de princípios e valores éticos; e c) ser sólida, tanto do ponto de vista técnico como do ponto de vista social, uma vez que, mesmo com boas intenções, os sistemas de IA podem causar danos não intencionais.²¹

Em relação ao aspecto de privacidade e governança de dados, o documento dispõe que ligado ao princípio de prevenção de danos está o direito à privacidade, um direito fundamental que é particularmente afetado pelos sistemas de IA. A prevenção da ameaça à privacidade também exige uma governança

17. OCDE. *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. 1980. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>. Acesso em: 04 de nov. 2024.

18. OCDE. *AI, Data Governance and Privacy*. 2024. Disponível em: https://www.oecd.org/en/publications/ai-data-governance-and-privacy_2476b1a4-en.html. Acesso em: 04 de ago. 2024. Apud Global Privacy Assembly, *Resolution on Generative Artificial Intelligence Systems*, 2023.

19. OCDE. *AI, Data Governance and Privacy*. 2024. Disponível em: https://www.oecd.org/en/publications/ai-data-governance-and-privacy_2476b1a4-en.html. Acesso em: 04 de ago. Apud OCDE. “OECD Framework for the Classification of AI systems”, *OECD Digital Economy Papers*, No. 323, OECD Publishing, Paris, 2022.

20. OCDE. *AI, Data Governance and Privacy*. 2024. Disponível em: https://www.oecd.org/en/publications/ai-data-governance-and-privacy_2476b1a4-en.html. Acesso em: 04 de ago. Apud OCDE. “Advancing accountability in AI: Governing and managing risks throughout the lifecycle for trustworthy AI”, *OECD Digital Economy Papers*, No. 349, OECD Publishing, Paris, 2023.

21. UNIÃO EUROPEIA. *Ethics guidelines for trustworthy AI*. 2019. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>. Acesso em 04 de ago. 2024.

adequada dos dados, que assegure a qualidade e a integridade dos dados utilizados, a sua relevância para o domínio em que os sistemas de IA serão implantados, os seus protocolos de acesso e a capacidade de tratar os dados de modo a proteger a privacidade.

3. Análise dos Estudos de Caso de Extração de Dados para Treinamento de IA Generativa

A análise abordará dois casos relacionados à coleta de dados pessoais para treinamento de IA generativa e restringe-se à legislação brasileira.

O primeiro caso diz respeito à extração de dados da internet por meio de raspagem de dados e o segundo está relacionado à mudança da política de privacidade da Meta para coletar dados de sua plataforma para treinamento de IA generativa.

3.1 Extração de dados da internet por meio de raspagem de dados

Inicialmente, cabe mencionar que existe um enorme desafio em equilibrar as extrações da internet com os princípios, fundamentos e garantias previstos na LGPD.

As empresas alegam que precisam de uma enorme quantidade de dados pessoais para melhorar a acurácia das decisões automatizadas dos sistemas de IA. Entretanto, essa atividade de coleta de dados publicados na internet tem conflito com os princípios de finalidade, necessidade, livre acesso, transparência, responsabilização e prestação de contas, previstos no art. 6º da LGPD.

O princípio de finalidade é a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. Já o princípio da necessidade é a limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Quando um agente de tratamento de dados realiza a extração dos dados da internet sob o propósito de fazer treinamento de IA, alguns pontos ficam nebulosos e de difícil conformidade com a lei, como por exemplo, como considerar a finalidade de treinamento de IA sendo específica, como informar essa finalidade ao titular e como mensurar quais dados são necessários se as aplicações de IA genéricas podem ser as mais diversas?

A finalidade do treinamento de IA muitas vezes não é claramente definida, resultando em uma coleta de dados indiscriminada. Esta prática visa melhorar a eficácia dos sistemas de IA, mas contraria o princípio da necessidade.

Outro destaque está relacionado à autodeterminação informativa, fundamento da LGPD, com previsão no inciso II do art. 2º, que confere à pessoa titular de dados o direito de controlar seus próprios dados pessoais, com base nos preceitos da boa-fé e da transparência.

O titular de dados não pode exercer esse direito de controle dos seus dados, considerando que nem sabe que seus dados estão sendo tratados. A falta de conformidade com essas diretrizes pode levar a sérias consequências legais e comprometer a confiança dos usuários nos sistemas de IA.

Observa-se que a raspagem de dados é atividade de difícil conformidade com o princípio da transparência, considerando ser uma atividade silente que ocorre sem o conhecimento do titular de dados.

Em relação às hipóteses legais para a atividade de coleta de dados para treinamento de IA, previstas nos art. 7 e 11 da LGPD, a hipótese mais utilizada é o legítimo interesse.

A LGPD dispõe de parâmetros mais rígidos para o tratamento de dados com base nessa hipótese, nos termos do art. 10, como por exemplo, somente poderá fundamentar o tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas. Ademais, pode-se utilizá-la para a proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as suas legítimas expectativas e os direitos e liberdades fundamentais, nos termos da Lei.

Além disso, a ANPD publicou guia²² que expõe a necessidade de teste de balanceamento para avaliar se a atividade de tratamento não se sobrepõe aos direitos e liberdade fundamentais, bem como respeitou a legítima expectativa do titular. Não há que se falar em legítima expectativa nesse caso, tendo em vista que o titular desconhece do tratamento.

Com relação aos direitos dos titulares, o titular de dados fica prejudicado no exercício dos direitos previstos nos artigos 9º, 18 e 20, como, por exemplo, confirmação da existência de tratamento, acesso aos dados, anonimização, bloqueio ou eliminação de dados desnecessários. O fato de desconhecer do tratamento que está sendo realizado e de não possuir canais de comunicação claros com o controlador fragiliza todo o modelo legal constituído.

22. ANPD. *Guia Orientativo de Hipóteses Legais de Tratamento de Dados Pessoais: Legítimo Interesse*. 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em: 28 out. 2024.

O art. 20 dispõe sobre a obrigação do agente de tratamento de 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. Esse dispositivo trata do chamado direito da explicação, que dialoga com a boa prática de explicabilidade.

Outro aspecto debatido diz respeito a dados da internet já estarem públicos²³, se esses poderiam ser tratados sem o consentimento do titular. O art. 7º, § 4º da LGPD, dispõe que é dispensada a exigência do consentimento previsto para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos na Lei.

Ademais, cabe destacar também que o art. 7º, § 3º dispõe que o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

Então, mesmo que se considere que não há necessidade do consentimento do titular, a coleta de dados pessoais públicos para o treinamento de IA deve observar a finalidade, a boa-fé, os direitos e os princípios previstos na LGPD.

Cabe ressaltar que o legislador dispôs que não seria necessário a obtenção do consentimento, entretanto, para realizar o tratamento de dados será necessário utilizar alguma hipótese legal que autorize o tratamento.

Nesse sentido, observa-se que a raspagem de dados para sistemas de IA genéricos tem elevado potencial de desconformidade com a LGPD e não observa as melhores práticas para o desenvolvimento de sistemas de IA, notadamente transparência, explicabilidade, governança dos dados, responsabilização e prestação de contas. Entretanto, a utilização de IA, como já mencionado nesse artigo, é inegável para o desenvolvimento de novos modelos de negócio e soluções tecnológicas, sendo necessárias salvaguardas legais, técnicas e administrativas, que serão apresentadas no item 3.3, para reduzir os riscos aos direitos fundamentais de proteção dos dados e privacidade.

3.2 Coleta de dados do Meta para o treinamento da IA

Recentemente, a Meta anunciou uma nova política de privacidade que gerou preocupações entre os usuários. A Meta divulgou que a partir de 26 de junho de 2024, as postagens públicas dos usuários seriam utilizadas para treinar IA generativa, sem a necessidade de obter permissão prévia.

23. SOLOVE, Daniel J; HARTZOG, Woodrow. The Great Scrape: The Clash Between Scraping and Privacy. SSRN. 2024. Disponível em: <http://dx.doi.org/10.2139/ssrn.4884485>. Acesso em: 02 de ago. 2024.

A política de privacidade do Meta aborda que os dados coletados são compartilhados com as empresas do grupo econômico Meta, no qual destacam-se Facebook, Messenger, Instagram, dentre outros.

Em pesquisa realizada na política de privacidade do Meta,²⁴ observa-se que são coletados os seguintes dados:

- O conteúdo criado, como publicações, comentários ou áudios;
- O conteúdo fornecido por meio do nosso recurso de câmera, das configurações do rolo da câmera ou dos nossos recursos habilitados para voz;
- As mensagens enviadas e recebidas, incluindo o conteúdo, sujeitas às leis aplicáveis;
- Os metadados sobre conteúdo e mensagens, sujeitos às leis aplicáveis;
- Os tipos de conteúdo, incluindo anúncios, que o usuário vê ou com o qual interage e o modo como faz isso;
- Os apps e recursos usados e quais ações o usuário realiza neles;
- As compras ou outras transações que o usuário realiza, como nas experiências de finalização da compra da Meta, incluindo as informações de cartão de crédito;
- As hashtags usadas;
- O horário, a frequência e a duração das suas atividades nos produtos da Meta.

Esclarece ainda que coleta dados de contatos, como por exemplo, informações sobre amigos, seguidores, grupos, contas, páginas do Facebook e outros usuários e comunidades com quem os usuários têm conexão ou interação. A empresa informa que coleta o nome e endereço de e-mail ou telefone, caso seja carregado ou importado de um dispositivo, como ao sincronizar uma agenda de contatos.

A Meta descreve como realiza o tratamento para o treinamento da IA na central de privacidade e que o modelo de IA generativa é capaz de criar conteúdo quando uma pessoa dá instruções ou faz uma pergunta, como texto, imagens e áudio.

Esclarece que utiliza modelos que geram texto e imagem que precisam de quantidades massivas de dados para estimar e ter melhor eficácia.

24. META. *Política de Privacidade da Meta*. 2024. Disponível em: <https://pt-br.facebook.com/privacy/genai>. Acesso em: 04 de ago. 2024.

Dispõe também que realiza o tratamento dos dados com base em cinco pilares: privacidade e segurança, imparcialidade e inclusão, robustez e segurança, transparência e controle, governança e responsabilidade.

Descreve ainda que realiza o tratamento com base no legítimo interesse, da mesma maneira que realiza na região europeia e Reino Unido.

Diante da possível alteração da política de privacidade da Meta, a ANPD, por meio do Despacho nº 20/2024/PR/ANPD, publicado no D.O.U. em 02 de julho de 2024, consubstanciado pelo Voto nº 11/2024/DIR-MW/CD, da diretora Miriam Wimmer, proferiu medida preventiva determinando a imediata suspensão, no Brasil, da vigência da nova política de privacidade da empresa Meta, que autorizava o uso de dados pessoais publicados em suas plataformas para fins de treinamento de sistemas de IA.²⁵

A empresa teve seu pedido de reconsideração negado por meio do Despacho Decisório PR/ANPD nº 24/2024, considerando necessidade de postergação da análise dos pedidos de concessão de efeito suspensivo e do pedido de reconsideração integral da decisão, até a realização de análise técnica das medidas propostas considerando e apresentação de plano de conformidade pela Meta, com a especificação de prazos concretos para a implementação das medidas nos termos do art. 36 do Regulamento de Fiscalização (Resolução CD/ANPD nº 01/2021), ou de documentação que comprove a sua entrada em vigor, e a apresentação do teste de balanceamento da hipótese legal referente ao Legítimo Interesse, no prazo de até 10 (dez) dias úteis.

Entretanto, após apresentar todas as documentações solicitadas, o Despacho Decisório PR/ANPD nº 33/2024, com base no VOTO Nº 23/2024/DIR-JR/CD, decidiu suspender a decisão cautelar nos seguintes termos: (i) aprovar o plano de conformidade atualizado apresentado pela empresa, nos termos da fundamentação apresentada no voto nº 23/2024/DIR-JR/CD e na Nota Técnica nº 39/2024/FIS/CGF/ANPD; e (ii) suspender a medida preventiva aplicada à Meta pelo Conselho Diretor, conforme Despacho Decisório PR/ANPD nº 20/2024, com a determinação de cumprimento integral do plano de conformidade.

No aspecto de privacidade e proteção de dados, a determinação da suspensão baseou-se em quatro pontos importantes: hipótese legal, princípios da finalidade, necessidade e transparência, limitação aos direitos dos titulares e uso de dados pessoais de crianças e adolescentes.

25. ANPD. ANPD determina suspensão cautelar do tratamento de dados pessoais para treinamento da IA da Meta. 2024. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta>. Acesso em: 04 de ago. 2024.

Hipótese Legal

Segundo o voto da diretora que subsidiou a decisão da medida preventiva, no que tange sobre a hipótese legal, concluiu-se que o legítimo interesse não parece ser a base mais adequada para o tratamento, considerando que podem ser tratados dados pessoais sensíveis, notadamente diante da possibilidade de uso de imagens, áudios, textos e vídeos, que possam revelar vinculações políticas, religiosas e sexuais dos titulares, entre outros aspectos da personalidade indicados no art. 5º, II, da LGPD.

Destacou, ainda, que para o uso adequado da hipótese legal, o interesse deve ser fundamentado em situações concretas, isto é, situações reais, claras e precisas, que objetivem interesses específicos e bem delineados, ainda que em futuro próximo, o que afasta interesses considerados a partir de situações abstratas ou meramente especulativas.

Além disso, a análise concluiu que é razoável supor que, a princípio, não há expectativa por parte dos titulares de que informações postadas na rede social de anos atrás fossem utilizadas para treinamento de IA generativa.

O voto também abordou a finalidade, que chamou de finalidade genérica e ampla de treinamento de sistemas de IA generativa. Verificou-se que há fortes indícios de que o tratamento realizado pela empresa para treinamento de sistemas de IA não encontra amparo na hipótese legal do legítimo interesse, seja em razão do tratamento de dados sensíveis, seja em razão da violação às legítimas expectativas dos titulares, seja em razão do não atendimento aos princípios da finalidade e da necessidade.

Diante da análise da diretora de que o legítimo interesse não seria a hipótese legal mais adequada para o tratamento de dados com a finalidade de treinamento de IA generativa e considerando que existem dados sensíveis ou que provavelmente o tratamento revele dados sensíveis, somente o consentimento poderia ser a base legal utilizada.

Entretanto, caso fosse utilizada a base legal do legítimo interesse seriam necessárias ressalvas para a adequação do tratamento à LGPD. Primeiramente, seria necessária maior governança de dados no âmbito da coleta dos dados, levando em conta o inventário para identificar os tipos de dados tratados com objetivo de segregar aqueles que não seriam considerados sensíveis, ter o registro das operações, previsto no art. 37, e a elaboração do Relatório de Impacto à Proteção de Dados.

Além disso, seria necessário a elaboração do teste de balanceamento para avaliar a finalidade específica do treinamento, a necessidade dos dados e a

proporcionalidade do interesse do agente sobre os direitos fundamentais dos titulares, bem como a sua legítima expectativa.

Nesse sentido, o voto do diretor relator do pedido de reconsideração da empresa, com base na Nota Técnica nº 39/2024/FIS/CGF/ANPD, apontou que a empresa apresentou toda a documentação exigida, incluindo o teste de balanceamento de legítimo interesse, do qual constam informações mais detalhadas sobre o tratamento de dados pessoais para a finalidade de treinamento de sistema de IA generativa, além de diversas salvaguardas implementadas a fim de evitar a identificação de titulares e de dados pessoais de terceiros por meio de inferências.

Segundo a Nota Técnica nº 39/2024/FIS/CGF/ANPD, a empresa ao aplicar as salvaguardas que garantam a possibilidade de pseudonimização dos dados pessoais de usuários, com o objetivo de mitigar eventuais efeitos lesivos aos titulares derivados do tratamento, possibilita a incidência das hipóteses legais do art. 7º da LGPD para o tratamento de dados pessoais com vistas ao treinamento de modelos de IA generativa.

Ademais, concluiu que as medidas de transparência a serem implementadas e a facilitação do exercício da opção de “opt-out” também são elementos que fortalecem o respeito aos direitos e às legítimas expectativas dos titulares.

Transparência do tratamento de dados

Quanto à transparência, a análise da diretora que subsidiou a medida preventiva concluiu que foi caracterizada ausência de divulgação de informações claras, precisas e facilmente acessíveis sobre a alteração da política de privacidade para permitir a utilização de dados pessoais para fins de treinamento de IA.

No entanto, o voto do diretor que analisou o pedido de reconsideração apontou que a empresa aprimorou os mecanismos de disponibilização de informações relativas ao tratamento de dados para IA generativa. Além disso, o plano de conformidade apresentado inclui uma série de medidas, como notificações, atualizações na política de privacidade e a criação de uma área dedicada no site, o que demonstra alterações significativas para proporcionar maior transparência no atendimento às determinações da ANPD.

Sob esse aspecto, deve-se entender que a política de privacidade é documento de normatização interna direcionada aos funcionários ou pessoas físicas ou jurídicas que se relacionam com o agente. A transparência, segundo a LGPD, deve garantir que informações claras, precisas e facilmente acessíveis

sobre a realização do tratamento e os respectivos agentes de tratamento sejam acessadas pelo titular, observados os segredos comercial e industrial.

Nesse sentido, entende-se que o mecanismo de transparência mais adequado para informar o titular sobre o tratamento seja o aviso de privacidade. Deve-se atentar para o uso de meios de comunicação que consiga orientar os titulares de maneira clara e simples. Por exemplo, se envolver dados de crianças e adolescentes deve-se considerar 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.

Exercício dos direitos dos titulares

Em relação ao exercício dos direitos dos titulares, o voto da diretora que subsidiou a medida efetiva afirmou que parece haver obstáculos que limitam excessivamente o exercício dos direitos. Evidenciou que para exercer o direito de oposição, o titular precisa passar por diversas etapas, chegando à necessidade de clicar em oito opções no caso do aplicativo Facebook.

Sob esse aspecto, diferentemente da raspagem de dados pessoais da internet, o agente de tratamento tem condições de desenvolver soluções e canais em que o titular de dados possa exercer os direitos previstos na LGPD.

Caso o agente consiga justificar a utilização da base legal do legítimo interesse, é interessante ter mecanismos de *opt-out*, tendo em vista a previsão de eliminação de dados desnecessários, excessivos ou em desconformidade com a LGPD, que parece se enquadrar no caso.

O voto do diretor relator que analisou a suspensão da medida apontou que a empresa aprimorou os mecanismos de *opt-out*, facilitou o acesso ao exercício de direitos para usuários e não-usuários, diminuindo a quantidade de cliques necessários para acessá-los, além de medidas facilitadas de transparência, conforme mencionado acima, nos termos do que foi determinado pela ANPD.

Tratamento de dados de crianças e adolescentes

Relativamente ao tratamento de dados de crianças e adolescentes, o voto que subsidiou a medida preventiva apontou que não parecem estar presentes as salvaguardas necessárias para o tratamento de dados pessoais de crianças e adolescentes para fins de treinamento de sistemas de IA, notadamente com base na hipótese legal do legítimo interesse.

A hipótese legal de legítimo interesse pode ser utilizada para o tratamento de criança e adolescente. A ANPD publicou guia sobre a base legal de legítimo interesse²⁶ e ratificou seu entendimento da possibilidade de sua utilização para o tratamento de menores. Entretanto, segundo as análises da ANPD no caso concreto, seriam necessárias salvaguardas para garantir maior proteção aos direitos fundamentais desses titulares para o tratamento de dados para fins de treinamento de IA, especificamente com base na hipótese legal do legítimo interesse.

Nesse sentido, a empresa apresentou, em seu plano de conformidade, que não será realizado tratamento de dados pessoais de contas de usuários menores de 18 anos com o intuito de treinar e desenvolver seus modelos de IA generativa, afastando os riscos a essa categoria de titulares por ora. No entanto, a Meta ressaltou que continuaria a discutir com a ANPD, no âmbito do processo de fiscalização em andamento, a legitimidade do tratamento de dados pessoais dessa categoria de titulares.

Nesse sentido, destaca-se que, na Europa, a Meta anunciou que “não está treinando os seus modelos Llama com conteúdos gerados por contas de Europeus com idade inferior a 18 anos”.²⁷

3.3 Possíveis Soluções Regulatórias

O artigo escrito por *Solove e Hartzog*²⁸ aponta algumas possíveis soluções, dentre as quais destaca-se, sob o aspecto de proteção de dados e privacidade, o banimento da raspagem de dados para uso em treinamento de IA generativa e o uso do consentimento. O artigo também propõe uma agenda para reguladores composta de quatro princípios que abrangem riscos e danos razoáveis, benefícios para a sociedade, processos de transparência, responsabilização e prestação de contas e proteção aos dados utilizados para o treinamento de IA.

Cabe destacar, ainda, que podem ser buscadas medidas técnicas ou de salvaguarda para aprimorar a coleta dos dados para o treinamento de sistemas de IA, notadamente com base na hipótese legal do legítimo interesse e, assim, garantir os direitos fundamentais.

O dado pessoal, segundo a LGPD, é a informação relacionada à pessoa natural identificada ou identificável. Para o treinamento dos sistemas de IA não parece haver necessidade de identificar o titular. Assim, parece haver sentido

26. ANPD. *Guia orientativo de hipóteses legais de tratamento de dados pessoais: Legítimo Interesse*. 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em 03 nov. 2024.

27. META. *Building AI Technology for Europeans in a Transparent and Responsible Way*. 2024. <https://about.fb.com/news/2024/06/building-ai-technology-for-europeans-in-a-transparent-and-responsible-way/>, Acesso em 04 nov. 2024.

28. SOLOVE, Daniel J; HARTZOG, Woodrow. *The Great Scrape: The Clash Between Scraping and Privacy*. SSRN. 2024. Disponível em: <http://dx.doi.org/10.2139/ssrn.4884485>. Acesso em: 02 de ago. 2024.

utilizar técnicas que garantam a não identificação da pessoa, como anonimização ou pseudonimização.

As técnicas de Tecnologias de Aprimoramento da Privacidade (em inglês: *Privacy-Enhancing Technologies* –PETs), que são um conjunto de ferramentas e metodologias projetadas para proteger a privacidade e a segurança dos dados pessoais durante a coleta, tratamento e armazenamento, bem como o uso de aprendizado profundo que criam dados sintéticos, podem ajudar a solucionar os problemas regulatórios para o uso de dados pessoais no treinamento de IA generativa.²⁹

Caso a hipótese legal utilizada seja o legítimo interesse, considera-se necessário o direito de oposição (*opt-out*) para que o titular tenha opção de não ter seus dados pessoais tratados para essa finalidade.

Nesse sentido, a autoridade de proteção de dados da França, a Commission Nationale de l'Informatique et des Libertés (CNIL), em recente publicação de consulta pública³⁰, sugeriu em relação ao treinamento de IA algumas salvaguardas, dentre elas destaca-se anonimização ou pseudonimização, uso de dados sintéticos, maior transparência do tratamento dos dados, desenvolvimento de sistemas mais transparentes e auditáveis e facilitação do exercício dos direitos.

Considerações Finais

A pesquisa evidenciou enormes desafios regulatórios, sob o aspecto de proteção de dados e privacidade, que deverão ser enfrentados para o desenvolvimento de soluções de IA generativa éticas e responsáveis e que tragam confiança e benefícios para a sociedade.

A proteção de dados e privacidade não pode ser objeto de limitação de inovação e novos modelos de negócio, entretanto, o agente de tratamento precisa observar os princípios e as garantias previstas na LGPD para proporcionar um ambiente de maior confiança e segurança para o desenvolvimento de sistemas de IA.

A governança de dados, a transparência, a responsabilização e a prestação de contas são pilares fundamentais para a utilização ética e legal dos dados no treinamento de IA generativa. Esses princípios garantem que as práticas estejam em conformidade com as legislações e regulamentações e ajudam a construir um ambiente de convicção e estabilidade para toda a sociedade.

29. PANGHANGAM. Nivarthi, K. S. How Privacy-Enhanced Technologies (Pets) are Transforming Digital Healthcare Delivery. *American Scientific Research Journal for Engineering, Technology, and Sciences*, 90(1), 351–361. 2022. Disponível em: https://asrjetsjournal.org/index.php/American_Scientific_Journal/article/view/8268. Acesso em 04 de nov. 2024.

30. CNIL. Relying on the legal basis of legitimate interests to develop an AI system. Disponível em: <https://www.cnil.fr/en/relying-legal-basis-legitimate-interests-develop-ai-system>. Acesso em 04 nov 2024.

A utilização de técnicas de anonimização ou pseudonimização, notadamente Tecnologias de Aprimoramento da Privacidade (PET), uso de dados sintéticos, medidas de transparência do tratamento e de favorecimento dos exercícios dos direitos pode apoiar na garantia dos direitos fundamentais de proteção de dados e de privacidade durante o tratamento de dados pessoais com vista ao treinamento de sistemas de IA generativa.

A atuação da ANPD, no caso de alteração da Política de Privacidade da Meta, está alinhada às preocupações internacionais debatidas nas academias e nas autoridades públicas sobre a coleta excessiva de dados para o treinamento de IA generativa.

A pesquisa pode evoluir para avaliar as oportunidades de soluções regulatórias e seus impactos nos direitos fundamentais de proteção de dados e privacidade, na inovação e no desenvolvimento socioeconômico.

Referências

ANPD. *ANPD determina suspensão cautelar do tratamento de dados pessoais para treinamento da IA da Meta*. 2024. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta>. Acesso em: 04 de ago. 2024.

ANPD. *Guia Orientativo de Hipóteses Legais de Tratamento de Dados Pessoais: Legítimo Interesse*. 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em: 28 out. 2024.

BARRADI, Thomas, OpenAI Offering Media Outlets as Little as \$1M to Use News Articles for AI Models, *New York Post*. 2024.

CARPRARO, Valerio, et al. The impact of generative artificial intelligence on socioeconomic inequalities and policy making. *Pnax Nexus*. 2024, 3, 191 p. Disponível em: <https://doi.org/10.1093/pnasnexus/pgae191>. Acesso em: 29 de jul. 2024.

CNIL. Relying on the legal basis of legitimate interests to develop an AI system. Disponível em: <https://www.cnil.fr/en/relying-legal-basis-legitimate-interests-develop-ai-system>. Acesso em 04 nov 2024.

GOODFELLOW, I., Bengio, Y., & Courville, A. *Deep Learning*. MIT Press. 2016.

<https://about.fb.com/news/2024/06/building-ai-technology-for-europeans-in-a-transparent-and-responsible-way/>. Acesso em 04 nov. 2024.

HUMAN RIGHTS WATCH. Brasil: *Fotos de crianças são usadas indevidamente para alimentar IA*. 2024. Disponível em: <https://www.hrw.org/pt/news/2024/06/10/brazil-childrens-personal-photos-misused-power-ai-tools>. Acesso em: 02 de ago. 2024.

ICO. What methods can we use to provide privacy information? Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/>. Acesso em: 03 de ago. 2024.

META. Building AI Technology for Europeans in a Transparent and Responsible Way. 2024.

META. *Política de Privacidade da Meta*. 2024. Disponível em: <https://pt-br.facebook.com/privacy/genai>. Acesso em: 04 de ago. 2024.

MITCHELL, Tom. *Machine Learning*. 1997. McGraw-Hill.

MOHRI, M; Rostamizadeh, A; Talwalkar, A. *Foundations of Machine Learning*. Second Edition. MIT Press. 2018.

OCDE. AI, *Data Governance and Privacy*. 2024. Disponível em: https://www.oecd.org/en/publications/ai-data-governance-and-privacy_2476b1a4-en.html. Acesso em: 04 de ago. 2024.

OCDE. *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. 1980. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>. Acesso em: 04 de nov. 2024.

Organização para a Cooperação e o Desenvolvimento Econômico (OCDE). Organização econômica intergovernamental com 38 países membros, fundada em 1961 para estimular o progresso econômico e o comércio mundial.

PANGHANGAM, Nivarthi, K. S. How Privacy-Enhanced Technologies (Pets) are Transforming Digital Healthcare Delivery. *American Scientific Research Journal for Engineering, Technology, and Sciences*, 90(1), 351–361. 2022. Disponível em: https://asrjetsjournal.org/index.php/American_Scientific_Journal/article/view/8268. Acesso em 04 de nov. 2024.

SAÚDE, Sandra; BARROS, João Paulo; ALMEIDA, Inês. Impacts of Generative Artificial Intelligence in Higher Education: Research Trends and Students' Perceptions. *Social Sciences*. 2024, 13, 410 p. Disponível em: <https://doi.org/10.3390/socsci13080410>. Acesso em: 27 de jul. 2024.

SOLOVE, Daniel J; HARTZOG, Woodrow. The Great Scrape: The Clash Between Scraping and Privacy. *SSRN*. 2024. Disponível em: <http://dx.doi.org/10.2139/ssrn.4884485>. Acesso em: 02 de ago. 2024.

SPRINGER NATURE. Tools such as ChatGPT threaten transparent science; here are our ground rules for their use. *Nature*. 2023. 613 p. Disponível em: doi: <https://doi.org/10.1038/d41586-023-00191-1>. Acesso em: 02 de ago. 2024.

UNIÃO EUROPEIA. *Artificial Intelligence Act*. 2024. Disponível em: <https://artificialintelligenceact.eu/ai-act-explorer/>. Acesso em: 03 de ago. 2024.

UNIÃO EUROPEIA. *Ethics guidelines for trustworthy AI*. 2019. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>. Acesso em 04 de ago. 2024.

ZHANG, Peng; BOULOS, Maged N.Kamel. Generative AI in Medicine and Healthcare: Promises, Opportunities and Challenges. *Future Internet*. 2023, 15, 286 p. Disponível em: <https://doi.org/10.3390/fi15090286>. Acesso em: 01 de ago. 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

5

Classificação de danos decorrentes de incidentes de IA

VINICIUS AZEVEDO COELHO

Sumário: Introdução. 1. Incidentes decorrentes de sistemas de inteligência artificial. 2. Tipos de danos relacionados a incidentes de IA. 3. Níveis de criticidade de danos em incidentes de IA. Considerações finais. Referências.

Introdução

Na sociedade em rede, as tecnologias de informação e de comunicação revolucionaram a forma como as pessoas interagem e se relacionam. Segundo o sociólogo Manuel Castells, um dos principais teóricos da era da informação, a transformação digital alterou profundamente a sociabilidade humana, com impactos que transcendem as fronteiras geográficas e culturais².

Entre essas tecnologias, a inteligência artificial (IA) destaca-se como um agente de mudança particularmente poderoso. Sua evolução rápida e contínua tem o potencial de remodelar setores inteiros, desde a economia até a ciência, promovendo um crescimento inclusivo e sustentável, e possibilitando avanços científicos significativos. Além disso, sua capacidade de integrar e analisar dados de várias fontes aprimora a tomada de decisões e a automação de processos complexos, demonstrando sua ampla utilidade em diferentes sistemas³.

Por exemplo, no comércio, a IA contribui para a automação de tarefas, personalização de experiências do cliente e previsão de tendências de mercado⁴. Na saúde, ela é usada para diagnóstico de doenças, desenvolvimento de tratamentos e atendimento personalizado⁵. No transporte, a IA está presente no desenvolvimento de carros autônomos, na melhoria da segurança e eficiência do transporte público e na gestão de tráfego⁶. No meio ambiente, auxilia no monitoramento da qualidade do ar e da água, no desenvolvimento de energias renováveis e na redução da poluição⁷. Na ciência, acelera a pesquisa, testa

1. Pós-graduando em Direito Digital pelo ITS/UERJ. E-mail: viniciusazedocoelho@gmail.com.

2. CASTELLS, Manuel. A era da informação: economia, sociedade e cultura, v. 1 - *A sociedade em rede*. Tradução de Roneide Venâncio Majer. 17. ed. São Paulo: Paz e Terra, 2016.

3. BALTRUŠAITIS, T.; AHUJA, C.; MORENCY, L. P. Multimodal Machine Learning: A Survey and Taxonomy. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, v. 41, n. 2, p. 423-443, 2019. DOI: 10.1109/TPAMI.2018.2798607.

4. Por exemplo, a IA já está sendo usada para recomendar produtos aos clientes com base em seus históricos de compras, e para prever a demanda por produtos e serviços.

5. A título ilustrativo, a IA já está sendo usada para desenvolver softwares que podem diagnosticar câncer com mais precisão do que os médicos, e para criar robôs que podem realizar cirurgias com mais precisão e segurança.

6. Por exemplo, a IA já está sendo usada para desenvolver carros autônomos que podem dirigir sem a intervenção humana, e para criar sistemas que podem gerenciar o tráfego em tempo real para reduzir congestionamentos.

7. A IA já está sendo usada para desenvolver sensores que podem monitorar a qualidade do ar em tempo real, e para criar sistemas que podem gerar energia solar e eólica de forma mais eficiente.

hipóteses, descobre novos medicamentos e desenvolve novas tecnologias⁸. Esses são alguns exemplos de como a IA pode transformar a sociedade. À medida que a tecnologia continua a se desenvolver, a IA terá um impacto ainda maior em nossas vidas.

No entanto, apesar de seus impactos transformativos, a IA também traz consigo uma série de riscos e desafios éticos. Esses riscos podem variar desde questões de privacidade e segurança até impactos sociais e econômicos mais amplos, podendo acarretar incidentes com danos substanciais. A compreensão e gestão dessas consequências adversas são fundamentais para assegurar que os benefícios da IA sejam maximizados, enquanto seus danos são minimizados.

Os incidentes de IA podem ser causados por uma variedade de fatores, incluindo vulnerabilidades sistêmicas, falhas humanas e ataques cibernéticos. Esses incidentes podem causar uma série de consequências negativas, tais como danos físicos e ambientais, e impactos reputacionais e financeiros. Os danos podem ter diferentes níveis de criticidade, desde impactos insignificantes até danos à propriedade, à saúde, em infraestruturas críticas e até mesmo causar mortes humanas. Nesse cenário, avaliar e classificar os danos é parte fundamental para uma resposta efetiva a incidentes de IA, e tem como intuito primordial mitigar consequências e proteger organizações e usuários de sistemas baseados em inteligência artificial.

Nesse contexto, o objetivo geral deste artigo será mapear e identificar os principais conceitos relacionados a danos decorrentes de incidentes de segurança de IA. Assim, espera-se que seja possível categorizar e compreender incidentes envolvendo IA e suas principais consequências, bem como elaborar quadros gerais indicando os tipos de danos decorrentes de incidentes de IA e seus níveis de criticidade. As duas questões-problema que orientaram a elaboração desta pesquisa foram: 1. Quais os tipos de danos relacionados aos diferentes sistemas de IA? e 2. Quais os níveis de criticidade dos danos decorrentes de incidentes de IA?.

Este trabalho parte, então, da problemática central de mapear e identificar os tipos de danos causados por incidentes de segurança em sistemas de inteligência artificial, bem como avaliar os níveis de criticidade desses danos. Este problema é relevante porque a crescente adoção de sistemas de IA em diversas áreas da sociedade aumenta a exposição a riscos associados a in-

8. Atualmente, a IA já está sendo empregada para analisar grandes conjuntos de dados científicos, bem como para criar modelos que podem prever o comportamento de moléculas e materiais.

cidentes de segurança. A falta de uma classificação clara e precisa desses danos dificulta a resposta adequada a tais incidentes, comprometendo tanto a mitigação dos impactos quanto a formulação de políticas de segurança eficazes. A pesquisa busca responder às questões sobre os tipos de danos que podem surgir e como eles variam em termos de criticidade, contribuindo para um entendimento dos desafios impostos pela IA e para o desenvolvimento de medidas que possam garantir um uso mais seguro dessas tecnologias.

A metodologia escolhida para buscar respostas para as questões-problema inclui revisão bibliográfica, especificamente em relação à base conceitual e terminológica, tendo como fontes primárias textos publicados por autores especializados em segurança cibernética, tecnologia da informação e inteligência artificial.

Além disso, este estudo também recorre às publicações de organizações internacionais, como a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), o Instituto Nacional de Padrões e Tecnologia (NIST) dos Estados Unidos e a União Europeia sobre incidentes em IA e suas consequências. Essas organizações têm publicado documentos sobre o tema da segurança da informação em IA, que podem ser úteis para pesquisadores e profissionais da área. Ainda em relação às fontes de pesquisa, para buscar exemplos práticos de incidentes de IA, utilizamos a plataforma AI Incident Database (<https://incidentdatabase.ai>), que coleta, categoriza e compartilha informações sobre incidentes envolvendo sistemas de inteligência artificial. Essa base de dados serve como um recurso para pesquisadores, desenvolvedores e formuladores de políticas, ajudando-os a entender melhor os danos associados à IA.

Os resultados desta pesquisa foram estruturados da seguinte forma: o primeiro tópico explora as definições essenciais para seu desenvolvimento, e é dedicado às definições de incidentes em IA e de dano. O segundo tópico trata dos tipos de danos em espécie. O terceiro e último tópico discute níveis de criticidade de danos decorrentes de incidentes de IA.

1. Incidentes decorrentes de sistemas de inteligência artificial

Este tópico introduz os conceitos fundamentais para a compreensão e desenvolvimento da pesquisa. Seu propósito é apresentar noções relacionadas à inteligência artificial e abordar, de forma sumária, a ideia de riscos relacionados a sistemas que utilizam IA, para então chegar a uma definição de incidentes decorrentes de IA.

Para o significado de inteligência artificial, foram utilizadas as contribuições de autores como McCarthy, Newell e Simon e Boden. Para as noções de risco e de dano, recorreu-se à teoria do sociólogo alemão Niklas Luhmann, que enfatiza a importância de uma avaliação dos impactos sociais em sua teoria do risco. Esta abordagem, com viés sociológico, foi preferida em detrimento de um tratamento quantitativo de risco, típico das ciências exatas.

A própria definição de inteligência artificial é desafiadora, por si só. Maria Regina Rigolon Korkmaz destaca que a busca polêmica por replicar a compreensão humana aparece em vários registros históricos, com o objetivo de entender os fundamentos do pensamento e da memória, seja de forma filosófica, fisiológica ou biológica. Não é por coincidência que a definição inicial de inteligência artificial, amplamente debatida, surgiu como uma área específica da informática voltada a desenvolver computadores que possam imitar a inteligência humana na execução de tarefas⁹.

Essa definição inicial, proposta por John McCarthy¹⁰, considerado por muitos o criador do termo, descreve a inteligência artificial como a engenharia de máquinas inteligentes. Isto é, máquinas que demonstram características associadas à inteligência humana. Na famigerada proposta de conferência, McCarthy e seus colegas se basearam na ideia de que “todo aspecto de aprendizado ou qualquer característica da inteligência consegue, por princípio, ser tão precisamente descrito que uma máquina pode ser criada para simulá-la”¹¹.

Algumas décadas depois, Allen Newell e Herbert Simon¹² incorporaram à definição a ideia de sistema cognitivo, indicando um sistema que pode aprender e resolver problemas de forma autônoma. Em uma das definições mais influentes sobre o tema, eles conceituaram a IA como forma de criar sistemas inteligentes¹³.

Margaret Boden, uma das principais especialistas em IA na atualidade, define IA como o modo de criar sistemas que possam pensar, aprender e agir de forma inteligente¹⁴.

9. KORKMAZ, Maria Regina Rigolon. *Decisões Automatizadas: explicação, revisão e proteção na era da inteligência artificial*. São Paulo: Thomson Reuters Brasil, 2023, p. 95.

10. McCarthy foi um premiado cientista da computação estadunidense, e utilizou o conceito de IA pela primeira vez em um convite para uma conferência acadêmica sobre o tema, que foi realizada no verão de 1956 na Universidade de Dartmouth.

11. MCCARTHY, John. *Proposta para o Dartmouth Summer Research Project on Artificial Intelligence*. Dartmouth College, 1955.

12. Newell e Simon foram pesquisadores norte-americanos. Receberam o Prêmio Turing de 1975 por suas contribuições sobre inteligência artificial relacionada à ciência cognitiva.

13. NEWELL, Allen; Simon, Herbert A. *Computer science as empirical inquiry: Symbols and search*. Communications of the ACM 19.3 (1976): 113-126.

14. BODEN, Margaret A. *Artificial intelligence: A very short introduction*. Oxford University Press, 2018.

Essas definições destacam diversos aspectos da IA. A definição de McCarthy enfatiza a criação de máquinas que exibem características inteligentes relacionadas até então ao comportamento humano. A definição de Newell e Simon destaca a criação de sistemas que podem aprender e resolver problemas de forma autônoma. A definição de Boden ressalta a criação de sistemas que podem atuar de forma inteligente.

É importante destacar que não existe um consenso sobre o que define inteligência artificial. Hoje, o termo é considerado um conceito abrangente, englobando aplicações bastante distintas, seja em relação a determinadas estruturas matemáticas, seja quanto às suas utilizações práticas¹⁵.

Embora diferentes ou complementares, essas definições nos mostram a versatilidade dessa nova tecnologia, capaz de ser utilizada em sistemas simples ou complexos. A compreensão dessa multivalência de sistemas de IA é relevante para uma compreensão adequada dos riscos e danos decorrentes de cada tipo.

Isso porque utilizações simples de inteligência artificial geralmente envolvem tarefas específicas e limitadas, como chatbots de atendimento a clientes, que usam processamento de linguagem natural para responder perguntas frequentes. Outro exemplo é a recomendação de produtos em e-commerce, em que algoritmos analisam histórico de compras e preferências do usuário para sugerir itens. Os riscos associados a essas utilizações simples são relativamente baixos, podendo incluir erros na compreensão de linguagem ou sugestões inadequadas, que normalmente resultam em pequenas insatisfações dos usuários e impacto limitado.

Por outro lado, utilizações complexas de inteligência artificial envolvem sistemas mais sofisticados e integrados, como veículos autônomos, que utilizam múltiplas fontes de dados (sensores, câmeras, GPS) para navegar e tomar decisões em tempo real. Outro exemplo é a análise preditiva em saúde, em que a IA processa grandes volumes de dados médicos para prever surtos de doenças ou personalizar tratamentos. Os riscos e consequências danosas dessas aplicações complexas são significativamente maiores, incluindo acidentes de trânsito fatais em caso de falha de um veículo autônomo ou diagnósticos médicos incorretos que podem levar a tratamentos inadequados. Portanto, enquanto os sistemas simples apresentam riscos menores e mais controláveis,

15. KORKMAZ, Maria Regina Rigolon. *Decisões Automatizadas: explicação, revisão e proteção na era da inteligência artificial*. São Paulo: Thomsom Reuters Brasil, 2023, p. 98.

as aplicações complexas requerem uma maior robustez, transparência e regulamentação para mitigar impactos potencialmente graves.

Para compreensão do risco, no escopo deste estudo, recorreu-se à perspectiva social de Niklas Luhmann¹⁶. De acordo com o autor, os riscos são inerentes à própria modernização da sociedade, cada vez mais contingente. Para Luhmann, cada vez mais o futuro da sociedade depende da tomada de decisão: o futuro se transforma em risco na medida em que aumentam as possibilidades

Luhmann propõe um conceito de risco que supõe a existência de incerteza quanto a danos futuros: fala-se de risco quando o dano provável é a consequência de uma ação. Para Luhmann, o conceito de risco está associado à condição de decisão. Toda decisão implica a possibilidade de que algo dê errado, ou seja, de que um risco se materialize em dano. Assim, o risco é a probabilidade de que um evento indesejável ocorra como resultado de uma decisão¹⁷. Tecnologias avançadas como a IA tornam a complexidade social cada vez maior, e fazem com que seja mais difícil prever e medir consequências.

Portanto, com base na teoria luhmanniana, os riscos são uma consequência inevitável da modernização e complexificação da sociedade. Para o contexto da inteligência artificial, essa perspectiva é particularmente relevante, pois a implementação de sistemas de IA em diversas esferas da vida moderna exemplifica essa complexidade crescente. Cada aplicação de IA, desde simples chatbots até veículos autônomos, envolve decisões que podem potencialmente transformar o futuro em um campo de incertezas. A capacidade de prever e controlar as consequências de tais decisões se torna cada vez mais desafiadora à medida que a tecnologia avança, aumentando as possibilidades e, conseqüentemente, os riscos.

Vimos que Luhmann sustenta que o risco é inerente à condição de decisão, onde qualquer escolha carrega a probabilidade de resultar em danos. Assim, aplicando isso à IA, cada implementação de um sistema de inteligência artificial envolve decisões sobre algoritmos, dados e contextos de aplicação que podem falhar ou produzir resultados indesejados. Por exemplo, um sistema de reconhecimento visual baseado em biometria em espaços públicos pode identificar erroneamente indivíduos, resultando em falsas acusações ou violações de privacidade. Essas decisões tecnológicas, embora projetadas para melhorar a segurança e a eficiência, carregam o risco de materialização de danos significativos à liberdade e à privacidade dos cidadãos.

16. Na sociologia do risco, Luhmann revela sua preocupação com a falta de precisão do conceito e a dificuldade que as *hard sciences* encontravam para analisar adequadamente o problema do risco. Seus conceitos eram vagos e baseados em modelos quantitativos. Luhmann propõe, então, uma avaliação dos riscos enquanto um problema social, amparados em fatores sociais.

17. LUHMANN, Niklas. *Risk: A Sociological Theory*. New York: Routledge, 1993.

À medida que a sociedade se torna mais dependente de tecnologias avançadas como a IA, a complexidade social aumenta, dificultando a previsão e mitigação de consequências adversas. Os riscos associados a sistemas complexos de IA, como veículos autônomos ou sistemas de vigilância, ilustram essa dificuldade. A incerteza quanto aos danos futuros é ampliada pela natureza contingente das decisões tecnológicas, onde a falha de um sistema pode ter consequências catastróficas.

Assim, com base nos elementos estudados até então, podemos definir risco em IA como a possibilidade incerta de ocorrência de uma consequência indesejável, decorrente de uma decisão tomada por um sistema baseado em inteligência artificial.

A materialização do risco em dano caracteriza um incidente de IA. Segundo a taxonomia do CSET, danos causados pela IA têm quatro elementos que, uma vez corretamente definidos, permitem a identificação dos danos causados pela IA. Estes componentes-chave servem para distinguir os danos dos não danos e os danos causados pela IA dos danos não causados pela IA. Para haver um dano causado pela IA, tem de haver: (1) uma entidade que sofreu (pode ser uma pessoa, coisa ou lugar); (2) um evento ou problema de dano que (3) possa estar diretamente ligado a uma consequência do comportamento de (4) um sistema de IA. Os quatro elementos têm de estar presentes para que haja danos causados pela IA¹⁸.

Adicionalmente, de acordo com um estudo realizado pela OECD para definição de incidente de IA, o dano é expresso como a probabilidade de que um prejuízo realmente ocorra¹⁹. O risco é uma função tanto da probabilidade de um evento ocorrer quanto da gravidade das consequências que resultariam. Nesse contexto, é necessário compreender e gerenciar riscos e danos relacionados à IA para garantir sua confiabilidade e uso seguro e responsável. Segundo estudo da OECD²⁰:

Definir o dano e avaliar seus tipos, níveis de gravidade e outras dimensões relevantes (por exemplo, escopo, escala geográfica, quantificação etc.) é fundamental para identificar os incidentes que levam ou podem levar a esse dano e elaborar um quadro eficaz para abordá-los²¹.

18. CENTRE FOR SECURITY AND EMERGING TECHNOLOGY (CSET). *CSET V1 AI Annotation Guide*. CSET, 2023.

19. OECD. *Stocktaking for the development of an AI incident definition*. Paris: OECD, 2023. 36 p. Disponível em: <https://www.oecd.org/publications/stocktaking-for-the-development-of-an-ai-incident-definition-c323ac71-en.htm>. Acesso em: 17 jan. 2024.

20. *Ibidem*, p. 8.

21. Tradução livre do original: “Defining harm and assessing its types, severity levels and other relevant dimensions (e.g. scope, geographic scale, quantifiability, etc.) is key to identifying the incidents that lead or might lead to that harm, and to elaborate an effective framework to address them”.

Tem-se, então, que a ideia de dano como consequência do risco é central para a compreensão de incidentes de IA. Feitas essas considerações, passa-se pela definição de incidentes de IA.

Amodei et al., no artigo *Concrete Problems in AI Safety*, descrevem incidentes de IA como eventos onde um sistema de inteligência artificial se comporta de maneira não intencional ou prejudicial devido a problemas como falhas de especificação, erros de robustez, falhas de escalabilidade, ou complexidade de segurança²².

Crawford e Calo, em *There is a Blind Spot in AI Research*, definem incidentes de IA como eventos onde tecnologias de inteligência artificial causam danos ou falham em operar conforme o esperado, geralmente devido a limitações na pesquisa e desenvolvimento que não consideram plenamente os seus impactos sociais e éticos²³.

Além dos autores acima, algumas organizações também trazem definições relevantes para incidentes de IA. Segundo a taxonomia do CSET desenvolvida para a AI Incident Database, incidentes de IA envolvem falhas ou quase falhas realizadas no mundo real pelo uso de sistemas de inteligência artificial²⁴. De forma complementar, o AI Index Report 2024 – Stanford HAI conceitua incidentes de IA como eventos em que sistemas de inteligência artificial apresentam mau funcionamento ou comportamento inesperado, resultando em consequências adversas. Esses incidentes podem incluir falhas técnicas, vieses em decisões automatizadas, ou violações de privacidade e segurança²⁵. Já a definição proposta pela OECD para incidente de IA diz que²⁶:

Incidente de IA: um evento no qual o desenvolvimento ou o uso de um sistema de IA:

- (i) causou dano a pessoa(s), propriedade ou ao meio ambiente;
- (ii) impactou direitos humanos, incluindo privacidade e não discriminação²⁷.

22. AMODEI, D. et al. *Concrete Problems in AI Safety*. 2016. Disponível em: <https://arxiv.org/abs/1606.06565>. Acesso em: 6 ago. 2024, p. 1-2.

23. Crawford, K., Calo, R. *There is a blind spot in AI research*. *Nature* 538, (2016). <https://doi.org/10.1038/538311a>. Acesso em: 07 ago. 2024, pp. 311-313.

24. AI Incident Database. *CSET Taxonomy AI Incident Database*. Disponível em: <https://incidentdatabase.ai/taxonomy/cset/>. Acesso em: 07 ago. 2024.

25. Stanford HAI. *AI Index Report 2024*. Stanford Institute for Human-Centered Artificial Intelligence, 2024. Disponível em: https://aiindex.stanford.edu/wp-content/uploads/2024/04/HAI_2024_AI-Index-Report.pdf. Acesso em: 07 ago. 2024.

26. OECD. *Stocktaking for the development of an AI incident definition*. Paris: OECD, 2023. 36 p. Disponível em: <https://www.oecd.org/publications/stocktaking-for-the-development-of-an-ai-incident-definition-c323ac71-en.htm>. Acesso em: 17 jan. 2024, p. 11.

27. Tradução livre do original: “AI Incident: an event where the development or use of an AI system: (i) caused harm to person(s), property, or the environment; or (ii) infringed upon human rights, including privacy and non-discrimination”.

Assim, com base nas contribuições acima, para fins deste estudo, um incidente de IA será considerado como um evento ou situação em que um sistema de IA falha ou se comporta de maneira inesperada, resultando em consequências negativas. Isso pode incluir erros técnicos, mau funcionamento, decisões incorretas ou vieses que levam a resultados prejudiciais para indivíduos, organizações ou a sociedade em geral. Esses incidentes podem ocorrer devido a problemas na concepção, treinamento, implementação ou operação dos sistemas de IA. Os tipos de danos relacionados a incidentes de IA serão tratados no tópico seguinte.

2. Tipos de danos relacionados a incidentes de IA

O aumento do uso de sistemas de IA em todo o mundo leva a um aumento no número de sistemas de IA, que, como visto no tópico anterior, podem causar danos reais a pessoas, organizações e ao meio ambiente.

As consequências indesejáveis relacionadas a sistemas de IA diferem dos riscos tradicionais de cibersegurança de diversas formas²⁸. Essa diferença surge, em parte, da natureza intrínseca dos sistemas de IA, que dependem intensamente de grandes volumes de dados para operar eficientemente. Este requisito por si só introduz problemas como a qualidade dos dados e o viés, que podem distorcer os resultados e as decisões tomadas pela IA. A precisão e a imparcialidade dos dados tornam-se, assim, questões críticas, impactando diretamente a eficácia e a confiabilidade dos sistemas de IA.

Além disso, a complexidade inerente aos sistemas de IA e sua dependência de dados para treinamento e tomada de decisões criam desafios adicionais, especialmente em termos de privacidade e segurança. Ao contrário de softwares tradicionais, os sistemas de IA podem ser opacos, dificultando o entendimento dos usuários sobre como as decisões são tomadas e os dados utilizados. Esta opacidade, juntamente com a complexidade, amplia o espectro de possíveis incidentes, que podem variar desde a afetação de um número reduzido de indivíduos até impactos significativos em diversos setores, com variados graus de dano. A gestão desses riscos exige uma abordagem mais sofisticada, envolvendo não só aspectos técnicos, mas também considerações éticas e regulatórias.

Até então, estabelecemos o conceito de risco como um dano em potencial. Quando esse risco se materializa, estamos diante de um dano real. As defi-

28. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST AI 100-1: *Artificial Intelligence Risk Management Framework*. Gaithersburg, MD: NIST, 2020. Disponível em: <https://doi.org/10.6028/NIST.AI.100-1>. Acesso em 17 jan. 2024.

nições de danos reais em padrões e regulamentações são altamente dependentes do contexto e geralmente se concentram em lesões físicas ou danos à saúde de pessoas, propriedade ou meio ambiente (IEC 61508-1:2010, ISO/IEC 51:2014, ISO 26262-1:2018). Em alguns casos, como nas regulamentações sobre proteção de dados pessoais, podem se referir a prejuízos causados por violações de dados, incluindo dano físico, material ou não material a pessoas naturais, como perda de controle sobre seus dados pessoais, limitação de seus direitos, discriminação, roubo de identidade ou fraude, perda financeira, dano à reputação, perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem econômica ou social significativa para a pessoa natural envolvida.

O centro de pesquisa focado em tecnologias emergentes, o CSET, em seu framework sobre danos de IA, divide esses danos em duas grandes categorias: danos tangíveis e danos intangíveis²⁹.

Dano tangível é aquele que possui natureza material, sendo, portanto, observável, verificável e definitivo. Exemplos comuns incluem lesão física (incluindo morte), perda financeira e danos a propriedades privadas ou públicas. Esse tipo de dano geralmente é quantificável e pode ser expresso em termos monetários. Exemplos incluem danos a um carro, um braço quebrado ou perda de renda.

Dano intangível, em contraste, geralmente não pode ser observado diretamente. Embora o evento causador do dano possa ser observável e seus efeitos e consequências possam ser expressos de maneira observável, o dano em si não o é. O dano intangível pode incluir, mas não se limita a danos mentais/psicológicos, dor e sofrimento, dano a propriedades intangíveis (por exemplo, roubo de propriedade intelectual, dano à reputação de uma empresa) e perda de confiança ou crença.

A figura abaixo, adaptada e traduzida do material do CSET, indica os tipos de danos categorizados em tangíveis e intangíveis.

29. HOFFMANN, Mia; FRASE, Heather. *Adding Structure to AI Harm: An Introduction to CSET's AI Framework*. Georgetown: Center for Security and Emerging Technology, 2023. Disponível em: <https://cset.georgetown.edu/wp-content/uploads/20230022-Adding-structure-to-AI-Harm-FINAL.pdf>. Acesso em: 6 ago. 2024, p. 9.

Tabela 1 – Danos tangíveis e intangíveis divididos em categorias (CSET)³⁰

Categoria de danos tangíveis	Categoria de danos intangíveis
Danos à Saúde/Segurança física	Conteúdo prejudicial
Danos à infraestrutura	Tratamento Diferenciado
Danos à propriedade material	Direitos Humanos/Civis
Perda financeira	Normas Democráticas
Danos ambientais	Privacidade
Outros	Outros

Segundo o CSET, os danos podem ser classificados, quanto ao seus tipos, em:

Sobre danos tangíveis:

- **Danos à saúde/segurança física:** incluem morte, lesão ou redução da expectativa de vida.
- **Danos à infraestrutura:** envolvem a rede de estradas, ferrovias, serviços públicos e edifícios necessários para manter o comércio, o transporte, as estruturas políticas e a normalidade da vida cotidiana. A infraestrutura pode ser prejudicada pela destruição, diminuição da capacidade ou redução da eficácia
- **Danos à propriedade física:** referentes à destruição de um objeto físico.
- **Perda financeira:** abrange qualquer perda de natureza econômica que não decorra de lesão ou dano.
- **Danos ambientais:** relacionados à degradação ecológica que resultam em poluição, destruição de habitats, desperdício de recursos naturais ou acidentes industriais.

Sobre danos intangíveis:

- **Conteúdo prejudicial:** envolve deepfakes, desinformação, cyberbullying, deturpação de identidade, insultos, ameaças de violência, promoção de distúrbios alimentares ou automutilação, conteúdo extremista, desinformação, material de abuso sexual e e-mails fraudulentos

30. Adaptado pelo autor de HOFFMANN, Mia; FRASE, Heather. *Adding Structure to AI Harm: An Introduction to CSET's AI Framework*. Georgetown: Center for Security and Emerging Technology, 2023. Disponível em: <https://cset.georgetown.edu/wp-content/uploads/20230022-Adding-structure-to-AI-Harm-FINAL.pdf>. Acesso em: 6 ago. 2024.

- **Tratamento diferenciado:** abrangendo questões de preconceito e justiça relacionadas à IA. Entretanto, o preconceito deve estar associado a um grupo que tenha uma característica protegida. O tratamento diferenciado com base em características protegidas geralmente se sobrepõe ou ocorre com uma violação dos direitos civis.
- **Violação de direitos humanos, liberdades civis, direitos civis ou normas democráticas:** relacionados a violações à proteção e à promoção de direitos e liberdades fundamentais.
- **Privacidade:** podem ocorrer por meio de vigilância injustificada, violações de dados ou coleta e uso de informações pessoais sem consentimento.
- **Outros danos:** outros danos que não se enquadram em nenhuma das outras categorias mencionadas.

Essa taxonomia do CSET é utilizada como referência principal para outros estudos específicos e relevantes sobre o tema, como o da proposta da OECD, que apresenta categorias similares, conforme indicação na tabela abaixo:

Tabela 2 – Tipos de danos relacionados a incidentes de IA³¹

Tipo de Dano	Descrição	Exemplo
Danos físicos	Refere-se a lesões corporais ou danos físicos diretos causados a uma pessoa. Pode envolver danos à saúde ou à segurança, ou outros impactos negativos na saúde física.	Falhas em robôs industriais, causando acidentes de trabalho.
Danos ambientais	Indicam consequências indesejáveis ao meio-ambiente como contaminação do solo, poluição do ar ou poluição da água.	Utilização de IA em processos industriais, resultando em vazamento de poluentes.
Danos financeiros, incluindo à propriedade	Inclui perdas econômicas, prejuízos financeiros ou impactos negativos nas finanças pessoais ou empresariais. Pode envolver danos materiais a propriedades físicas, como edifícios, veículos, equipamentos, entre outros.	Falhas em sistemas de negociação automatizados, acarretando perdas financeiras.

Continua

31. Elaborado pelo autor, com base em OECD. *Stocktaking for the development of an AI incident definition*. Paris: OECD, 2023. 36 p. Disponível em: <https://www.oecd.org/publications/stocktaking-for-the-development-of-an-ai-incident-definition-c323ac71-en.htm>. Acesso em: 17 jan. 2024.

Tabela 2 – Tipos de danos relacionados a incidentes de IA

Continuação

Tipo de Dano	Descrição	Exemplo
Danos reputacionais	Refere-se à perda de confiança, credibilidade ou respeito que uma organização, instituição ou indivíduo pode sofrer como resultado de um erro, falha ou uso indevido de sistemas baseados em IA.	Algoritmo de IA que discrimina clientes injustamente, causando uma percepção negativa da instituição.
Dano ao interesse público	Refere-se a danos que afetam a proteção de infraestruturas críticas e instituições sociais.	IA usada em manipulação de informações públicas, afetando a confiança nas instituições governamentais
Restrições às liberdades civis	Danos que resultam na restrição ou violação dos direitos civis de um indivíduo, como discriminação, violações de privacidade, entre outros.	Sistemas de reconhecimento facial levando a vigilância massiva e invasão de privacidade.
Danos psicológicos	Refere-se a danos emocionais, mentais ou psicológicos, como estresse, trauma, ansiedade, entre outros.	Inteligência artificial em redes sociais, contribuindo para ansiedade e depressão.

A classificação dos danos decorrentes de incidentes de IA é fundamental para a compreensão e mitigação eficaz dos riscos associados ao uso dessa tecnologia. A categorização dos danos, tanto em relação à sua tangibilidade ou intangibilidade, ou em relação ao tipo, permite uma análise mais precisa e detalhada das consequências de incidentes. Danos tangíveis, como lesões físicas, perdas financeiras e danos materiais, são mais facilmente quantificáveis e verificáveis, o que facilita a resposta imediata e as medidas corretivas. Por outro lado, danos intangíveis, como sofrimento psicológico, perda de confiança e violações de privacidade, embora mais difíceis de quantificar, são igualmente importantes e requerem abordagens específicas para serem tratados adequadamente.

A clareza na classificação dos danos também melhora a coleta e a análise de dados sobre incidentes de IA, permitindo a identificação de padrões e tendências. Isso contribui para o desenvolvimento de melhores práticas e políticas de segurança, ajudando a prevenir a recorrência de incidentes semelhantes. Além disso, a categorização detalhada dos tipos de danos facilita a comunicação entre diferentes partes interessadas, incluindo desenvolvedores de IA, usuários finais e pesquisadores, promovendo uma compreensão comum sobre os riscos e as consequências associadas ao uso de IA.

No contexto regulatório, a classificação dos danos decorrentes de incidentes de IA desempenha um papel importante na formulação de leis e políticas eficazes. Reguladores precisam de uma compreensão precisa dos tipos de danos que podem ocorrer para estabelecer normas de segurança e responsabilidade adequadas. Assim, a classificação dos danos não apenas melhora a resposta e a mitigação de incidentes, mas também sustenta a criação de um framework regulatório robusto que protege a sociedade contra os riscos potenciais da IA.

3. Níveis de criticidade de danos em incidentes de IA

Um segundo fator relevante para ser considerado em relação a danos decorrentes de IA diz respeito à sua criticidade. A avaliação da criticidade dos danos causados por incidentes de Inteligência Artificial (IA) é um aspecto fundamental para a gestão de riscos nessa área. Uma abordagem estratificada para a classificação da criticidade dos danos possibilita uma análise mais acurada e diferenciada dos impactos que esses incidentes podem gerar. Isso é essencial não apenas para o desenvolvimento de políticas regulatórias apropriadas, mas também para a implementação de medidas preventivas e corretivas eficazes.

Adicionalmente, a categorização em níveis de criticidade assume um papel crítico na priorização das respostas aos incidentes. Ao identificar e focar nos incidentes de maior gravidade, é possível alocar recursos de maneira mais eficiente, visando a proteção dos interesses públicos e a salvaguarda da segurança e dos direitos individuais. Este sistema de classificação também promove a comunicação clara sobre os riscos e consequências associados ao uso da IA, reforçando a transparência e a responsabilidade no manejo desta tecnologia.

De acordo com o já citado estudo da OECD, não existe, até então, um sistema de classificação amplamente aceito e abrangente para contabilizar todas as dimensões do dano causado por sistemas de IA (isto é, em relação ao escopo, escala, gravidade, tipos e impactos etc.). Um passo importante dado nessa direção é a taxonomia desenvolvida pelo CSET, na qual se propõe cinco níveis de criticidade do dano causado por sistemas de IA, quais sejam, dano negligenciável (*negligible*), dano leve (*minor*), dano moderado (*moderate*), dano grave (*severe*) e dano crítico (*critical*). Com base nesses níveis, elaboramos a tabela abaixo:

Tabela 3 – Níveis de criticidade de danos em incidentes de IA³²

Criticidade	Descrição	Exemplos
Negligenciável (Negligible)	Danos mínimos, facilmente remediados.	Erro de arredondamento em cálculos financeiros de baixo impacto por um sistema de IA.
Leve (Minor)	Danos limitados a propriedades, estabilidade social, sistema político ou liberdades civis.	IA de moderação de conteúdo falhando em detectar e remover postagens ofensivas em uma rede social, causando desconforto limitado.
Moderado (Moderate)	Ferimento ou quase ferimento de seres humanos. Danos significativos a interesses financeiros.	Sistema de IA para diagnóstico médico fornecendo resultado incorreto, resultando em tratamento desnecessário. Erro em um algoritmo de IA utilizado para negociação automatizada no mercado de ações.
Grave (Severe)	Ferimento grave ou quase morte de seres humanos. Perturbação significativa a interesses financeiros em escala regional ou nacional. Danos graves à propriedade ou ao meio ambiente.	Falha de IA em veículos autônomos levando a um acidente de trânsito com ferimentos graves. Falha em sistemas de IA utilizados para previsão e gestão de redes elétricas de uma cidade.
Crítico (Critical)	Morte ou quase morte de muitos seres humanos. Perturbação crítica a interesses financeiros em escala nacional ou global.	Falha em sistemas de IA responsáveis pela gestão de infraestruturas críticas, como usinas nucleares ou barragens. Colapso de sistemas de negociação de alta frequência baseados em IA, causando uma crise no mercado de ações com impacto econômico global.

A relevância de classificar danos pode ser exemplificada pelo disposto no art. 73 do EU IA Act. Ainda que não compreenda todos os níveis de criticidade englobados pela taxonomia do CSET, o marco regulatório europeu tipifica a obrigação legal de reportar incidentes graves decorrentes de IA às autoridades de fiscalização. Segundo o EU IA Act (art. 3, ponto 49, b),

(49) “incidente grave” significa um incidente ou mau funcionamento de um sistema de IA que, direta ou indiretamente, leva a qualquer um dos seguintes fatos: (a) a morte de uma pessoa ou danos

32. Elaborado pelo autor, com base em OECD. *Stocktaking for the development of an AI incident definition*. Paris: OECD, 2023. 36 p. Disponível em: <https://www.oecd.org/publications/stocktaking-for-the-development-of-an-ai-incident-definition-c323ac71-en.htm>. Acesso em: 17 jan. 2024.

graves à saúde de uma pessoa; (b) uma interrupção grave e irreversível do gerenciamento ou da operação de uma infraestrutura crítica; (c) a violação das obrigações previstas na legislação da União destinadas a proteger os direitos fundamentais; (d) danos graves à propriedade ou ao meio ambiente.

Em suma, a categorização de danos é determinante para garantir a conformidade com as disposições do AI Act, que exige respostas proporcionais à gravidade dos incidentes, contribuindo para a transparência e a eficácia na gestão de riscos e na resposta a incidentes envolvendo IA. Isso poderá servir de base para legislações futuras, à medida que os incidentes com IA se tornem mais frequentes e as regulamentações evoluam para acompanhar os avanços tecnológicos.

Considerações finais

Ao concluir este estudo introdutório sobre incidentes decorrentes de Inteligência Artificial (IA), diversas reflexões emergem, integrando os aspectos teóricos e práticos explorados nos tópicos anteriores.

Primeiramente, a conceituação da própria IA, conforme apresentada por McCarthy, Newell e Simon e Boden, estabelece um pano de fundo teórico essencial. Essas definições, que enfatizam a engenharia de máquinas inteligentes, a autonomia de sistemas cognitivos, e a capacidade de sistemas de pensar e agir inteligentemente, são fundamentais para a compreensão de sua base de funcionamento e servem como ponto de partida para refletir sobre riscos e danos associados a esses sistemas. A abordagem de Luhmann ao conceito de risco, que considera as complexidades e incertezas associadas às decisões, oferece uma lente crítica para avaliar os riscos e danos da IA em um contexto social.

Este estudo destacou como a IA, apesar de seu potencial transformador em setores variados como saúde, transporte e meio ambiente, carrega consigo riscos e consequências inerentes. Essas consequências, variando em probabilidade e impacto, podem afetar indivíduos, grupos, ambientes e sociedades de maneiras significativas. A análise dos tipos de danos relacionados à IA, abordada no segundo tópico, revelou uma gama de consequências potenciais, desde danos físicos e ambientais até impactos financeiros, reputacionais e psicológicos.

A definição dos níveis de criticidade dos danos, conforme proposto pela taxonomia do CSET, ilustra a necessidade de um framework regulatório bem fundamentado e adaptável. Estabelecer uma classificação precisa dos danos

em níveis de criticidade não apenas ajuda na avaliação precisa dos impactos, mas também orienta na formulação de respostas apropriadas e priorizadas a incidentes de IA.

Em síntese, este trabalho revela a complexidade e o dinamismo dos desafios apresentados pela IA. Enquanto a tecnologia oferece oportunidades sem precedentes para avanços e inovações, ela também exige uma reflexão cuidadosa sobre os riscos e responsabilidades associados ao seu uso.

Olhando para possibilidades de trabalhos futuros pretendemos continuar explorando esta temática, com um enfoque particular na avaliação de incidentes de IA. Aprofundar o entendimento sobre como melhor gerenciar os riscos e mitigar os danos será fundamental para assegurar o uso seguro e responsável da IA, alinhado com os valores éticos e sociais. Assim, o estudo de riscos e danos associados à IA permanece não apenas relevante, mas essencial, à medida que avançamos na era da transformação digital.

Referências

AI Incident Database. *CSET Taxonomy AI Incident Database*. Disponível em: <https://incidentdatabase.ai/taxonomy/cset/>. Acesso em: 07 ago. 2024.

AMODEI, D. et al. *Concrete Problems in AI Safety*. 2016. Disponível em: <https://arxiv.org/abs/1606.06565>. Acesso em: 6 ago. 2024.

BALTRUŠAITIS, T.; AHUJA, C.; MORENCY, L. P. Multimodal Machine Learning: A Survey and Taxonomy. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, v. 41, n. 2, p. 423-443, 2019. DOI: 10.1109/TPAMI.2018.2798607.

BODEN, Margaret A. *Artificial intelligence: A very short introduction*. Oxford University Press, 2018.

BRASIL. Lei n.º 13.709 de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em 17 jan. 2024.

Crawford, K.; Calo, R. *There is a blind spot in AI research*. *Nature* **538**, 311–313 (2016). <https://doi.org/10.1038/538311a>. Acesso em: 07 ago. 2024.

CASTELLS, Manuel. *A era da informação: economia, sociedade e cultura, v. 1 – A sociedade em rede*. Tradução de Roneide Venâncio Majer. 17. ed. São Paulo: Paz e Terra, 2016.

CENTRE FOR SECURITY AND EMERGING TECHNOLOGY (CSET). *Understanding AI Harms: An Overview*. Disponível em: <https://cset.georgetown.edu/article/understanding-ai-harms-an-overview/>. Acesso em: 06 ago. 2024.

CENTER FOR SECURITY AND EMERGING TECHNOLOGY (CSET). *CSET V1 AI Annotation Guide*. CSET, 2023.

HOFFMANN, Mia; FRASE, Heather. *Adding Structure to AI Harm: An Introduction to CSET's AI Framework*. Georgetown: Center for Security and Emerging Technology, 2023. Disponível em: <https://cset.georgetown.edu/wp-content/uploads/20230022-Adding-structure-to-AI-Harm-FINAL.pdf>. Acesso em: 6 ago. 2024.

KORKMAZ, Maria Regina Rigolon. *Decisões Automatizadas: explicação, revisão e proteção na era da inteligência artificial*. São Paulo: Thomsom Reuters Brasil, 2023.

LUHMANN, Niklas. *Risk: A Sociological Theory*. New York: Routledge, 1993.

MCCARTHY, John. *Proposta para o Dartmouth Summer Research Project on Artificial Intelligence*. Dartmouth College, 1955.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST AI 100-1: *Artificial Intelligence Risk Management Framework*. Gaithersburg, MD: NIST, 2020. Disponível em: <https://doi.org/10.6028/NIST.AI.100-1>. Acesso em 17 jan. 2024.

NEWELL, Allen; Simon, Herbert A. *Computer science as empirical inquiry: Symbols and search*. Communications of the ACM 19.3 (1976): 113-126.

OECD. *Stocktaking for the development of an AI incident definition*. Paris: OECD, 2023. 36 p. Disponível em: <https://www.oecd.org/publications/stocktaking-for-the-development-of-an-ai-incident-definition-c323ac71-en.htm>. Acesso em: 17 jan. 2024.

REGULAMENTO (UE) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation). Disponível em: <https://eurlex.europa.eu/legalcontent/PT/TXT/?uri=CELEX%3A32016R0679>. Acesso em: 07 ago. 2024.

Stanford HAI. *AI Index Report 2024*. Stanford Institute for Human-Centered Artificial Intelligence, 2024. Disponível em: https://aiindex.stanford.edu/wp-content/uploads/2024/04/HAI_2024_AI-Index-Report.pdf. Acesso em: 07 ago. 2024.

UNIÃO EUROPEIA. *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 9 de agosto de 2024 que estabelece regras harmonizadas sobre a inteligência artificial (AI Act) e altera certos atos legislativos da União*. Jornal Oficial da União Europeia, Bruxelas, 2024. Disponível em: <https://eur-lex.europa.eu/eli/reg/2024/1689>. Acesso em: 06 out. 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

6

PL 2.338/2023: um estudo sobre as disposições de direitos autorais

NINA RAMALHO PINHEIRO

Sumário: Introdução. 1. A Lei de Direitos Autorais (Lei nº 9.610/1998) e conceitos-chave: obras protegidas, direitos morais e patrimoniais e limitações. 2. Direitos de autor e conexos à luz do 4º substitutivo do PL 2.338/23 e as propostas de emenda. 2.1. Direitos dos titulares e limitação aos direitos autorais. 2.2. Remuneração. 2.3. Transparência e Sandbox regulatório. 2.4. Direitos de personalidade e uso de imagem. Considerações finais. Referências.

Introdução

O avanço no desenvolvimento e uso de sistemas de inteligência artificial (IA) é perceptível em nível global e a incorporação acelerada dessa tecnologia nas mais diversas áreas atrai desafios regulatórios que envolvem o enfrentamento de questões como competitividade, risco de concentração econômica, impactos em emprego/trabalho etc.

A necessidade de se estabelecer regras claras para o desenvolvimento e aplicação da tecnologia de forma segura, responsável, sustentável e em observância aos direitos fundamentais faz surgir diferentes modelos de regulação (ex. geral/setorial, principiológica, vertical/horizontal) baseados nas estratégias de cada política nacional.

No Brasil, ainda que existam iniciativas anteriores², é com o PL 21/2020, de autoria do deputado Eduardo Bismarck, que os debates sobre o tema ganharam contornos mais definidos, culminando, em 2022, na formação da Comissão de Juristas do Senado Federal para elaboração de minuta do substitutivo para instruir a regulamentação da inteligência artificial no país³.

O trabalho da Comissão (CJUSBIA) marca um avanço significativo na estruturação das diretrizes legais para IA no Brasil, pois, a partir da realização de audiências públicas e consultas a mais de cinquenta especialistas de diferentes setores (poder público, empresarial, sociedade civil e comunidade acadêmica), foi apresentada a proposta do substitutivo, convertida no PL nº 2338/2023⁴.

1. Bacharel em Direito pela Pontifícia Universidade Católica de São Paulo (PUC/SP). Pós-graduada em Processo Civil pela FGV Direito SP (FGV LAW). Pós-graduada em Direito Digital pelo Instituto de Tecnologia e Sociedade (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 na área de Contencioso Estratégico, com foco em temas envolvendo Direito Digital, Tecnologia e Proteção de Dados. Contato: nina.rpinheiro@gmail.com.

2. Exemplo: PLs 5051/20219 e 5691/2019, que estabelecem princípios gerais para o uso da IA.

3. A partir da apreciação dos Projetos de Lei nº 5051/2019, 21/2020 e 872/2021.

4. BRASIL. Senado Federal. *Projeto de Lei nº 2338, de 2023*. Dispõe sobre o uso da Inteligência Artificial. Brasília: Senado Federal, 2023. <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 15 jul. 2024.

O PL nº 2338/2023 pode ser interpretado como um avanço, pois é reflexo de um longo processo de discussão multissetorial, e buscou conciliar uma abordagem⁵ regulatória baseada em riscos com a promoção da proteção de direitos fundamentais, sem ignorar a promoção da inovação e a responsabilização de agentes.

Em que pese o avanço, inúmeros pontos ainda têm sido objeto de amadurecimento e debates encabeçados por Notas Técnicas⁶, emitidas por entidades representativas da sociedade, e contribuições em audiências públicas. Como reflexo, até novembro de 2024, foram apresentadas no Senado Federal 150 propostas de emenda e quatro substitutivos ao texto de lei.

Dentre os temas que despertam mais divergência e insegurança, destaca-se a proteção aos direitos autorais no âmbito do desenvolvimento e uso de sistemas de inteligência artificial, principalmente a generativa. O tema é objeto de dezenove emendas⁷, até o momento, das quais duas foram acatadas⁸, uma foi parcialmente acatada⁹, uma foi retirada pelo autor¹⁰ e quinze foram rejeitadas¹¹.

Sob essa perspectiva, este estudo tem como objetivo principal analisar essas emendas, as justificativas apresentadas, os argumentos para aprovação ou não e a alteração na redação dos artigos correlatos no PL 2.338/23, a fim de identificar os principais pontos de discussão para aperfeiçoamento da regulação relativa à proteção aos direitos autorais.

Para tanto, o material primário de pesquisa consiste nas emendas que tratam de direitos autorais contrapostas aos artigos da “Seção IV – Direitos de autor e conexos” do 4º substitutivo do PL 2.338/23, de 28 de novembro de 2024. O material secundário é composto por orientações aplicáveis ao tema, legislação específica, experiência regulatória estrangeira, bibliografia de suporte e notas técnicas emitidas por entidades competentes. A partir do material primário, buscou-se extrair os temas macros abordados, ora denominados “pontos”, que serão analisados individualmente a partir das questões-problema identificadas e possíveis soluções considerando o material secundário analisado.

5. LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET (LAPIN). *Projeto de Lei nº 2338/2023 - Nota Técnica*. Agosto, 2023. Disponível em: <https://direitosnarede.org.br/2023/08/23/coalizao-direitos-na-rede-divulga-nota-tecnica-sobre-o-pl-2338-2023-que-busca-regular-a-ia/>. Acesso em: 13/07/2024.

6. Por exemplo: IDEC, ANDP, Coalizão Direitos na Rede.

7. Emendas nº 4, 6, 20, 24, 36, 44, 45, 55, 56, 61, 72, 102, 103, 109, 110, 112, 118, 119, 128.

8. Emendas nº 4 e 44.

9. Emenda nº 45.

10. Emenda nº 24.

11. Emendas nº 6, 20, 36, 40, 55, 56, 61, 72, 102, 103, 109, 110, 112, 118, 119, 128.

Para apresentação do estudo, optou-se por abordar no primeiro capítulo, a partir do mapeamento da Lei de Direitos Autorais (Lei n. 9.619/98 ou “LDA”), definições essenciais para o entendimento de seu escopo, como obra protegida, direitos morais e patrimoniais e direitos conexos. Neste capítulo, também foram apresentados conceitos básicos de inteligência artificial, introduzindo a definição de treinamento de modelos e mineração de dados e texto. No segundo capítulo, os quatro pontos selecionados a partir da análise do material primário de pesquisa, a saber (i) direitos dos titulares e limitação aos direitos autorais, (ii) remuneração, (iii) transparência e sandbox regulatório e (iv) direitos da personalidade e uso de imagem, passam a ser tratados com base na redação dos artigos do 4º substitutivo do PL e das emendas correlatas apresentadas. O estudo se encerra com um balanço dos avanços e incertezas envolvendo o tema e perspectivas futuras para enfrentamento dos desafios apurados.

1. A Lei de Direitos Autorais (Lei nº 9.610/1998) e conceitos-chave: obras protegidas, direitos morais e patrimoniais e limitações

Antes de adentrar na análise dos dispositivos do PL 2.338/23 que buscam traçar as balizas para conformar direitos autorais no âmbito da inteligência artificial, importante tecer breves comentários acerca da legislação especial aplicável ao tema, a fim de trazer definições essenciais para entendimento dos pontos tratados no Projeto de Lei.

No Brasil, a tutela dos direitos autorais e conexos é positivada na Lei de Direitos Autorais (Lei n. 9.619/98). Para compreender o objeto de proteção do direito autoral, a partir do art. 7º da LDA¹², extrai-se que serão protegidas as criações do espírito exteriorizadas por qualquer meio ou suporte, independentemente se relacionada ao domínio das letras, das artes ou das ciências. A partir da previsão legal, é evidente que não serão protegidos conceitos, estilos ou ideias, mas apenas a expressão exteriorizada desses elementos.

12. Art. 7º São obras intelectuais protegidas as criações do espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se invente no futuro, tais como: I - os textos de obras literárias, artísticas ou científicas; II - as conferências, alocuções, sermões e outras obras da mesma natureza; III - as obras dramáticas e dramático-musicais; IV - as obras coreográficas e pantomímicas, cuja execução cênica se fixe por escrito ou por outra qualquer forma; V - as composições musicais, tenham ou não letra; VI - as obras audiovisuais, sonorizadas ou não, inclusive as cinematográficas; VII - as obras fotográficas e as produzidas por qualquer processo análogo ao da fotografia; VIII - as obras de desenho, pintura, gravura, escultura, litografia e arte cinética; IX - as ilustrações, cartas geográficas e outras obras da mesma natureza; X - os projetos, esboços e obras plásticas concernentes à geografia, engenharia, topografia, arquitetura, paisagismo, cenografia e ciência; XI - as adaptações, traduções e outras transformações de obras originais, apresentadas como criação intelectual nova; XII - os programas de computador; XIII - as coletâneas ou compilações, antologias, enciclopédias, dicionários, bases de dados e outras obras, que, por sua seleção, organização ou disposição de seu conteúdo, constituam uma criação intelectual. (BRASIL. Presidência da República. Lei nº 9.610, de 19 de fevereiro de 1998. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências.) Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9610.htm. Acesso em 3 jul. 2024.

Em que pese a legislação não seja expressa, e existam posicionamentos contrários, a doutrina majoritária também defende a originalidade da obra como requisito à concessão da proteção legal. Tal originalidade, como ressalva Sérgio Branco¹³, não se confunde com “novidade absoluta”, devendo ser compreendida como o elemento capaz de diferenciar determinada obra das demais, em razão do esforço intelectual e criativo do autor.

Para além desses pontos, a proteção de uma obra também deve observar o prazo de proteção fixado na lei, atualmente limitado a 70 anos a contar de 1º de janeiro do ano subsequente a marcos como: o falecimento (obras em geral), a publicação (obras anônimas, pseudônimas ou postumamente publicadas) e a divulgação (obras coletivas, audiovisuais e fotográficas), período após o qual a obra entra em domínio público.

Ainda que o art. 7º da LDA enumere espécies de obras protegidas, considerando a mutabilidade associada a fatores externos como questões culturais e desenvolvimento tecnológico, a doutrina especializada defende que o rol apresentado é exemplificativo, de modo que, atendidos os requisitos essenciais ora apresentados, a obra terá proteção autoral.

Para além do objeto de proteção, a LDA define que as obras protegidas precisam de um autor, responsável por deter o controle criativo da obra¹⁴. De acordo com o art. 11 da LDA, o autor é a “pessoa física criadora de obra literária, artística ou científica”.

Como suscita Luca Schirru¹⁵, embora o desenvolvimento tecnológico e o interesse de mercado atraiam outras formas de criação colocando em xeque o caráter individual e humano atribuído à autoria, o conceito de autor reproduzido na lei, como bem observado por Guilherme Carboni¹⁶, partiu da concepção do Romantismo reproduzida na Convenção de Berna (1886), a partir da qual, assumindo que as obras seriam verdadeira extensão da personalidade de seu criador, justificou-se a concessão de direito exclusivo ao autor pessoa física sobre as suas obras.

13. BRANCO, Sérgio. *Direitos autorais na Internet e o uso de obras alheias*. Rio de Janeiro: Lumen Juris, 2007. Disponível em: <https://repositorio.fgv.br/items/9d286b3c-c77e-46f2-ad95-1bc48debd48c>. Acesso em: 13 jul. 2024.

14. CANTALI, Fernanda Borghetti. Inteligência artificial e direito de autor: tecnologia disruptiva exigindo reconfiguração de categorias jurídicas. *Revista de Direito, Inovação, Propriedade Intelectual e Concorrência*. Porto Alegre. v. 4. p. 1-21. Jul/Dez. 2018. Disponível em: <https://www.indexlaw.org/index.php/revistadipic/article/view/4667/pdf>. Acesso em: 20 jul. 2024.

15. SCHIRRU, Luca. *Direito autoral e inteligência artificial: autoria e titularidade nos produtos da IA*. Tese (Doutorado em Políticas Públicas, Estratégias e Desenvolvimento) - Instituto de Economia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2020. P. 99. Disponível em: https://www.ie.ufrj.br/images/IE/PPED/Teses/2020/Vers%C3%A3o%20final_Tese%20Luca_PDF.pdf. Acesso em: 13 jul. 2024.

16. CARBONI, Guilherme. *Direito Autoral, Diversidade das Expressões Culturais e Pluralidade de Autorias*. In: *Direito da Propriedade Intelectual, Vol II: estudos em homenagem ao Pe. Jorge Hammes* (Org. por Luiz Gonzaga Silva Adolfo e Marcos Wachowicz). Curitiba: Juruá. 2014.

Para compreensão da exclusividade dos direitos conferidos ao autor é essencial definir a natureza desses direitos. Embora não seja um entendimento pacífico, a LDA adotou a teoria dualista, que prevê duas categorias de direito distintas sobre a obra: a de ordem moral e a de ordem patrimonial.

Os direitos morais, tratados nos artigos 24, 25, 26 e 27 da LDA, resultariam da projeção da personalidade do autor na obra¹⁷ em razão do vínculo indissolúvel¹⁸ entre os dois. Nesse contexto, refletem a relação do autor com a própria obra e compreendem o direito de indicação de autoria¹⁹, de controle de circulação²⁰ e de alteração da obra²¹.

Embora questionável a conceituação dos direitos morais de autor como direitos da personalidade²², uma vez que não são inatos ao indivíduo, se manifestando apenas a partir da criação de obra protegida, por força do art. 27 da LDA referidos direitos também são inalienáveis, irrenunciáveis, imprescritíveis e impenhoráveis.

Por sua vez, os direitos patrimoniais, que podem ser transacionados e transferidos de forma onerosa ou gratuita, parcial ou integralmente, dizem respeito às formas de exploração econômica da obra a partir do exercício das faculdades do autor ou do titular²³ de utilizar, fruir e dispor da obra antes dela cair em domínio público.

Conforme defende Eliane Abrão²⁴, tais direitos também podem ser considerados exclusivos, uma vez que, por força do art. 28 da LDA, as modalidades de uso da obra previstas no art. 29 da LDA, dentre as quais destaca-se a reprodução, a edição, a adaptação, a tradução, a distribuição e a inclusão da obra em base de dados, dependerão de prévia e expressa aprovação do autor/titular.

Além dos direitos autorais, a LDA, nos artigos 89 a 96, estabelece direitos conexos para garantir a participação e remuneração dos artistas em utilizações futuras de uma obra que teve sua participação. Isso inclui os direitos dos artis-

17. SOUZA, Allan Rocha de. Direitos morais do autor. *Civilistica.com*. Rio de Janeiro, a. 2, n. 1, jan.-mar./2013. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/73/53>. Acesso em: 27 jul.2024.

18. STAUT JÚNIOR, Sérgio Said. *Direitos Autorais: entre as relações sociais e as relações jurídicas*. Moinho do Verbo. Curitiba. 2006.

19. Direito de reivindicar a autoria de sua obra e ter seu nome ou pseudônimo creditado (art. 24, I e II, LDA).

20. Direito de manter a obra inédita e o de retirá-la de circulação (art. 24, III e VI, LDA).

21. Visando assegurar a integridade da obra perante terceiros, ao mesmo tempo que confere ao autor a possibilidade de alterá-la mesmo após a colocação em circulação (art. 24, IV e V, LDA).

22. BRANCO, Sérgio. PARANAGUÁ, Pedro. *Direitos Autorais*. 1ª ed. Rio de Janeiro: Editora FGV. 2009. p. 50. Disponível em: <https://repositorio.fgv.br/server/api/core/bitstreams/3df3edc6-9a6f-486d-bff8-c1a717da24b4/content>. Acesso em: 13 jul.2024.

23. Diante da possibilidade de transmissão de direitos, o titular nem sempre será o autor da obra, podendo ele assumir a titularidade originária da obra em decorrência de negócios jurídicos, da morte ou determinação legal.

24. ABRÃO, Eliane. *Direitos de autor e direitos conexos*. São Paulo: Ed. do Brasil, 2002.

tas intérpretes ou executantes, produtores fonográficos e empresas de radio-difusão, no que diz respeito à interpretação, execução ou difusão de uma obra.

Assim como se observa nos direitos de autor, aos titulares de direitos conexos também é conferido o direito exclusivo de autorizar ou proibir a gravação, reprodução, execução e comunicação pública da obra; a transmissão, retransmissão e fixação das interpretações/emissões; a disponibilização ao público para acesso em qualquer momento e lugar; e qualquer outra forma de uso de suas interpretações ou execuções.

Apesar de proteger o autor da obra, até como forma de estimular a diversidade e a economia criativa, os direitos e a proteção conferidos pela LDA não são absolutos, sendo mitigados sob a perspectiva do interesse público e da promoção de outros direitos fundamentais (ex. cultura, acessibilidade, educação), nos termos dos artigos 46, 47 e 48 da lei.

Esses dispositivos preveem situações nas quais uma obra protegida tem o seu uso autorizado independentemente de prévia autorização do autor/titular, sem que isso importe em violação legal ou aos direitos de terceiros. Exemplificativamente, é permitido citar pequenos trechos de uma obra literária em um livro acadêmico para fins de crítica ou estudo, instituições de ensino podem reproduzir partes de obras para uso exclusivo nas atividades didáticas, é autorizada a reprodução de notícias ou artigos informativos na imprensa, são livres as paráfrases e paródias que não sejam verdadeiras reproduções da obra original e que não lhe causem descrédito etc.

No âmbito da proteção de direitos autorais aplicada ao uso, desenvolvimento e treinamento de sistemas de inteligência artificial a interpretação dessas limitações e de sua taxatividade, mostra-se relevante.

Embora não seja unânime²⁵, a interpretação extensiva das limitações legais à luz da constituição federal tem ganhado força como forma de refletir a evolução tecnológica, de modo a abarcar as novas formas de criação e superar a aparente obsolescência da legislação vigente²⁶.

Para compreensão dos dispositivos tratados na “Seção IV – Direitos de autor e conexos” do 4º substitutivo do PL 2.338/23, também se mostra relevante o entendimento de conceitos como: sistema de inteligência artificial; desenvolvedor e agente de IA; e processo de mineração de textos e dados.

25. Autores como Carlos Alberto Bittar e Plínio Cabral defendem a interpretação restritiva das limitações.

26. SCHIRRU, Luca. *Direito autoral e inteligência artificial: autoria e titularidade nos produtos da IA*. Tese (Doutorado em Políticas Públicas, Estratégias e Desenvolvimento) - Instituto de Economia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2020. P. 157. Disponível em: https://www.ie.ufrj.br/images/IE/PPED/Teses/2020/Vers%C3%A3o%20final_Tese%20Luca_PDFa.pdf. Acesso em: 13 jul. 2024.

No esboço de regulamentação um sistema de IA é definido²⁷ como um sistema baseado em máquina, com diferentes graus de autonomia, capaz de inferir a partir de conjunto de dados e informações e gerar resultados como previsões, recomendações ou decisões.

Para que possa desempenhar as suas funções, a maioria dos sistemas de inteligência artificial é formado por algoritmos capazes de aprender a partir de uma base de dados (*machine learning*)²⁸, podendo, por vezes, processarem esses dados de forma similar às redes neurais (*deep learning*)²⁹.

Independentemente da forma de funcionamento e aprendizagem do sistema, o sucesso e acurácia das predições, recomendações e decisões depende de um grande volume de dados de entrada, utilizados para o treinamento dos algoritmos, identificação de padrões significativos e melhoria do desempenho dos sistemas.

É nesse contexto que a mineração de textos e dados (TDM³⁰), técnica automatizada de extração de grandes volumes de dados, diretamente ou através de outras ferramentas, para identificar padrões e correlações³¹, torna-se relevante, pois é a partir da obtenção de informações extraídas de imensas quantidades de dados³² que serão obtidos *insights* para utilização em pesquisa, desenvolvimento ou aplicação em sistemas de inteligência artificial.

Sob a perspectiva dos direitos autorais, embora exista quem defenda a legalidade da mineração de textos e dados independentemente de previsão legal expressa, por envolver um uso não expressivo a partir do qual são extraídos elementos e padrões factuais³³ – não protegidos pelos direitos de autor

27. Art. 4º [...] I – sistema de inteligência artificial: sistema baseado em máquina que, com graus diferentes de autonomia e para objetivos explícitos ou implícitos, infere, a partir de um conjunto de dados ou informações que recebe, como gerar resultados, em especial, previsão, conteúdo, recomendação ou decisão que possa influenciar o ambiente virtual, físico ou real; (BRASIL. Senado Federal. Projeto de Lei nº 2338, de 2023. Dispõe sobre o uso da Inteligência Artificial. Brasília: Senado Federal, 2023. <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 29 nov. 2024.)

28. No original: “Machine Learning: algoritmos que analisam dados, aprendem com eles e depois aplicam o que aprenderam para tomar decisões informadas. Eles usam recursos extraídos de dados por humanos e melhoram com a experiência” (CERON, Rodrigo. *AI, machine learning and deep learning: What’s the difference?* IBM, 5 dez 2019, tradução livre). Disponível em: <https://www.ibm.com/blog/ai-machine-learning-and-deep-learning-whats-the-difference/>. Acesso em 13 jul 2024.

29. No original: “Deep Learning: algoritmos de rede neural que aprendem sozinhos sobre as características relevantes dos dados. Capaz de se adaptar através de treinamento repetitivo para descobrir padrões e insights ocultos” (CERON, Rodrigo. *AI, machine learning and deep learning: What’s the difference?* IBM, 5 dez 2019, tradução livre). Disponível em: <https://www.ibm.com/blog/ai-machine-learning-and-deep-learning-whats-the-difference/>. Acesso em 13 jul. 2024.

30. Text and Data Mining.

31. Art. 4º [...] XIII - mineração de textos e dados: processo de extração e análise com alto grau de automação de grandes quantidades de dados, realizados de forma direta nos dados primários, ou indireta a partir de outra ferramenta, a partir dos quais são extraídos padrões e correlações que gerarão informações relevantes para a pesquisa, o desenvolvimento ou a utilização de sistemas de inteligência artificial. (BRASIL. Senado Federal. Projeto de Lei nº 2338, de 2023. Dispõe sobre o uso da Inteligência Artificial. Brasília: Senado Federal, 2023. <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 29 nov. 2024)

32. ROCHA, Maria Victória. Prospecção de texto e dados (text and data mining) na diretiva relativa aos direitos de autor e direitos conexos no mercado único digital. *RRDDIS – Revista Rede de Direito Digital, Intelectual & Sociedade*, Curitiba, v. 2, n. 4, p. 99-164, 2022, p. 103. Disponível em: <https://revista.ioda.org.br/index.php/rrddis/article/view/76/45>. Acesso em 16 jul. 2024

33. SOUZA, Allan Rocha de. SCHIRRU, Luca. Alvarenga. MIGUEL BARROS. Mineração de textos e dados na pesquisa em saúde: reflexões sobre direitos autorais. *Cadernos de Saúde Pública* 2024. Disponível em: <https://cadernos.ensp.fiocruz.br/ojs/index.php/csp/article/view/8597/19335>. Acesso em: 27 jul.2024.

– considerando que há acesso a base de dados (artigo 7º, XII, XIII, §2º LDA) e a obras protegidas, uma previsão normativa expressa acerca da limitação incidente é importante para garantir segurança jurídica.

Nesse cenário, refletindo experiências legislativas internacionais, a exemplo das reformas nas legislações de direitos autorais realizadas no Japão³⁴, em Singapura³⁵ e em Israel³⁶, no Brasil, o PL 2.338/23 reconhece a insuficiência das limitações do artigo 46, da LDA, pois mesmo com uma interpretação extensiva, essas limitações se referem apenas à reprodução de obras para fins específicos, sem abranger outras formas de uso necessárias para a TDM. O PL propõe então uma limitação específica para essa atividade, buscando equilibrar e flexibilizar a exclusividade do sistema autoral em benefício do interesse público.

Para atendimento das obrigações do PL 2.338/23, importante compreender quem são os sujeitos a quem a lei se aplica. De acordo com o artigo 4º, VIII do 4º substitutivo do PL 2.338/23, os agentes de inteligência artificial, que podem ser pessoa natural ou jurídica, de natureza pública ou privada, são os desenvolvedores (art. 4º, V)³⁷, os distribuidores (art. 4º, VI)³⁸ e os aplicadores (art. 4º, VII)³⁹ que atuam na cadeia de valor e na governança interna de sistemas de inteligência artificial.

Apesar da legislação vigente, o dinamismo no desenvolvimento das tecnologias de IA expõe lacunas que suscitam dúvidas sobre a aplicação e suficiência dos mecanismos existentes para proteção dos direitos autorais. Reconhecendo esses hiatos o PL 2.338/23 e as emendas propostas buscam a construção de regulação que considere a nova realidade e equilibre os interesses públicos e privados. Para verificar a compatibilidade das sugestões regulatórias para promover a proteção dos autores sem inviabilizar o avanço tecnológico, o próximo capítulo analisará a proposta de atualização legislativa sob as perspectivas dos direitos dos titulares, limitações aos direitos autorais, regime de remuneração, dever de transparência e sandbox regulatório, e direitos da personalidade e uso de imagem.

34. No Japão, a lei de direitos autorais foi ajustada para permitir a mineração de dados com fins de pesquisa, inclusive para o desenvolvimento de IA, sem a necessidade de obter consentimento prévio dos detentores de direitos.

35. Em Singapura, a Lei de Direitos Autorais de 2021 inclui uma exceção para mineração de dados, que permite o uso de obras protegidas para análise computacional, incluindo o desenvolvimento de IA, sem a necessidade de autorização prévia dos titulares de direitos.

36. Israel permite o uso de dados para IA sob condições que garantem a privacidade e a segurança, mas não impõe restrições severas sobre o uso de dados protegidos para fins de treinamento de IA.

37. Responsáveis pelo desenvolvimento do sistema de inteligência artificial (desde a criação, treinamento, implementação e aprimoramento), diretamente ou por encomenda, com vistas a sua colocação no mercado ou a sua aplicação em serviço por ele fornecido, sob seu próprio nome ou marca, a título oneroso ou gratuito.

38. Responsável por disponibilizar e distribuir o sistema de IA para que terceiro o opere a título oneroso ou gratuito.

39. Responsável pelo emprego ou utilização, em seu nome ou benefício, do sistema de inteligência artificial, inclusive para fins de configuração, manutenção ou apoio com o fornecimento de dados para a operação e o monitoramento do sistema de IA.

2. Direitos de autor e conexos à luz do 4º substitutivo do PL 2.338/23 e das propostas de emenda

Embora as diretrizes para alinhar os direitos autorais com o acesso a dados para treinamento de máquina e o desenvolvimento de sistema de inteligência artificial sejam uma preocupação desde o relatório final da CJUSBIA, convertido no texto inicial no PL nº 2.338/2023, após a análise de inúmeras emendas propostas sobre o tema alguns avanços relevantes já foram realizados, de modo que os principais “pontos” do PL 2.338/23 afetos aos direitos autorais serão apresentados neste trabalho a partir da redação dos artigos do 4º substitutivo, de 28 de novembro de 2024, que inclusive passou a reconhecer a proteção dos direitos autorais como um dos fundamentos da lei, ao lado de propriedade intelectual e segredo comercial e industrial.

2.1 Direitos dos titulares e limitação aos direitos autorais

Os artigos 63 e 64 do 4º substitutivo do PL 2.338/23, tratam das limitações e dos principais direitos dos titulares de direitos de autor e conexos, tais como o de proibir a utilização de conteúdo de sua titularidade no desenvolvimento de sistemas de IA⁴⁰.

Como visto, considerando que os arts. 46 a 48 da LDA, ainda que possam ser interpretados extensivamente, não trazem limitações claras aos direitos de autor em processos de mineração de textos e dados para desenvolvimento, treinamento e uso dos sistemas de IA, alinhado às práticas internacionais e respondendo às necessidades contemporâneas de pesquisa e desenvolvimento tecnológico, o art. 63 do 4º substitutivo do PL 2.338/23 inova ao prever exceções aos direitos autorais em que o direito de proibição de utilização previsto no art. 64 é mitigado.

A exceção, contudo, a fim de preservar os interesses (principalmente econômicos) dos autores limita-se a situações nas quais o interesse público se sobrepõe, sendo permitido o uso por organizações e instituições educacionais, de pesquisa, de jornalismo, por museus, arquivos, e bibliotecas⁴¹ desde que o acesso tenha se dado de forma lícita (inciso I), o uso não tenha fins comerciais

40. Art. 64. O titular de direitos de autor e conexos poderá proibir a utilização dos conteúdos de sua titularidade no desenvolvimento de sistemas de IA nas hipóteses não contempladas pelo art. 61 desta Lei, na forma do regulamento. Parágrafo único. A proibição do uso de obras e conteúdos protegidos nas bases de dados de um sistema de IA posterior ao processo de treinamento não exime o agente de IA de responder por perdas e danos morais e materiais, nos termos da legislação aplicável.

41. Art. 63. Não constitui ofensa aos direitos de autor e conexos a utilização automatizada de conteúdos protegidos em processos de mineração de textos e dados para os fins de pesquisa ou desenvolvimento de sistemas de IA por organizações e instituições de pesquisa, jornalismo, museus, arquivos, bibliotecas e educacionais, desde que observadas as seguintes condições:

(inciso II), a atividade não vise a reprodução, exibição ou disseminação da obra original (inciso III), e a utilização seja feita apenas para atingir o seu objetivo, sem prejudicar os interesses econômicos dos titulares ou concorrer com a exploração normal das obras e conteúdos protegidos (inciso IV).

Desses requisitos, talvez o que gere mais questionamentos seja a vedação a propósitos comerciais decorrentes da mineração. Conforme tratado por Miguel Bastos Alvarenga⁴², mostra-se importante lembrar que mesmo a atividade de pesquisa pode culminar em publicações postas à venda, de modo que vincular a exceção a uma finalidade estritamente não-comercial poderia impactar na divulgação de trabalhos científicos e comprometer diversas atividades de pesquisa.

Nesse ponto, entende-se que a proibição de finalidade comercial merece maior amadurecimento, a partir da avaliação da suficiência da vedação de interferência na exploração normal da obra em prejuízo dos interesses econômicos do titular, até porque o próprio art. 46 da LDA admite exceções com fins lucrativos⁴³.

Para além desses pontos, o dispositivo legal traz ainda deveres de segurança e adequação do período de guarda de eventuais cópias de conteúdos protegidos para uso no treinamento de sistemas de IA (§1º) e aplicação estendida para uso de processos de mineração no contexto de sistemas de inteligência artificial para combate a ilícitos cíveis e criminais contra direitos de autor e conexos (§3º)⁴⁴.

Embora os dispositivos prevejam a possibilidade de uso de obras para fins de mineração e uso por inteligência artificial em determinados contextos, importante destacar que o PL não autoriza o uso amplamente, conferindo aos titulares o direito de se opor ao uso, mesmo quando não houver prejuízo efetivo aos seus interesses econômicos. Tal proibição, mais rígida do que em outras legislações internacionais, pode representar uma barreira ao investimento e avanço tecnológico no país, com impactos à competitividade. Por esse motivo, também se considera importante maior amadurecimento das discussões e avaliação, por exemplo, de mecanismos de compensação obrigatória – para proteger o interesse dos titulares – sem a possibilidade de proibição do uso

42. ALVARENGA, Miguel Bastos. *Mineração de dados, Big Data e Direitos Autorais no Brasil*. Tese (Mestrado em Políticas Públicas, Estratégias e Desenvolvimento) - Instituto de Economia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2019. p. 92. Disponível em: https://onda.org.br/resources/2020_Miguel%20ALVARENGA_Mest.pdf. Acesso em 27 jul 2024.

43. “Art. 46. Não constitui ofensa aos direitos autorais: I - a reprodução: (...) V - a utilização de obras literárias, artísticas ou científicas, fonogramas e transmissão de rádio e televisão em estabelecimentos comerciais, exclusivamente para demonstração à clientela, desde que esses estabelecimentos comercializem os suportes ou equipamentos que permitam a sua utilização.”

44. Entende-se que para o uso com essa finalidade não se aplicam os requisitos dos incisos do art. 63.

nos casos em que não houver prejuízo aos interesses econômicos dos titulares ou concorrência com a exploração normal das obras protegidas⁴⁵.

2.2 Remuneração

Uma das maiores inquietações trazidas pelas ferramentas de IA envolve a garantia de remuneração aos titulares em razão da apropriação de suas produções para desenvolvimento e treinamento de modelos de IA.

Até o 2º substitutivo do PL 2.338/23, de 18 de junho de 2024, a remuneração dos titulares pelo uso de conteúdos protegidos para treinamento e desenvolvimento de sistemas de inteligência artificial estava submetida à criação de um ambiente regulatório experimental (sandbox) para discussão de modelos de remuneração.

Apenas com a redação do 3º substitutivo, o dever de remuneração foi positivado, prevendo o art. 65 do 4º substitutivo que “o agente de IA que utilizar conteúdos protegidos por direitos de autor e direitos conexos em processos de mineração, treinamento ou desenvolvimento de sistemas de IA deve remunerar os respectivos titulares desses conteúdos em virtude dessa utilização.”.

Sobre o direito à remuneração, importante citar a rejeição, em 04/07/2024, das emendas 56⁴⁶, 61⁴⁷ e 72⁴⁸, que buscavam respectivamente (i) a prevalência de oferta final de preço fixo a ser fixada pela Autoridade Setorial ou pela Câmara Arbitral Privada em caso de inviabilidade da negociação entre os agentes de IA e o titular de direitos autorais e conexos; (ii) a supressão dos dispositivos correlatos a direitos autorais; e (iii) o afastamento de autorização prévia para desenvolvimento de sistemas de IA com o cabimento eventual de remuneração aos titulares, sob o fundamento de que a garantia de direitos à indústria criativa é importante para incentivar a inovação responsável e a proteção dos frutos do espírito humano.

Embora alguns⁴⁹ defendam que a remuneração pela exploração econômica de obras protegidas já esteja amparada pela Constituição Federal, de 1988⁵⁰, e pela LDA, sendo redundante tratar tema na legislação sobre inteligência artificial, o PL 2.338/23 reconhece que existem especificidades no contexto de IA que não se enquadram nas modalidades de uso previstas na

45. Hipótese com maior probabilidade de configuração em casos envolvendo sistemas de IA generativa.

46. De autoria do Senador Weverton, apresentada em 18/06/2024.

47. De autoria do Senador Astronauta Marcos Pontes, apresentada em 18/06/2024.

48. De autoria do Senador Astronauta Marcos Pontes, apresentada em 18/06/2024.

49. As emendas 61 e 72 buscando a supressão dos artigos com reflexos nos direitos autorais são exemplos disso.

50. Art. 5º, XXVII, da CF.

LDA⁵¹. Portanto, a previsão de remuneração nessas situações é crucial para coibir abusos decorrentes de ambiguidades e da obsolescência da legislação atual, além de elucidar como esse direito será exercido no novo contexto tecnológico, que envolve o uso de grandes volumes de dados.

Sobre o tema, os parágrafos e incisos do art. 65 do 4º substitutivo do PL dispõem que a remuneração será devida para os titulares domiciliados no Brasil ou em países que assegurem reciprocidade na proteção (inciso V, alíneas a e b), apenas em caso de disponibilização comercial dos sistemas de IA (inciso IV), e com a possibilidade de prazo diferido para pagamento por startups e pequenas empresas (inciso VI), assegurando: (i) a capacidade de negociação direta ou coletiva, de forma onerosa ou gratuita (inciso I), no primeiro caso independente de regulamentação (§2º); (ii) que o valor considere o poder econômico do agente de IA, o grau de utilização dos conteúdos e os efeitos concorrenciais em relação aos conteúdos originais, a complexidade do sistema de IA, o ciclo de realização econômica e o valor relativo da obra ao longo do tempo (inciso II); (iv) a livre negociação, com a promoção de um ambiente de pesquisa e experimentação, sem restrição à liberdade de pactuação (inciso III).

Isto é, ressalvadas as limitações introduzidas pelo art. 63, desde que autorizado o uso prévio do conteúdo de sua titularidade, o titular deverá ser remunerado pelo agente de IA que utilizar suas obras.

Em que pese o dispositivo responda a anseios da indústria criativa, entende-se que a redação atual é insuficiente para garantir a almejada segurança jurídica, em especial, pois: faz menção genérica ao dever dos “agentes de inteligência artificial”, sendo importante delimitar em qual medida e sobre qual agente o dever de remuneração recairá para afastar dúvidas que podem surgir do envolvimento de múltiplos agentes no ciclo de vida dos sistemas de IA; os critérios para o cálculo da remuneração são subjetivos, dificultando a aplicação prática, sendo importante estabelecer critérios mais objetivos para mensurar “poder econômico”, “grau de utilização”, “efeitos concorrenciais”, “complexidade do sistema de IA”, “ciclo de realização econômica” e “valor da obra ao longo do tempo”, a fim de orientar as negociações, sem ignorar a liberdade de pactuação.

Para além desses pontos, embora não se ignore a importância da previsão de mecanismos para proteção dos titulares de direitos de autor e conexos, especialmente sob a perspectiva econômica e no âmbito do uso de obras por sistemas de IA generativa – com maior potencial de impactos de ordem con-

51. Tanto é que cria exceção para o uso de obras para mineração, treinamento e desenvolvimento de sistemas de IA.

correncial e prejuízo aos interesses do autor – a dificuldade técnica para controle e obtenção prévia de autorização para uso de dados gera preocupação, inclusive diante da importância de treinamento de modelos com conteúdo brasileiro (para refletir nuances e garantir a aplicação adequada no país). Nessa perspectiva, até para preservação da competitividade e soberania do Brasil no cenário global de IA, se torna relevante o amadurecimento das discussões e avaliação de alternativas como a criação de fundos de compensação coletiva, licenciamento obrigatório com taxa padrão etc.

2.3 Transparência e Sandbox regulatório

Para permitir o controle pelos titulares e garantir a efetividade do exercício dos direitos de proibição e remuneração pelo uso das obras, a transparência é um elemento crucial.

Embora tecnologias de Gestão de Direitos Digitais (DRM), blockchain, marcas digitais e marcas d'água possam ser empregadas para controlar e monitorar o acesso e o uso de obras, atribuir o ônus do controle e fiscalização aos titulares poderia inviabilizar o exercício pleno de direitos. Nesse sentido, o art. 62 do 4º substitutivo do PL 2.338/23 determina que o desenvolvedor de IA que utilizar conteúdo protegido por direitos de autor e conexos deve tornar público quais conteúdos foram utilizados nos processos de treinamento dos sistemas de IA, por meio da publicação de sumário em sítio eletrônico de fácil acesso ou conforme disposto em regulamento.

A limitação da responsabilidade ao desenvolvedor de IA, em razão do acolhimento da emenda 44⁵², representa um avanço significativo. Isso não apenas esclarece quem deve cumprir a obrigação legal, mas também justifica o fato de que, como “criador” do sistema, o desenvolvedor detém a melhor posição para monitorar e relatar o uso de conteúdos protegidos por direitos autorais e conexos. Ao simplificar a cadeia de responsabilidade, o dispositivo também reduz custos associados ao cumprimento de obrigações legais por outros agentes de IA incentivando a competitividade e a inovação.

Embora a atribuição da responsabilidade seja inequívoca, a forma como essa obrigação será implementada ainda gera inúmeros questionamentos, especialmente no tocante à viabilidade técnica de se listar todos os conteúdos acessados e obter a prévia autorização para utilização (quando não aplicáveis as exceções do art. 63).

52. De autoria do Senador Chico Rodrigues, proposta em 17/06/2024.

Justamente em razão disso, a efetividade do dispositivo está condicionada a regulamentação do tema, que poderá se aproveitar das experiências colhidas em ambiente regulatório experimental (*sandbox*) estabelecido pelo Sistema Nacional de Regulação e Governança de Inteligência Artificial (SIA) e pelo órgão setorial competente⁵³, nos termos do Capítulo X, Seção I do 4º substitutivo.

Esse ambiente, inicialmente referenciado especificamente na Seção IV do PL, dedicada aos direitos de autor e conexos, foi originalmente destinado a abordar tanto a transparência quanto a remuneração (até o 2º substitutivo). No 3º substitutivo, seu escopo foi reduzido para tratar apenas da transparência e, finalmente, no 4º substitutivo, foi completamente suprimido desta seção.

Nesse contexto, embora a criação de um *sandbox* regulatório para experimentar e adaptar regras, visando garantir a transparência no uso de obras protegidas, esteja alinhada com as experiências internacionais, é crucial considerar o risco de abuso e violação de direitos nesse ambiente mais flexível, o que pode ter justificado a sua exclusão da Seção IV.

Sem prejuízo, a dificuldade na implementação de medidas de transparência e as incertezas decorrentes da falta de regulamentação específica merecem atenção, sendo essencial que eventual discussão do dever de transparência no âmbito de ambiente regulatório experimental sejam precedidas da delimitação clara dos parâmetros e limites do *sandbox*, juntamente com a implementação de mecanismos robustos de supervisão e o envolvimento de todas as partes interessadas, para assegurar que a flexibilidade regulatória não comprometa a proteção dos direitos autorais.

2.4 Direitos da personalidade e uso de imagem

O art. 66 do 4º substitutivo do PL 2.338/23 prevê que utilização de imagem, áudio, voz ou vídeo que retratem ou identifiquem pessoas deverá respeitar os direitos da personalidade, na forma do Código Civil e legislação pertinente.

Como forma de combate à desinformação causada, por exemplo, por *deep fakes*, também merece destaque o art. 19, que prevê a necessidade de indicação de conteúdo sintético gerado a partir de sistemas de IA, de modo a permitir a verificação de autenticidade e características de sua proveniência, modificações e transmissão. Tal previsão, é um reflexo da incorporação da disciplina da inteligência artificial generativa contemplada no PL nº 3.592, de 2023; no PL nº 145,

53. Antes do 3º substitutivo, chegou a ser defendida a responsabilidade exclusiva da autoridade setorial, ouvido o órgão central competente, e da SIA. Nesse sentido, a emenda 45, de autoria do Senador Chico Rodrigues, parcialmente acolhida, defendia que a tomada de decisões no âmbito do *sandbox* pela autoridade setorial teria a sua lisura comprometida, na medida em que sendo a autoridade composta por departamentos e órgãos federais da administração direta, poderia sofrer interferências políticas.

de 2024; e no PL nº 146, de 2024 – agregados ao texto do PL 2.338/23 para harmonizar as diversas iniciativas sobre o tema – e acolhimento da emenda nº 4⁵⁴.

No tocante às previsões correlatas aos direitos da personalidade, o PL vem sendo criticado em razão da aparente redundância com disposições do Código Civil, da LDA e da LGPD.

Nesse sentido, conforme se extrai dos fundamentos das sugestões de emenda nº 61, 72, 109 e 128, alguns dispositivos da nova normativa seriam, na verdade, uma reafirmação daquilo que já é tratado no Código Civil, especificamente nos artigos 11 e 20⁵⁵, que protegem os direitos da personalidade, assegurando que o uso da imagem, voz e outros atributos pessoais só poderá ocorrer mediante autorização ou em situações específicas, como a manutenção da ordem pública.

Da mesma forma, a legislação autoral brasileira já possuiria mecanismos para proteger os direitos dos autores em relação ao uso de suas obras por sistemas de IA⁵⁶, pois os artigos 29 e 31 dispõe que qualquer utilização, transformação ou adaptação de uma obra protegida por direitos autorais – como a criação de conteúdos derivados a partir de IA generativa – depende de autorização expressa do titular. Essas previsões, portanto, seriam suficientes para tratar grande parte dos problemas levantados pelo uso de IA relacionados à modificação ou geração de conteúdo derivado a partir do uso de obras protegidas, como imagens, vozes ou textos (ainda que utilizados apenas para treinamento dos sistemas).

Ainda, conforme pontuado pela ANPD⁵⁷, existem intersecções entre o PL 2.338/23 e a LGPD no tocante a coleta, uso de dados pessoais e exercício de direitos por titulares⁵⁸, de modo que a criação de uma nova autoridade regulatória responsável pela fiscalização do uso de sistemas de IA poderia gerar fragmentação regulatória.

54. De autoria do Senador Vanderlan Cardoso, apresentada em 18/04/2024, propondo a inclusão de marcas identificadoras em conteúdo gerado ou manipulado por inteligência artificial.

55. Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais. Parágrafo único. Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes.

56. Ver Nota Técnica nº 2/2024 da Coordenação-Geral de Regulação de Direitos Autorais do Ministério da Cultura. Disponível em: https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?yPDszXhdoN-cWQHJaQIHJmJlqCNXRK_Sh2SMdn1U-tzNsXmaDPgth6TWQbVegDsJUpxKCGrlfpqgd2LPweVjfrVUs865P0Y_aohlycyNue1ge1wXB9NIS-a8VWrNBh-Xw. Acesso em 13/10/24.

57. Ver Nota Técnica nº 16/2023/CGTP/ANPD: Sugestões de incidência legislativa em projetos de lei sobre a regulação da Inteligência Artificial no Brasil, com foco no PL nº 2338/2023.

58. Por exemplo, o direito à informação, à explicação e à solicitação de revisão poderia ser objeto de regulamentação e supervisão simultânea.

Nessa perspectiva, buscando uma maior harmonização com a legislação vigente, a fim de evitar sobreposição e/ou aplicação inconsistente da nova norma, a delimitação de cenários e inclusão de diretrizes que abordam especificamente o uso de IA⁵⁹ no contexto de direitos autorais e direitos da personalidade, como a inclusão de mecanismos claros para autorização e compensação dos autores no caso de uso de obras para treinamento de modelos, é recomendável.

Considerações finais

Este trabalho inicialmente abordou as definições a partir da legislação aplicável aos direitos autorais e, posteriormente, mapeou os dispositivos relacionados no PL 2.338/23 para regulamentar os direitos autorais e conexos no âmbito da IA. Através da análise de definições legislativas, da doutrina especializada, do texto do 4º substitutivo do PL e das emendas apresentadas, foram identificados quatro pontos principais que a nova normativa aborda, além de problemáticas que requerem maior amadurecimento e possíveis ajustes na redação atual.

Ao final, conclui-se que embora o PL nº 2338/2023 seja um marco importante para equilibrar a proteção dos direitos dos autores com a promoção da inovação tecnológica e integração da inteligência artificial, ainda existem incertezas significativas quanto à aplicação e eficácia das medidas propostas. A complexidade de se estabelecer a proteção dos direitos dos autores sem inviabilizar atividades de mineração e o uso de conteúdo protegido para desenvolvimento e treinamento de sistemas, evidencia os desafios enfrentados. Questões como a remuneração justa, a transparência nos usos e a implementação de modelos de licenciamento também dependem de previsões mais detalhadas para uma aplicação prática eficaz.

De modo a garantir que a legislação acompanhe o ritmo das inovações tecnológicas, sem se tornar um obstáculo para o desenvolvimento e competitividade do país e, ao mesmo tempo, promova um sistema de fiscalização robusto capaz de garantir o respeito aos direitos autorais e conexos mostra-se imprescindível que os debates sobre os direitos dos titulares, limitações aos direitos autorais, garantia de transparência e remuneração continuem a

59. Na contramão da delimitação de situações específicas, cabe mencionar a rejeição, em razão da limitação, no PL, da disciplina da inteligência artificial no aspecto do Direito Civil e com caráter geral e principiológico, das emendas nº 20, 102, 103 e 112 que tratavam, respectivamente, da tipificação de *deep fakes* como crime no Código Penal, da indicação do uso de IA em peças publicitárias, regras para o uso da imagem e áudio da pessoa falecida por meio de IA para fins comerciais, da exclusão de indicação de geração de conteúdo sintético para obras artísticas e literárias realizadas com fins culturais em contexto em que houver responsabilidade editorial.

amadurecer, com a participação multissetorial, equitativa dos interessados e observância das experiências internacionais. O tema, ao ser trazido para o debate, enriquece o processo legislativo, permitindo a coleta de pontos de vista diversos e o mapeamento de controvérsias.

Dado que o PL ainda está em discussão, esse trabalho permanece aberto para desenvolvimento posterior, sendo possível, por exemplo, comparar o texto final do regulamento aprovado com a redação ora analisada.

Referências

ABRÃO, Eliane. *Direitos de autor e direitos conexos*. São Paulo: Ed. do Brasil, 2002.

ALVARENGA, Miguel Bastos. *Mineração de dados, Big Data e Direitos Autorais no Brasil*. Tese (Mestrado em Políticas Públicas, Estratégias e Desenvolvimento) – Instituto de Economia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2019. p. 92. Disponível em: https://onda.org.br/resources/2020_Miguel%20ALVARENGA_Mest.pdf. Acesso em 27 jul 2024.

BITTAR, C.A. *Direito de Autor*. 5.ed. rev. atual. e ampl. por Eduardo C.B. Bittar. Rio de Janeiro: Forense, 2013.

BRANCO, Sérgio. *Direitos autorais na Internet e o uso de obras alheias*. Rio de Janeiro: Lumen Juris, 2007. Disponível em: <https://repositorio.fgv.br/items/9d286b3c-c77e-46f2-ad95-1bc48deb-d48c>. Acesso em: 13 jul 2024.

BRANCO, Sérgio. PARANAGUÁ, Pedro. *Direitos Autorais*. 1ª ed. Rio de Janeiro: Editora FGV. 2009. p. 50. Disponível em: <https://repositorio.fgv.br/server/api/core/bitstreams/3df3edc6-9a6f-486d-bff8-c1a717da24b4/content>. Acesso em: 13 jul 2024.

BRASIL. Autoridade Nacional de Proteção de Dados. *Análise preliminar do Projeto de Lei nº 2338/2023, que dispõe sobre o uso da Inteligência Artificial*. Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338_2023-formatado-as-com.pdf. Acesso em: 27 jul 2024.

BRASIL. Autoridade Nacional de Proteção de Dados. *Nota Técnica nº 16/2023/CGTP/ANPD: Sugestões de incidência legislativa em projetos de lei sobre a regulação da Inteligência Artificial no Brasil, com foco no PL nº 2338/2023*. Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf. Acesso em: 27 jul 2024.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 21, de 2020*. Estabelece princípios, direitos e deveres para o uso de inteligência artificial no Brasil, e dá outras providências. Brasília: Câmara dos Deputados, 2020. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2236340&fichaAmigavel=nao>. Acesso em: 20 jul 2024.

BRASIL. Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito. *Relatório Final da Comissão de Juristas responsável por subsidiar a elaboração de substitutivo sobre inteligência artificial no Brasil*. Disponível em: <https://legis.senado.leg.br/comissoes/mnas?cod-col=2504&tp=4>. Acesso em: 20 jul 2024.

BRASIL. Senado Federal. *Projeto de Lei nº 5691, de 2019*. Institui a Política Nacional de Inteligência Artificial, com o objetivo de estimular a formação de um ambiente favorável ao desenvolvimento de tecnologias em Inteligência Artificial. Brasília: Senado Federal, 2019. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/139586>. Acesso em: 20 jul 2024.

BRASIL. Senado Federal. *Projeto de Lei nº 5051, de 2019*. Estabelece os princípios para o uso da Inteligência Artificial no Brasil. Brasília: Senado Federal, 2019. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/138790>. Acesso em: 20 jul 2024.

BRASIL. Senado Federal. *Projeto de Lei nº 872, de 2021*. Dispõe sobre o uso da Inteligência Artificial. Brasília: Senado Federal, 2019. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/147434>. Acesso em: 20 jul 2024.

BRASIL. Senado Federal. *Projeto de Lei nº 2338, de 2023*. Dispõe sobre o uso da Inteligência Artificial. Brasília: Senado Federal, 2023. <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 29 nov 2024.

CABRAL, Plínio. *A Nova Lei de Direitos Autorais*. 4ª Edição. Editora Harbra. 2003.

CANTALI, Fernanda Borghetti. Inteligência artificial e direito de autor: tecnologia disruptiva exigindo reconfiguração de categorias jurídicas. *Revista de Direito, Inovação, Propriedade Intelectual e Concorrência*. Porto Alegre. v. 4. p. 1–21. Jul/Dez. 2018. Disponível em: <https://www.indexlaw.org/index.php/revistadipic/article/view/4667/pdf>. Acesso em: 20 jul. 2024.

CARBONI, Guilherme. *Direito Autoral, Diversidade das Expressões Culturais e Pluralidade de Autorias*. In: *Direito da Propriedade Intelectual, Vol II: estudos em homenagem ao Pe. Jorge Hammes* (Org. por Luiz Gonzaga Silva Adolfo e Marcos Wachowicz). Curitiba: Juruá. 2014.

CERON, Rodrigo. *AI, machine learning and deep learning: What's the difference?* IBM, 5 dez 2019. Disponível em: <https://www.ibm.com/blog/ai-machine-learning-and-deep-learning-whats-the-difference/>. Acesso em 13 jul 2024.

EUROPEAN PARLIAMENT NEWS. *What is artificial intelligence and how is it used?* 4 set. 2020. Disponível em: <https://www.europarl.europa.eu/news/en/headlines/society/20200827ST085804/what-is-artificial-intelligence-and-how-is-it-used>. Acesso em 13 jul 2024.

INSTITUTO DE DEFESA DE CONSUMIDORES (IDEC). *Contribuição do Idec ao Substitutivo da CTIA ao Projeto de Lei 2.338/2023 (Inteligência Artificial)*. Maio, 2024. Disponível em: https://idec.org.br/sites/default/files/2024_idec_-_analise_do_substitutivo_ao_pl_2338_23_-_inteligencia_artificial_08.05.2024_.docx.pdf. Acesso em: 13 jul 2024.

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET (LAPIN). *Projeto de Lei nº 2338/2023 – Nota Técnica*. Agosto, 2023. Disponível em: <https://direitosnarede.org.br/2023/08/23/coalizao-direitos-na-rede-divulga-nota-tecnica-sobre-o-pl-2338-2023-que-busca-regular-a-ia/>. Acesso em: 13 out 2024.

MINISTÉRIO DA CULTURA – COORDENAÇÃO-GERAL DE REGULAÇÃO DE DIREITO AUTORAIS CGREG/DIREG/SDAI/GM/MinC. *Nota Técnica nº 2/2024*. Disponível em: https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?yPDszXhdoNcWQHJa-QLHJmJlqCNXRK_Sh2SMdn1U-tzNsXmaDPgth6TWQbVegDsJUpxKCGrlfpqgd2LPweVjfrVUs-865P0Y_aohlycyNue1ge1wXB9NlS-a8VWrNBh-Xw. Acesso em 13 out 2024.

ROCHA, Maria Victória. Prospecção de texto e dados (text and data mining) na diretiva relativa aos direitos de autor e direitos conexos no mercado único digital. *RRDDIS – Revista Rede de Direito Digital, Intelectual & Sociedade*, Curitiba, v. 2, n. 4, p. 99-164, 2022, p. 103. Disponível em: <https://revista.ioda.org.br/index.php/rrddis/article/view/76/45>. Acesso em 16 jul. 2024.

SCHERER, Matthew U. Regulating Artificial Intelligence Systems: risks, challenges, competencies, and strategies. *Harvard Journal of Law & Technology*, vol, 29, nº 2, 2016, p. 354-400. Disponível em: <https://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf>. Acesso em 13 jul 2024.

SCHIRRU, Luca. *Direito autoral e inteligência artificial: autoria e titularidade nos produtos da IA*. Tese (Doutorado em Políticas Públicas, Estratégias e Desenvolvimento) – Instituto de Economia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2020. Disponível em: https://www.ie.ufrj.br/images/IE/PPED/Teses/2020/Vers%C3%A3o%20final_Tese%20Luca_PDFA.pdf. Acesso em: 13 jul. 2024.

SOUZA, Allan Rocha de. Direitos morais do autor. *Civilistica.com*. Rio de Janeiro, a. 2, n. 1, jan.-mar./2013. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/73/53>. Acesso em: 27 jul.2024.

SOUZA, Allan Rocha de. SCHIRRU, Luca. Alvarenga. MIGUEL BARROS. Mineração de textos e dados na pesquisa em saúde: reflexões sobre direitos autorais. *Cadernos de Saúde Pública* 2024. Disponível em: <https://cadernos.ensp.fiocruz.br/ojs/index.php/csp/article/view/8597/19335>. Acesso em: 27 jul.2024.

STAUT JÚNIOR, Sérgio Said. *Direitos Autorais: entre as relações sociais e as relações jurídicas*. Moinho do Verbo. Curitiba. 2006.

TURING, A. M. Computing Machinery and Intelligence. *Mind*, v. 59, n. 236, p. 433-460, out. 1950. Disponível em: <https://academic.oup.com/mind/article/LIX/236/433/986238>. Acesso em: 13 jul 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

7

Originalidade Algorítmica: há originalidade nos outputs da inteligência artificial generativa?

TAÍS BIGARELLA LEMOS

Sumário: Introdução. 1. Conceito de originalidade para o direito autoral. 2. Mas como funciona a inteligência artificial? 3. Métricas de avaliação da originalidade dos *outputs* gerados por inteligência artificial. Considerações finais. Referências. Anexo I.

Introdução

O tema da inteligência artificial está cada vez mais em voga, não apenas no meio acadêmico e profissional, mas também em ambientes mais informais, no cotidiano da população. Assim sendo, por vezes tem-se a incorreta percepção do que ela significa, inclusive com o imaginário de que inteligência artificial seria vinculada a robôs e itens futuristas, como carros voadores. A inteligência artificial, contudo, caracteriza-se por ser um campo de estudo conhecido pelo desenvolvimento e uso de máquinas capazes de realizar tarefas que normalmente demandariam inteligência humana.²

O desenvolvimento de uma inteligência artificial envolve “*machine learning*” e “*deep learning*”. O “*machine learning*” é um ramo da inteligência artificial e da ciência da computação que estuda o uso de dados e algoritmos para possibilitar que a inteligência artificial imite a forma como os humanos aprendem, para aprimorar a sua precisão.³ Já o “*deep learning*” caracteriza-se por usar multicamadas de redes neurais para simular o complexo processo decisório da mente humana.⁴

A inteligência artificial consiste, assim, em diferentes modelos de “*machine learning*”, sendo o que os diferencia a forma como usam e compreendem os dados.⁵ Os *softwares* das inteligências artificiais estão se tornando cada vez mais complexos, produzindo trabalhos nunca antes realizados por computadores.⁶ Por exemplo, a última geração de inteligência artificial generativa, que

1. Mestre em Direito pela Universidade Federal do Rio Grande do Sul (2022). Bacharela em Ciências Jurídicas e Sociais pela Universidade Federal do Rio Grande do Sul (2018). Assessora de Desembargadora no Tribunal de Justiça do Rio Grande do Sul. E-mail: taisbigarella@gmail.com.

2. FEINGOLD, S. What is artificial intelligence – and what is it not?. World Economic Forum, 2023. Disponível em: <https://www.weforum.org/agenda/2023/03/what-is-artificial-intelligence-and-what-is-it-not-ai-machine-learning>. Acesso em: 02 ago. 2024.

3. IBM. What is machine learning?. IBM, 2024. Disponível em: <https://www.ibm.com/topics/machine-learning>. Acesso em: 02 ago. 2024.

4. HOLDSWORTH, J.; SCARPICCHIO, M. What is deep learning?. IBM, 2024. Disponível em: <https://www.ibm.com/topics/deep-learning>. Acesso em: 02 ago. 2024.

5. FEINGOLD, S. What is artificial intelligence – and what is it not?. World Economic Forum, 2023. Disponível em: <https://www.weforum.org/agenda/2023/03/what-is-artificial-intelligence-and-what-is-it-not-ai-machine-learning>. Acesso em: 02 ago. 2024.

6. NAQVI, Zack. Artificial Intelligence, Copyright, and Copyright Infringement. *Marquette Intellectual Property Law Review*, vol. 24, no. 1, Inverno 2020, p. 16. Acesso via HeinOnline.

vem surpreendendo à população e trazendo novos questionamentos, especialmente com o lançamento do ChatGPT, consegue aprender e sintetizar não apenas a linguagem humana, mas outros dados, como imagens e vídeos.⁷ Esses sistemas são um tipo de modelo de inteligência artificial, denominado modelo de linguagem de grande escala, normalmente chamados pelo seu nome em inglês “*Large Language Model*” ou apenas pela sigla “LLM”, e são capazes de executar diversas tarefas de entendimento de linguagem e geração de texto em um nível sem precedentes.⁸ Para treinar esses modelos a pensar e a agir, algumas estratégias podem ser utilizadas e, dentre elas, estão a seleção de documentos, a vinculação a mecanismos de pesquisa e o treinamento de sistemas de respostas a perguntas.⁹ São colocados “*inputs*” no sistema, que resultam em “*outputs*”.

Essas novas tecnologias desafiam o ordenamento jurídico e, dentre estes desafios, estão os que envolvem a tutela de direitos autorais, tanto dos documentos utilizados para treinamento do sistema, como daqueles resultados obtidos pelo sistema, os “*outputs*”. No que se refere aos dados utilizados para aprendizado dos modelos, muito se vem discutindo acerca da possibilidade de utilização de obras protegidas por direitos autorais, especialmente em razão de caso conhecido, em que o The New York Times processou a OpenAI e a Microsoft em razão do uso dos seus artigos para o treinamento das inteligências artificiais.¹⁰

Outro tema em voga é se a inteligência artificial poderia ser autora de obra intelectual, considerando o entendimento de que apenas pessoas físicas teriam tal capacidade, porquanto as únicas que seriam capazes de criar uma obra.¹¹ Contudo, há um aspecto essencial para que uma criação seja protegida por direitos autorais que parece pouco observada quando se analisa os produtos de inteligência artificial, ainda que, sem ela, não exista proteção por direitos autorais: a originalidade.

7. IBM. What is artificial intelligence?. IBM, 2024. Disponível em: <https://www.ibm.com/topics/artificial-intelligence>. Acesso em: 02 ago. 2024.

8. MIALON, Grégoire; DESSI, Roberto; LOMELI, Maria; NALMPANTIA, Christoforos; PASUNURU, Ram; RAILEANU, Roberta; ROZIÈRE, Baptiste; SCHICK, Timo; DWIVEDI-YU, Jane; CELIKYILMAZ, Asli; GRAVE, Edouard; LECUN, Yann; e SCIALOM, Thomas. *Augmented Language Models: a Survey*. arXiv, 2023, <https://doi.org/10.48550/arXiv.2302.07842> 2302.07842. p. 2.

9. MIALON, Grégoire; DESSI, Roberto; LOMELI, Maria; NALMPANTIA, Christoforos; PASUNURU, Ram; RAILEANU, Roberta; ROZIÈRE, Baptiste; SCHICK, Timo; DWIVEDI-YU, Jane; CELIKYILMAZ, Asli; GRAVE, Edouard; LECUN, Yann; e SCIALOM, Thomas. *Augmented Language Models: a Survey*. arXiv, 2023, <https://doi.org/10.48550/arXiv.2302.07842> 2302.07842. p. 17.

10. POPE, A. NYT v. OpenAI: The Time’s About-Face. Harvard Law Review, 2024. Disponível em: <https://harvardlawreview.org/blog/2024/04/nyt-v-openai-the-timess-about-face/>. Acesso em: 06 ago. 2024.

11. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; e RAMOS, Carolina Tinoco. *O Contributo Mínimo na Propriedade Intelectual: Atividade Inventiva, Originalidade, Distinguibilidade e margem mínima*. Rio de Janeiro: Lumen Juris, 2010. p. 434.

Apenas são objeto de proteção aquelas criações que tenham um *algo a mais*, para que assim possam fazer jus à qualidade de obra.¹² Seja denominada como originalidade, criatividade, individualidade ou contributo mínimo, necessário que esse *algo a mais* exista para que haja proteção autoral. E, nesse sentido, antes mesmo de pensar acerca da autoria dos *outputs* da inteligência artificial, parece essencial analisar se esses resultados teriam esse *algo a mais*, autorizando a proteção autoral. Ora, se a “criação” não for considerada uma obra intelectual protegida, não há por que debater quem teria os direitos como seu autor, porquanto sequer seria objeto de proteção.

Assim, o problema de pesquisa do presente trabalho é analisar se existe originalidade nos resultados/*outputs* obtidos pelos usuários de sistemas de inteligência artificial generativa, considerando a doutrina do direito autoral.

Para tanto, será analisado, no primeiro capítulo, o conceito de originalidade para o direito autoral, para depois examinar, no segundo capítulo, a forma de funcionamento das inteligências artificiais e finalizar, no terceiro e último capítulo, com as métricas para avaliação da originalidade dos *outputs* e entendimentos de outros ordenamentos jurídicos sobre o tema.

1. Conceito de originalidade para o direito autoral

A compreensão da extensão dos direitos autorais é complexa, desafiando muitas dúvidas nas análises dos casos concretos. Ao contrário daqueles direitos tutelados pela Propriedade Industrial,¹³ a Lei de Direitos Autorais, de nº 9.610/98,¹⁴ doravante referida pela sua sigla, LDA, é mais ampla ao definir o objeto da sua proteção, demandando uma análise de cada criação, a fim de verificar se atende aos requisitos para proteção.

Iniciando pela análise legislativa, o *caput* do artigo 7º da LDA define como obras intelectuais protegidas “as criações do espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se

12. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; e RAMOS, Carolina Tinoco. *O Contributo Mínimo na Propriedade Intelectual: Atividade Inventiva, Originalidade, Distinguibilidade e margem mínima*. Rio de Janeiro: Lumen Juris, 2010. p. 307.

13. A Lei de Propriedade Industrial (nº 9.279/96) protege direitos de propriedade intelectual com características menos amplas e mais requisitos, inclusive com a necessidade de registro no Instituto Nacional de Propriedade Industrial (INPI), como as patentes, os desenhos industriais e as marcas. Por isso, é muito comum o entendimento de que, quando um produto/uma criação não se encaixa em nenhuma desses direitos, há a tentativa de encaixá-la como uma criação protegível por direitos autorais.

14. BRASIL. *Lei n. 9.610 de 19 de fevereiro de 1998*. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/l9610.htm>.

invente no futuro, tais como” os exemplos trazidos em seus treze incisos.¹⁵ Dentre eles, pode-se destacar os textos de obras literárias, artísticas ou científicas, as obras audiovisuais, as composições musicais, as ilustrações e os desenhos.

A previsão legal é, conforme se verifica do próprio teor do *caput* do artigo, bastante ampla, sendo o rol dos seus incisos meramente exemplificativo,¹⁶ de forma que outras obras intelectuais, não elencadas, podem ser objeto de proteção, desde que atendam aos demais requisitos legais. Nesse ponto, importante destacar que o direito de autor decorre de uma política de proteção, tentando sopesar o acesso da sociedade às obras e o incentivo ao autor,¹⁷ mediante a concessão do direito de monopólio sobre a obra.

Assim, é de suma importância a análise, primeiramente, de se a criação tem os atributos necessários para ser objeto de proteção autoral, sob pena de até mesmo influenciar neste balanceamento entre o acesso à sociedade e o monopólio dado ao autor. E, nesse sentido, mostra-se essencial examinar se há originalidade em uma criação para que ela tenha direito à proteção. Isso porque a originalidade, também denominada pela doutrina como “contributo mínimo” ou criatividade, é o único filtro existente no ordenamento brasileiro e que serve como estímulo para que o autor, o sujeito, externe o seu espírito criativo, criando algo distinto do que o antecedeu.¹⁸

Inexiste, no entanto, uma unanimidade sobre o que caracteriza a originalidade. Tradicionalmente, verifica-se uma distinção entre a interpretação do termo nos países de tradição de *common law*, que adotam o *copyright*,¹⁹ como os Es-

15. Art. 7º São obras intelectuais protegidas as criações do espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se invente no futuro, tais como:

- I - os textos de obras literárias, artísticas ou científicas;
- II - as conferências, alocações, sermões e outras obras da mesma natureza;
- III - as obras dramáticas e dramático-musicais;
- IV - as obras coreográficas e pantomímicas, cuja execução cênica se fixe por escrito ou por outra qualquer forma;
- V - as composições musicais, tenham ou não letra;
- VI - as obras audiovisuais, sonorizadas ou não, inclusive as cinematográficas;
- VII - as obras fotográficas e as produzidas por qualquer processo análogo ao da fotografia;
- VIII - as obras de desenho, pintura, gravura, escultura, litografia e arte cinética;
- IX - as ilustrações, cartas geográficas e outras obras da mesma natureza;
- X - os projetos, esboços e obras plásticas concernentes à geografia, engenharia, topografia, arquitetura, paisagismo, cenografia e ciência;
- XI - as adaptações, traduções e outras transformações de obras originais, apresentadas como criação intelectual nova;
- XII - os programas de computador;
- XIII - as coletâneas ou compilações, antologias, enciclopédias, dicionários, bases de dados e outras obras, que, por sua seleção, organização ou disposição de seu conteúdo, constituam uma criação intelectual.

16. ABRÃO, Eliane Yachouh. *Direitos de autor e Direitos conexos*. 1ª ed. São Paulo: Editora do Brasil, 2002. p. 97.

17. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; e RAMOS, Carolina Tinoco. *O Contributo Mínimo na Propriedade Intelectual: Atividade Inventiva, Originalidade, Distinguibilidade e margem mínima*. Rio de Janeiro: Lumen Juris, 2010. p. 309.

18. BARBOSA, Pedro Marcos Nunes. Originalidade em Crise. *Revista Brasileira de Direito Civil*, vol. 15, 2018, p. 38-39. Acesso via HeinOnline.

19. A origem do *copyright* deu-se na Inglaterra, com o Estatuto da Rainha Ana, posteriormente influenciando os Estados Unidos da América, com uma perspectiva de ser voltado para sociedade, para promover a disseminação das obras. Para maiores informações sobre o tema, veja-se GINSBURG, Jane C. A Tale of Two Copyrights: Literary Property in Revolutionary France and America. *Tulane Law Review*, vol. 64, nº 5, maio de 1990. p. 991-1031.

tados Unidos da América, que empregava a “*sweat of the brow doctrine*”, para, depois, passar para a teoria da criatividade *de minimis*; e aqueles de tradição romano-germânica ou de *civil law*, que utilizam a ideia da doutrina da criatividade.²⁰

A “*sweat of the brow doctrine*”, traduzida como teoria do suor na testa, é a que entende que o trabalho e a indústria, ainda sem qualquer criatividade, poderiam ser suficientes para atendimento ao requisito da originalidade para o *copyright*.²¹ O *copyright* nasce da ideia de uma certa materialização do direito de autor, pois, como diz o próprio nome, tinha o objetivo de proteger o “direito de cópia”, ou seja, a base do direito era a obra copiável. Assim, nesse sistema, a ideia original é de que a utilidade econômica da cópia seria mais relevante que a criatividade da matéria,²² de forma que a teoria do suor na testa nasce dentro desse contexto, em que realmente dava-se menos importância para a criatividade envolvida na criação.

A doutrina da criatividade, por sua vez, entende que deve ser estabelecido um *quantum* mínimo de criatividade para que haja a proteção pelo direito autoral, ainda que seja módico, bem como exigir que o trabalho não seja cópia de outro. Nesse raciocínio, a mera compilação de informações sem um mínimo de criatividade não poderia ser objeto de proteção.²³

Nos Estados Unidos da América, em 1991, com o julgamento do caso Feist²⁴, foi afastada a aplicação da teoria “*sweat of the brow*”, sendo fixado o entendimento no sentido de que, para atender ao requisito da originalidade, a obra deve demonstrar nível mínimo de criatividade.²⁵ No caso, tratava-se de uma compilação e entendido que, a seleção, coordenação e organização da compilação não satisfaziam o mínimo constitucional para proteção pelo *copyright*, pois eram comuns, apenas com a listagem em ordem alfabética. Assim, entende-se que foi aplicada a teoria da criatividade *de minimis*.

Passando para o contexto brasileiro, a LDA não é clara em relação a qual teoria foi adotada, contudo, sendo o Brasil um país que faz parte da tradição

20. PONTES, Leonardo Machado. *Direito de Autor: a teoria da dicotomia entre a ideia e a expressão*. Belo Horizonte: Arraes Editora, 2012. p. 43.

21. PONTES, Leonardo Machado. *Direito de Autor: a teoria da dicotomia entre a ideia e a expressão*. Belo Horizonte: Arraes Editora, 2012. p. 44.

22. ASCENSÃO, José de Oliveira. Direito de autor sem autor e sem obra. *Stvdia Ivridica*, Ad Honorem –3, Boletim da Faculdade de Direito, Universidade de Coimbra, 1991. p. 88.

23. PONTES, Leonardo Machado. *Direito de Autor: a teoria da dicotomia entre a ideia e a expressão*. Belo Horizonte: Arraes Editora, 2012. p. 45.

24. ESTADOS UNIDOS DA AMÉRICA. U.S. Supreme Court. Feist Pubs., Inc. v. Rural Tel. Svc. Co., Inc., 499, U.S. 340. Recorrente: Feist Pubs. Inc.. Recorrido: Rural Tel. Svc. Co., Inc. Relatora: Justice Sandra Day O'Connor, 27 de março de 1991. Disponível em: <https://supreme.justia.com/cases/federal/us/499/340/>. Acesso em: 27 jul. 2024.

25. Conforme parte do voto no caso Feist, em que assim refere: “Originality requires only that the author make the selection or arrangement independently (i.e., without copying that selection or arrangement from another work), and that it display some minimal level of creativity”. Disponível em: <https://supreme.justia.com/cases/federal/us/499/340/>. Acesso em: 27 jul. 2024.

romana-germânica, há uma inclinação para a teoria da criatividade.²⁶ Ademais, partindo das previsões da Convenção de Berna e do TRIPs, explica Leonardo Pontes que, na legislação brasileira:

o termo “criação intelectual” será mais corretamente interpretado no sentido de *creativity doctrine*, na medida em que, por meio dessa doutrina, a lei não protegeria compilações de *produções*, uma vez que estas *não representam algo mais que trivial ou mecânico em sua natureza*.²⁷

Explicam Barbosa, Souto Maior e Tinoco que parece fazer parte do consciente coletivo, tanto da doutrina como da jurisprudência brasileira, ser necessária a presença do “*algo a mais*”, ou seja, de um contributo mínimo, para que uma criação possa ser considerada uma obra. O termo utilizado para identificar este contributo pode variar na doutrina, com a utilização de diferentes termos como “criatividade”, “originalidade”, “individualidade” e congêneres.

José de Oliveira Ascensão, por exemplo, ao conceituar criatividade, refere que a obra deve ter o mínimo de criatividade ou originalidade, explicando que, quando se passa da criação para a descrição, quando é o objeto que comanda, em vez do papel predominante ser a visão do autor, já não se está mais no âmbito da tutela autoral.²⁸

No presente trabalho, utiliza-se a expressão “originalidade” no sentido da doutrina da criatividade, entendendo pela necessidade de a obra apresentar um grau mínimo de criatividade, um contributo mínimo, para a proteção autoral. Ainda, a escolha do termo “originalidade” se dá por ser o termo considerado mais popular para designar tal atributo da criação autoral, inclusive por se tratar de expressão comumente utilizada na língua inglesa²⁹ e que, portanto, mais interessante para o caso, em que se tem como enfoque a originalidade na inteligência artificial.

Posto o conceito de originalidade para o direito autoral, passa-se à análise da inteligência artificial e métricas possíveis para avaliação da originalidade de *outputs*.

26. PONTES, Leonardo Machado. *Direito de Autor: a teoria da dicotomia entre a ideia e a expressão*. Belo Horizonte: Arraes Editora, 2012. p. 49.

27. PONTES, Leonardo Machado. *Direito de Autor: a teoria da dicotomia entre a ideia e a expressão*. Belo Horizonte: Arraes Editora, 2012. p. 51.

28. ASCENSÃO, José de Oliveira. *Direito autoral*. 2ª. ed., ref. e ampl. Rio de Janeiro: Renovar, 1997. p. 57.

29. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; e RAMOS, Carolina Tinoco. *O Contributo Mínimo na Propriedade Intelectual: Atividade Inventiva, Originalidade, Distinguibilidade e margem mínima*. Rio de Janeiro: Lumen Juris, 2010. p. 311.

2. Mas como funciona a inteligência artificial?

Conforme já referido em introdução, inteligência artificial é um grupo de técnicas ou instruções que tem como objetivo simular a cognição biológica, a inteligência humana, utilizando máquinas. Atualmente, a maior parte das inteligências artificiais utiliza-se da técnica de “*machine learning*” que, como também já referido, usa algoritmos que podem “aprender” ou aprimorar em performance para tarefas específicas, com base nas instruções programadas. Pode, contudo, se entender que a inteligência artificial seria uma “caixa preta”, pois o programador apenas visualiza aquilo que coloca para “alimentar” o sistema, o “*input*”, e o resultado, o “*output*”, sem conseguir observar especificamente o processo de aprendizagem da máquina.³⁰

No presente trabalho, o enfoque da análise dá-se nas inteligências artificiais generativas, que geram no seu *output*, ou resultado, criações que poderiam ser consideradas objeto de proteção autoral. Como referido no capítulo acima, o artigo 7º da LDA elenca algumas hipóteses de criações que poderiam ser protegidas e, dentre as hipóteses trazidas pelos seus incisos,³¹ destacam-se, para fins da presente análise, os textos de obras literárias e as ilustrações.

Isso porque, atualmente, existem inteligências artificiais capazes, aparentemente, de gerar esses tipos de criações. A mais famosa das ferramentas é o ChatGPT, um *chatbot* capaz de criar parágrafos coerentes, por meio da previsão de qual seria a próxima palavra mais provável em uma frase.³² Essa ferramenta é capaz de criar textos completos, que poderiam, em uma primeira visão, ser consideradas obras literárias. O ChatGPT é um modelo de linguagem de grande escala, normalmente denominado em inglês, um “*Large Language Model*” ou LLM, construído com base em treinamento com uma quantidade massiva de documentos/textos. Os modelos incorporam as informações obtidas pelo conjunto de dados e, assim, aprendem padrões de palavras para um determinado contexto, processo que possibilita que o usuário obtenha como resultado a combinação de palavras mais provável, gerando uma linguagem mais natural.³³

No Anexo I do presente trabalho, demonstra-se uma resposta dada pela ferramenta, quando solicitada a “Escrever uma obra literária de romance, de

30. NAQVI, Zack. Artificial Intelligence, Copyright, and Copyright Infringement. *Marquette Intellectual Property Law Review*, vol. 24, no. 1, Inverno 2020, p. 19. Acesso via HeinOnline.

31. Vide nota de rodapé nº 14.

32. FEINGOLD, S. What is artificial intelligence – and what is it not?. World Economic Forum, 2023. Disponível em: <https://www.weforum.org/agenda/2023/03/what-is-artificial-intelligence-and-what-is-it-not-ai-machine-learning>. Acesso em: 02 ago. 2024.

33. POPE, A. NYT v. OpenAI: The Time’s About-Face. *Harvard Law Review*, 2024. Disponível em: <https://harvardlawreview.org/blog/2024/04/nyt-v-openai-the-timess-about-face/>. Acesso em: 06 ago. 2024.

quatro parágrafos, retratando uma história de amor com final feliz”. Do resultado, confirma-se que, de uma primeira análise, seria inclusive intuitivo ao leitor entender que aquele texto se trata de uma obra literária, ainda mais não sabendo a sua origem, ou seja, que fruto de inteligência artificial.

Outra ferramenta muito interessante, também de inteligência artificial generativa, é a DALL-E, inclusive de mesmo desenvolvedor do ChatGPT, a empresa OpenAI. Essa ferramenta não gera textos, mas, conforme explica no seu *site*, é um sistema capaz de criar imagens realistas ou arte pela descrição dada pelo usuário.³⁴ Da mesma forma referida para o ChatGPT, o seu resultado, em um primeiro olhar, pode igualmente ser entendido como passível de proteção autoral, por criar ilustrações e obras visuais.

Ambos esses sistemas têm proteção pelo ordenamento brasileiro pela Lei de *Software* (Lei nº 9.609/98), que protege o programa de computador, enquanto “expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados”³⁵. Contudo, como bem refere o legislador, essa proteção é para a expressão do conjunto organizado de instruções, ou seja, para o modelo em si utilizado, e não necessariamente para os produtos dele obtidos. É diferente, portanto, a proteção do *software* em si, dos códigos utilizados pela inteligência artificial, que parece pacífico estar abrangido pela Lei de *Software*, e dos seus *outputs*, que se discute se poderiam ser objeto de proteção autoral.

Essencial, assim, analisar o que preveem os Termos de Uso das plataformas mencionadas, ChatGPT e DALL-E, acerca da titularidade e proteção dos resultados por elas obtidos. Os Termos de Uso de ambas são o mesmo, enquanto serviços oferecidos pela mesma empresa, a OpenAI.³⁶ O primeiro esclarecimento dado é que os Termos de Uso constituem um acordo entre o usuário e a OpenAI, incluindo previsões importantes para a resolução de disputas e que, ao usar os serviços, o usuário está concordando com estes Termos. Ressalvada, ainda, a existência de outros Termos de Uso para residentes da União

34. Conforme informações em: OpenAI. DALL-E 2. OpenAI, 2024. Disponível em: <https://openai.com/index/dall-e-2/>. Acesso em: 03 ago. 2024.

35. Conforme art. 1º da Lei nº 9.609/98. BRASIL. *Lei n. 9.609 de 19 de fevereiro de 1998*. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9609.htm.

36. Os termos de uso estão disponíveis em: OpenAI. Terms of use. OpenAI, 2024. Disponível em: <https://openai.com/policies/terms-of-use/>. Acesso em: 04 ago. 2024.

Europeia, Suíça e Reino Unido, que não serão analisados no presente trabalho, pois o enfoque se dá na regulação brasileira.

Dito isto, no que se refere especificamente aos *outputs*, os Termos de Uso consignam que os *inputs* e *outputs*, conjuntamente, são denominados “conteúdo”. A titularidade do conteúdo, por sua vez, é prevista no sentido de que, na extensão permitida pela legislação aplicável, o usuário detém os direitos de titularidade sobre o *input* colocado e, ainda, é dono do *output*. Assim prevê o item:

Propriedade do conteúdo. Entre o usuário e a OpenAI, na medida do permitido pela lei aplicável, o usuário (a) mantém os seus direitos de propriedade sobre o *input* e (b) é proprietário do *output*. Pelo presente, atribuímos ao usuário todos os nossos direitos, títulos e interesses, se houver, pelo *output*.³⁷

Especificamente quanto à existência de direitos autorais sobre esses resultados, não há menção nos Termos de Uso, que apenas traz uma parte referindo a possibilidade de envio de notificação pelo usuário, caso entenda que o seu direito de *copyright* esteja sendo infringido pela plataforma. Interessante, no entanto, pontuar que há uma sessão nos Termos em que são elencadas as atividades que não podem ser realizadas pelo usuário (“*What you cannot do*”) e, dentre elas, está apresentar o *output* como gerado por humanos, quando não o foi.³⁸

Verifica-se que não há, portanto, ao menos nos Termos de Uso, uma pretensão expressa pela empresa de entender que os resultados obtidos seriam protegidos por direito autoral e, ainda se fossem, são atribuídos aos usuários os direitos sobre essas obras, ressalvando, contudo, que esses resultados não podem ser apresentados como gerados por seres humanos, pois não o foram.

Parece fazer sentido que não se presuma, nos Termos de Uso, a existência de uma proteção autoral sobre esses resultados. Isso porque, conforme já referido, para que uma criação seja protegida por direito autoral, necessário que ela cumpra diferentes requisitos e, dentre eles, está o da originalidade, objeto do presente trabalho, motivo pelo qual passa-se à análise das métricas para avaliações da originalidade desses resultados/*outputs*.

37. Tradução livre da autora de: “**Ownership of content.** As between you and OpenAI, and to the extent permitted by applicable law, you (a) retain your ownership rights in Input and (b) own the Output. We hereby assign to you all our right, title, and interest, if any, in and to Output.” Disponível em: OpenAI. Terms of use. OpenAI, 2024. Disponível em: <https://openai.com/policies/terms-of-use/>. Acesso em: 04 ago. 2024.

38. No original, assim é redigido o item: “Represent that Output was human-generated when it was not”. OpenAI. Terms of use. OpenAI, 2024. Disponível em: <https://openai.com/policies/terms-of-use/>. Acesso em: 04 ago. 2024.

3. Métricas de avaliação da originalidade dos outputs gerados por Inteligência Artificial

Para avaliação de se existente um *quantum* mínimo de originalidade ou criatividade a justificar a proteção pelo direito autoral, também denominado pela doutrina de contributo mínimo, primeiro essencial pensar na definição de obra, uma vez que não é possível dizer que uma criação é uma obra se não estiver presente uma criatividade mínima na sua realização.³⁹ Para identificação de uma criação como obra, entende a doutrina que se deve, em um primeiro momento, olhar para o seu criador, podendo ser obra apenas se o seu criador intelectual for pessoa humana que possua imputação no seu resultado final. Após, ainda, necessário identificar se a criação foi exteriorizada, não está dentre as proibições legais e, por fim, apresente um contributo mínimo.⁴⁰

O contributo mínimo, por sua vez, caracteriza-se pela mínima criatividade necessária para existência de uma obra e, inclusive, auxilia a separação entre as obras, de forma que, se existente o contributo mínimo, inexiste plágio.⁴¹ Nesse ponto, importante entender que, se há contributo mínimo para diferenciar uma obra de outra, ainda que a primeira tenha se baseado na segunda, entende-se que há uma obra, no entanto, essas obras são denominadas obras derivadas. As obras derivadas são obras como de tradução e adaptação e, dessa forma, demandam autorização do titular da obra original, mas a elas se atribui titularidade originária, por ser uma criação intelectual, com suficiente criatividade, independente dos direitos de autores das obras pré-existentes, que continuam íntegros.⁴²

Já para a medição do *quantum* de criatividade ou originalidade necessário para a proteção da obra como direito autoral, Leonardo Machado Pontes sugere a utilização de três critérios: (i) a pessoa responsável pela composição do trabalho e seu direito desenvolvimento deve ser o autor, ao contrário da pessoa que simplesmente segue ordens para executar o trabalho; (ii) quanto maior a participação mecânica no processo da obra, mais deve o autor demonstrar que merece a proteção; e (iii) a autoria equivale à originalidade e à criatividade.⁴³

39. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; e RAMOS, Carolina Tinoco. *O Contributo Mínimo na Propriedade Intelectual: Atividade Inventiva, Originalidade, Distinguibilidade e margem mínima*. Rio de Janeiro: Lumen Juris, 2010. p. 446.

40. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; e RAMOS, Carolina Tinoco. *O Contributo Mínimo na Propriedade Intelectual: Atividade Inventiva, Originalidade, Distinguibilidade e margem mínima*. Rio de Janeiro: Lumen Juris, 2010. p. 449.

41. BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; e RAMOS, Carolina Tinoco. *O Contributo Mínimo na Propriedade Intelectual: Atividade Inventiva, Originalidade, Distinguibilidade e margem mínima*. Rio de Janeiro: Lumen Juris, 2010. p. 470.

42. COSTA NETTO, José Carlos. *Direito Autoral no Brasil*. Coordenação Hélio Bicudo. São Paulo: FTD, 1998. p. 63.

43. PONTES, Leonardo Machado. *Direito de Autor: a teoria da dicotomia entre a ideia e a expressão*. Belo Horizonte: Arraes Editora, 2012. p. 88-94.

Quanto ao primeiro critério, reside na diferenciação entre o autor da obra e aquele *mero executor*, que apenas cumpre ordens de terceiro, sem qualquer aprimoramento. Já o segundo critério trata da necessidade, ainda quando a obra for criada com o auxílio de máquinas, de se seguir um *standard*, ainda que baixo, a fim de demonstrar a expressão da criatividade, mesmo que mínima. A proteção apenas existiria quando identificado que a obra não é *produção automática de uma máquina*, mas há expressão de um autor.⁴⁴ Por fim, o terceiro e último critério refere-se à constatação de que, ao fim, para existir a proteção autoral, a originalidade e a criatividade significam apenas que a criação precisa prover de trabalho do autor, não sendo *cópia de outro trabalho*.⁴⁵

Assim, para avaliar se há originalidade ou criatividade, ainda que em *quantum* mínimo, nos *outputs* da inteligência artificial generativa, mostra-se necessário analisar se atendem estes três critérios. Pelas premissas estabelecidas nos tópicos anteriores, sabe-se que as inteligências artificiais ora em estudo funcionam de forma que, realizada uma solicitação pelo usuário (*input*), obtido um resultado ou *output* que pode, superficialmente, parecer uma obra protegida por direito autoral.

Contudo, analisando os critérios necessários para o reconhecimento da originalidade da obra, a autorizar a sua proteção, parece que nenhum deles estaria presente nas criações realizadas por essas inteligências artificiais.

Iniciando pelo primeiro requisito, parece difícil interpretar que a inteligência artificial não seja mera executora de ordens, porquanto apenas prevê aquela que seria a resposta mais coerente com base no aprendizado que obteve e na solicitação realizada pelo usuário.⁴⁶ Assim, o resultado obtido pelo sistema parece mais com a produção automática de uma máquina, que afronta igualmente ao segundo critério mencionado, pois a máquina é ensinada a raciocinar, a fazer inferências com base no treinamento que recebeu. Nesse sentido, inclusive, quanto mais interatividade houver entre a máquina e o usuário, maior a chance de que se obtenha um melhor resultado, ou *output*.⁴⁷

44. PONTES, Leonardo Machado. *Direito de Autor: a teoria da dicotomia entre a ideia e a expressão*. Belo Horizonte: Arraes Editora, 2012. p. 88-89 e 91.

45. PONTES, Leonardo Machado. *Direito de Autor: a teoria da dicotomia entre a ideia e a expressão*. Belo Horizonte: Arraes Editora, 2012. p. 93.

46. Conforme FEINGOLD, S. What is artificial intelligence — and what is it not? World Economic Forum, 2023. Disponível em: <https://www.weforum.org/agenda/2023/03/what-is-artificial-intelligence-and-what-is-it-not-ai-machine-learning>. Acesso em: 02 ago. 2024. Explica que o ChatGPT é um *chatbot* que é capaz de prever a próxima palavra mais provável em uma frase, com base em previsões numerosas e relativamente precisas.

47. MIALON, Grégoire; DESSI, Roberto; LOMELI, Maria; NALMPANTIA, Christoforos; PASUNURU, Ram; RAILEANU, Roberta; ROZIÈRE, Baptiste; SCHICK, Timo; DWIVEDI-YU, Jane; CELIKYILMAZ, Asli; GRAVE, Edouard; LECUN, Yann; e SCIALOM, Thomas. *Augmented Language Models: a Survey*. arXiv, 2023, <https://doi.org/10.48550/arXiv.2302.07842> 2302.07842. p. 9.

Ainda, no que se refere ao terceiro e último critério, interessante refletir se, considerando que os resultados obtidos nesses sistemas têm como base os dados nele imputados, responsáveis pelo seu aprendizado e que o ensinam a raciocinar, não se estaria diante, de uma certa forma, de uma forma de plágio.

Como já referido, para que exista separação entre as obras e sejam entendidas como distintas e, portanto, não sendo caso de plágio, resta necessário que exista um contributo mínimo do autor. No caso da inteligência artificial generativa, a utilização de imagens e de artigos para ensinar o sistema, a fim de obter o resultado mais preciso possível, leva à conclusão de que o resultado obtido quando se solicita, por exemplo, a elaboração de um texto ao ChatGPT, é, ao fim, um resultado da combinação desses diversos dados que foram imputados para “ensinar” o modelo. Mesmo que não seja, portanto, uma cópia direta daqueles documentos que alimentam o sistema, os *outputs* apenas são possíveis e apresentam a precisão desejada também em razão deles.

No ponto, interessante destacar o processo movido pelo The New York Times em face da OpenAI e da Microsoft, pelo alegado uso não autorizado de artigos do Times para o treinamento do modelo de linguagem de grande escala do ChatGPT e do BingChat (ou Copilot). Defende o Times que o problema no uso não autorizado dos artigos seria agravado por duas razões: o modelo de linguagem de grande escala memoriza parte das obras e pode, então, eventualmente gerar resultados que são reproduções dos trabalhos; e, ainda, produz resultados de pesquisa “sintéticos” e pode acabar possibilitando que leitores leiam artigos do Times que não estariam disponíveis sem que houvesse o pagamento da assinatura do jornal, prejudicando o seu modelo de negócio.⁴⁸

Esses argumentos são interessantes para a análise ora realizada porque fazem a mesma reflexão acerca da originalidade dos *outputs* desses modelos de inteligência artificial, que pode até mesmo incorrer em plágio evidente, ao reproduzir artigos utilizados para o treinamento do modelo de linguagem.

Nesse sentido, importante a reflexão que o ser humano, ao criar, invariavelmente, tem como base e inspiração outras obras, contudo, é capaz de raciocinar, pensar, fazer relações e utilizar essas informações de diversas maneiras. Diferentemente, os sistemas de inteligência artificial não têm propriamente “inteligência”, mas realizam previsões, dada a melhora da habilidade das máquinas, cada vez com maior precisão e com a obtenção do resultado desejado. Contudo, não é comparável à inteligência humana, que consegue obter a

48. POPE, A. NYT v. OpenAI: The Time's About-Face. Harvard Law Review, 2024. Disponível em: <https://harvardlawreview.org/blog/2024/04/nyt-v-openai-the-timess-about-face/>. Acesso em: 06 ago. 2024.

informação de uma fonte e utilizá-la de várias maneiras, sendo transferível, ao contrário da “inteligência” das máquinas.⁴⁹ Ainda, para que não incorra em plágio, o autor humano também precisa indicar as suas fontes, característica que não se observa nos resultados obtidos da inteligência artificial.

No mesmo sentido, a tendência dos ordenamentos jurídicos parece ser pelo reconhecimento da inexistência de criatividade suficiente nos resultados da inteligência artificial para obtenção da proteção por direitos autorais. Isso porque as máquinas não têm consciência interna e sensibilidade do que estão fazendo, não se inspiram em um nível de subconsciente,⁵⁰ requisitos normalmente exigidos para a caracterização de obra protegida, conforme inclusive se verifica da decisão no caso Feist, já mencionado, em que a Suprema Corte dos Estados Unidos da América indicou a necessidade de o autor provar a “existência desses fatos de originalidade, de produção intelectual, de pensamento e concepção”.⁵¹

Possível, ainda, identificar essa mesma interpretação em outros ordenamentos, como no Plano Estratégico de Propriedade Intelectual de 2016 do Japão, que indica não serem passíveis de proteção por direitos autorais, pelo atual ordenamento, os produtos criados automaticamente por inteligência artificial, bem como possível deduzir de decisões francesas que, ainda que seja possível a proteção de resultados realizados por humanos com a ajuda de máquinas, nega-se que as máquinas possam substituir os humanos e realizar o trabalho independentemente.⁵²

Em sentido contrário vem, no entanto, sendo o entendimento da China. Desde 2019, as cortes chinesas vêm afirmando que os produtos gerados por inteligência artificial constituem obras protegidas por direitos autorais.⁵³ A lei chinesa não trata especificamente do tema, mas o entendimento das cortes afirma a possibilidade de proteção, por quatro fatores: (i) adoção de uma interpretação mais ampla de participação humana, considerando atendido o

49. FEINGOLD, S. What is artificial intelligence – and what is it not? World Economic Forum, 2023. Disponível em: <https://www.weforum.org/agenda/2023/03/what-is-artificial-intelligence-and-what-is-it-not-ai-machine-learning>. Acesso em: 02 ago. 2024.

50. ZURTH, Patrick. Artificial Creativity? A Case against Copyright Protection for AI-Generated Works. *UCLA Journal of Law and Technology*, vol. 25, no. 2, Primavera 2021, p. 11. Acesso via HeinOnline.

51. Conforme ESTADOS UNIDOS DA AMÉRICA. U.S. Supreme Court. Feist Pubs., Inc. v. Rural Tel. Svc. Co., Inc., 499, U.S. 340. Recorrente: Feist Pubs. Inc. Recorrido: Rural Tel. Svc. Co., Inc. Relatora: Justice Sandra Day O'Connor, 27 de março de 1991. Disponível em: <https://supreme.justia.com/cases/federal/us/499/340/>. Acesso em: 27 jul. 2024. Tradução livre da autora de: “the importance of requiring an author who accuses another of infringement to prove “the existence of those facts of originality, of intellectual production, of thought, and conception.”

52. DAI, Zhe; e JIN, Banggui. The Copyright Protection of AI-Generated Works under Chinese Law. *Juridical Tribune*, vol. 13, no. 2, Junho 2023, p. 243-244. Acesso via HeinOnline.

53. DAI, Zhe; e JIN, Banggui. The Copyright Protection of AI-Generated Works under Chinese Law. *Juridical Tribune*, vol. 13, no. 2, Junho 2023, p. 245. Acesso via HeinOnline.

requisito ainda que a participação humana seja apenas no estágio de preparação, antes das operações da inteligência artificial; (ii) ausência de distinção entre a assistência por máquinas e os resultados gerados por inteligência artificial; (iii) adoção de um *standard* objetivo para o conceito de originalidade, que pode ser cumprido mesmo que não haja participação humana, pois se entende que o conteúdo gerado por inteligência artificial reflete seleção, julgamento e análise de dados relevantes, o que seria suficiente para satisfazer o requisito de originalidade; e, por fim, o que pode ser entendido como o principal motivo para a diferença entre o entendimento chinês e dos demais países, (iv) os fortes princípios utilitaristas da sua lei de direitos autorais. O valor da participação humana tem menor relevância na legislação chinesa, sendo a questão de proteção menos voltada a quem criou, e mais para a análise de se a proteção é de interesse social.⁵⁴

Ainda que interessante a análise do entendimento chinês, parece que a sua adoção pelos demais países é pouco provável considerando as suas legislações autorais atuais, especialmente naqueles da família romano-germânica, que adotam a teoria da criatividade, pois dão mais ênfase às características humanas e à conexão entre o autor e sua obra, àquilo que apenas humanos poderiam fazer. De qualquer sorte, o debate é inevitável, pois os modelos de inteligência artificial generativa vêm ganhando cada vez mais espaço e protagonismo, até mesmo econômico, mostrando-se essencial entender como regulá-los e qual proteção receberão, inclusive no que se refere aos seus *outputs*, aos resultados por eles produzidos.

Considerações finais

A inteligência artificial, apesar de não ser mais uma novidade, vem se tornando cada vez mais presente e protagonista no cotidiano da população. Dentre os diversos desafios que essa tecnologia impõe ao ordenamento jurídico, estão aqueles referentes à proteção autoral dos seus *outputs*, dos seus resultados, enquanto podem parecer, em uma primeira análise, obras protegidas por direito autoral, como textos literários e ilustrações.

Contudo, para que uma criação seja passível de proteção pelo direito autoral, necessário que ela detenha originalidade, apresente um *quantum* mínimo de criatividade que a diferencie daquelas criações já realizadas por terceiros e justifique o monopólio do autor, que apenas ele tenha direitos sobre aquela

54. DAI, Zhe; e JIN, Banggui. The Copyright Protection of AI-Generated Works under Chinese Law. *Juridical Tribune*, vol. 13, no. 2, Junho 2023, p. 249-254. Acesso via HeinOnline.

obra. Não parece, no entanto, que os *outputs* da inteligência artificial detemham essa característica, porquanto esses modelos aparentam mais serem mero executores de ordens e, por sua vez, o seu resultado constituiria uma produção automática da máquina, o que não lhe daria a característica de ser original.

Ainda, o fato de os resultados obtidos por esses modelos terem como base os dados neles imputados, que por vezes são textos e imagens protegidos por direitos autorais, faz com que se conclua que não detêm originalidade suficiente para serem entendidos como obras autônomas e que merecem proteção autoral, mas, ao contrário, poderiam inclusive incorrer em plágio, por apenas reproduzir obras protegidas que utilizam para a sua aprendizagem.

Dessa forma, conclui-se, portanto, que os *outputs* dos sistemas de inteligência artificial não apresentam, em regra, originalidade suficiente para serem objeto de proteção pelo direito autoral.

Referências

ABRÃO, Eliane Yachouh. *Direitos de autor e Direitos conexos*. 1ª ed. São Paulo: Editora do Brasil, 2002.

ASCENSÃO, José de Oliveira. *Direito autoral*. 2ª. ed., ref. e ampl. Rio de Janeiro: Renovar, 1997.

ASCENSÃO, José de Oliveira. Direito de autor sem autor e sem obra. *Stvdia Ivridica*, Ad Honorem –3, Boletim da Faculdade de Direito, Universidade de Coimbra, 1991.

BARBOSA, Denis Borges; MAIOR, Rodrigo Souto; e RAMOS, Carolina Tinoco. *O Contributo Mínimo na Propriedade Intelectual: Atividade Inventiva, Originalidade, Distinguibilidade e margem mínima*. Rio de Janeiro: Lumen Juris, 2010.

BARBOSA, Pedro Marcos Nunes. Originalidade em Crise. *Revista Brasileira de Direito Civil*, vol. 15, 2018, p. 33-48. Acesso via HeinOnline.

BRASIL. *Lei n. 9.609 de 19 de fevereiro de 1998*. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9609.htm>.

BRASIL. *Lei n. 9.610 de 19 de fevereiro de 1998*. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/l9610.htm>.

COSTA NETTO, José Carlos. *Direito Autoral no Brasil*. Coordenação Hélio Bicudo. São Paulo: FTD, 1998.

DAI, Zhe; e JIN, Banggui. The Copyright Protection of AI-Generated Works under Chinese Law. *Juridical Tribune*, vol. 13, no. 2, Junho 2023, pp. 241-260. Acesso via HeinOnline.

ESTADOS UNIDOS DA AMÉRICA. U.S. Supreme Court. *Feist Pubs., Inc. v. Rural Tel. Svc. Co., Inc.*, 499, U.S. 340. Recorrente: Feist Pubs. Inc. Recorrido: Rural Tel. Svc. Co., Inc. Relatora: Justice Sandra Day O'Connor, 27 de março de 1991. Disponível em: <https://supreme.justia.com/cases/federal/us/499/340/>. Acesso em: 27 jul. 2024.

FEINGOLD, S. What is artificial intelligence—and what is it not? World Economic Forum, 2023. Disponível em: <https://www.weforum.org/agenda/2023/03/what-is-artificial-intelligence-and-what-is-it-not-ai-machine-learning>. Acesso em: 02 ago. 2024.

HOLDSWORTH, J.; SCARPICCHIO, M. What is deep learning? IBM, 2024. Disponível em: <https://www.ibm.com/topics/deep-learning>. Acesso em: 02 ago. 2024.

IBM. What is artificial intelligence? IBM, 2024. Disponível em: <https://www.ibm.com/topics/artificial-intelligence>. Acesso em: 02 ago. 2024.

IBM. What is machine learning? IBM, 2024. Disponível em: <https://www.ibm.com/topics/machine-learning>. Acesso em: 02 ago. 2024.

OpenAI. DALL-E 2. OpenAI, 2024. Disponível em: <https://openai.com/index/dall-e-2/>. Acesso em: 03 ago. 2024.

OpenAI. Terms of use. OpenAI, 2024. Disponível em: <https://openai.com/policies/terms-of-use/>. Acesso em: 04 ago. 2024.

PONTES, Leonardo Machado. *Direito de Autor: a teoria da dicotomia entre a ideia e a expressão*. Belo Horizonte: Arraes Editora, 2012.

POPE, A. NYT v. OpenAI: The Time's About-Face. Harvard Law Review, 2024. Disponível em: <https://harvardlawreview.org/blog/2024/04/nyt-v-openai-the-timess-about-face/>. Acesso em: 06 ago. 2024.

MIALON, Grégoire; DESSI, Roberto; LOMELI, Maria; NALMPANTIA, Christoforos; PASUNURU, Ram; RAILEANU, Roberta; ROZIÈRE, Baptiste; SCHICK, Timo; DWIVEDI-YU, Jane; CELIKYILMAZ, Asli; GRAVE, Edouard; LECUN, Yann; e SCIALOM, Thomas. *Augmented Language Models: a Survey*. arXiv, 2023, <https://doi.org/10.48550/arXiv.2302.07842> 2302.07842.

NAQVI, Zack. Artificial Intelligence, Copyright, and Copyright Infringement. *Marquette Intellectual Property Law Review*, vol. 24, no. 1, Inverno 2020, pp. 15-52. Acesso via HeinOnline.

ZURTH, Patrick. Artificial Creativity? A Case against Copyright Protection for AI-Generated Works. *UCLA Journal of Law and Technology*, vol. 25, no. 2, Primavera 2021, pp. i-18. Acesso via HeinOnline.

Anexo I – Resposta do ChatGPT



ChatGPT 4o mini Entrar Cadastrar

Escrever uma obra literária de romance, de quatro parágrafos, retratando uma história de amor com final feliz.

Em uma pequena cidade costeira, onde o mar e o céu se fundem em um azul profundo, vivia Ana, uma jovem que passava seus dias na livraria do avô. Era um local encantador, repleto de histórias e segredos, e Ana se perdia entre as páginas de romances antigos, sonhando com um amor que parecia tão distante quanto as estrelas. Um dia, enquanto rearrumava as prateleiras, ela encontrou um livro antigo, empoeirado e com uma capa desgastada, que chamou sua atenção de uma maneira inexplicável.

No mesmo dia, Lucas, um artista que havia se mudado recentemente para a cidade em busca de inspiração, entrou na livraria. Seus olhos brilhavam com uma curiosidade genuína e, ao esbarrar na prateleira, fez com que o livro caísse diretamente em suas mãos. Ana, curiosa, se aproximou e uma conversa fluida e encantadora começou entre os dois. Descobriram que, apesar de suas vidas serem diferentes, compartilhavam uma paixão por histórias e uma sede por aventuras.

Com o tempo, Ana e Lucas se encontraram frequentemente, explorando os cantos pitorescos da cidade e criando memórias em cada encontro. Entre passeios pela praia e tardes na livraria, eles começaram a se apaixonar, descobrindo uma conexão profunda que transcendia as palavras e as páginas dos livros. O amor deles era uma mistura perfeita de amizade e romance, um conto que parecia ter sido escrito pelos próprios deuses do destino.

Finalmente, em uma tarde dourada de verão, Lucas preparou uma surpresa para Ana. Ele a levou a uma pequena galeria onde exibiu suas pinturas inspiradas na beleza da cidade e na magia dos momentos que passaram juntos. Em meio às obras, uma pintura especial retratava o exato instante em que se conheceram na livraria. Com um sorriso no rosto e lágrimas de felicidade nos olhos, Lucas pediu a Ana que passasse o resto de sua vida ao seu lado. Ela aceitou com um beijo suave e um abraço apertado, e assim, com o final feliz que ambos haviam sonhado, eles começaram a escrever seu próprio capítulo eterno.

Não compartilhe informações confidenciais. Os chats podem ser revisados e usados para treinar nossos modelos. [Saiba mais](#)

Mensagem ChatGPT

ChatGPT pode cometer erros. Considere verificar informações importantes.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

8

**Os desafios envolvidos a
utilização e regulamentação
da inteligência artificial
diante da discriminação
algorítmica**

MARIA FERNANDA LONGATO MATURANA

Sumário: Introdução. 1. As maneiras de aprendizagem das inteligências artificiais e o âmago do problema envolto a discriminação algorítmica 2. Os desafios envolvidos a regulamentação da inteligência artificial para assegurar a promoção de igualdade e evitar a discriminação 3. Novos horizontes nas redes de internet à luz do projeto de lei nº 2.338/2023. Considerações finais. Referências.

Introdução

Diante das constantes evoluções do mundo moderno, a inteligência artificial tem se consolidado como uma das tecnologias mais transformadoras e com maior projeção de uso da era moderna, possibilitando transformações e soluções inovadoras, céleres e relevantes em diversas áreas, desde a saúde até as mais vastas áreas do agronegócio.

O intuito do uso da tecnologia de inteligência artificial está no fato de “humanizar” essa máquina, de maneira que suas respostas possam ser relevantes para a sociedade tendo em vista que a máquina se torna o reflexo dela. Tal pensamento possibilitou diversos avanços tecnológicos, porém, ao mesmo tempo, o uso de algoritmos de inteligência artificial traz à tona questões complexas e preocupantes para a sociedade, especialmente no que diz respeito à discriminação algorítmica, tendo em vista que a inteligência artificial possui como objetivo refletir o pensamento de uma sociedade e isso também inclui suas imperfeições.

A discriminação algorítmica ocorre quando sistemas de inteligência artificial reproduzem ou até mesmo amplificam estereótipos discriminatórios aliados a preconceitos existentes dentro de uma sociedade, resultando em decisões e criações enviesadas que afetam negativamente determinados grupos de pessoas que já estão sujeitos à discriminação estrutural.

A problemática da discriminação algorítmica surge de diversas maneiras e de várias fontes, incluindo dados de treinamento enviesados por estereótipos discriminatórios, escolhas de design inadequadas e até mesmo a falta de diversidade entre os desenvolvedores de inteligência artificial. Esses desafios não apenas comprometem a equidade e a justiça nas decisões automatizadas, como também revelam problemas estruturais presentes na sociedade. Desta forma, é crucial compreender e abordar esses desafios para garantir que a

1. Pós-Graduada em Direito Digital pela Universidade do Estado do Rio de Janeiro (UERJ) em parceria com o Instituto de Tecnologia e Sociedade (ITS). Advogada no escritório Abramides e Gonçalves. E-mail: mariafernandalm@icloud.com

inteligência artificial seja utilizada para auxiliar a sociedade promovendo inclusão e equidade, em vez de perpetuar desigualdades.

A pesquisa deste artigo tem como objetivo explorar os diversos aspectos da discriminação algorítmica, analisando a matriz de suas causas, seus impactos na sociedade e possíveis soluções. Inicialmente, será fornecida uma visão geral dos conceitos fundamentais relacionados à aprendizagem da inteligência artificial, evidenciando os pontos sensíveis que possibilitam a discriminação algorítmica demonstrando casos reais onde esses problemas se manifestaram, destacando as consequências sociais e éticas. Em seguida, serão discutidos os desafios éticos envoltos à ciência de dados da inteligência artificial. Por fim, serão examinadas as estratégias e as melhores práticas para mitigar a discriminação algorítmica, promovendo um desenvolvimento sadio para esta tecnologia.

1. As maneiras de aprendizagem das inteligências artificiais e o âmago do problema envolto a discriminação algorítmica

Muito se discute a respeito da discriminação algorítmica, porém, para entender o âmago dessa discussão é necessário compreender a maneira como é feita a aprendizagem das diversas gamas de inteligências artificiais.

A aprendizagem da inteligência artificial é uma técnica, um processo complexo, onde em uma explicação curta, podemos dizer que se analisa uma variedade de casos e se faz uma relação entre todos eles. Dessa forma, a inteligência artificial analisa uma gama diversificada de dados e adquire conhecimento por meio desses padrões de dados.

Os algoritmos e todos os sistemas envolvidos na inteligência artificial são extremamente voláteis, estando em constante adaptação para alcançar objetivos. Tal fenômeno só é possível por meio da técnica de aprendizado de máquina, popularmente conhecida como *machine learning*, que permite que os sistemas aprendam e melhorem seu desempenho através de um conjunto de dados, de maneira a possibilitar o desempenho de diversas ações sem que tenham sido explicitamente programados para tal.²

Dito de forma elucidada, o aprendizado de máquina, ou *machine learning*, se dá com base em um conjunto de dados. Calculados pela máquina por meio

2. JANIESCH, C.; ZSCHENCH, P.; HEINRICH, K. Machine learning and deep learning. arXiv.org, Springer, [2331-8422], 2021. Disponível em: <https://arxiv.org/pdf/2104.05314>. Acesso em: 17 jul. 2024.

de diversos treinamentos de repetições, passa a encontrar padrões, gerando respostas que auxiliam nos mais diversos campos da atividade humana, desde o prognósticos de doenças, passando pela detecção de fraudes e até mesmo no popular reconhecimento facial e reconhecimento de voz.

Sobre o tema, discorre Arthur Samuel ³ “Aprendizado de máquina é o campo de estudo que dá aos computadores a capacidade de aprender sem serem explicitamente programados.”

Com base nas questões apresentadas e na disponibilidade dos dados, existem diversas maneiras de implantar o *machine learning*. Os autores Lloyd, Mohseni e Rebentrost apostam três tipos de machine learning.⁴

O primeiro modelo apresentado é conhecido por aprendizado supervisionado onde os algoritmos são treinados com base em conjuntos de dados rotulados, por meio do qual a máquina é treinada para classificar previsões destes dados, onde cada exemplo de entrada é associado a uma saída desejada. O objetivo deste aprendizado é que a máquina vá de forma interativa classificando diversas características para ao final alcançar o resultado desejado diante das características classificadas.

O segundo modelo apresentado é o aprendizado não supervisionado, diferentemente do primeiro modelo, neste os algoritmos são treinados a trabalhar com dados não rotulados, e procuram descobrir padrões ou estruturas ocultas nos dados, ele é comumente utilizado em situações na qual é necessário utilizar de aprendizagem de dados em grande escala, o popular *big data*, de maneira que a utilização deste modelo possibilita uma maior na segmentação dentre a cartela de clientes gerando uma comunicação mais efetiva com o público-alvo do operador do sistema.

O terceiro modelo é conhecido por aprendizagem por reforço, sendo o mais diferente entre os mencionados, neste contexto a dinâmica dos algoritmos funciona com base no uso de recompensas e penalidades diante da ação realizada, por meio do qual o objetivo é aprender uma política que maximize a recompensa acumulada ao longo do tempo, sua utilização está comumente voltada para jogos.⁵

Diante da disposição de todas essas tecnologias o mercado vem avançando cada dia mais, o uso das inteligências artificiais tem se tornado cada dia

3. SAMUEL, A. Some studies in machine learning using the game of checkers. IBM Journal of Research and Development, v. 3, n. 3, p. 210-229, 1959. Disponível em: <https://people.csail.mit.edu/brooks/idocs/Samuel.pdf>. Acesso em: 17 jul. 2024.

4. LLOYD, S.; MOHSENI, M.; REBENTROST, P. Quantum algorithms for supervised and unsupervised machine learning. Disponível em: <https://arxiv.org/pdf/1307.0401>. Acesso em: 17 jul. 2024.

5. LLOYD, S.; MOHSENI, M.; REBENTROST, P. Quantum algorithms for supervised and unsupervised machine learning. Disponível em: <https://arxiv.org/pdf/1307.0401>. Acesso em: 17 jul. 2024.

mais dinâmico, atingindo diversos grupos de consumidores deste produto em várias áreas da sociedade. Com a popular disseminação das mais diversas inteligências artificiais criou-se a equivocada ideia de que tal tecnologia é tomada de neutralidade, de maneira que todas as suas decisões seriam tomadas diante de um ponto de vista totalmente neutro, tal entendimento evidencia o âmago do problema a ser discutido neste artigo.

Sobre o tema discorre Safiya Umoja Noble “Os algoritmos não são neutros; eles refletem as prioridades, valores e julgamentos daqueles que têm o poder de moldá-los.”⁶

O mundo se olvida de que a inteligência artificial possui sua funcionalidade intimamente atrelada à maneira pela qual ela foi programada e a base de dados que foi utilizada em sua programação, de maneira que os seus resultados sempre estarão relacionados aos dados que foram fornecidos para aquela máquina. É importante salientar que esses dados não estão tomados de neutralidade, muito pelo contrário, podem estar intimamente relacionados por diversos vieses discriminatórios de seus programadores e de toda uma sociedade.

É importante ressaltar que a sociedade humana está muito distante de ser uma sociedade ideal, estando cada vez mais tomada por preconceitos. Neste contexto, o âmago da questão envolta da discriminação algorítmica se inicia logo nos próprios algoritmos, que podem estar embuídos de vieses ideológicos de seus próprios programadores. Tal transmissão desses vieses não necessariamente está ligada a uma má intenção de repassar tais preconceitos, podendo estar ligada a um erro humano que foi transmitido para a programação sem maiores percepções. Porém, de toda forma, tal transmissão afetará diretamente os resultados das decisões da ferramenta.

Todavia, ainda que os algoritmos não estejam tomados pelos vieses ideológicos de seus programadores, eles ainda podem possuir vieses discriminatórios que estejam embutidos em seus próprios conjunto de dados, de maneira que estes algoritmos podem gerar resultados nitidamente preconceituosos quando alimentados com conceitos e valores completamente deturpados.

É importante ressaltar que as inteligências artificiais replicam aquilo que lhes foi ensinado, de maneira que aprendem com os vieses dos dados que lhe foram disponibilizados, sendo muito fácil para os seus programadores criarem inteligências artificiais tomadas por dados totalmente discriminatórios,

6. NOBLE, S. U. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press, 2018.

de maneira que todas as suas decisões irão estar tomadas por esses mesmos vieses, propagando ainda mais esses preconceitos. Na sociedade atual, tais pensamentos discriminatórios estão em rápida ascensão, de maneira que as inteligências artificiais construídas com base em dados deturpados e discriminatórios estão se tornando cada vez mais comuns.

Elucidadas tais questões tem-se a conclusão de que a máquina por si só não é preconceituosa, não possui vieses discriminatórios, porém os seres humanos que estão por trás de seu desenvolvimento podem fazer com que estes vieses deturpados sejam inseridos em sua forma de aprendizado, afetando todas as suas decisões⁷.

A discriminação algorítmica funciona como uma fórmula matemática, sempre que um sistema for alimentado com dados de vieses discriminatórios as suas decisões algorítmicas irão replicar estes mesmos vieses, resultado em ainda mais discriminação e conseqüentemente uma grave ofensa aos direitos humanos. Como exemplo de tal afirmação, é possível analisar a utilização de algoritmos no sistema de policiamento com base em estatísticas criminais explicitamente tendenciosas. As decisões deste sistema de policiamento tendenciosamente executam um maior monitoramento em bairros que possuem maior concentração de imigrantes, dessa forma esse sistema sugere o deslocamento de uma maior quantidade de policiais para estas localizações, de forma que todas as ocorrências policiais passam a ser registradas, sugerindo que os bairros com maior concentração de imigrantes possuem alta criminalidade. Tal constatação, porém, não é verdadeira. O que acaba ocorrendo é que por conta da maior quantidade de policiais, todas as ocorrências passam a ser registradas, diferentemente de outros bairros que, por terem uma menor quantidade de policiais deslocados, conseqüentemente possuem menos registros de ocorrência e por isso, um menor índice de criminalidade. Esse tipo de policiamento preditivo precisa ser analisado e utilizado com extrema cautela, tendo em vista que pode criar um ciclo de resultados extremamente tendenciosos e perigosos, onde decisões humanas preconceituosas são amplificadas, resultando em novas decisões que exaltam os posicionamento discriminatórios e, conseqüentemente, ofendem gravemente os direitos humanos.⁸

7. WEST, Sarah Myers; WHITTAKER, Meredith; CRAWFORD, Kate. Discriminating systems: gender, race and power in AI. Nova Iorque: New York University, AI Now Institute, 2019. Disponível em: <https://ainowinstitute.org/discriminatingystems.pdf>. Acesso em: 22 jul. 2024.

8. BORGESIU, F. J. Z. Strengthening legal protection against discrimination by algorithms and artificial intelligence. The International Journal of Human Rights, v. 24, n. 10, p. 1572-1593, 2020. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3561441. Acesso em: 18 jul. 2024.

Sobre o tema, Frank Pasquale elucida que “O algoritmo é um espelho: reflete nossas prioridades e preconceitos, mas amplificados e tornados invisíveis.”⁹

Diante de tudo que foi apresentado, conclui-se que a discriminação algorítmica no contexto das inteligências artificiais se inicia antes mesmo das decisões de tais tecnologias serem inseridas no mundo real. Assim, demonstra-se que a base para a discriminação algorítmica se encontra no próprio aprendizado da máquina, evidenciando que o grande âmago de toda essa questão está centralizado no momento em que a inteligência artificial está sendo desenvolvida. É indicado então que a fiscalização destas inteligências artificiais deva se iniciar no momento da criação de tal tecnologia.

Sobre a discussão, Joy Buolamwini e Timnit Gebru ressaltam que “O perigo da discriminação algorítmica é que ela pode escalar a um ritmo e em uma escala que ultrapassa as capacidades humanas de monitoramento e intervenção.”¹⁰

Elucidando tal afirmação, é evidente que a temática da discriminação algorítmica requer atenção. O mundo da tecnologia é imensurável e as consequências desse mundo possuem as mesmas proporções, que não necessariamente serão positivas.

A fala de Joy Boulamwini e de Timnit Gebru evidencia a temática que vem sendo discutida neste capítulo de que a discriminação algorítmica precisa ser discutida no momento da criação da inteligência artificial. Tendo em vista que a partir do momento que os dados com vieses discriminatórios alimentam a inteligência artificial, os resultados das decisões desta tecnologia são imensuráveis, de maneira que configuram grave atentado aos direitos humanos, a constituição e exaltam os princípios discriminatórios erroneamente inseridos há muitos anos na sociedade.¹¹

2. Os desafios envoltos a regulamentação da inteligência artificial para assegurar a promoção de igualdade e evitar a discriminação.

Há um consenso sobre a necessidade de regulamentação das inteligências artificiais; no entanto, a dificuldade em efetivar essa regulamentação é

9. PASQUALE, F. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press, 2015. Disponível em: <https://raley.english.ucsb.edu/wp-content/Engl800/Pasquale-blackbox.pdf>. Acesso em: 18 jul. 2024.

10. BUOLAMWINI, J.; GEBRU, T. *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. *Proceedings of Machine Learning Research*, v. 81, p. 1-15, 2018. Disponível em: <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>. Acesso em: 15 jul. 2024.

11. *Ibidem*

evidente. Essa tecnologia está entre as situações que urgem por regulamentação, mas pouco se sabe sobre como implementar uma regulamentação verdadeiramente efetiva.

A regulamentação de inteligência artificial envolve vários tópicos do mundo do direito, porém é evidente que o tópico que diz respeito à discriminação algorítmica urge uma maior atenção diante dos estrondosos casos recentes envolvendo tal tecnologia.

Ainda que não exista uma legislação específica que regule a inteligência artificial e seus efeitos, é importante ressaltar que a legislação brasileira garante a promoção de igualdade entre todos e pune toda e qualquer conduta com viés discriminatório.

A Constituição Federal expressamente dispõe que “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.”¹²

A Lei nº 7.716, popularmente conhecida por Lei do Crime Racial, dispõe em seu artigo primeiro que “Serão punidos, na forma desta Lei, os crimes resultantes de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.”¹³

A Lei nº 7.716, acima mencionada, ainda regulamenta que qualquer prática de qualquer ato discriminatório é crime e será passível de punição, salientando ainda que qualquer ato discriminatório realizado na rede mundial de computadores também é crime e agrava a punição:

Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.

Pena: reclusão de um a três anos e multa.

§ 2º Se qualquer dos crimes previstos neste artigo for cometido por intermédio dos meios de comunicação social, de publicação em redes sociais, da rede mundial de computadores ou de publicação de qualquer natureza.

Pena: reclusão de dois a cinco anos e multa.¹⁴

12. BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988*. Brasília, DF: Senado Federal: Centro Gráfico, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 19 jul. 2024

13. BRASIL. Lei nº 7.716, de 5 de janeiro de 1989. Define os crimes resultantes de preconceito de raça ou de cor. *Diário Oficial da União: seção 1*, Brasília, DF, p. 240, 6 jan. 1989. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em: 19 jul. 2024.

14. *Ibidem*

Elucidadas tais questões e ressaltando a ideia já mencionada, há um consenso sobre a necessidade de avançar na busca pela justiça algorítmica, especialmente para mitigar os riscos de discriminação direta (tratamento desigual) e indireta (impacto desigual) nas decisões algorítmicas. No entanto, ainda não existe uma resposta para a maneira como será feita esta regulamentação. Tem-se a ideia de que uma possibilidade para mitigar esses riscos é investindo em pesquisas que esclareçam a natureza dos riscos éticos, fornecendo orientações sólidas e transparentes para a governança do design dos algoritmos e do uso da tecnologia.¹⁵

A ideia de Tsamados é de extrema relevância, porém envolve novamente a problemática de que todas estas estratégias nunca saíram do mundo das ideias, de maneira que a regulamentação vai se tornando cada vez mais distante e a discriminação envolta a inteligência artificial vai se expandindo cada dia mais. Desta forma, a regulamentação de tais atos discriminatórios acaba caminhando de maneira oposta ao que parece ser a solução para a questão.

Enquanto não existir uma legislação que regule a inteligência artificial, os efeitos do mau uso desta tecnologia continuarão existindo, de forma que a matriz para este problema se encontra na ausência de transparência dos mecanismos e dos dados atrelados à inteligência artificial, resultando na ausência de proteção dos direitos individuais.¹⁶

Em relação a ausência de transparência dos mecanismos e dados atrelados à inteligência artificial, é válido ressaltar que estas informações não possuem um autor claro. As mesmas não possuem um responsável pelos dados utilizados para tomar estas decisões, de maneira que essa falta de transparência dificulta ao máximo a possibilidade de encontrar a fonte para responsabilizar tal discriminação tendo em vista os vieses discriminatórios dos algoritmos.¹⁷

A transparência é fundamental para prevenir vieses discriminatórios e evitar um cenário de insegurança para os usuários de tal tecnologia. Sobre o tema ressalta-se:

15. TSAMADOS, A.; AGGARWAL, N.; COWLS, J.; MORLEY, J.; ROBERTS, H.; TADDEO, M.; FLORIDI, L. The ethics of algorithms: key problems and solutions. *AI & SOCIETY*, v. 37, p. 215–230, 2022. Disponível em: <https://link.springer.com/article/10.1007/s00146-021-01154-8>. Acesso em: 22 jul. 2024.

16. AZEVEDO, Ingrid Borges de. Reconhecimento facial e direito: propostas para uma IA antidiscriminatória. 2021. 65 f. Trabalho de Conclusão de Curso (Graduação em Direito)- Universidade de Brasília, Brasília, 2021. Disponível em: <https://bdm.unb.br/handle/10483/29805>. Acesso em: 22 jul. 2024.

17. BONA, Celito de; SCHONS, Eduarda Arruda; LOPES-FLOIS, Luiza. Inteligências artificiais: existe ética na implementação de algoritmos? *Ciências Sociais Aplicadas em Revista*, [S.L.], v. 25, n. 45, p. 225-246, 18 ago. 2023. Universidade Estadual do Oeste do Paraná - UNIOESTE. Disponível em: <https://e-revista.unioeste.br/index.php/csaemrevista/article/view/31510/22369>. Acesso em: 21 jul. 2024.

Essa ausência de regulamentação, responsabilidade, auditoria e transparência na utilização da IA, vem angariando consequências nefastas do ponto de vista jurídico social, por perpétua e amplia as discriminações e a seletividade que permeia o controle penal e as agências que o integram. E tudo sob a ilusória impressão de que se baseia em modelos matemáticos imparciais, precisos e objetivos. Em verdade, os resultados estão carregados de subjetividade e vieses racistas tendentes a catalisar setores sociais bem delimitados para a marginalização e a discriminação.¹⁸

Sobre a temática apresentada diante da dificuldade de regularização, surge uma nova discussão a respeito da responsabilidade da empresa ou do programador que desenvolveu a inteligência artificial.

A questão principal a ser analisada em respeito da responsabilidade da empresa ou do programador é a intenção deste agente desenvolvedor, analisando se possuía alguma intenção de gerar resultados discriminatórios ou se possuía alguma possibilidade de monitoramento sobre estes resultados. Dessa maneira, caso seja demonstrado que o agente desenvolvedor possuía clara influência ou intenção nos resultados discriminatórios, ele precisa ser responsabilizado.

Neste aspecto surge novamente a problemática pela falta de regulamentação, tendo em vista que a única maneira de poder analisar a intenção e o monitoramento do agente desenvolvedor é por meio da rastreabilidade do algoritmo utilizado pela máquina. Essa informação fica disponível apenas ao agente desenvolvedor, de maneira que, pela falta de regulamentação em face do tema, a informação se torna inacessível e conseqüentemente prejudica a responsabilização dos sujeitos envolvidos nos resultados discriminatórios da inteligência artificial.

A regulamentação da inteligência artificial no Brasil parece estar cada dia mais distante da realidade, porém já existe uma lei que regulamenta o tratamento de dados pessoais: a Lei nº 13.709/2018, Lei Geral de Proteção de Dados (LGPD). Esta regulamenta o tratamento de dados pessoais no Brasil, tanto no âmbito online quanto offline, por pessoas físicas ou jurídicas, de direito público ou privado. Seus principais objetivos são proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural.

18. CHAVES JUNIOR, Airto; GUASQUE, Bárbara; PÁDUA, Thiago Santos Aguiar de. Segregação racial e vieses algorítmicos: máquinas racistas no âmbito do controle penal. *Revista Brasileira de Direito*, [S.L.], v. 19, n. 2, p. 1-30, 22 set. 2023. Complexo de Ensino Superior Meridional S.A. Disponível em: <https://doi.org/10.18256/2238-0604.2023.v19i2.4768>. Acesso em: 22 jul. 2024.. *Revista Brasileira de Direito*, [S.L.], v. 19, n. 2, p. 1-30, 22 set. 2023. Complexo de Ensino Superior Meridional S.A. Disponível em: <https://doi.org/10.18256/2238-0604.2023.v19i2.4768>. Acesso em: 22 jul. 2024.

A Lei Geral de Proteção de Dados representa um marco importante na proteção de dados pessoais no Brasil, porém se distancia da regulamentação de dados no sentido de evitar a discriminação algorítmica, de maneira que esta lei e seus artigos não solucionam os problemas anunciados neste capítulo. É possível utilizar alguns artigos do diploma legal como base para a legislação específica sobre o tema, no entanto, é claro que há necessidade de uma regulamentação complementar à Lei Geral de Proteção de Dados.

O diploma do Art.6º da Lei Geral de Proteção de Dados ratifica questões a respeito da discriminação de dados:

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

(...)

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

(...)

IX – Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;¹⁹

O mencionado artigo 6º elucida que os dados pessoais não podem ser utilizados para fins discriminatórios ilícitos ou abusivos, porém tal diploma resta incompleto, tendo em vista que há uma clara proibição para esta prática discriminatória com uso de dados. Porém, não há qualquer punição para tal conduta, de maneira que resta a todos entender que por mais que tal conduta seja proibida, se for praticada, ela não será punida.

Atualmente, muito se fala da justiça algorítmica, no mundo todo se estuda o tema em face da regulamentação da inteligência artificial, porém nenhuma análise preditiva poderá indicar com segurança que não haverá risco discriminatório de sistemas de inteligência artificial.²⁰

Portanto, constata-se que a única forma de estrear uma tentativa para erradicar a discriminação algorítmica se iniciará no momento em que desenvolvedores de tal tecnologia e governos passem a trabalhar juntos para garantir que a inteligência artificial seja utilizada de maneira ética e justa, de forma na qual tecnologia deverá ser regulada por um arcabouço legislativo com um

19. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, p. 1, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 22 jul. 2024.

20. HUPFFER, Haide Maria; SANTANNA, Gustavo da Silva. Inteligência artificial e discriminação algorítmica: marcos regulatórios e parâmetros éticos. Disponível em: <http://www.guaritadigital.com.br/casaleirialivros/iasg/iasg.4.pdf>. Acesso em: 15 jul. 2024

conjunto de regras que devem ser seguidas pela ferramenta, com a finalidade de que ela reconheça atos e dados discriminatórios e não os alastrem.²¹

Em uma sociedade em que a tecnologia é utilizada em grande escala, a formulação de uma lei que regule a inteligência artificial é indispensável para a proteção dos direitos individuais dos cidadãos, principalmente das populações mais vulneráveis. As normativas devem estar alicerçadas em antecedentes éticos de forma que a decisão algorítmica seja transparente e não discriminatória.

3. Novos horizontes nas redes de internet a luz do Projeto de Lei nº2338/2023

Considerando todas as temáticas dispostas neste artigo, é de fácil análise que a regulamentação da inteligência artificial é necessária, porém é preciso também compreender que mesmo com toda a regulamentação em face do tema, só haverá mudanças significativas no âmbito da discriminação algorítmica quando houver uma conscientização social em face de todo o tema da discriminação, não só no mundo digital, mas sim em todo o mundo real.

A sociedade encontra-se em insistente tentativa de combater todos os atos discriminatórios e preconceituosos, esta luta, porém, está muito distante do ideal. Mesmo com tantos avanços na sociedade, ainda a cultura discriminatória é disseminada por todo o mundo e a internet não está excluída desta onda de disseminação, por isso, é preciso buscar novos horizontes nas redes para combater esses atos.

Para os enfrentamentos de todos estes desafios éticos, a conscientização da sociedade precisa estar alinhada a uma forte regulamentação que, por sua vez, precisa ser desenvolvida por especialistas no tema de maneira a possibilitar que essa regulamentação cause efeitos reais, saindo do mundo das ideias para regulamentar o tema e punir aqueles que disseminarem os atos com vieses discriminatórios.

A Organização das Nações Unidas (ONU) elucida a necessidade de novos horizontes no mundo da regulamentação da inteligência artificial:

A inteligência artificial promete impulsionar avanços em vários setores, mas sua implantação deve ser gerida cuidadosamente para evitar impactos adversos nos direitos humanos e valores sociais.

21. SINGAPURA. Comissão de Proteção de Dados Pessoais. Modelo de Estrutura de Governança de IA. Disponível em: <https://www.p.gov.sg/ajuda-e-recursos/2020/01/model-ai-vai-estrutura>. Acesso em: 17 jul. 2024

Medidas regulatórias devem ser implementadas para garantir que as tecnologias de IA sejam desenvolvidas e utilizadas de maneiras que promovam a inclusão e a equidade. Isso envolve criar políticas que exijam a avaliação dos sistemas de IA quanto a vieses e seus potenciais efeitos em diferentes grupos demográficos. Além disso, a transparência nos processos de tomada de decisão da IA e os mecanismos de responsabilização devem ser estabelecidos para construir a confiança pública e prevenir abusos. É essencial que os benefícios da IA sejam amplamente compartilhados e que salvaguardas estejam em vigor para proteger contra consequências não intencionais.²²

Em mesmo sentido ao posicionamento da ONU, se posiciona a OCDE (Organização para Cooperação e Desenvolvimento Econômico):

A governança da inteligência artificial deve estar fundamentada em princípios que enfatizem inclusão, transparência e responsabilização. Estruturas regulatórias precisam ser voltadas para o futuro, antecipando a rápida evolução das tecnologias de IA e seus potenciais impactos sociais. Políticas devem incentivar o desenvolvimento e a implantação responsável da IA garantindo que esteja alinhada com valores democráticos e direitos humanos. Isso envolve criar mecanismos para monitoramento e avaliação contínua dos sistemas de IA, bem como fomentar a cooperação internacional para abordar os desafios globais impostos pela IA. Ao adotar uma abordagem holística para a regulamentação da IA, podemos aproveitar seu potencial transformador enquanto salvaguardamos contra riscos e garantimos que seus benefícios sejam distribuídos equitativamente. (OCDE, 2019, tradução nossa)²³

Conforme tais posicionamentos apresentados, o mundo todo vem entendendo a importância da regulamentação da inteligência artificial e vem iniciando o movimento de regulamentação dando início a uma nova era de horizontes nas redes. Atualmente o Brasil se encontra deveras atrasado neste tema em relação aos outros países do mundo, para tal afirmação podemos citar a União Europeia, que como uma referência global em maio de 2024 promulgou a Lei de Inteligência Artificial, que regulamenta todo o tema e enfatiza o combate a discriminação algorítmica.

22. NAÇÕES UNIDAS. The Age of Digital Interdependence: Report of the UN Secretary-General's High-level Panel on Digital Cooperation. 2019. Disponível em: <https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf>. Acesso em: 17 jul. 2024.

23. OCDE. Principles on Artificial Intelligence. 2019. Disponível em: <https://www.oecd.org/going-digital/ai/principles/>. Acesso em: 17 jul. 2024.

No Brasil, existem mais de 46 projetos de lei para a regulamentação da inteligência artificial, e por mais que a gama de projetos seja extensa o país ainda está muito longe da efetiva regulamentação. Dentre os 46 projetos o que se encontra em maior avanço é o projeto de lei (PL) nº 2338/2023, relatado pelo senador Eduardo Gomes (PL-TO). Por mais que o projeto em questão se encontre em maior avanço, este avanço ainda é pouco, tendo em vista que sua votação foi adiada pela terceira vez na data de 09 de julho de 2024.

Tratando-se especificamente do projeto de lei (PL) nº 2338/2023, em seu texto ele possui alguns claros objetivos, como a promoção da inovação tecnológica em face do desenvolvimento sustentável da inteligência artificial, o estabelecimento de diretrizes para a transparência diante da explicabilidade dos sistemas de inteligência artificial e o mais importante para este artigo, a garantia do respeito aos direitos fundamentais, à dignidade humana e à privacidade.

O projeto de lei (PL) nº 2338/2023 exalta o princípio da transparência no mundo da inteligência artificial, este sendo o princípio essencial para combater a discriminação algorítmica, tendo em vista que é necessário que os sistemas de IA sejam projetados de maneira transparente, permitindo que as pessoas entendam como funcionam e como as decisões são tomadas. A transparência de mesma forma obriga a divulgação de informações sobre os dados utilizados e os critérios adotados para as decisões automatizadas, possibilitando que seja compreendido a maneira como as possíveis decisões discriminatórias seriam geradas e como consequência possibilita a punição dos agentes que usarem tais tecnologias para a promoção de atos discriminatórios.

O artigo 5º do projeto de lei (PL) nº 2338/2023 evidencia a não discriminação no mundo da inteligência artificial:

Art. 5º Pessoas afetadas por sistemas de inteligência artificial têm os seguintes direitos, a serem exercidos na forma e nas condições descritas neste Capítulo:

(...)

V – direito à não-discriminação e à correção de vieses discriminatórios diretos, indiretos, ilegais ou abusivos; (BRASIL, Projeto de Lei nº 2338, 2023).²⁴

Ainda em seu artigo 19 informa que haverá adoção de medidas para combater a discriminação algorítmica:

24. BRASIL. Congresso Nacional. Projeto de Lei nº 2338, de 2023. Dispõe sobre a regulamentação da inteligência artificial. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1720798347645&disposition=inline>. Acesso em: 24 jul. 2024

Art. 19. Os agentes de inteligência artificial estabelecerão estruturas de governança e processos internos aptos a garantir a segurança dos sistemas e o atendimento dos direitos de pessoas afetadas, nos termos previstos no Capítulo II desta Lei e da legislação pertinente, que incluirão, pelo menos:

(...)

III – medidas de gestão de dados adequadas para a mitigação e prevenção de potenciais vieses discriminatórios; (BRASIL, Projeto de Lei nº 2338, 2023).²⁵

O projeto de lei (PL) nº 2338/2023 evidencia a tentativa de combater a discriminação algorítmica, de maneira que daria início para a regulamentação necessária sobre o tema em busca de extinguir a discriminação dentro das tecnologias digitais.

O projeto de lei (PL) nº 2338/2023 possui diversas críticas a respeito de seu conteúdo e de sua forma de operação, conforme a ideia de Thiago Marcílio, o referido projeto de lei não reflete as verdadeiras necessidades da regulamentação da inteligência artificial e até mesmo se torna controverso com a própria Lei Geral de Proteção de Dados (LGPD), porém ele inaugura os novos horizontes das redes no Brasil, de maneira que precisa ser entendido como uma avanço para o ideal no mundo das redes.²⁶

Embora essas propostas representem um ideal normativo, sua efetiva implementação no Brasil permanece distante. O país ainda carece de um arcabouço jurídico robusto e eficaz para regulamentar a inteligência artificial, o que impede o alcance desses objetivos em um futuro próximo. No entanto, analisando diante de um olhar otimista, apenas a criação de um forte projeto de lei, ainda que com diversos problemas, já evidencia o início de uma trajetória para o ideal.

Considerações finais

A discriminação algorítmica representa um desafio crítico no uso crescente de tecnologias de inteligência artificial, refletindo e amplificando os vieses e preconceitos existentes na sociedade. Esse fenômeno não surge com a tecnologia em si, mas sim da forma como os dados são coletados e processados, bem como das escolhas de vieses de seus próprios desenvolvedores. Portanto,

25. Ibidem

26. MARCÍLIO, Thiago. Quatro polêmicas sobre o projeto que regula a inteligência artificial. Consultor Jurídico, São Paulo, 29 fev. 2024. Disponível em: <https://www.conjur.com.br/2024-fev-29/quatro-polemicas-sobre-o-projeto-que-regula-a-inteligencia-artificial/>. Acesso em: 14 out. 2024

a inteligência artificial, se não regulamentada e monitorada adequadamente, pode perpetuar e intensificar a discriminação algorítmica, perpetuando diretrizes discriminatórias que estão enraizadas na sociedade.

Para que haja o efetivo combate à discriminação algorítmica é essencial que a regulamentação da inteligência artificial seja robusta e eficaz. No Brasil, embora a Constituição e a Lei do Crime Racial já estabeleçam a proibição de atos discriminatórios, ainda há uma lacuna significativa na legislação específica que aborde os desafios únicos apresentados pela inteligência artificial. A falta de transparência e a dificuldade de rastrear a responsabilidade pelos dados e algoritmos usados dificultam a aplicação de punições e a garantia de justiça algorítmica.

A regulamentação da inteligência artificial deve ser desenvolvida de maneira muito cautelosa evidenciando a transparência, para que seja possível responsabilizar aqueles que perpetuarem a discriminação algorítmica. Isso requer a colaboração entres os desenvolvedores da tecnologia e formuladores de políticas para criar um marco legal que garanta a proteção dos direitos individuais e promova a equidade.

O movimento global em direção à regulamentação da inteligência, exemplificado pela recente Lei de Inteligência Artificial da União Europeia, destaca a urgência e a importância desse esforço. No Brasil, o Projeto de Lei nº 2338/2023 representa um passo significativo, mas ainda há um longo caminho a percorrer.

Em conclusão, a discriminação algorítmica é um reflexo dos pensamentos da sociedade, se tornando uma questão complexa que exige uma abordagem multifacetada, envolvendo legislação, monitoramento e uma conscientização social mais ampla. Somente através de um esforço coordenado e contínuo entre toda a sociedade será possível garantir que a inteligência artificial contribua para uma sociedade mais justa e inclusiva, ao invés de perpetuar as desigualdades enraizadas na sociedade atual.

Referências

AZEVEDO, Ingrid Borges de. *Reconhecimento facial e direito: propostas para uma IA antidiscriminatória*. 2021. 65 f. Trabalho de Conclusão de Curso (Graduação em Direito)– Universidade de Brasília, Brasília, 2021. Disponível em: <https://bdm.unb.br/handle/10483/29805>. Acesso em: 22 jul. 2024.

BONA, Celito de; SCHONS, Eduarda Arruda; LOPES-FLOIS, Luiza. Inteligências artificiais: existe ética na implementação de algoritmos? *Ciências Sociais Aplicadas em Revista*, [S.L.], v. 25, n. 45, p. 225-246, 18 ago. 2023. Universidade Estadual do Oeste do Paraná – UNIOESTE. Disponível em:

<https://e-revista.unioeste.br/index.php/csaemrevista/article/view/31510/22369>. Acesso em: 21 jul. 2024.

BORGESIUS, F. J. Z. Strengthening legal protection against discrimination by algorithms and artificial intelligence. *The International Journal of Human Rights*, v. 24, n. 10, p. 1572-1593, 2020. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3561441. Acesso em: 18 jul. 2024.

BRASIL. Congresso Nacional. *Projeto de Lei nº 2338, de 2023*. Dispõe sobre a regulamentação da inteligência artificial. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1720798347645&disposition=inline>. Acesso em: 24 jul. 2024.

BUOLAMWINI, J.; GEBRU, T. *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. *Proceedings of Machine Learning Research*, v. 81, p. 1-15, 2018. Disponível em: <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>. Acesso em: 15 jul. 2024.

CHAVES JUNIOR, Airto; GUASQUE, Bárbara; PÁDUA, Thiago Santos Aguiar de. Segregação racial e vieses algorítmicos: máquinas racistas no âmbito do controle penal. *Revista Brasileira de Direito*, [S.L.], v. 19, n. 2, p. 1-30, 22 set. 2023. Complexo de Ensino Superior Meridional S.A. Disponível em: <https://doi.org/10.18256/2238-0604.2023.v19i2.4768>. Acesso em: 22 jul. 2024.

HENRIQUES, Isabella Vieira Machado; SAMPAIO, Inês Vitorino. *Discriminação algorítmica e inclusão em sistemas de inteligência artificial – uma reflexão sob a ótica dos direitos da criança no ambiente digital*. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5993/pdf>. Acesso em: 19 jul. 2024.

HUPFFER, Haide Maria; SANTANNA, Gustavo da Silva. *Inteligência artificial e discriminação algorítmica: marcos regulatórios e parâmetros éticos*. Disponível em: <http://www.guaritadigital.com.br/casaleirialivros/iasg/iasg.4.pdf>. Acesso em: 15 jul. 2024.

JANIESCH, C.; ZSCHENCH, P.; HEINRICH, K. Machine learning and deep learning. arXiv.org, *Springer*, [2331-8422], 2021. Disponível em: <https://arxiv.org/pdf/2104.05314>. Acesso em: 17 jul. 2024.

LLOYD, S.; MOHSENI, M.; REBENTROST, P. *Quantum algorithms for supervised and unsupervised machine learning*. Disponível em: <https://arxiv.org/pdf/1307.0401>. Acesso em: 17 jul. 2024.

MARCÍLIO, Thiago. Quatro polêmicas sobre o projeto que regula a inteligência artificial. *Consultor Jurídico*, São Paulo, 29 fev. 2024. Disponível em: <https://www.conjur.com.br/2024-fev-29/quatro-polemicas-sobre-o-projeto-que-regula-a-inteligencia-artificial/>. Acesso em: 14 out. 2024.

NAÇÕES UNIDAS. *The Age of Digital Interdependence: Report of the UN Secretary-General's High-level Panel on Digital Cooperation*. 2019. Disponível em: <https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf>. Acesso em: 17 jul. 2024.

NOBLE, S. U. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press, 2018.

OCDE. *OECD Principles on Artificial Intelligence*. 2019. Disponível em: <https://www.oecd.org/goiing-digital/ai/principles/>. Acesso em: 17 jul. 2024.

PASQUALE, F. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press, 2015. Disponível em: <https://raley.english.ucsb.edu/wp-content/Engl800/Pasquale-blackbox.pdf>. Acesso em: 18 jul. 2024.

RESMINI, Carol; PAGLIARINI, Eduarda; MORAES, Júlia D'Alascio Rangel de; LANDMEIER, Laura Vardanega. *Os desafios sociais na era da inteligência artificial: um enfoque na lacunar equidade racial*. Disponível em: <https://ojs.sites.ufsc.br/index.php/avant/article/view/7661/6164>. Acesso em: 17 jul. 2024.

SAMUEL, A. Some studies in machine learning using the game of checkers. *IBM Journal of Research and Development*, v. 3, n. 3, p. 210-229, 1959. Disponível em: <https://people.csail.mit.edu/brooks/idocs/Samuel.pdf>. Acesso em: 17 jul. 2024.

SINGAPURA. *Comissão de Proteção de Dados Pessoais. Modelo de Estrutura de Governança de IA*. Disponível em: <https://www.p.gov.sg/ajuda-e-recursos/2020//01/model-ai-vai-estrutura>. Acesso em: 17 jul. 2024

TSAMADOS, A.; AGGARWAL, N.; COWLS, J.; MORLEY, J.; ROBERTS, H.; TADDEO, M.; FLORIDI, L. The ethics of algorithms: key problems and solutions. *AI & SOCIETY*, v. 37, p. 215-230, 2022. Disponível em: <https://link.springer.com/article/10.1007/s00146-021-01154-8>. Acesso em: 22 jul. 2024.

WEST, Sarah Myers; WHITTAKER, Meredith; CRAWFORD, Kate. *Discriminating systems: gender, race and power in AI*. Nova Iorque: New York University, AI Now Institute, 2019. Disponível em: <https://ainowinstitute.org/discriminatingystems.pdf>. Acesso em: 22 jul. 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

9

**Uma análise crítica
acerca da algoritmização
discriminatória no âmbito do
direito penal**

LUISA AMÉLIA

Sumário: Introdução. 1. Inteligência Artificial: conceito, evolução e desdobramentos. 2. Discriminação algorítmica e os seus efeitos. 3. Análise crítica sobre o uso de algoritmos discriminatórios no âmbito do direito penal. Considerações finais. Referências.

Introdução

A sociedade moderna, denominada sociedade da informação², é movida por dados dos mais variados níveis, os quais recaem sobre as pessoas, seus hábitos e suas características e somente após alguns anos de evolução das tecnologias coletoras, tornou possível o seu processo de mineração e a sua compreensão, denominado de processamento. Nesse cenário, é fato que tudo o que fazemos e, até o que não fazemos, como quando abrimos uma página de vendas, mas decidimos não comprar algo *on-line*, por exemplo, permanece gravado, sendo considerado um dado de navegação.

Registra-se, nessa conjuntura, que os dados sempre foram um ativo importante, mas as formas de interpretá-los, mesmo com os recursos computacionais, nem sempre foram tão assertivas. No entanto, isso vem mudando com a ascensão das tecnologias de processamento de dados e, mais recentemente, com a ascensão da Inteligência Artificial.

Desse modo, atividades que eram consideradas hipercomplexas tornaram-se simples por serem realizadas com precisão pelos sistemas, de modo que seu uso avançou para áreas como a medicina e o direito. No Brasil, por exemplo, o STF admite a utilização de IA para a análise de recursos protocolados, a fim de identificar em seus assuntos matéria de recursos repetitivos, o que se mostrou como uma solução eficiente do ponto de vista da celeridade e economicidade processual.

No entanto, apesar da relevância desse tipo de tecnologia para o progresso científico mundial, o seu uso e ascensão vem acompanhado de preocupações quanto às suas implicações sociais, éticas e jurídicas, haja vista que esses

1. Advogada associada do Escritório Peter Fernandes e Marihá Viana Advogados Associados. É bacharel em Direito pelo Centro Universitário de Brasília (UniCEUB) e mestre em Criminologia com especialização em Política Criminal pela Universität de Barcelona/Espanha. Atualmente, cursa pós-graduação em Direito Digital no Instituto de Tecnologia e Sociedade (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).

2. WEBSTER, Frank. *Theories of the information society*. Londres: Routledge, 1995.

sistemas não devem se colocar acima dos direitos das pessoas³. Isso chama a atenção para a necessidade de discutir a utilização ética, transparente e responsável da IA, além de sua necessária regulação. No entanto, não se pode perder de vista, nessa discussão, a necessidade da coexistência do contínuo progresso tecnológico como uma tutela efetiva dos direitos dos cidadãos.

Dessa forma, na presente investigação, almeja-se a realização de uma análise crítica acerca dos riscos de decisões discriminatórias protagonizadas pela Inteligência Artificial no âmbito do Direito Penal, assim como suas implicações e possíveis propostas para contornar a situação. Ressalta-se que o estudo foi realizado a partir do método dialético dedutivo, por meio de pesquisa bibliográfica em artigos científicos, livros e na legislação atinente ao tema e foi estruturado em três capítulos.

No primeiro capítulo, realizou-se uma análise quanto à Inteligência Artificial, especificamente, em relação ao conceito, aos usos e à dinâmica de sua discussão no Brasil. Foram abordadas, igualmente, as impressões elencadas pela literatura, as questões concorrenciais e éticas, assim como as propostas de regulação e o que se espera de uma regulação eficiente sobre a matéria no Brasil.

Por sua vez, no segundo capítulo, houve a abordagem do tema da discriminação algorítmica, considerando os riscos correlatos na tomada de decisões pela IA. Diante das possíveis resoluções enviesadas com preconceitos e concepções humanas negativas, propôs-se a apreciação dos limites éticos e pressupostos legais a esse respeito.

Por fim, no terceiro capítulo, partindo da hipótese de utilização da Inteligência Artificial no âmbito do Direito Penal, ficou demonstrado, pela literatura atinente ao tema, que o seu uso pode perpetuar decisões racistas e segregacionistas. Por essa razão, a proposta a que se chegou para contornar o problema foi impedir a utilização de sistemas que possam apresentar vieses discriminatórios, em conformidade com o que já dispõe a Resolução nº 332 do Conselho Nacional de Justiça (CNJ)⁴ e nova minuta de Resolução desenvolvida pelo Grupo de Trabalho sobre Inteligência Artificial no Poder Judiciário (GTIA) do também CNJ⁵, bem como a importância de inserção da participação humana nos processos de tomada de decisão da IA.

3 MOURÃO, Licurgo; INDUSTRIAL, Revolução. Regulação da inteligência artificial no Brasil. *Intellegentiae artificialis, imperium et civitatem*, p. 73-89, 2022. Disponível em: <https://idus.us.es/bitstream/handle/11441/146766/1/eBook%20Intellegentiae%20Artificialis%20Imperium%20et%20Civitatem.pdf?sequence=1#page=74>. Acesso em 27 jul. 2024.

4. Conselho Nacional de Justiça. *Resolução n. 332, de 21 de agosto de 2020*. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3429>. Acesso em: 29 jul. 2024.

5 CONSELHO NACIONAL DE JUSTIÇA (CNJ). *Minuta de proposta da resolução 332*. Brasília: CNJ, 2024. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2024/09/minuta-proposta-resolucao-332-cnj-rev.pdf>. Acesso em: 13 out. 2024.

Nas considerações finais, foi destacado que se demonstra arriscado o uso de sistemas automatizados em atuações que envolvam o direito penal, na medida em que já é um sistema discriminatório por si.

1. Inteligência Artificial: conceito, evolução e desdobramentos

A comunidade científica conceitua o termo “inteligência artificial” como “a capacidade de raciocínio de máquinas que reproduz o funcionamento da mente humana”⁶, como tem sido feito pelo ChatGPT⁷ (*Generative Pre-Trained Transformer*), um *software* desenvolvido pela OpenAI.

É considerado um tema em alta no debate social, político, jurídico e na grande mídia mundial. Isso decorre, em especial, pela promessa de transformação da forma como a sociedade se organiza, marcando o ápice do desenvolvimento tecnológico em escala global. Nota-se, em decorrência disso, uma corrida desenvolvimentista, disputada pelos países que querem ser os protagonistas no desenvolvimento e uso da IA e, que vem se concentrando, diga-se de passagem, entre potências já conhecidas como Estados Unidos e China.⁸

Esse acelerado desenvolvimento somado ao seu potencial transformativo tem servido de base para a compreensão de que o planeta está diante de uma nova era. Essas tecnologias realmente possuem um grande potencial modificativo, a ponto de trazer o questionamento sobre a substituição de algumas profissões em breve. Nota-se, portanto, que a IA está transformando as estruturas sociais, inclusive, a forma como o homem lida com a tecnologia, o que faz com que a literatura considere a ascensão de uma quarta Revolução Industrial.⁹

Tanto é assim que a Organização para Cooperação e Desenvolvimento Econômico (OCDE), ao avaliar o potencial transformativo e modificativo desse tipo de tecnologia, chamou a atenção para a necessidade de delimitação de limites éticos quanto ao seu uso, sobretudo, pelas implicações concorrenciais e democráticas que elas podem ocasionar, como explica Mourão:

6. MOURÃO, Licurgo. Regulação da inteligência artificial no Brasil. *Intellegentiae artificialis, imperium et civitatem*, p. 73, 2022. Disponível em: <https://idus.us.es/bitstream/handle/11441/146766/1/eBook%20Intellegentiae%20Artificialis%20Imperium%20et%20Civitatem.pdf?sequence=1#page=74>. Acesso em 27 jul. 2024.

7. O ChatGPT “funciona a partir de uma base de conhecimento atualizada que permite decodificar palavras para oferecer respostas textuais às pessoas. Trata-se de um modelo treinado a partir de dados de textos disponíveis na internet” (FIA, 2024).

8. PARENTONI, Leonardo Netto; VALENTINI, Rômulo Soares; ALVES, Tárík César Oliveira E. Panorama da Regulação da Inteligência Artificial no Brasil: com ênfase no PL’s N. 5.051/2019. *Revista Eletrônica do Curso de Direito da UFSM*, v. 15, n. 2, p. 2, 2020.

9. MOURÃO, Licurgo; INDUSTRIAL, Revolução. Regulação da inteligência artificial no Brasil. *Intellegentiae artificialis, imperium et civitatem*, p. 73, 2022. Disponível em: <https://idus.us.es/bitstream/handle/11441/146766/1/eBook%20Intellegentiae%20Artificialis%20Imperium%20et%20Civitatem.pdf?sequence=1#page=74>. Acesso em 27 jul. 2024.

[...] a Organização para Cooperação e Desenvolvimento Econômico (OCDE), ao reconhecer que a inteligência artificial está transformando sociedades, setores econômicos e o futuro do trabalho e que possui potencial de contribuir para a solução dos principais desafios globais, ressaltou que as transformações acarretadas pelo avanço tecnológico podem afetar desigualmente sociedades e economias, sobretudo no que diz respeito à concorrência, transições no mercado de trabalho, desigualdades e implicações para as democracias e direitos humanos, privacidade e proteção de dados e segurança digital.

Nesse cenário, observa-se a crescente preocupação mundial com a definição dos padrões e limites éticos do emprego da inteligência artificial, buscando regulamentar o uso das novas tecnologias de forma a zelar pelos direitos dos cidadãos.¹⁰

Em um curto período, evidencia-se que a inteligência artificial se desenvolveu de modo a conseguir decidir de forma autônoma, isto é, sem a intervenção humana nas fases posteriores à formulação do algoritmo, o que lhe foi possibilitado a partir da utilização de mecanismos de *machine learning* (aprendizagem de máquina) somada às técnicas de *deep learning* (aprendizagem profunda). Isso ocorreu de uma forma tão surpreendente que, em 2024, um determinado sistema de inteligência artificial já possui a capacidade de criar outro, além de conseguir se integrar a outros, objetivando o aprimoramento de resultados.¹¹

No Brasil, a título exemplificativo, desde 2020, o Supremo Tribunal Federal (STF) tem utilizado modelos de *machine learning* para a análise de recursos recebidos pelo Tribunal que versam sobre temas em repercussão geral.¹²

Esse mecanismo de utilização pela Suprema Corte do Brasil permitiu a inserção de uma “celeridade e acurácia na análise de uma quantidade expressiva de processos e situações, contemplando princípios relevantes de celeridade, eficiência e economia”¹³. Isso mostra a vantagem da utilização de sistemas como esse, na medida em que facilitam a atividade humana e podem

10. MOURÃO, Licurgo. Regulação da inteligência artificial no Brasil. *Intellegentiae artificialis, imperium et civitatem*, p. 75-76, 2022. Disponível em: <https://idus.us.es/bitstream/handle/11441/146766/1/eBook%20Intellegentiae%20Artificialis%20Imperium%20et%20Civitatem.pdf?sequence=1#page=74>. Acesso em 27 jul. 2024.

11. REQUIÃO, Maurício; COSTA, Diego. Discriminação algorítmica: ações afirmativas como estratégia de combate. *Civilistica.com*, v. 11, n. 3, p. 3, 2022. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/804/650>. Acesso em: 24 jul. 2024.

12. MAIA FILHO, Mamede Said; JUNQUILHO, Tainá Aguiar. Projeto Victor: perspectivas de aplicação da inteligência artificial ao direito. *Revista de Direitos e Garantias Fundamentais*, v. 19, n. 3, p. 218, 2018.

13. PEIXOTO, Fabiano Hartmann. Projeto Victor: relato do desenvolvimento da inteligência artificial na repercussão geral do Supremo Tribunal Federal. *Revista Brasileira de Inteligência Artificial e Direito-RBIAD*, v. 1, n. 1, p. 18. Disponível em: <https://www.rbiad.com.br/index.php/rbiad/article/view/4/4>. Acesso em: 25 jul. 2024.

entregar um resultado positivo à sociedade. Todavia, conforme mencionado anteriormente, um resultado positivo nesse sentido não anula a necessidade de lidar com o tema com o cuidado que ele requer e não exclui a urgência de uma regulação que delimite critérios éticos e jurídicos, de modo que o seu desenvolvimento continue ocorrendo em estrita observância à legislação.

No que se refere a esse último ponto, no Brasil, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) abriu as portas para uma regulação da matéria ao prever a possibilidade de o titular de dados pessoais solicitar a revisão de decisões automatizadas, conforme art. 20¹⁴. Contudo, a respectiva lei, longe de regulamentar o assunto, apenas evidenciou a necessidade de um tratamento cuidadoso da matéria, tendo em vista que o seu impacto abrange não apenas dados pessoais, mas uma gama de outros direitos e questões sociais.

Em 2020, a Resolução nº 332/2020 do Conselho Nacional de Justiça¹⁵ tratou do estabelecimento de regras quanto à ética, transparência e governança para o uso da inteligência artificial pelo Poder Judiciário¹⁶. Tal legislação foi realmente um marco importante para o tratamento do assunto no âmbito do judiciário brasileiro, especialmente, pelos dados alarmantes de decisões enviesadas de caráter discriminatório e, até mesmo, racista, que serão abordados especificamente mais adiante neste estudo. Atualmente, há nova minuta de Resolução desenvolvida pelo Grupo de Trabalho sobre Inteligência Artificial no Poder Judiciário (GTIA) do também CNJ.¹⁷

O Executivo Federal, igualmente, intenta esforços no sentido de traçar uma “Estratégia Brasileira de Inteligência Artificial” (EBIA), instituída pela Portaria MCTI nº 4.617/2021 e tem como premissa “nortear as ações do Estado brasileiro em prol do desenvolvimento das ações, em suas várias vertentes, que estimulem a pesquisa, inovação e desenvolvimento de soluções em Inteligência Artificial, bem como, seu uso consciente, ético e em prol de um futuro melhor”¹⁸.

14. 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.

15. Conselho Nacional de Justiça. *Resolução n. 332, de 21 de agosto de 2020*. Disponível em: <<https://atos.cnj.jus.br/atos/detalhar/3429>>. Acesso em: 29 jul. 2024.

16 MOURÃO, Licurgo; INDUSTRIAL, Revolução. Regulação da inteligência artificial no Brasil. *Intellegentiae artificialis, imperium et civitatem*, p. 82, 2022. Disponível em: <https://idus.us.es/bitstream/handle/11441/146766/1/eBook%20Intellegentiae%20Artificialis%20Imperium%20et%20Civitatem.pdf?sequence=1#page=74>. Acesso em 27 jul. 2024.

17 CONSELHO NACIONAL DE JUSTIÇA (CNJ). *Minuta de proposta da resolução 332*. Brasília: CNJ, 2024. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2024/09/minuta-proposta-resolucao-332-cnj-rev.pdf>. Acesso em: 13 out. 2024.

18 BRASIL. Ministério da Ciência, Tecnologia e Inovação. *Inteligência Artificial*. Disponível em: <<https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial>>. Acesso em: 29 jul. 2024.

Revela-se que a EBIA representa uma notável movimentação do Poder Executivo Federal, no âmbito do Ministério da Ciência e Tecnológica, por ter permitido uma discussão transversal do tema desde a abertura de uma consulta pública, na qual permitiu a participação de diversos atores da sociedade, até a publicação de seu escopo abrangendo diversos eixos. No entanto, a literatura diz que ela está longe de ser uma estratégia, se assemelhando mais a uma mera carta de intenções devido às proposições genéricas e sem um viés pragmático.¹⁹

Nesse sentido, fica claro que as poucas movimentações vistas na prática pelo Estado brasileiro ainda não correspondem a uma expectativa legítima de regulação da matéria, apesar de sua urgência e imprescindibilidade.

Importante ressaltar, ainda, que, no Congresso Nacional (CN) encontra-se em tramitação diversos Projetos de Lei, cujo objeto é a regulação da matéria. Nessa conjuntura, chama-se a atenção ao PL 2.338/2023, de iniciativa do Senador Rodrigo Pacheco (PSD/MG), o qual tem apresentado um escopo propositivo e orientado pela centralidade da pessoa humana como fundamento (art. 2º, inciso I do PL), e que propõe a livre iniciativa, também, como premissa (art. 2º, inciso VII), tendo um viés declaradamente orientado pela Liberdade Econômica. Sendo que, após uma longa tramitação por diversas comissões no CN, o cenário no segundo semestre de 2024 ainda destoa de um consenso na casa legislativa pela abrangência do tema.

De modo que, a grande parte das discussões no Congresso Nacional versam pela busca de um equilíbrio entre a centralidade da pessoa humana, com o respectivo resguardo de sua dignidade e direitos fundamentais, e o prosseguimento do desenvolvimento tecnológico e científico.

Nesse cenário de regência da estrutura de uma regulação para a Inteligência Artificial, Mourão pondera que:

Diante dos desafios observados pelo uso da inteligência artificial, avultam como principais princípios regulatórios que devem nortear a elaboração de leis sobre o tema: a) interesse geral, garantindo inclusão e equidade, uma vez que o poder público não pode visar à satisfação de interesses particulares em detrimento do interesse público; b) direitos humanos, pois devem ser respeitados os direitos fundamentais, tais como as liberdades individuais, a igualdade e a diversidade, combatendo-se práticas discriminatórias rea-

19. GASPAR, Walter Britto; MENDONÇA, Yasmin Curzi de. A Inteligência Artificial no Brasil ainda precisa de uma estratégia. *Fundação Getúlio Vargas*, Rio de Janeiro, 2021. Disponível em: <<https://diretorio.fgv.br/sites/default/files/2022-08/ebia-pt-br.pdf>>. Acesso em: 27 jul. 2024.

lizadas por sistemas de inteligência artificial; c) transparência, de modo a assegurar a compreensão do seu funcionamento (quanto a algoritmos, dados, provas e validações realizadas, além da lista das áreas que utilizam tais tecnologias).²⁰

Denota-se, portanto, a relevância, em especial, do interesse geral, dos direitos humanos e da transparência. Nada obstante, não se pode perder de vista a necessidade de assegurar o progresso tecnológico para o desenvolvimento de soluções cada vez mais adequadas. Em outras palavras, a regulação da IA não deve ser vista como uma barreira para o seu progresso, pelo contrário, deve servir para garantir que a sua evolução ocorra em conformidade com a justiça e a ética, sendo esse equilíbrio chamado de ponto alto da regulação.

2. Discriminação algorítmica e seus efeitos

A utilização de inteligência artificial nos processos cotidianos apresenta vantagens, como a otimização do tempo, parametrização de escolhas e a facilitação de diversas atividades. Há, inclusive, opiniões na comunidade científica de que a razão pela qual se recorre à tomada de decisões automatizadas²¹ estaria ligada à sua neutralidade, devido à objetividade e à utilização de critérios matemáticos, que poderia, em tese, solucionar os problemas relacionados à tomada de decisão humana, que é dotada de falhas e vieses cognitivos.²²

No entanto, conforme já explanado, há diversas dificuldades observadas na prática, a depender da forma de uso. Nesse contexto, registra-se que a IA é dotada de diversas características, dentre elas:

“i) a opacidade, que faz com que muitas vezes nem mesmo os desenvolvedores saibam ao certo as razões pelas quais os algoritmos chegaram às conclusões” e, ainda, pode ser questionada a “ii) qualidade dos dados utilizados para “rodar” os algoritmos, que podem trazer consigo vieses implícitos à programação ou adquiri-los posteriormente com a interação em rede, tornando as decisões automatizadas um campo fértil para ocorrência de discriminações, sobretudo contra grupos mais vulneráveis”.²³

20. MOURÃO, Licurgo; INDUSTRIAL, Revolução. Regulação da inteligência artificial no Brasil. *Intellegentiae artificialis, imperium et civitatem*, p. 79, 2022. Disponível em: <https://idus.us.es/bitstream/handle/11441/146766/1/eBook%20Intellegentiae%20Artificialis%20Imperium%20et%20Civitatem.pdf?sequence=1#page=74>. Acesso em 27 jul. 2024.

21. Decisão algorítmica ou automatizada refere-se às decisões tomadas pelo algoritmo sem a intervenção humana.

22. REQUIÃO, Maurício; COSTA, Diego. Discriminação algorítmica: ações afirmativas como estratégia de combate. *Civilistica.com*, v. 11, n. 3, p. 3, 2022. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/804/650>. Acesso em: 24 jul. 2024.

23. REQUIÃO, Maurício; COSTA, Diego. Discriminação algorítmica: ações afirmativas como estratégia de combate. *Civilistica.com*, v. 11, n. 3, p. 2, 2022. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/804/650>. Acesso em: 24 jul. 2024.

Veja-se a explicação de Costa Requião em que minucia acerca do viés discriminatório do algoritmo:

[...] a IA e o processo algorítmico não apenas são incapazes de corrigir o erro subjetivo humano, como também podem replicar e até reforçar os preconceitos existentes na sociedade, ocasionando distinções, preferências ou exclusões capazes de afetar a igualdade de tratamento entre os indivíduos, sobretudo os grupos vulneráveis. É o que se chama de viés discriminatório do algoritmo ou, simplesmente, discriminação algorítmica²⁴.

O autor explica, ainda, que a discriminação algorítmica pode ocorrer de duas formas: “i) quando os algoritmos refletirem os preconceitos humanos (conscientes ou não) embutidos desde a programação; ii) quando entrarem em contato com bases de dados contendo vieses preconceituosos, o que faz com o que o algoritmo “aprenda” a discriminar”.²⁵

Nesse tema, Mendes e Matiuzzo pontuam de forma interessante:

[...] o termo “discriminação algorítmica” é utilizado, neste artigo, para englobar tanto cenários que envolvem afirmações estatisticamente inconsistentes quanto cenário em que as afirmações, embora estatisticamente lógicas, de alguma forma tomam os indivíduos que dela são objeto não de forma efetivamente individualizada, mas apenas como parte de um grupo. Isso porque, a nosso ver, uma classificação, ainda que consistente sob o ponto de vista estatístico, pode em alguns casos se mostrar injusta.²⁶

Ainda nesse artigo, as autoras destacam 4 (quatro) espécies de discriminação algorítmica, sem excluirmos outros tipos. Sustentam, portanto, a “discriminação por erro estatístico”, que se referem a erros técnicos, isto é, falhas no código do algoritmo que podem acarretar uma incorreta análise dos dados, por exemplo. Sinalizam, também, a “discriminação por generalização”, que ocorre quando o algoritmo toma a generalização como

24. REQUIÃO, Maurício; COSTA, Diego. Discriminação algorítmica: ações afirmativas como estratégia de combate. *Civilistica.com*, v. 11, n. 3, p. 4, 2022. Disponível em: <<https://civilistica.emnuvens.com.br/redc/article/view/804/650>>. Acesso em: 24 jul. 2024.

25. REQUIÃO, Maurício; COSTA, Diego. Discriminação algorítmica: ações afirmativas como estratégia de combate. *Civilistica.com*, v. 11, n. 3, p. 4, 2022. Disponível em: <<https://civilistica.emnuvens.com.br/redc/article/view/804/650>>. Acesso em: 24 jul. 2024.

26. MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. *Direito Público*, v. 16, n. 90, p. 51, 2019. Disponível em: <<https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766>>. Acesso em: 24 jul. 2024.

verdade absoluta desprezando variações e exceções, o que no contexto da probabilidade é um erro.²⁷

A terceira espécie consiste na “discriminação pelo uso de informações sensíveis”, que se refere à utilização de dados como saúde ou religião para formular decisões, no sentido de envolve dados que não deveriam ser utilizados para certas finalidades e que encontra vedação na legislação brasileira. Por fim, a “discriminação limitadora do exercício de direitos”, que surge quando a relação entre a informação usada e o direito é tão direta que acaba restringindo ou prejudicando a capacidade de uma pessoa de exercer determinado direito.²⁸

A partir dessa compreensão, evidencia-se que a sua ocorrência fragiliza importantes direitos fundamentais, como o da igualdade e isonomia ao restringir direitos e benesses a pessoas por meio das generalizações. Além disso, a utilização dessas generalizações como base para processos decisórios “pode trazer efeitos colaterais, isto é, a discriminação de certos grupos na sociedade pode ser intensificada”.²⁹

Wimmer e Doneda consideram, nesse tema, que sistemas de IA são, por si, predispostos a falhas, sobretudo, por realizarem escolhas baseadas em mecanismos que não possuem precisão, tampouco neutralidade, o que pode ter como consequência resultados inadmissíveis, que decorrem, por exemplo, da internalização de vieses da cultura, estigmas raciais e de gênero, além de prejudicar indivíduos pertencentes a grupos étnicos e sociais específicos³⁰.

Notou-se, desse modo, a partir da análise das generalizações e alimentação com dados que as decisões de IA expressam o *status quo* humano, fazendo previsões e perpetuando padrões de desigualdade, “pior, são capazes de reforçá-los ainda mais: ao deliberadamente ignorar as desigualdades estruturais dos dados que se utilizam, eles acabam por potencializá-las”³¹.

Dessa forma, denota-se que, para que haja o funcionamento do sistema digital de forma coesa, é necessário que haja, minimamente, uma vultosa mi-

27. MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. *Direito Público*, v. 16, n. 90, p. 52-53, 2019. Disponível em: <<https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766>>. Acesso em: 24 jul. 2024.

28. MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. *Direito Público*, v. 16, n. 90, p. 52-53, 2019. Disponível em: <<https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766>>. Acesso em: 24 jul. 2024.

29. MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. *Direito Público*, v. 16, n. 90, p. 54, 2019. Disponível em: <<https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766>>. Acesso em: 24 jul. 2024.

30. WIMMER, Miriam e DONEDA, Danilo. “Falhas de IA” e a Intervenção Humana em Decisões Automatizadas: Parâmetros para a Legitimação pela Humanização, *Revista de Direito Público*, Brasília, Vol. 18, n. 100, p. 380, out./dez. 2021.

31. BEZERRA, Arthur Coelho; COSTA, Camila Mattos. Pele negra, algoritmos brancos: informações e racismo nas redes sociotécnicas. *Liinc em Revista*, Rio de Janeiro, v. 18, n. 2, p. 6, e6043, nov. 2022.

neração de dados³² (*data mining*), pois são eles que alimentam e orientam o funcionamento dos aplicativos e as soluções de inteligência artificial.

Quanto a essa dinâmica, diga-se de passagem, diversos protocolos devem ser adotados, principalmente, pelo fato de que muitos dos dados corriqueiramente utilizados pela tecnologia são sensíveis e possuem uma proteção mais incisiva.

3. O uso de algoritmos discriminatórios no âmbito do direito penal

Diante do fenômeno discriminatório em alguns algoritmos, demonstra-se de extrema relevância uma breve análise da aplicação da inteligência artificial no, então, ramo do direito penal brasileiro, também perpetrador de segregações, na medida que pretos, pardos e pessoas com baixa escolaridade são a maioria da população carcerária, segundo o Relatório de Informações Penais de 2023.³³

Conforme mencionado, esse âmbito do direito público possui diversas complexidades ligadas à discriminação que resulta em etiquetamento social e em seletividade penal.

Acerca do etiquetamento social, Howard S. Becker destaca que:

Como o desvio é, entre outras coisas, uma consequência das reações de outros ao ato de uma pessoa, os estudiosos do desvio não podem supor que estão lidando com uma categoria homogênea quando estudam pessoas rotuladas de desviantes. Isto é, não podem supor que essas pessoas cometeram realmente um ato desviante ou infringiram alguma regra, porque o processo de rotulação pode não ser infalível; algumas pessoas podem ser rotuladas de desviantes sem ter de fato infringido uma regra. Além disso, não podem supor que a categoria daqueles rotulados conterà todos os que realmente infringiram uma regra, porque muitos infratores podem escapar à detecção e assim deixar de ser incluídos na população de “desviantes” que estudam.³⁴

32. Mineração de dados refere-se ao processo de explorar grandes conjuntos de dados para descobrir padrões, tendências e relações significativas (Gropp, Motta, 2020).

33. SENAPEN – Secretaria Nacional de Políticas Penais. *Sistema Nacional de Informações Penais*. 15º Ciclo SISDEPEN. Período Julho a Dezembro de 2023. Relatório de Informações Penais. Brasília, 2024. Disponível em: <<https://www.gov.br/senappen/pt-br/servicos/sisdepen/relatorios>>. Acesso em: 03 jul. 2024.

34 BECKER, Howard. *Outsiders*. Tradução Maria Luiza X. de Borges; revisão técnica Karina Kuschmir. Rio de Janeiro: Zahar, 2008, p. 22.

De acordo com essa abordagem criminológica, evidencia-se que, para que determinada conduta seja considerada crime, ela passa por um processo de rotulação no qual aquela ação, realizada por determinada pessoa, deve ser assim caracterizada. Nesse sentido, em conformidade ao trecho citado, inúmeras pessoas podem realizar comportamentos ditos como criminosos, mas não serem considerados desviantes, assim como ao contrário.

Em outras palavras, a identidade do indivíduo importa muito mais do que a própria conduta propriamente dita. Assim, de forma entrelaçada e como consequência lógica, surge a seletividade penal.

No contexto da criminalização, referindo-se a esse processo de seletividade, Vera Batista pontua:

[...] é muito mais verdadeiro chamarmos ‘criminalidade registrada’ de criminalização, porque a seletividade operativa do sistema penal, modelando qualitativa e quantitativamente o resultado final da criminalização secundária – isto é, quem e quantos ingressarão nos registros –, faz dele um procedimento configurador da realidade social. Podemos acreditar ou não que o número de carros que ultrapassaram a velocidade permitida (‘criminalidade’) é idêntico ao número de multas impostas sob esse motivo pelas autoridades do trânsito (criminalização); mas é apenas neste segundo número, em verdade um construto humano (na dependência de fatores tão distintos quanto os humores do guarda, a localização da câmera de vigilância etc.) que poderemos estudar a incidência das transgressões.³⁵

Nesse sentido, frisa-se, uma vez mais, que a rotulagem existente na sociedade é refletida na população carcerária, como explica Luisa Silva:

A seletividade demonstra a existência de um perfil preferencial do público submetido ao cárcere no Brasil. Ela consiste na filtragem entre a criminalidade latente e a criminalidade perseguida, que ocorre tanto no âmbito da criminalização primária quanto no da secundária. As razões para tanto são questões como nível social, escolaridade, etnia, forma de vestir-se, comunicar-se e portar-se, sendo que as três últimas escancaram a que classe pertence o indivíduo no que tange às duas primeiras, dentre outros mecanismos de clivagem. Tem-se de considerar, ainda, que, uma vez que as agências de controle estatal não possuem os meios necessários para o efetivo processamento de todo e qualquer fato típico que ocorre, elas

35. BATISTA, Vera Malaguti. *Introdução crítica à criminologia brasileira*. 2ª edição. Rio de Janeiro: Revan, 2012, p. 22.

selecionam a qualidade da atenção dada aos que chegam ao seu conhecimento.³⁶

Verifica-se que esse fenômeno da seletividade é um problema, *per si*, realizado no contexto racista e classista da sociedade moderna. Agrava-se, no entanto, quando sistemas de decisões automatizadas, alimentados por dados condizentes à realidade social, reproduzem estigmas e vieses preconceituosos por meio de generalizações e da reprodução dos preconceitos humanos.

Muitos dos que defendem a utilização de IA pelos sistemas de justiça, sobretudo no Direito Penal, argumentam que a automatização dos processos pode trazer ganhos como a economia e a celeridade processual. No entanto, tais benefícios acabam ocorrendo às custas de sacrifícios aos direitos humanos e à dignidade da pessoa humana, como explica Piló e Brasil³⁷.

Posto isso, Bichara, Cascardo Junior e Perazzoni explicam que:

O uso de IA para examinar dados relacionados a crimes traz consigo o risco de intensificar estereótipos e preconceitos já presentes na sociedade. Algoritmos empregados na previsão de delitos ou na identificação de suspeitos tendem a replicar vieses existentes nos dados utilizados, resultando na continuação de desigualdades raciais e sociais.³⁸

Assim, Santos, Torres e Celestino, ao realizarem uma análise quanto à utilização da IA na justiça criminal, aferiram que as chances de encarcerar pessoas negras eram maiores do que pessoas brancas, o que ocorria pela generalização realizada pela máquina³⁹.

Os autores, ainda, explicam ao discutir o serviço de segurança policial:

No setor de justiça criminal, há a argumentação que uma vez que as previsões dos algoritmos baseados em machine learning dependem da qualidade dos dados de treino o serviço de segurança policial pública de diferentes regiões pode ser afetado pelo menos

36. SILVA, Luisa Cypriano Moreira da. *Sistema carcerário brasileiro: uma análise do perfil dos presos a partir das teorias da seletividade penal e do etiquetamento social*. 2019, p. 20. Universidade Federal de Ouro Preto. Departamento de Direito. Monografia. Disponível em: <https://monografias.ufop.br/bitstream/35400000/2399/7/MONOGRRAFIA_SistemaCarcer%20c3%a1rioBrasileiro.pdf>. Acesso em: 29 jul. 2024.

37. PILÓ, Xenofontes Curvelo; BRASIL, Deilton Ribeiro. A utilização da inteligência artificial no direito penal e seus reflexos nas garantias e direitos fundamentais. *Revista EJEJF*, n. 1, p. 294-295, 2022.

38. BICHARA, Anderson Andrade; CASCARDIO JR, Agostinho Gomes; PERAZZONI, Franco. Racismo algorítmico, reforço de preconceitos e uso de IA: perspectivas e desafios para a investigação criminal digital. *Boletim IBCCRIM*, v. 32, n. 379, p. 24, 2024.

39. SANTOS, Adriane de Almeida; TORRES, Marck de Souza; CELESTINO, Victor. Discriminação algorítmica e o acirramento do racismo estrutural: revisão de escopo. *Revista Científica Integrada*, v. 7, n. 1, p. 5, e202415-e202415, 2024. Disponível em: <<https://revistas.unaerp.br/rci/article/view/3233/2422>>. Acesso em: 24 jul. 2024.

de duas formas distintas: (1) comunidades com histórico de uma relação prejudicada com a polícia podem subnotificar atividade criminosa na sua região e uma vez que estes dados são utilizados em sistemas de tomada de decisão algoritmizados, o sistema pode decidir que estas regiões possuem um nível de criminalidade e segurança não condizente com a realidade e não direcionar recursos e assistência policial adequados; (2) Sistemas algorítmicos que não treinados com base em dados que incorporam estereótipos raciais relacionados à criminalidade podem indicar que regiões com maior pressão policial do que regiões com maior densidade populacional de negros recebam maior pressão policial do que regiões de população predominantemente branca. A combinação de ambas as práticas algorítmicas contribui para que a concentração de recursos de segurança fique em regiões privilegiadas predominantemente habitadas por pessoas brancas enquanto os territórios periféricos de maioria negra recebem coerção policial, demarcando ainda mais as disparidades raciais.⁴⁰

No caso descrito, fica evidente o potencial de segregação que as decisões algorítmicas possuem, ao passo que, pode abranger desde a articulação da estratégia de enfrentamento ao problema até a própria ação no caso concreto.

Relevante considerar, desse modo, o risco de permitir que a IA assuma uma postura mais punitivista direcionada a grupos específicos em detrimento de outros. Ou seja, o que também é visto no cotidiano forense brasileiro pode ser agravado no contexto de uma IA, que utiliza desse tipo de métrica para racionalizar os padrões por meio da generalização.

Nesse contexto, já há casos explícitos de algoritmização discriminatória em IAs operadas no direito penal brasileiro. É o caso, por exemplo, do sistema de reconhecimento facial, que está sendo amplamente utilizado pelas autoridades policiais a fim de identificar possíveis criminosos. Em que pese a utilização desse tipo de tecnologia esteja se mostrando problemática em países como os EUA, em que ficou comprovado o viés racista e segregacionista, além da baixa precisão na identificação de pessoas, o Brasil importou tal modelo a fim de auxiliar na prisão de indivíduos procurados pela polícia.⁴¹

Entretanto, o mesmo resultado está ocorrendo no Brasil, nos termos da literatura atinente ao tema:

40 SANTOS, Adriane de Almeida; TORRES, Marck de Souza; CELESTINO, Victor. Discriminação algorítmica e o acirramento do racismo estrutural: revisão de escopo. *Revista Científica Integrada*, v. 7, n. 1, p. 5, e202415-e202415, 2024. Disponível em: <<https://revistas.unaerp.br/rci/article/view/3233/2422>>. Acesso em: 24 jul. 2024.

41. CHAVES JÚNIOR, Airto; GUASQUE, Bárbara; DE PÁDUA, Thiago Santos Aguiar. Segregação racial e vidas algorítmicas: máquinas racistas no âmbito do controle penal. *Revista Brasileira de Direito*, v. 2, p. 19, 2023. Disponível em: <<https://seer.attus.edu.br/index.php/revistadedireito/article/view/4768>>. Acesso em: 05 ago. 2024.

[...] após cerca de um ano de utilização, as estatísticas relativas ao enviesamento do modelo já começaram a aparecer. Levantamento realizado pela Rede de Observatórios da Segurança constatou que, das 151 prisões pela via do sistema de reconhecimento fácil que aconteceram no país, 90% eram de pessoas negras (Chaves Jr., Guasque, De Pádua, 2023, p. 20).

Interessante verificar que, no cenário internacional, há uma crescente movimentação de casos que denunciam a discriminação algorítmica no processo de identificação facial, alguns deles que, inclusive, estão propondo o banimento desse tipo de tecnologia. Por sua vez, no Brasil, em sentido contrário, há o fomento do uso desse tipo de ferramenta pelos Estados membros, com financiamento pelo governo federal, como formato de política de segurança pública.⁴²

Catiane Steffen explica que um dos meios de maior potencial discriminatório pelos algoritmos que se valem da IA é o direito penal⁴³. A autora menciona a funcionalidade de técnicas que numa primeira análise poderia, em tese, auxiliar as autoridades a confirmar a autoria e a materialidade de crimes, ao passo que, otimizaria a produção de provas. Contudo, expõe que:

[...] ao mesmo tempo em que se aumenta a capacidade preventiva e punitiva do Estado, abre-se a possibilidade de se violar o direito dos cidadãos sobre os seus dados pessoais armazenados – com ou sem o seu consentimento – nas bases estatais de segurança pública. Outra das várias possibilidades de lesão a direito está na criação de perfis criminosos que concluam pelo potencial de lesividade de um indivíduo a partir de características físicas, emocionais e sociais, aumentando-se a atuação do Estado sobre núcleos já estigmatizados ou discriminados numa determinada sociedade.⁴⁴

Diante de todos os percalços demonstrados, a Resolução nº 332 do CNJ foi um marco importante para o tratamento da matéria aqui discutida, ao disciplinar o seu uso no âmbito do Poder Judiciário. Mourão, inclusive, assim esclarece acerca da saída apresentada pela norma para os casos em que o sistema de IA pode apresentar vieses discriminatórios, diz que:

42. CHAVES JÚNIOR, Airto; GUASQUE, Bárbara; DE PÁDUA, Thiago Santos Aguiar. Segregação racial e vidas algorítmicas: máquinas racistas no âmbito do controle penal. *Revista Brasileira de Direito*, v. 2, p. 20, 2023. Disponível em: <<https://seer.atitus.edu.br/index.php/revistadedireito/article/view/4768>>. Acesso em: 05 ago. 2024.

43. STEFFEN, Catiane. A inteligência artificial e o processo penal: a utilização da técnica na violação de direitos. *Revista da EMERJ*, v. 25, n. 1, p. 112, 2023.

44. STEFFEN, Catiane. A inteligência artificial e o processo penal: a utilização da técnica na violação de direitos. *Revista da EMERJ*, v. 25, n. 1, p. 113, 2023.

A Resolução prevê a obrigatoriedade de que o desenvolvimento, a implantação e o uso da inteligência artificial observem os direitos fundamentais e que a utilização de tecnologias deve buscar garantir a segurança jurídica e a igualdade. Para tanto, previu que, antes de ser implementado, o sistema deverá ser homologado, de forma a identificar se preconceitos ou generalizações influenciaram seu desenvolvimento, acarretando tendências discriminatórias no seu funcionamento. Caso não possa ser sanado o viés discriminatório, o modelo não poderá ser utilizado⁴⁵.

Nesse caso, o CNJ já anteviu a necessidade de homologação e realização de testes aptos a aferir o viés discriminatório de uma IA para que ela seja permitida e após, utilizada no âmbito do Poder Judiciário, abrangendo decisões sobre direito penal.

A resolução em comento tratou do tema especificamente no contexto penal em seu artigo 23, da seguinte forma:

Art. 23. A utilização de modelos de Inteligência Artificial em matéria penal não deve ser estimulada, sobretudo com relação à sugestão de modelos de decisões preditivas.

§ 1º Não se aplica o disposto no caput quando se tratar de utilização de soluções computacionais destinadas à automação e ao oferecimento de subsídios destinados ao cálculo de penas, prescrição, verificação de reincidência, mapeamentos, classificações e triagem dos autos para fins de gerenciamento de acervo.

§ 2º Os modelos de Inteligência Artificial destinados à verificação de reincidência penal não devem indicar conclusão mais prejudicial ao réu do que aquela a que o magistrado chegaria sem sua utilização. (BRASIL, 2020).

Chaves Júnior, Guasque, De Pádua atestam que a ausência de regulação sobre a matéria oferece riscos a todas as esferas, sobretudo ao uso indiscriminado pela justiça criminal. Para os autores:

Essa ausência de regulamentação, responsabilidade, auditoria e transparência na utilização da IA, vem angariando consequências nefastas do ponto de vista jurídicosocial, por perpetua e amplia as discriminações e a seletividade que permeia o controle penal e as agências que o integram. E tudo sob a ilusória impressão de que se baseia em modelos matemáticos imparciais, precisos e objeti-

45. MOURÃO, Licurgo; INDUSTRIAL, Revolução. Regulação da inteligência artificial no Brasil. *Intellegentiae artificialis, imperium et civitatem*, p. 81, 2022. Disponível em: <https://idus.us.es/bitstream/handle/11441/146766/1/eBook%20Intellegentiae%20Artificialis%20Imperium%20et%20Civitatem.pdf?sequence=1#page=74>. Acesso em 27 jul. 2024.

vos. Em verdade, os resultados estão carregados de subjetividade e vieses racistas tendentes a catalisar setores sociais bem delimitados para a marginalização e a discriminação.⁴⁶

A literatura jurídica especializada, igualmente, tem oferecido como solução aos tipos de problemas aqui evidenciados, a limitação da obtenção e do processamento de dados pessoais de caráter sensível, bem como tem chamado a atenção para a utilização das ferramentas de governança dos algoritmos dispostas na LGPD, como a auditoria de decisões de máquina. No entanto, tal atividade, por si só, ainda não é suficiente para sanar a questão, haja vista que “em um cenário de interação com a *big data*, na qual todos os dados são potencialmente sensíveis, apenas assegurar uma “neutralidade algorítmica” e um controle *a posteriori* algoritmo não é o bastante para mitigar a ocorrência das discriminações”.⁴⁷

Requião e Costa, nesse cenário, destacam:

Segundo a doutrina especializada, para resolver o problema da opacidade é preciso seguir à risca o princípio da transparência, visualizando através do direito à explicação das decisões algorítmicas. Com esteio em tal princípio, é preciso ter certeza que todas as etapas do algoritmo possam ser explicadas de maneira que um indivíduo não especializado possa entender. Além disso, os criadores de algoritmos devem sempre manter a capacidade de fornecer transparência em relação a todo o processo algorítmico envolvido e explicações para as decisões e resultados atingidos.⁴⁸

No entanto, apenas esta solução não se mostra suficiente, pois a discussão não está restrita ao princípio da não discriminação, transparência e explicação, em razão da alta complexidade e autonomia de que as IAs são dotadas.⁴⁹

Dessa forma, Wimer e Doneda ponderam a necessidade de participação humana na tomada de decisão de máquinas, especialmente, pelo fato de que

46. CHAVES JÚNIOR, Aírto; GUASQUE, Bárbara; DE PÁDUA, Thiago Santos Aguiar. Segregação racial e vidas algorítmicas: máquinas racistas no âmbito do controle penal. *Revista Brasileira de Direito*, v. 2, p. 20, 2023. Disponível em: <<https://seer.atitus.edu.br/index.php/revistadedireito/article/view/4768>>. Acesso em: 05 ago. 2024.

47. REQUIÃO, Maurício; COSTA, Diego. Discriminação algorítmica: ações afirmativas como estratégia de combate. *Civilistica.com*, v. 11, n. 3, p. 2-3, 2022. Disponível em: <<https://civilistica.emnuvens.com.br/redc/article/view/804/650>>. Acesso em: 24 jul. 2024.

48. REQUIÃO, Maurício; COSTA, Diego. Discriminação algorítmica: ações afirmativas como estratégia de combate. *Civilistica.com*, v. 11, n. 3, p. 6, 2022. Disponível em: <<https://civilistica.emnuvens.com.br/redc/article/view/804/650>>. Acesso em: 24 jul. 2024.

49. REQUIÃO, Maurício; COSTA, Diego. Discriminação algorítmica: ações afirmativas como estratégia de combate. *Civilistica.com*, v. 11, n. 3, p. 6-7, 2022. Disponível em: <<https://civilistica.emnuvens.com.br/redc/article/view/804/650>>. Acesso em: 24 jul. 2024.

muitos dos equívocos por elas cometidos ocorrem devido à ausência de uma compreensão crítica quanto à situação avaliada.⁵⁰

Evidencia-se, portanto, a importância em se ter interferência humana, tendo em vista a presença de algoritmos discriminatórios em ferramentas de IA. Contudo, não se pode desconsiderar que os dados inseridos nos sistemas são reflexo da sociedade. Assim, no que se refere, especificamente, ao direito penal, não se demonstra, por ora, coeso, o uso da inteligência artificial até que haja uma regulamentação efetiva, na medida em que representa risco sistêmico à dignidade da pessoa humana.

Considerações finais

Posteriormente à análise da literatura com a observância, inclusive, de casos concretos, concluiu-se pela existência de alarmante risco na utilização de inteligência artificial na prática cotidiana no direito penal, que já é, *per se*, dotada de seletividade, estigmas e preconceitos.

Em outras palavras, a utilização de inteligência artificial no ramo do direito criminal se mostra extremamente arriscada, em razão das evidências quanto ao viés discriminatório que a tecnologia pode assumir e as consequências do seu modelo de generalização. Tais ações contribuem para reforçar estigmas sociais e perpetuar injustiças relacionadas à criminalização de pessoas negras e de baixa renda.

Nesse sentido, constata-se como precoce a utilização da IA no âmbito penal, tanto pelos riscos discriminatórios do algoritmo, quanto pelas margens de erro que a tecnologia oferece, assim como entende-se correto o desincentivo ao uso de sistemas automatizados no âmbito do direito penal pela Resolução nº 332 do CNJ, que ressalta a sensibilidade do tema e os riscos às pessoas.

Ficou evidente, ainda, que, caso haja o seu uso, percebe-se a necessidade da participação humana em fases de tomada de decisão, sem que haja deliberações autônomas por parte dessas tecnologias, especialmente, quando houver algum impacto sobre direitos fundamentais individuais e coletivos. Essa interferência justifica-se sob o pretexto de se assegurar o cumprimento de limites éticos.

Por fim, após o estudo, demonstra-se relevante a importância de uma base educacional de formação com temas como o racismo estrutural, criminologia,

50. WIMMER, Miriam e DONEDA, Danilo. “Falhas de IA” e a Intervenção Humana em Decisões Automatizadas: Parâmetros para a Legitimação pela Humanização, *Revista de Direito Público*, Brasília, Vol. 18, n. 100, p. 382, out./dez. 2021.

dentre outros, direcionada aos desenvolvedores dos programas de inteligência artificial para que interrompam o reflexo racista da sociedade.

Assim, a tecnologia poderá ser desenvolvida levando-se em consideração a ética, a dignidade da pessoa humana e todos os demais direitos fundamentais garantidos constitucionalmente. Isso representaria uma abordagem preventiva com protocolo de segurança já no início do desenvolvimento das tecnologias e evitaria problemas durante o uso.

Referências

BATISTA, Vera Malaguti. *Introdução crítica à criminologia brasileira*. 2ª edição. Rio de Janeiro: Revan, 2012.

BECKER, Howard. *Outsiders*. Tradução Maria Luiza X. de Borges; revisão técnica Karina Kuschnir. Rio de Janeiro: Zahar, 2008.

BEZERRA, Arthur Coelho; COSTA, Camila Mattos. Pele negra, algoritmos brancos: informações e racismo nas redes sociotécnicas. *Liinc em Revista*, Rio de Janeiro, v. 18, n. 2, e6043, nov. 2022.

BICHARA, Anderson Andrade; CASCARDI JR, Agostinho Gomes; PERAZZONI, Franco. Racismo algorítmico, reforço de preconceitos e uso de IA: perspectivas e desafios para a investigação criminal digital. *Boletim IBCCRIM*, v. 32, n. 379, p. 23-26, 2024.

BRASIL. Ministério da Ciência, Tecnologia e Inovação. *Inteligência Artificial*. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial>. Acesso em: 29 jul. 2024.

_____. Conselho Nacional de Justiça. *Resolução n. 332, de 21 de agosto de 2020*. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3429>. Acesso em: 29 jul. 2024.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). *Minuta de proposta da resolução 332*. Brasília: CNJ, 2024. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2024/09/minuta-proposta-resolucao-332-cnj-rev.pdf>. Acesso em: 13 out. 2024.

_____. Presidência da República. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 31 jul. 2024.

_____. Senado Federal. *Projeto de Lei nº 2338, de 2023*. Dispõe sobre o uso da Inteligência Artificial. Brasília, DF: Senado Federal, 2023. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 31 jul. 2024.

CHAVES JÚNIOR, Airto; GUASQUE, Bárbara; DE PÁDUA, Thiago Santos Aguiar. Segregação racial e vidas algorítmicas: máquinas racistas no âmbito do controle penal. *Revista Brasileira de Direito*, v. 2, p. 4768, 2023. Disponível em: <https://seer.atitus.edu.br/index.php/revistadedireito/article/view/4768>. Acesso em: 05 ago. 2024.

FIA – Fundação Instituto de Administração. *ChatGPT: o que é, como funciona e como usar a ferramenta*. Disponível em: <https://fia.com.br/blog/chat-gpt/>. Acesso em: 25 jul. 2024.

GASPAR, Walter Britto; MENDONÇA, Yasmin Curzi de. A Inteligência Artificial no Brasil ainda precisa de uma estratégia. *Fundação Getúlio Vargas*, Rio de Janeiro, 2021. Disponível em: <https://diretorio.fgv.br/sites/default/files/2022-08/ebia-pt-br.pdf>. Acesso em: 27 jul. 2024.

MOURÃO, Licurgo. Regulação da inteligência artificial no Brasil. *Intellegentiae artificialis, imperium et civitatem*, p. 73-89, 2022. Disponível em: <https://idus.us.es/bitstream/handle/11441/146766/1/eBook%20Intellegentiae%20Artificialis%20Imperium%20et%20Civitatem.pdf?sequence=1#page=74>. Acesso em: 27 jul. 2024.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. *Direito Público*, v. 16, n. 90, 2019. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766>. Acesso em: 24 jul. 2024.

MAIA FILHO, Mamede Said; JUNQUILHO, Tainá Aguiar. Projeto Victor: perspectivas de aplicação da inteligência artificial ao direito. *Revista de Direitos e Garantias Fundamentais*, v. 19, n. 3, p. 218-237, 2018.

PARENTONI, Leonardo Netto; VALENTINI, Rômulo Soares; ALVES, Tárík César Oliveira E. Panorama da Regulação da Inteligência Artificial no Brasil: com ênfase no PL's N. 5.051/2019. *Revista Eletrônica do Curso de Direito da UFSM*, v. 15, n. 2, 2020.

PEIXOTO, Fabiano Hartmann. Projeto Victor: relato do desenvolvimento da inteligência artificial na repercussão geral do Supremo Tribunal Federal. *Revista Brasileira de Inteligência Artificial e Direito-RBIAD*, v. 1, n. 1, p. 1-22, 2020. Disponível em: <https://www.rbiad.com.br/index.php/rbiad/article/view/4/4>. Acesso em: 25 jul. 2024.

PILÓ, Xenofontes Curvelo; BRASIL, Deilton Ribeiro. A utilização da inteligência artificial no direito penal e seus reflexos nas garantias e direitos fundamentais. *Revista EJEF*, n. 1, p. 269-299, 2022.

REQUIÃO, Maurício; COSTA, Diego. Discriminação algorítmica: ações afirmativas como estratégia de combate. *Civilistica.com*, v. 11, n. 3, p. 1-24, 2022. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/804/650>. Acesso em: 24 jul. 2024.

SANTOS, Adriane de Almeida; TORRES, Marck de Souza; CELESTINO, Victor. Discriminação algorítmica e o acirramento do racismo estrutural: revisão de escopo. *Revista Científica Integrada*, v. 7, n. 1, p. e202415-e202415, 2024. Disponível em: <https://revistas.unaerp.br/rci/article/view/3233/2422>. Acesso em: 24 jul. 2024.

SENAPEN – Secretaria Nacional de Políticas Penais. *Sistema Nacional de Informações Penais*. 15º Ciclo SISDEPEN. Período Julho a Dezembro de 2023. Relatório de Informações Penais. Brasília, 2024. Disponível em: <https://www.gov.br/senappen/pt-br/servicos/sisdepen/relatorios>. Acesso em: 03 jul. 2024.

SILVA, Luisa Cypriano Moreira da. *Sistema carcerário brasileiro: uma análise do perfil dos presos a partir das teorias da seletividade penal e do etiquetamento social*. 2019. Universidade Federal de Ouro Preto. Departamento de Direito. Monografia. Disponível em: https://monografias.ufop.br/bitstream/35400000/2399/7/MONOGRAFIA_SistemaCarcer%c3%a1rioBrasileiro.pdf. Acesso em: 29 jul. 2024.

STEFFEN, Catiane. A inteligência artificial e o processo penal: a utilização da técnica na violação de direitos. *Revista da EMERJ*, v. 25, n. 1, p. 105-129, 2023.

WEBSTER, Frank. *Theories of the information society*. Londres: Routledge, 1995.

WIMMER, Miriam e DONEDA, Danilo. “Falhas de IA” e a Intervenção Humana em Decisões Automatizadas: Parâmetros para a Legitimação pela Humanização, *Revista de Direito Público*, Brasília, Vol. 18, n. 100, p. 374-406, out./dez. 2021.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

10

Entre Cérebro e Computador: Diálogos sobre Neurodireitos e Inteligência Artificial

HENRIQUE SEGOLIN MOLINA

Sumário: Introdução; 1. Como as neurotecnologias e a IA estão influenciando a criação de novos direitos; 2. Caminhos e propostas para efetivação dos Neurodireitos; 2.1. Análise de leis e normativas ao redor do mundo; 2.3. O Caso Chileno: Girardi vs Emotiv Inc.; Considerações Finais; Referências Bibliográficas

Introdução

O cérebro humano é diferente de qualquer outro órgão, visto que gera todas as nossas atividades mentais e cognitivas, de tal maneira que podemos considerá-lo como o computador mais complexo e poderoso do mundo.²

A busca por novas formas de entender e ampliar os limites de nossas capacidades mentais tem sido objeto de pesquisa e desenvolvimento, há algumas décadas, e encontra-se no epicentro do campo da Neurociência e tecnologias invasivas, permitindo que máquinas interajam, diretamente, com regiões do cérebro.

Em 1924, Hans Berger realizou o primeiro eletroencefalograma (EEG) em seres humanos, um feito que representou uma verdadeira revolução para a época. Com a utilização de eletrodos de prata e um galvanômetro, Berger conseguiu capturar e registrar as primeiras ondas cerebrais, agora conhecidas como ondas alfa e beta. Esse momento histórico não apenas comprovou a viabilidade de registrar e analisar a atividade elétrica do cérebro humano, mas também deu início a um novo e promissor campo de pesquisa científica.

Mais adiante, a invenção dos implantes cocleares, em 1957, foi um ponto crucial no desenvolvimento das neurotecnologias com o intuito de controlar dispositivos elétricos, como lâmpadas, usando eletrodos que podem medir e reagir a sinais cerebrais, consistindo no que chamamos hoje de Interfaces Cérebro-Computador (BCIs).³

Normalmente, quando se quer interagir com algum objeto em nosso ambiente, nosso sistema nervoso passa por diversas etapas neurológicas prévias ao envio de impulsos nervosos, os quais, conseqüentemente, permitirão que determinada interação ocorra. As BCIs, por seu turno, encurtam esse cami-

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.

2. MARR, B. *AI's next frontier: are brain-computer interfaces the future of communication?* Forbes Innovation, 2023. Disponível em: <https://www.forbes.com/sites/bernardmarr/2023/08/11/ais-next-frontier-are-brain-computer-interfaces-the-future-of-communication/>. Acesso em: 10 jun 2024.

3. LOTTE, F. NAM, C. S. *Introduction: Evolution of Brain-Computer Interfaces*. Hal Open Science: Brain-Computer Interfaces Handbook: Technological and Theoretical Advance, Taylor & Francis (CRC Press), p.1-11, 2018. Disponível em: <https://inria.hal.science/hal-01656743/document>. Acesso em: 10 jun.2024.

nho, uma vez que se utilizam de softwares e tecnologias que identificam a ação pretendida e a executam de prontidão e, por essa razão, têm aplicações potenciais em diversos campos.

Sobre o tema, em meados de 2017, o neurocientista brasileiro Miguel Nicolelis, expressava uma visão otimista e provocadora sobre o potencial das BCIs para transformar não apenas a medicina, mas também a maneira como interagimos com o mundo ao nosso redor:

Nas próximas décadas, ao combinar essa visão relativística do cérebro com nossa crescente capacidade tecnológica de ouvir e decodificar sinfonias neurais cada vez mais complexas, a neurociência acabará expandindo a limites quase inimagináveis a capacidade humana, que passará a se expressar muito além das fronteiras e limitações impostas tanto por nosso frágil corpo de primatas como por nosso senso de eu [...] Surpreendentemente as futuras aplicações de BCIS prometem avançar muito além dos limites da medicina. Em algumas gerações, seu desenvolvimento tecnológico capacitará nossos descendentes a realizar ações e experimentar sensações que poucos serão capazes de imaginar uma maneira de verbalizar hoje em dia. As BCIS podem transformar a maneira como interagimos com as ferramentas que fabricamos para dialogar com o mundo que nos cerca, a forma como nos comunicamos uns com os outros, bem com a nossa interação com o ambiente distante e outros mundos. Para compreender o que esse futuro pode representar, você precisaria primeiro imaginar como nossa vida mudaria dramaticamente, caso algumas de nossas tarefas mais rotineiras pudessem ser executadas diretamente sob o controle de nossa atividade elétrica cerebral disseminada livremente pelo ar da mesma forma que ondas de rádio navegam hoje em dia [...] A perspectiva dessa maravilhosa alforria, que hoje ainda pode soar para alguns como magia, milagre ou alquimia, não mais pertence ao domínio da ficção científica. Esse mundo do futuro está começando a se delinear, diante de nossos olhos, aqui e agora. (g.n)⁴

No tempo presente, podemos dizer que estamos na “segunda era da máquina”⁵, na qual as novas descobertas ocorrem, simultaneamente, nas mais diversas áreas, em uma completa fusão entre a tecnologia mais avançada e os domínios físicos, digitais, biológicos⁶ e neurocientíficos.

4. NICOLELIS, M. *Muito além do nosso eu: a nova neurociência que une cérebro e máquinas – e como ela pode mudar nossas vidas*. 1. ed. São Paulo: Planeta, 2017. 25-28 p.

5. MCAFEE, A. BRYNJOLFSSON, E. *A segunda era das máquinas*. Rio de Janeiro: Alta Books, 2014.

6. SCHWAB, K. *A quarta revolução industrial* – São Paulo: Edipro, 2016. 115 p.

Note-se que, ao mencionar que as futuras aplicações de tais ferramentas poderiam ir além das fronteiras da medicina, Nicolelis pressentiu que essas tecnologias abririam portas para experiências e ações que, à época, seriam difíceis de conceber, mas, atualmente, já se mostram capazes, muito em função da integração da Inteligência Artificial (IA) neste campo⁷, devido à capacidade algorítmica de analisar grandes quantidades de dados e identificar padrões subjacentes, aprimorando, assim, a precisão e eficiência das BCIs na interpretação dos dados neurais.⁸

Essa incorporação propiciou o crescimento de conjuntos de dados de grande escala e alta qualidade, contribuindo para a expansão das aplicações das interfaces-cérebro-máquina, as quais, agora, além de auxiliarem pessoas com deficiência, também, melhoram capacidades humanas, ao ampliar nossa compreensão sobre o funcionamento complexo do cérebro, assim como ao promover o surgimento de novos mercados.

Um dos *players* mais conhecidos neste cenário é a *Neuralink*, alvo de notícias ao redor do globo, em função de seu estágio avançado, considerando que, em 28 de janeiro de 2024, a empresa realizou, com sucesso seu primeiro implante cerebral, fazendo com que um homem chamado Noland Arbaugh, depois de viver com paralisia por oito anos, reconquistasse a capacidade de realizar tarefas que, para ele, eram inacessíveis⁹

Outra companhia que está trazendo produtos para o mercado nesse espaço é a *NextMind*. Além de criar ferramentas que permitem controlar computadores com sinais cerebrais, a empresa espera criar um dispositivo que possa traduzir a imaginação visual em sinais digitais; ou seja, qualquer imagem que você imaginar será recriada em uma tela de computador – algo parecido com o modelo de geração de imagens, usado por aplicações de IA incluindo DALL-E e Midjourney.¹⁰

Entretanto, embora haja grande entusiasmo com os avanços das BCIs, à medida que essas tecnologias continuam a amadurecer, surgem questões associadas ao seu desenvolvimento e uso ético e responsável. Tais questões precisam ser abordadas, para que sua aplicação melhore vidas, sem causar danos não antecipados e, potencialmente, graves, considerando, inclusive, que

7. KUMAR, B. Integration of AI and Neuroscience for Advancing Brain-Machine Interfaces: A Study. *International Journal of New Media Studies (IJNMS)*, Volume 9 Issue 1, January-June, 2022. Disponível em: https://www.researchgate.net/profile/BharathKumarNagaraj/publication/380785142_Integration_of_AI_and_Neuroscience_for_Advancing_Brain-Machine_Interfaces_A_Study/links/664e2edfbc86444c72f79492/Integration-of-AI-and-Neuroscience-for-Advancing-Brain-Machine-Interfaces-A-Study.pdf. Acesso em: 11 jun.2024.

8. KAWALASTE-STERNIUK, A. BROWASKA, N. Summary of over Fifty Years with Brain-Computer Interfaces-A Review. *Brain Sciences* 2021 Jan 3;11(1):43. doi: 10.3390/brainsci11010043. PMID: 33401571; PMCID: PMC7824107. Disponível em: <https://doi.org/10.3390/brainsci11010043>. Acesso em: 11 jun.2024.

9. DREW, L. *Elon Musk's Neuralink brain chip: what scientists think of firts human trial*. *Nature*, 2024. Disponível em: <https://www.nature.com/articles/d41586-024-00304-4>. Acesso em: 11 jun. 2024.

10. AR - SNAP AR. *Welcome Nextmind*. Disponível em: <https://ar.snap.com/welcome-nextmind>. Acesso em: 11 jun. 2024

muitas das ameaças associadas às BCIs já se manifestam na forma como os dados neurais são explorados pelas empresas de tecnologia, no dia a dia.¹¹

De acordo com Adrian Carter, a utilização de ferramentas de Inteligência Artificial e algoritmos, que interpretam movimentos oculares e detectam mudanças na cor e temperatura da pele, já estão sendo empregados para ler os resultados da atividade cerebral e, a partir daí, prever e influenciar comportamentos, fazendo com que certas empresas lucrem bilhões com a utilização desses dados.¹²

Além disso, os dados neurais provenientes dessas atividades são, por sua própria natureza, informações de extrema sensibilidade, uma vez que têm a capacidade de revelar elementos muito íntimos sobre os consumidores.

A esse respeito, em recentíssimo estudo, realizado por Jared Genser, Stephen Damianos, e Rafael Yuste, os autores apontaram que uma das preocupações mais prementes desses avanços é a mineração de dados neurais para fins comerciais, visto que, de acordo com eles, à medida que os consumidores utilizam, cada vez mais, dispositivos de neurotecnologia, as empresas estão construindo bancos de dados maiores de imagens cerebrais e outros dados neurais, os quais, assim como o material genético e as impressões digitais, poderão levar à identificação imediata dos indivíduos.

Ainda, segundo o estudo, os avanços na IA estão aumentando, rapidamente, a capacidade de decodificar informações, de modo a fornecer às empresas níveis sem precedentes de percepção sobre os estados cognitivos e os mundos internos dos consumidores, bem como ajudar a prever traços de personalidade, vícios, saúde mental e vários distúrbios¹³.

Desta forma, não é difícil imaginar como esses dados poderão ser mal utilizados pelas corporações, o que, por sua vez, impõe desafios complexos, em especial no que se refere ao desenvolvimento dessas ferramentas e na proteção da privacidade, autonomia do usuário – especialmente, onde os usuários têm controle limitado sobre as interfaces cérebro-máquina implantadas e os dados que produzem – e desafios de segurança de dados e dispositivos.

Diante de tal cenário, antevendo a crescente capacidade da Neurociência e da neurotecnologia de acessar e influenciar os processos mentais humanos, Marcello Ienca e Roberto Andorno apontaram a necessidade de determinar

11. GENSER, J., DAMIANOS, S., YUSTE, R. *Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies*. Neurorights Foundation, 2024. Disponível em: https://www.perseus-strategies.com/wp-content/uploads/2024/04/FINAL_Consumer_Neurotechnology_Report_Neurorights_Foundation_April-1.pdf. Acesso em: 12. Jul. 2024.

12. WILD, K. 'Our notion of privacy will be useless': what happens if technology learns to read our minds? *The Guardian*, 2021. Disponível em: <https://www.theguardian.com/technology/2021/nov/07/our-notion-of-privacy-will-be-useless-what-happens-if-technology-learns-to-read-our-minds>. Acesso em: 17 jun.2024.

13. GENSER, J., DAMIANOS, S., YUSTE, R. *Op cit*; 17-18 p.

quais direitos os indivíduos devem exercer em relação à sua própria dimensão mental, de modo a proteger a integridade, privacidade e autonomia, bem como a garantir que as pessoas tenham controle sobre seus próprios pensamentos, memórias e decisões, além de serem protegidas contra possíveis abusos ou manipulações, advindas desses avanços. Em particular, eles defenderam a criação de novos direitos humanos, aos quais chamaram de “Neurodireitos”¹⁴.

Assim, considerando que as interfaces cérebro-computador representam avanços tecnológicos que, apesar de, potencialmente, transformadores de maneira positiva, já enfrentam obstáculos não técnicos que podem limitar seu uso – se não houver uma compreensão ampla e sofisticada de como desenvolvê-las – o presente artigo tem por objetivo analisar os desafios éticos e regulatórios dos avanços decorrentes da intersecção entre BCIs e IA, focando: (i) na necessidade premente de consentimento; e (ii) na salvaguarda dos Neurodireitos dos indivíduos, diante do tratamento de dados neurais.

Para alcançar esse objetivo, entre os métodos científicos tradicionais, a metodologia adotada será a hipotético-dedutiva. Já no campo jurídico, por sua vez, o estudo empregará os métodos hermenêutico, empírico e argumentativo, além de adotar uma abordagem crítico-metodológica. Essas dimensões abarcarão uma pesquisa descritiva, com análise reflexiva da produção acadêmica e doutrinária sobre os temas abordados, bem como uma análise minuciosa das normativas e propostas aplicáveis, se houver.

1. Como as Neurotecnologias e a IA estão influenciando a criação de novos direitos?

Para iniciar, cita-se o relatório da Organização Mundial da Saúde (OMS), segundo o qual uma a cada seis pessoas, aproximadamente 16% da população global, enfrenta algum tipo de incapacidade significativa.¹⁵ No Brasil, a população com deficiência foi estimada em 18,6 milhões de pessoas, e os dados da pesquisa mostram, também, que estes indivíduos estão menos inseridos no mercado de trabalho e nas escolas – e, por consequência, têm o acesso à renda mais dificultado.¹⁶

14. IENCA, M.. ANDORNO, R.. *A new category of human rights: neurorights*. BMC, 2017. Disponível em: <https://blogs.biomed-central.com/bmcblog/2017/04/26/new-category-human-rights-neurorights/>. Acesso em 15 jul. 2024.

15. WHO - World Health Organization. *Global report on health equity for persons with disabilities*. Geneva: WHO, 2022. Disponível em: <https://www.who.int/publications/i/item/9789240063600> Acesso em 31 de Jul de 2024.

16. BRASIL, Ministério dos Direitos Humanos e da Cidadania. *Brasil tem 18,6 milhões de pessoas com deficiência, indica pesquisa divulgada pelo IBGE e MDHC*. Gov.br, 2023. Disponível em: <https://www.gov.br/mdh/pt-br/assuntos/noticias/2023/julho/brasil-tem-18-6-milhoes-de-pessoas-com-deficiencia-indica-pesquisa-divulgada-pelo-ibge-e-mdhc>. Acesso em 31 de Jul de 2024.

A despeito de já existirem várias técnicas de neurotecnologia aplicadas na vida cotidiana, como o eletroencefalograma, a ressonância magnética funcional, bem como técnicas para estimular o cérebro, a fim de mitigar sintomas de doenças, como Parkinson ou epilepsia, as inovações mais interessantes e polêmicas têm surgido em sua relação com as tecnologias cognitivas.

A interação entre as BCIs e os dados obtidos sobre as funções cerebrais por meio de aprendizado de máquina (*machine learning*) e aprendizado profundo (*deep learning*), bem como o processamento de linguagem natural são utilizados para gerar o que se chama de “redes neurais artificiais”, que estão transformando, radicalmente, as aplicações de IA.

Com a ajuda de uma interface cérebro-computador, uma pessoa pode controlar e operar dispositivos eletrônicos externos, apenas com os pensamentos, comunicando-se por meio de fala sintetizada, movendo membros protéticos, operando um computador e desempenhando outras funções importantes, que melhoram a qualidade de vida de pessoas com deficiências.¹⁷

Nesta conjuntura, como bem observam Rafael Yuste e Sara Goering:

Os avanços tecnológicos indicam que estamos caminhando para um mundo em que será possível decodificar os processos mentais das pessoas e manipular diretamente os mecanismos cerebrais subjacentes às suas intenções, emoções e decisões; onde os indivíduos poderiam se comunicar com os outros, simplesmente pensando; e onde sistemas computacionais poderosos ligados diretamente aos cérebros das pessoas auxiliariam suas interações com o mundo de tal forma que suas habilidades mentais e físicas seriam enormemente aprimoradas [...] Tais avanços poderiam revolucionar o tratamento de muitas condições, desde lesões cerebrais e paralisia até epilepsia e esquizofrenia, e transformar a experiência humana para melhor. Mas a tecnologia também poderia exacerbar as desigualdades sociais e oferecer a corporações, hackers, governos ou qualquer outra pessoa novas formas de explorar e manipular as pessoas. E poderia alterar profundamente algumas características humanas fundamentais: a vida mental privada, a autonomia individual e a compreensão dos indivíduos como entidades limitadas por seus corpos (g.n)¹⁸

17. ZHANG, X. MA, Z. ZHENG, H. et al. The combination of brain-computer interfaces and artificial intelligence: applications and challenges. *Ann Transl Med.* 2020 Jun;8(11):712. doi: 10.21037/atm.2019.11.109. PMID: 32617332; PMCID: PMC7327323. Disponível em: <https://doi.org/10.21037/atm.2019.11.109>. Acesso em: 18 jun. 2024.

18. YUSTE, R. GOERING, S. et al. *Four ethical priorities for neurotechnologies and AI.* Nature. 2017. Disponível em: <https://www.nature.com/articles/551159a>. Acesso em: 18 jun. 2024.

O mercado global de BCIs, atualmente, avaliado em, aproximadamente, US\$ 1,2 bilhões, demonstra um avanço impressionante, com uma taxa de crescimento anual composta, projetada de 13-15% até 2030¹⁹. No entanto, a rápida expansão deste setor levanta preocupações significativas relacionadas à privacidade e à segurança dos dados neurais, pois, de um lado, não se pode descartar o fato de que nossos dados pessoais já são tratados em larga escala e de que os agentes supramencionados pelos autores já traçam um perfil individual de cada pessoa. De outro, que a motivação de geração de riquezas viabiliza a ocorrência de diversos malefícios aos aspectos sociais e mentais da população, influenciando-a, sem que consiga, ao menos, perceber que está sendo manipulada.

Diante deste cenário, surge a necessidade de abordarmos aquilo que os eticistas denominaram como Neurodireitos, isto é, as regras normativas fundamentais para a proteção e preservação do cérebro e da mente humana²⁰, levando em consideração que a ausência de regulamentações claras pode levar a abusos, exacerbando desigualdades sociais e comprometendo a integridade mental dos indivíduos.

Portanto, é imperativo que formas de regular tais direitos sejam desenvolvidas, para garantir que os benefícios das BCIs sejam aproveitados de maneira ética e justa.²¹

2. Caminhos e propostas para a efetivação dos Neurodireitos

Apresentados tais aspectos, visto que a maioria das leis de privacidade existentes não trata, de forma explícita, acerca dos dados neurais e, tampouco, dos Neurodireitos, recorre-se, então, a uma análise comparada da legislação e demais frameworks sobre o tema, a fim de estabelecer salvaguardas legais para o cérebro e para o tratamento de tais dados.

Desta forma, o subcapítulo a seguir se prestará a realizar um *overview* dos esforços legislativos ao redor do mundo, em especial na União Europeia, Amé-

19. GRAND VIEW RESEARCH. *Brain Computer Interface Market Size, Share & Trends Analysis Report By Application (Healthcare, Communication & Control), By Product (Invasive, Non-invasive), By End Use (Medical, Military), And Segment Forecasts, 2023 - 2030*. Report ID: 978-1-68038-459-8 Disponível em: <https://www.grandviewresearch.com/industry-analysis/brain-computer-interfaces-market>. Acesso em 19 Jun de 2024.

20. IENCA, M. ANDORNO, R. *A new category of human rights: neurorights*. BMC, 2017. Disponível em: <https://blogs.biomed-central.com/bmcblog/2017/04/26/new-category-human-rights-neurorights/>. Acesso em: 20 Jun. 2024.

21. RODRÍGUEZ, J. *Inteligencia artificial y neuroderechos. Retos y perspectivas*. *Cuestiones Constitucionales, Revista Mexicana de Derecho Constitucional*, Núm. 46, Enero-Junio 2022 ISSN (versión electrónica): 2448-4881. Disponível em: <https://www.scielo.org.mx/pdf/cconst/n46/1405-9193-cconst-46-93.pdf>. Acesso em: 26 jul. 2024.

rica Latina e nos Estados Unidos, a fim de reconhecer trejeitos comuns acerca dos desafios de proteção para a privacidade mental na era da neurotecnologia.

2.1 Análise de leis e normativas ao redor do mundo

Na maioria das vezes, ao discutir-se inovação, proteção de dados e novas tecnologias, percebe-se a União Europeia (UE) como uma precursora na normatização global, destacando-se em um cenário carente de regulação e repleto de potenciais e irreparáveis prejuízos, devido à velocidade do desenvolvimento tecnológico.

Essa postura da UE não é novidade. Ao se posicionar como referência mundial, esse grupo econômico visa impulsionar outras nações a ampliar o debate, a acelerar suas propostas legislativas e diretrizes relacionadas a sistemas de BCI e IA artificial, e a planejar o desenvolvimento tecnológico de forma ética, a fim de conquistar espaço nos debates mundo afora.

A título elucidativo, podem-se relembrar as regulações precursoras de dados pessoais, primeiro, com a Diretiva 95/46 e, posteriormente, com o *General Data Protection Regulation* (GDPR), que, inclusive, serviu de base para a criação da Lei Geral de Proteção de Dados (LGPD), no Brasil e, mais, recentemente, o *AI Act*, a nova legislação europeia para a regulação de IA.

Na discussão sobre BCIs, Neurodireitos e dados neurais, por sua vez, a UE figura, tão somente, como precursora acadêmica, visto que os debates ainda se encontram na alçada da Rede Europeia de Neuroética, que congrega uma ampla gama de atores, incluindo pesquisadores renomados, tais como Rafael Yuste, Adrian Owen, e Emmanuelle Charpentier.

Um marco significativo nesse contexto foi o *Human Brain Project* (HBP), um projeto ambicioso, lançado em 2013, com o objetivo de aprofundar a compreensão do cérebro humano e impulsionar o desenvolvimento de neurotecnologias. Ativo por 10 anos, o projeto gerou mais de 3.000 publicações acadêmicas, desenvolveu mais de 160 ferramentas digitais, aplicações médicas e tecnológicas, e criou a infraestrutura de pesquisa aberta *EBRAINS*. Além disso, impulsionou avanços significativos na pesquisa cerebral e no desenvolvimento de tecnologias médicas, como medicina personalizada para o cérebro e novas tecnologias inspiradas no cérebro, incluindo ferramentas de IA e computação neuromórfica.²²

22. HBP - HUMAN BRAIN PROJECT. *The Human Brain Project ends: What has been achieved*. Human Brain Project, Press release, 2023. Disponível em: <https://www.humanbrainproject.eu/en/follow-hbp/news/2023/09/28/human-brain-project-ends-what-has-been-achieved/>. Acesso em: 22 Jul. 2024.

Outro destaque, na Europa, é o “Plano de Ação Estratégica” do Conselho da Europa, que foca em direitos humanos e novas tecnologias biomédicas, incluindo as recentes mudanças na neurotecnologia.

Contrariando a regra, no quesito de incorporação desses conceitos aos regramentos jurídicos, o destaque é Latino-Americano, em especial, pelo fato do Chile ter se tornado referência no tema, sendo o primeiro país no mundo a incorporá-los em sua Constituição, ao aprovar uma emenda constitucional, através da Ley 21.383²³, que modificou o artigo 19, para proteger a atividade cerebral e as informações associadas, e enfatizando a necessidade de se balancear a integridade física e mental com os avanços das neurotecnologias.

Outro arco crucial no cenário Latino-Americano²⁴ foi a aprovação da Declaração Interamericana de Princípios sobre Neurociências, Neurotecnologias e Direitos Humanos²⁵, pela Organização dos Estados Americanos (OEA), em meados de 2023, demonstrando um compromisso regional com a proteção dos direitos individuais, em face dos avanços da ciência cerebral.

Seguindo estes exemplos, outros países como Costa Rica, Colômbia, Argentina, Uruguai, Peru, México e Brasil, também, caminham para regular as neurotecnologias e fornecer salvaguardas para a integridade cerebral e para os dados neurais, estando os últimos em um estágio regulatório mais avançado, considerando que, até a data em que se tecem estas considerações, foram constatados dois projetos de lei, referentes à “neuro privacidade”, em tramitação no México, e diversas propostas no âmbito brasileiro. Vide o quadro a seguir:

23. STRICKLAND, E. *Worldwide campaign for neurorights notches its first win*. IEE Spectrum, 2021. Disponível em: <https://spectrum.ieee.org/neurotech-neurorights>. Acesso em: 22 Jul. 2024

24. DO, B. SPIVACK, J. BADILO, M. *Privacy and the rise of “neurorights” in Latin America*. Future of Privacy Forum, 2024. Disponível em: <https://fpf.org/blog/privacy-and-the-rise-of-neurorights-in-latin-america/>. Acesso em: 23 jul. 2024.

25 OEA - ORGANIZAÇÃO DOS ESTADOS AMERICANOS. *Declaração Interamericana de Princípios sobre Neurociências, Neurotecnologias e Direitos Humanos*. Disponível em: https://www.oas.org/es/sla/cji/temas_culminados_recientemente_Neurociencias_Neurotecnologias_y_Derechos_Humanos.asp. Acesso em: 23 jul. 2024.

Quadro 01 –Regulação de Neurodireitos na América-Latina

País	Proposta/regulação	Principais pontos	Status atual	Fontes
Chile	Ley 21383	Modifica a Constituição para estabelecer balizas ao desenvolvimento científico e tecnológico, a serviço das pessoas, defendendo a integridade física e psicológica dos indivíduos, além de exigir o consentimento para o uso dessas ferramentas.	Em Vigor	Biblioteca del Congreso Nacional de Chile
México	Proposta pela Deputada María Eugenia Hernández Pérez	Assume redação idêntica à da emenda constitucional chilena.	Em discussão	Sistema de Información Legislativa
	Proposta pela Senadora Alejandra Lagunes Soto Ruiz	Emendar, o art. 73 da Constituição, de modo regular, de maneira unificada, a inteligência artificial, a cibersegurança e os Neurodireitos	Em Discussão	Senado de la República
Uruguai	Iniciativas legislativas baseadas no diálogo com especialistas e parlamentares chilenos	Regular os Neurodireitos	Em fase preliminar de discussão	Unesco
Argentina	Projeto de Lei 2446/23	Criar um comitê específico para desenvolver novas normativas acerca dos Neurodireitos	Em discussão	Senado de la nación Argentina
Costa Rica	Proposta de emenda à lei de proteção de dados	Categorizar os dados neurais como dados biométricos	Em discussão	Unesco
Colômbia	Proposta de emenda à lei de proteção de dados	Criar uma seção específica, com o intuito de estabelecer as balizas norteadoras do tratamento desses dados, por meio de IA e neurotecnologias	Em discussão.	Unesco

(continua)

Quadro 01 –Regulação de Neurodireitos na América-Latina

(continuação)

País	Proposta/regulação	Principais pontos	Status atual	Fontes
Peru	Projeto de Lei N° 5968/2023-CR (Carlos Javier Zeballos Madariaga)	Visa proteger os direitos fundamentais das pessoas, regulando o uso de provas neurocientíficas em processos judiciais.	Em análise na Comissão de Justiça e Direitos Humanos do Congresso do Peru desde setembro de 2023	<u>Congresso Peruano</u>
Brasil	PEC 298 de 2023 (Rio Grande do Sul)	Emendar a Constituição Estadual, com o intuito de incluir os Neurodireitos, elevando a integridade mental ao caráter de princípio constitucional.	Em vigor no Rio Grande do Sul.	<u>Assembleia Legislativa do Rio Grande do Sul</u>
	PEC n° 29/2023 (Senador Randolph Rodrigues)	Inclusão de normativas, voltadas à proteção da integridade mental e transparência algorítmica, sob o pretexto de que a integridade mental se encontra umbilicalmente atrelada à dignidade da pessoa humana, neste novo contexto social.	Parada no Senado, aguardando relator.	<u>Senado Federal</u>
	PL 2174/2023 (Rubens Pereira Júnior)	Estabelece as normas e princípios para proteção dos direitos fundamentais relacionados ao cérebro e ao sistema nervoso humano, objetivando garantir a proteção e promoção dos neurodireitos dos indivíduos.	Aguardando Designação de Relator(a) na Comissão de Constituição e Justiça e de Cidadania (CCJC)	<u>Câmara dos Deputados</u>
	PL 1229/2021 (Carlos Henrique Gaguim)	Modifica a Lei n° 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.	Retirado pelo Autor	<u>Câmara dos Deputados</u>

(continua)

Quadro 01 –Regulação de Neurodireitos na América-Latina

(continuação)

País	Proposta/regulação	Principais pontos	Status atual	Fontes
Brasil	PL 522/2022 (Carlos Henrique Gaguim)	Alteração da Lei Geral de Proteção de Dados Brasileira (LGPD), a fim de se reconhecerem os dados neurais como uma espécie de dados pessoais sensíveis.	Aprovado na CSAÚDE, em outubro de 2023 e teve a Dep. Adriana Ventura (NOVO-SP) designada como relatora em 10 de abril de 2024	<u>Câmara dos Deputados</u>
	Anteprojeto de atualização do Código Civil (2024)	Inserção dos Neurodireitos, no Código Civil.	Apresentado ao Senado, em análise.	<u>Senado Federal</u>

Fonte: elaborada pelo autor, a partir de fontes diversas de canais governamentais oficiais, 2024.

Por fim, nos Estados Unidos, os esforços para abordar os Neurodireitos são liderados por organizações acadêmicas, profissionais e órgãos consultivos governamentais. Destacam-se as contribuições de acadêmicos, como Martha J. Farah, Hank Greely, cujo trabalho tem sido fundamental na discussão dessa temática.

Em abril, o estado do Colorado aprovou uma legislação promissora, destinada a proteger os consumidores de dispositivos que coletam dados de atividade cerebral, promovendo a defesa da integridade mental e a proteção dos dados neurais. Sobre o tema, a deputada estadual Cathy Kipp, do Partido Democrata do Colorado, destacou que, embora a tecnologia tenha potencial benéfico, “deveria haver salvaguardas para aqueles que não desejam ter seus pensamentos lidos e seus dados biológicos utilizados”.²⁶

Ainda, recentemente, a Califórnia alterou sua Lei de Privacidade do Consumidor da (CCPA), para incluir dados neurais como informações sensíveis, buscando proteger os dados gerados pela atividade cerebral de potenciais

26. MOENS, J. *Your Brain Waves Are Up for Sale. A New Law Wants to Change That.* New York Times, 2024. Disponível em: <https://www.nytimes.com/2024/04/17/science/colorado-brain-data-privacy.html>. Acesso em: 24 jun. 2024.

usos indevidos, permitindo que os usuários controlem, deletem ou limitem esses dados²⁷.

Ante o exposto, fica claro que, no geral, diversos países buscam formas para tratar dos Neurodireitos e da gestão de dados neurais, não com o intuito de proibir as novas tecnologias, mas sim de regulá-las de maneira a proteger os direitos dos indivíduos. Logo, o que essas medidas visam garantir é, justamente, promover um ambiente, no qual os avanços na Neurociência e neurotecnologia respeitem a autonomia cognitiva, a privacidade e a dignidade das pessoas.

2.2 O caso chileno: Girardi vs Emotiv Inc.

Como visto, até o momento, o Chile é o único país no mundo a englobar os Neurodireitos em seu ordenamento jurídico, conferindo-lhes, inclusive, caráter de direito fundamental, em um manifesto reconhecimento da relevância de se fornecer um quadro para enfrentar os desafios éticos e legais emergentes da neurotecnologia, com o intuito de moldar um ambiente, no qual a inovação possa prosperar sem comprometer os direitos à liberdade cognitiva, à privacidade mental, à integridade mental e à continuidade psicológica dos indivíduos.

Desta forma, esperava-se que o primeiro litígio judicial, a respeito dessa questão, também se desse no país. E foi, justamente, o que aconteceu, em agosto de 2023. À época, a Terceira Sala da Corte Suprema do Chile deparava-se com um caso emblemático, cujas minúcias e motivos de decidir representariam um marco, para muito além das suas fronteiras.²⁸

No caso em questão, o Sr. Guido Girardi Lavín ajuizou uma ação de proteção constitucional, em face da Emotiv Inc., uma empresa de bioinformática, com sede em São Francisco, Estados Unidos, que desenvolve e fabrica produtos portáteis de eletroencefalografia, junto com neuro-fones de ouvido, kits de desenvolvimento de software, software, aplicativos móveis e produtos de dados.

Na inicial, o autor aduzia ter adquirido um dispositivo chamado “*Insight*” – o qual funciona como uma faixa de cabeça com sensores que captam informações sobre a atividade elétrica do cérebro, obtendo dados sobre gestos, movimentos, preferências, tempos de reação e atividade cognitiva do usuário – e que em função disso, teria aceito os termos de serviço do software, que pre-

27. CANTER, L. BRIM, E. *California Enacts Health AI Bill and Protections for Neural Data*. Covington, 2024. Disponível em: <https://www.insideprivacy.com/uncategorized/california-enacts-health-ai-bill-and-protections-for-neural-data/>>. Acesso em: 16 out. 2024.

28. CORNEJO-PLAZA, M. I. CIPPITANI, R. PASQUINO, V. *Chilean Supreme Court ruling on the protection of brain activity: neurorights, personal data protection, and neurodata*. *Frontiers in Psychology*, 2024. Disponível em: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10929545/>. Acesso em: 25 jul. 2024.

viam o armazenamento de seus dados neurais pela empresa, de forma anonimizada, para fins de pesquisa científica.

No entanto, para a surpresa do autor, a Emotiv passou a utilizar seus dados para finalidades diversas e, em razão deste tratamento indevido, ele aduz ter sido exposto a riscos diversos, apontando violações ao disposto no artigo 11, da Lei N° 19.628, a respeito da devida diligência no cuidado de dados pessoais à qual estão obrigados os responsáveis por registros ou bases de dados pessoais, e o disposto no artigo 13, da mesma lei, sobre o direito das pessoas a cancelamento ou bloqueio de seus dados pessoais, uma vez que, mesmo com a conta de usuário encerrada, a empresa retinha suas informações cerebrais para fins de pesquisa científica e histórica.

Na peça de defesa, a Emotiv alegou que seu produto consiste em um dispositivo de neurotecnologia não invasiva, sem fins terapêuticos, de tipo eletroencefalograma móvel, projetado para auto-quantificação e pesquisa de campo, não sendo vendido como dispositivo médico; além disso, apontou que o produto e sua instalação contêm uma explicação detalhada dos termos e condições, na qual é solicitado consentimento expresso para o tratamento de dados pessoais e cerebrais, o que teria sido concedido pelo autor.

Em sede de Acórdão, a Corte manteve a sentença que decidiu em favor do autor, aditando-a, tão somente, para determinar, ao Instituto de Saúde Pública e à autoridade aduaneira, que garantam que a comercialização e o uso de dados do dispositivo Insight estejam em conformidade com os regulamentos vigentes, bem como confirmar o pleito de exclusão de quaisquer dados armazenados, relacionados ao uso do dispositivo pelo autor.

Na fundamentação, o Tribunal enfatizou a necessidade do consentimento informado, para o uso de informações em pesquisas, conforme exigido pela Lei n° 20.120 e referiu-se, especialmente, ao art. 19 da Constituição Política da República, que constitui um mandato direto de proteção aos Neurodireitos, além de citar acordos internacionais como o Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais (Artigo 15) e as declarações da UNESCO, enfatizando a busca pelo equilíbrio entre o progresso científico e suas aplicações aos direitos humanos. Em resumo, a Corte consolidou o entendimento de que:

Diante do desenvolvimento de novas tecnologias que envolvem cada vez mais aspectos da pessoa humana – aspectos que, há alguns anos, seria impensável conhecer –, deve-se dedicar especial atenção e cuidado na sua revisão por parte do Estado, com o objetivo de prevenir e antecipar possíveis efeitos, além de proteger diretamente a integridade humana em sua totalidade, incluindo sua

privacidade e confidencialidade, bem como os direitos inerentes à integridade psíquica e ao sujeito de experimentação científica [...] Dessa forma (...) torna-se absolutamente necessário que, antes de permitir sua comercialização e uso no país, essa tecnologia e seus dispositivos sejam analisados pela autoridade competente, considerando que ela apresenta problemáticas até então não estudadas [...] as condutas denunciadas nos autos, nas circunstâncias anotadas, violam as garantias constitucionais contidas nos incisos 1 e 4 do artigo 19 da Constituição Política da República, que se referem à integridade física e psíquica e ao direito à privacidade [...] Por essas considerações, e tendo em vista que o dispositivo não possui Certificado de Destinação Aduaneira, acolher-se-á a presente ação conforme se indicará no resolutivo deste acórdão, a fim de que a autoridade sanitária e aduaneira estude de forma completa o dispositivo Insight à luz da normativa mencionada neste acórdão. (g.n)²⁹

Além de paradigmático, este caso estabeleceu parâmetros fundamentais que deverão orientar as análises futuras sobre o tema. Dentre os aspectos destacados, podem-se mencionar: (i) o reconhecimento de que dados neurais, também, configuram dados pessoais, e, portanto, estão sob a proteção das legislações de proteção de dados. Essa consideração, embora pareça básica, é crucial, pois demonstra que a proteção de dados emerge como o principal fundamento jurídico, na análise das neurotecnologias; (ii) a clara conexão entre a legislação de proteção de dados e os direitos fundamentais à integridade psíquica e à privacidade, evidenciando que a ausência de consentimento para o tratamento específico das informações cerebrais configura simultaneamente uma violação legal e constitucional; e (iii) o debate sobre a necessidade de consentimento expresso, ressaltando a imprescindibilidade de se enquadrar o tratamento em uma base legal adequada, sob pena de incorrer em ilicitude.

Neste sentido, entende-se que os julgadores chilenos decidiram, acertadamente, visto que sopesaram os benefícios associados ao desenvolvimento das neurotecnologias e buscaram uma solução equilibrada, não radical, que poderia culminar na proibição das atividades da Emotiv Inc., no país, e, consequentemente, desincentivar outras empresas atuantes nesse mercado.

29. CHILE. Base Jurisprudencial del Poder Judicial. *GIRARDI/EMOTIV INC: 09-08-2023 (CIVIL) APELACIÓN PROTECCIÓN*, Rol N° 105065-2023. En Buscador Jurisprudencial de la Corte Suprema. Disponível em: https://juris.pjud.cl/busqueda/pagina_detalle_sentencia?k=L2FadjlzYUdmbGx1UWNKWmV6ZjZ3dz09. Acesso em: 30 jul.2024.

Em suma, essa abordagem não só evidencia a importância e a efetividade dos Neurodireitos, ante os desafios decorrentes destas novas tecnologias, mas também revela a possibilidade de se delimitar um caminho comunicativo, no qual a inovação possa se aperfeiçoar, de forma ética e responsável.

Considerações finais

Este artigo concentra-se, em síntese, na análise de como as neurotecnologias e a Inteligência Artificial estão moldando a criação de novos direitos, explorando os caminhos, atualmente, propostos para promover um desenvolvimento ético e responsável dessas inovações, com o objetivo de proteger os chamados Neurodireitos, diante dos riscos associados ao tratamento de dados neurais.

Nos capítulos iniciais, apresenta-se um breve retrospecto histórico das interfaces cérebro-computador (BCIs), destacando seus benefícios e a evolução impulsionada pela integração com ferramentas de IA. Examinam-se algumas aplicações práticas das BCIs, evidenciando seu potencial transformador e impacto positivo, especialmente, para pessoas com deficiência. Além disso, discutem-se os desafios e preocupações que esses avanços podem trazer, a curto prazo, para a sociedade, considerando a sensibilidade e o potencial lesivo do tratamento de dados neurais, e sublinhando a importância do estudo dos Neurodireitos.

O capítulo subsequente foi dividido em duas partes. A primeira, analisa as propostas e normativas existentes ao redor do mundo, buscando identificar pontos de convergência e destacando como a diversidade de propostas e a falta de um consenso uniforme demonstram o interesse crescente e a necessidade de um marco regulatório para garantir a proteção dos Neurodireitos. A segunda, oferece uma análise detalhada do caso *Girardi vs Emotiv Inc.*, trazendo considerações importantes sobre as potencialidades da aplicação desses direitos em cenários práticos, sua efetivação e a abordagem dos Neurodireitos, no âmbito judicial.

Finalmente, embora o debate sobre o tema esteja longe de ser concluído, o objetivo deste artigo é estimular uma reflexão mais profunda e incisiva sobre as questões nele apresentadas, visando promover uma maior efetividade na proteção dos Neurodireitos.

Diante da complexidade das tecnologias envolvidas e da rapidez com que se desenvolvem, a construção de um arcabouço jurídico robusto e adaptável, que equilibre a inovação com a proteção dos titulares, é um desafio que exige uma abordagem colaborativa entre legisladores, cientistas e a sociedade civil.

Em conclusão, o estudo sobre Neurodireitos deve, portanto, ser contínuo e dinâmico, buscando garantir que as inovações, por mais disruptivas que sejam, respeitem a dignidade e a autonomia dos indivíduos, para que possamos avançar com segurança no terreno cada vez mais incerto das BCIs e da IA, de modo a aproveitarmos suas benesses e evitar abusos, protegendo os indivíduos contra os riscos inerentes ao tratamento de dados neurais.

Referências Bibliográficas

ARMSTRONG, W. MICHAEL, K. The Implications of Neuralink and Brain Machine *Interface Technologies*. *IEEE International Symposium on Technology and Society (ISTAS)*, Tempe, AZ, USA, 2020, pp. 201-203. Disponível em: <https://ieeexplore.ieee.org/abstract/document/9462223>. Acesso em: 20 abr.2024.

AR-SNAP AR. Welcome Nextmind. Disponível em: <https://ar.snap.com/welcome-nextmind>. Acesso em: 11 jun. 2024.

BOSELLI, G. *Neurodireitos: a urgência de proteção jurídica das neurotecnologias*. Consultor Jurídico, 2024. Disponível em: <https://www.conjur.com.br/2024-fev-06/neurodireitos-a-urgencia-de-protecao-juridica-das-neurotecnologias/>. Acesso em: 10 jun. 2024.

BRASIL. *Lei nº. 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 jun. 2024.

BRASIL, Ministério dos Direitos Humanos e da Cidadania. *Brasil tem 18,6 milhões de pessoas com deficiência, indica pesquisa divulgada pelo IBGE e MDHC*. Gov.br, 2023. Disponível em: <https://www.gov.br/mdh/pt-br/assuntos/noticias/2023/julho/brasil-tem-18-6-milhoes-de-pessoas-com-deficiencia-indica-pesquisa-divulgada-pelo-ibge-e-mdhc>. Acesso em 31 de Jul de 2024.

CANTARINI, P. *A nova fronteira da manipulação comportamental e o papel do “compliance” na mitigação de riscos em IA*. *Jornal da USP*, 2024. Disponível em: <https://jornal.usp.br/artigos/a-nova-fronteira-da-manipulacao-comportamental-e-o-papel-do-compliance-na-mitigacao-de-riscos-em-ia/>. Acesso em: 30 jul. 2024.

CANTER, L. BRIM, E. California Enacts Health AI Bill and Protections for Neural Data. Covington, 2024. Disponível em: <https://www.insideprivacy.com/uncategorized/california-enacts-health-ai-bill-and-protections-for-neural-data/>>. Acesso em: 16 out. 2024.

CHILE. Base Jurisprudencial del Poder Judicial. GIRARDI/EMOTIV INC: 09-08-2023 (CIVIL) APELACIÓN PROTECCIÓN), Rol N° 105065-2023. En Buscador Jurisprudencial de la Corte Suprema. Disponível em: https://juris.pjud.cl/busqueda/pagina_detalle_sentencia?k=L2FadjlzYUdmbGx1UWNKWmV6ZjZ3dz09. Acesso em: 30 jul.2024.

CORNEJO-PLAZA, M. I. CIPPITANI, R. PASQUINO, V. Chilean Supreme Court ruling on the protection of brain activity: neurorights, personal data protection, and neurodata. *Frontiers in Psychology*, 2024. Disponível em: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10929545/>. Acesso em: 25 jul. 2024.

DREW, L. Elon Musk's Neuralink brain chip: what scientists think of first human trial. *Nature*, 2024. Disponível em: <https://www.nature.com/articles/d41586-024-00304-4>. Acesso em: 11 jun. 2024.

DO, B. SPIVACK, J. BADILO, M. Privacy and the rise of "neurorights" in Latin America. *Future of Privacy Forum*, 2024. Disponível em: <https://fpf.org/blog/privacy-and-the-rise-of-neurorights-in-latin-america/>. Acesso em: 23 jul. 2024.

FIANI, Brian. Reardon, Taylor *et al.* *An Examination of Prospective Uses and Future Directions of Neuralink: The Brain-Machine Interface*. *Cureus*, 2021. Disponível em: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8083990/#>. Acesso em: 14. jun. 2024.

FLORES FILHO, E. FIRMO, M. Dignidade humana e neurodireitos na era digital. *Revista do Instituto de Direito Constitucional e Cidadania – IDCC*, Londrina, v. 7, n. 2, e063,, 2022. Disponível em: <file:///C:/Users/hsmol/Downloads/157-Texto%20do%20Artigo-386-2-10-20230523.pdf>. Acesso em: 15 jul.2024.

GAGUIM, C. *Projeto de Lei nº 522, de 2022*. Câmara dos Deputados, 2022. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2317524>. Acesso em: 29 jul. 2024.

GENSER, J. DAMIANOS, S. YUSTE, R. Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies. *Neurorights Foundation*, 2024. Disponível em: https://www.perseus-strategies.com/wp-content/uploads/2024/04/FINAL_Consumer_Neurotechnology_Report_Neurorights_Foundation_April-1.pdf. Acesso em: 12. Jul. 2024.

GRAND VIEW RESEARCH. *Brain Computer Interface Market Size, Share & Trends Analysis Report By Application (Healthcare, Communication & Control), By Product (Invasive, Non-invasive), By End Use (Medical, Military), And Segment Forecasts, 2023 – 2030*. Report ID: 978-1-68038-459-8 Disponível em: <https://www.grandviewresearch.com/industry-analysis/brain-computer-interfaces-market>; Acesso em 19 Jun de 2024.

HALLINAN, D. *et al Neurodata and Neuroprivacy: Data Protection Outdated?* *Surveillance & Society*, 2014. Disponível em: <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/neurodata>. Acesso em: 12. jul. 2024.

HIGGINS, N. *Neuralink implanta chip em cérebro humano: o que pode dar errado*. *Galileu*, 2024. Disponível em: <https://revistagalileu.globo.com/tecnologia/noticia/2024/02/neuralink-implanta-chip-em-cerebro-humano-o-que-pode-dar-errado.ghtml>. Acesso em: 02. jun. 2024.

HBP – HUMAN BRAIN PROJECT. *The Human Brain Project ends: What has been achieved*. *Human Brain Project*, Press release, 2023. Disponível em: <https://www.humanbrainproject.eu/en/follow-hbp/news/2023/09/28/human-brain-project-ends-what-has-been-achieved/>. Acesso em: 22 Jul. 2024.

IENCA, M.. ANDORNO, R.. A new category of human rights: neurorights. *BMC*, 2017. Disponível em: <https://blogs.biomedcentral.com/bmcblog/2017/04/26/new-category-human-rights-neurorights/>. Acesso em 15 jul. 2024.

IENCA, M. ANDORNO, R. *Towards new human rights in the age of neuroscience and neurotechnology*. *Life Sciences, Society and Policy*, 2017. Disponível em: <https://lssjournal.biomedcentral.com/articles/10.1186/s40504-017-0050-1>. Acesso em: 01 jul, 2024.

KAWALASTE-STERNIUK, A. BROWASKA, N. Summary of over Fifty Years with Brain-Computer Interfaces-A Review. *Brain Sciences* 2021 Jan 3;11(1):43. doi: 10.3390/brainsci11010043. PMID: 33401571; PMCID: PMC7824107. Disponível em: <https://doi.org/10.3390/brainsci11010043>. Acesso em: 11 jun.2024.

KUMAR, B. Integration of AI and Neuroscience for Advancing Brain-Machine Interfaces: A Study. *International Journal of New Media Studies (IJNMS)*, Volume 9 Issue 1, January-June, 2022. Disponível em: https://www.researchgate.net/profile/BharathKumarNagaraj/publication/380785142_Integration_of_AI_and_Neuroscience_for_Advancing_Brain-Machine_Interfaces_A_Study/links/664e2edfbc86444c72f79492/Integration-of-AI-and-Neuroscience-for-Advancing-Brain-Machine-Interfaces-A-Study.pdf. Acesso em: 11 jun.2024.

LOTTE, F. NAM, C. S. Introduction: Evolution of Brain-Computer Interfaces. *Hal Open Science: Brain-Computer Interfaces Handbook: Technological and Theoretical Advance*, Taylor & Francis (CRC Press), pp.1-11, 2018, 9781498773430. fhal-01656743f. Disponível em: <https://inria.hal.science/hal-01656743/document>. Acesso em: 10 jun.2024.

MARDEN, C. MARTINS, G. *Direito e neurociência: além das primeiras impressões*. Curitiba: Juruá, 2020.

MARR, B. AI's next frontier: are brain-computer interfaces the future of communication? *Forbes Innovation*, 2023. Disponível em: <https://www.forbes.com/sites/bernardmarr/2023/08/11/ai-next-frontier-are-brain-computer-interfaces-the-future-of-communication/>. Acesso em: 10 jun 2024.

MAYNARD, A. SCRAGG, M. *The Ethical and Responsible Development and Application of Advanced Brain Machine Interfaces*. *J Med Internet Res*, 2019. Disponível em: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7351257/> Acesso em: 10 jul. 2024.

MCAFEE, A. BRYNJOLFSSON, E. *A segunda era das máquinas*. Rio de Janeiro: Alta Books, 2014.

METHA, D. *Como implante cerebral Neuralink de Elon Musk 'amplia as fronteiras da mente'*. *BBC News Brasil*, 2024. Disponível em: <https://www.bbc.com/portuguese/articles/cp0gyj3lv01o>. Acesso em: 23. jul. 2024.

MUSK, E. Neuralink. An Integrated Brain-Machine Interface Platform With Thousands of Channels. *J Med Internet Res* 2019;21(10):e16194. Disponível em: <https://www.jmir.org/2019/10/e16194>. Acesso em: 20. jul. 2024.

MOENS, J. Your Brain Waves Are Up for Sale. A New Law Wants to Change That. *New York Times*, 2024. Disponível em: <https://www.nytimes.com/2024/04/17/science/colorado-brain-data-privacy.html>. Acesso em: 24 jun. 2024.

NICOLELIS, M. Are we at risk of becoming biological digital machines? *Nature Human Behaviour*. *Nat Hum Behav* 1, 2017. Disponível em: <https://doi.org/10.1038/s41562-016-0008>. Acesso em: 02. jul. 2024.

NICOLELIS, M. *Muito além do nosso eu: a nova neurociência que une cérebro e máquinas – e como ela pode mudar nossas vidas*. 1. ed. São Paulo: Planeta, 2017. 25-28 p.

NIETO-CHAUPIS, H. "The Internet of Brain Things: Theoretical Basis for the Usage of Neuralink Chip." *IEEE 13th International Conference on Consumer Electronics – Berlin (ICCE-Berlin)*, Berlin, Germany, 2023, pp. 1-6. Disponível em: <https://ieeexplore.ieee.org/abstract/document/10375671>. Acesso em: 02. Ago. 2024.

OCHANG, P. EKE, D. STAHL, B. *Towards an understanding of global brain data governance: ethical positions that underpin global brain data governance discourse*. *Front Big Data*. 2023. Disponível em: <https://pubmed.ncbi.nlm.nih.gov/38025947/>. Acesso em: 08 jul. 2024. 03 p.

OEA – ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Declaração Interamericana de Princípios sobre Neurociências, Neurotecnologias e Direitos Humanos. Disponível em: https://www.oas.org/es/sla/cji/temas_culminados_recientemente_Neurociencias_Neurotecnologias_y_Derechos_Humanos.asp. Acesso em: 23 jul. 2024.

PIVA, S. *Neurodireitos: a necessária proteção da mente humana em tempos de avanço de neurotecnologias e da IA*. Fenalaw, 2023. Disponível em: <https://www.fenalaw.com.br/fenalawlab/neurodireitos-a-necessaria-protecao-da-mente-humana-em-tempos-de-avanco-de-neurotecnologias-e-da-ia/>. Acesso em: 02 de ago. 2024.

RODRÍGUEZ, J. Inteligencia artificial y neuroderechos. Retos y perspectivas. *Cuestiones Constitucionales, Revista Mexicana de Derecho Constitucional*, Núm. 46, Enero-Junio 2022 ISSN (versión electrónica): 2448-4881. Disponível em: <https://www.scielo.org.mx/pdf/cconst/n46/1405-9193-c-const-46-93.pdf>. Acesso em: 26 jul. 2024.

SALOMÃO, L. et al. *Relatório Final – Comissão de Juristas Responsável pela revisão e atualização do Código Civil*. Brasília. Senado Federal, 05.04.2024. Disponível em: <https://legis.senado.leg.br/comissoes/comissao?codcol=2630>. Acesso em: 28 jul. 2024.

SCHWAB, K. *A quarta revolução industrial* – São Paulo: Edipro, 2016. 115 p.

SILVA, G. A. A New Frontier: The Convergence of Nanotechnology, Brain Machine Interfaces, and Artificial Intelligence. *Front. Neurosci.* 12:843. Disponível em: <https://www.frontiersin.org/journals/neuroscience/articles/10.3389/fnins.2018.00843/full>. Acesso em: 20 jul. 2024.

STRICKLAND, E. Worldwide campaign for neurorights notches its first win. *IEE Spectrum*, 2021. Disponível em: <https://spectrum.ieee.org/neurotech-neurorights>. Acesso em: 22 Jul. 2024

THE NEURORIGHTS FOUNDATION. *The Five Neurorights*. Disponível em: <https://neurorightsfoundation.org/mission>. Acesso em: 01 jun. 2024.

WHO – World Health Organization. *Global report on health equity for persons with disabilities*. Geneva: WHO, 2022. Disponível em: <https://www.who.int/publications/i/item/9789240063600>. Acesso em 31 de Jul de 2024.

WILD, K. ‘Our notion of privacy will be useless’: what happens if technology learns to read our minds? *The Guardian*, 2021. Disponível em: <https://www.theguardian.com/technology/2021/nov/07/our-notion-of-privacy-will-be-useless-what-happens-if-technology-learns-to-read-our-minds>. Acesso em: 17 jun.2024.

YUSTE, R. GOERING, S. et al. Four ethical priorities for neurotechnologies and AI. *Nature*. 2017. Disponível em: <https://www.nature.com/articles/551159a>. Acesso em: 18 jun. 2024.

ZHANG, X. MA, Z. ZHENG, H. et al. The combination of brain-computer interfaces and artificial intelligence: applications and challenges. *Ann Transl Med.* 2020 Jun;8(11):712. doi: 10.21037/atm.2019.11.109. PMID: 32617332; PMCID: PMC7327323. Disponível em: <https://doi.org/10.21037/atm.2019.11.109>. Acesso em: 18 jun. 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

EIXO II

Cidades inteligentes e novas tecnologias

AUTORES

Carolina Freitas Gomide de Araujo

Cláudio Mendes da Silva

Daniel Santiago Diniz

Luís Henrique de Menezes Acioly

Victor Chame Alvim

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

11

Cidades Inteligentes e Necropolítica: A proteção de dados e os direitos fundamentais na Era Digital

CLÁUDIO MENDES DA SILVA

Covardes são quem tem tudo de bom e fornecem o mal pra favela morrer. Criolo.

Sumário: Introdução. 1. Cidades Inteligentes e Desigualdades Sociais: Um debate não paritário 2. “Dadificação” da vida e os direitos fundamentais na era digital 3. Do Colonialismo à Era Digital: A Persistência da Vigilância e do Controle Social no Brasil. Considerações finais. Referências.

Introdução

As primeiras décadas do século XXI vêm sendo marcadas pelo aumento massivo da utilização de dados, especialmente dados pessoais, para sustentar o novo estilo de mercado, baseado nesse tipo de insumo para o fornecimento de produtos ou serviços. Nesse cenário, considera-se não só o manuseio de dados através de técnicas de *big data*² por agentes empresariais, mas também por governos, em virtude da informatização das cidades e das políticas públicas fundamentadas no uso das tecnologias de informação e automatização, em uma perspectiva de construção dos novos modelos de *Smart Cities* também chamadas de “Cidades Inteligentes”. Insta salientar que, no presente estudo, não serão abordados os dilemas e controvérsias conceituais sobre este tema, mas se buscará tornar a sua compreensão mais acessível, em maior ou menor grau, destacando sua aplicação prática e implicações sociais.

Em que pese a inegável possibilidade de os cidadãos usufruírem dos produtos, políticas e facilidades geradas por meio do uso de dados, é necessário avaliarmos também os impactos nos próprios cidadãos no que diz respeito aos seus direitos constitucionais à privacidade, autonomia e proteção de dados. Este último foi positivado mais recentemente no rol dos direitos fundamentais, na forma do Art. 5º, LXXIX, Constituição da República Federativa do Brasil (CRFB/88), através da Emenda Constitucional nº 115, de 2022.

Nesse aspecto, nota-se, ainda, vasta relevância da Lei Geral de Proteção de Dados, que foi aprovada no ano de 2018, na forma da Lei nº 13.709, de 14 de

1. Graduado em Direito pela Universidade do Estado do Rio de Janeiro - UERJ; Pós-graduando em Direito Digital pelo Instituto de Tecnologia e Sociedade (ITS Rio), em parceria com a UERJ; Advogado; Assessor Jurídico do Instituto Decodifica.

2. Que segundo o relatório produzido pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro do Rio (ITS-Rio), “é, literalmente, o conjunto de dados cuja existência só é possível em consequência da coleta massiva de dados que se tornou possível nos últimos anos, graças à onipresença de aparelhos e sensores na vida cotidiana e do número crescente de pessoas conectadas a tais tecnologias por meio de redes digitais e também de sensores”. *Big data no Sul Global. Relatório sobre estudos de caso*. Instituto de Tecnologia & Sociedade do Rio. Rio de Janeiro, 2016. Disponível em: https://itsrio.org/wp-content/uploads/2017/02/ITS_Big-Data_PT-BR_v4.pdf. Acesso em: jul. 2024.

agosto de 2018, com entrada em vigor em 18 de setembro de 2020. A normativa surge em um cenário no qual se busca definir diretrizes para a consolidação da regulação de um ecossistema de proteção dos direitos à privacidade e de dados pessoais. Isso, considerando que a LGPD passa a figurar como a primeira normativa geral sobre tal tema no Brasil.

A inovação, no sentido mais amplo da palavra, não deve emergir a qualquer custo. A chamada 4ª Revolução Industrial pela qual o globo está passando, vem provocando uma mudança profunda nas estruturas das cidades, exigindo uma reflexão abrangente e contextualizada sobre seus impactos sociais e éticos. O citado evento tem redefinido a forma como interagimos com os espaço urbano, trazendo novas dinâmicas de poder e controle que têm afetado diretamente a qualidade de vida e os direitos individuais dos cidadãos.

O presente artigo, a seu turno, visa trazer percepções mais locais, inicialmente focadas no Brasil, e examinar os impactos e os potenciais altamente lesivos dessas tecnologias, a exemplo daquelas utilizadas para fins de monitoramento, em especial na área da segurança pública, dado o acentuado uso de dados, nas populações historicamente vulneráveis, sobretudo as populações pretas e periféricas. Esse exame se dará à luz das garantias das legislações civis-constitucionais que vislubram tutelar os direito à privacidade e proteção de dados, mesmo a despeito da não incidência direta da LGPD, conforme seu art. 4º, inciso III, alínea “a”.

Para além, busca-se refletir sobre o que se entende sobre a temática de *Smart Cities*, a atuação do Estado como ente soberano na formulação e implementação de políticas públicas, as tecnologias de vigilância e o controle de dados em cidades inteligentes e como tal atuação pode influenciar e potencialmente reforçar práticas de necropolítica na vida e nos direitos dos grupos historicamente vulneráveis, como já citado, mas considerando a perspectiva de Achille Mbembe³.

A urgência do tema se dá em razão do modelo de mercado em vigência, no qual os dados pessoais são importantes ativos para os diferentes atores da economia, levando-se em conta que o Estado ocupa uma posição de agente atuante nesse sentido. Isso sem mencionar o quesito de seu poder político da formulação de políticas públicas, sendo crucial ressaltar como a ausência de participação cidadã na formulação destas pode exacerbar ainda mais as desigualdades já experienciadas. De mais a mais, cabe registrar que a pergunta norteadora desta obra se consubstancia na seguinte questão: como ou em que

3. MBEMBE, Achille. *Necropolítica. Biopoder, soberania, estado de exceção, política da morte* (ebook). São Paulo: N-1 edições, 2018.

medida as Cidades Inteligentes podem ser um ambiente de não discriminação no que tange ao contexto tecnológico atual?

A busca de possíveis soluções ou mitigação para este problema já em franca ascensão em nosso cenário perpassará por uma breve, porém não tão simplória, análise e contextualização histórico-social-política do Brasil, partindo-se do pressuposto que, o que entendemos por discriminação, no geral, não é algo novo, em se considerando a era da informação e de insumos tecnológicos, mas que esta reproduz o que já é algo intrínseco a sociedade, em si, tanto de quem fornece essas ferramentas, no caso do Norte Global, quanto de quem as consome, caso do Brasil, como um dos representantes do Sul Global.

1. Cidades Inteligentes e Desigualdades Sociais: Um debate não paritário

Logo de face, cabe aqui colocarmos que todas as sociedades, em alguma medida, são tecnológicas. O que metrifica o grau de inovação – se é que é “justa” esse tipo de mensuração para fins de comparação – é o contexto em que um certo grupo ou sociedade se encontram. Por exemplo, a faca feita de pedra foi uma grande inovação na sociedade que vivia há 3.000 anos antes de cristo (ac), por ser um objeto cortante e que podia ser usada para a caça e defesa⁴. Igualmente, em um recorte de período de tempo mais atual, ela também é uma tecnologia altamente funcional e que nos serve para alimentação – considerando, é claro, o estilo de vida ocidental. Portanto, o uso de dispositivos tecnológicos como *tablets* e *smartphones*, com ou sem Inteligência Artificial (IA), não define necessariamente o que é moderno e/ou inovador.

As Cidades Inteligentes, a seu turno, são comumente caracterizadas pelo uso massivo de tecnologia com o emprego de dados que, pelo menos em tese, tem o condão de melhorar a qualidade de vida dos seus cidadãos, bem como aprimorar o importante elemento da eficiência no que concerne a gestão dos recursos – financiados e pertencentes a sua população – e sustentabilidade do próprio espaço urbano^{5,6}.

4. BOLLA, Carla. *Como a França popularizou o uso de talheres*. *Forbes*. 15 set, 2022. Disponível em: <https://forbes.com.br/forbeslife/2022/09/carla-bolla-como-a-franca-popularizou-o-uso-de-talheres/>. Acesso em: jul. 2024.

5. OB.BR. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Cidades Inteligentes*. Disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/publicacao_radar_tecnologico_jan_2024.pdf. Acesso em: jul. 2024.

6. Ainda: A norma ABNT, com base na ISO 37122 (ABNT, 2021), conceitua cidade inteligente como uma cidade que aumenta o ritmo em que proporciona resultados de sustentabilidade social, econômica e ambiental e que responde a desafios como mudanças climáticas, rápido crescimento populacional e instabilidades de ordem política e econômica, melhorando fundamentalmente a forma como engaja a sociedade, aplica métodos de liderança colaborativa, trabalha por meio de disciplinas e sistemas municipais, e usa informações de dados e tecnologias modernas, para fornecer melhores serviços e qualidade de vida para os que nela habitam (residentes, empresas, visitantes), agora e no futuro previsível, sem desvantagens injustas ou degradação do ambiente natural. *Ibidem*.

O Projeto de Lei (PL) nº 976 apresentado em 19/03/2021, com vistas a instituir a Política Nacional de Cidades Inteligentes (PNCI)⁷, conceitua o termo assim, *in verbis*:

Art. 2º Para os efeitos desta Lei, entende-se por:

I – cidade inteligente: espaço urbano orientado para o investimento em capital humano e social, o desenvolvimento econômico sustentável e o uso de tecnologias disponíveis para aprimorar e interconectar os serviços e a infraestrutura das cidades, de modo inclusivo, participativo, transparente e inovador, com foco na elevação da qualidade de vida e do bem estar dos cidadãos.

Esse atual estilo de vida que comumente estamos experienciando cada vez mais em nosso cotidiano, a exemplo também e, especialmente, do emprego do uso de tecnologias na área da segurança pública, está diretamente associado a uma importação de um modelo produzido no Norte Global, onde estão concentradas as mais poderosas empresas do ramo, do ponto de vista econômico. Essa dinâmica vem sendo conduzida pelo mercado privado, dentro do sistema capitalista de produção, no qual as grandes empresas de tecnologia são as principais agentes. Estas, por sua vez, regulam a vida social contemporânea, perspectiva na qual temos nossos dados pessoais coletados e/ou vendidos por ou para outras empresas, que se utilizarão dos mesmos em seu próprio benefício⁸, haja vista que a obtenção do lucro é condição *sine qua non* para as empresas assim se constituírem.

Nesse aspecto, verifica-se a necessidade de refletirmos acerca dos impactos desta internalização em um contexto que, por si só, é de extrema desigualdade. A despeito disso, vale considerar também que:

Cidades são organismos vivos (não-estáticos) e, portanto, quando gerenciadas por sistemas tecnológicos, estes devem ter flexibilidade suficiente para contemplar, não só mudanças de rumo ditadas pelas necessidades dos habitantes, como desafios impostos por novos problemas urbanos. Seriam os atuais sistemas capazes desta flexibilidade? Mais ainda, seriam estes sistemas inclusivos ou direcionados para uma pequena parcela da população, capaz de ter acesso a estes recursos?⁹

7. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1977843&filename=PL%20976/2021. Acesso em: jul. 2024.

8. RIBEIRO, Laura Talho. *Tecnologias inteligentes de vigilância: percepções sobre segurança nos centros urbanos*. Disponível em: https://itsrio.org/wp-content/uploads/2018/03/laura_talho_smartsurveillance.pdf. Acesso em: jul. de 2024.

9. MENDES, Teresa Cristina M. *Smart Cities: Solução para as cidades ou aprofundamento das desigualdades sociais?* Rio de Janeiro, 2020. p.4. Disponível em: https://www.observatoriodasmetroles.net.br/wp-content/uploads/2020/01/TD-011-2020_Teresa-Mendes_Final.pdf Acesso em: jul.de 2024.

Teresa Cristina Mendes destaca que a flexibilidade dos sistemas tecnológicos é crucial para atender às necessidades dos habitantes¹⁰. Isso levanta a questão de como as Cidades Inteligentes podem ser adaptadas para não perpetuar desigualdades existentes, considerando-se as dinâmicas sociais vivenciadas nas cidades, entendendo-se, ainda, o contexto histórico do país, como um todo, visto que tal aspecto reflete também nas desigualdades sociais. A esse respeito, a posição da população negra na atual conjuntura não pode ser analisada isoladamente, pois seria um erro ignorar os quase quatrocentos anos de escravidão sofridos, as suas limitações estruturais e, mais ainda, a questão referente à total alienação de sua dignidade – aqui em alusão ao princípio já consolidado da dignidade da pessoa humana –, cenário o qual fora marcado pelo esvaziamento da humanidade de tal público.

Fato notório ao qual devemos também ter em mente para tentar compreender como essa nova dinâmica trazida pelas Cidades Inteligentes, importada de uma outra realidade, pode ser igualmente nociva e excludente atingindo indireta e diretamente a comunidade negra, é de que o colonizador português, em seu processo de alienação de toda uma cultura, desenvolveu também um mecanismo neutralizador da consciência étnica através de sua ideologia imperialista de um “agente da evolução e da civilização”. Processo este expressado por Clóvis Moura nos dizeres tais como: “*verbalização democrática*”¹¹. Isso fez com que parcela significativa da população negra, tendo assimilado tal imposição ideológica, procurasse a se passar por brancos, ou, pelo menos, promover-se nessa escala cromática que o colonizador havia estabelecido, tendo como modelo superior a ser alcançado, o branco. Essa política fenotípica procurou e procura ainda fazer com que os componentes deste grupo específico fujam das suas origens, procurando assimilar a escala de valores e padrões brancos.

Embora estejamos fazendo um salto temporal, é crucial ressaltar que essa ideologia permanece arraigada em nossa sociedade, tendo em vista que estamos ainda em processo histórico de resgate da identidade, dignidade, autonomia e bem estar da população negra. Exemplificativamente, vale o registro de que a Lei nº 12.711, de 29 de agosto de 2012, a Lei de Cotas, é uma política de reparação à escravidão extremamente recente em nossa linha do tempo, uma das únicas existentes explicitamente, inclusive, sem mencionar a Lei Áurea, norma que marcou a abolição da escravidão no Brasil. Pode-se inferir, através desses fatos, o quão delicado e urgente é o abismo social existente.

10. Ibidem.

11. MOURA, Clovis. *Escravidão, colonialismo, imperialismo e racismo*. Afro-Ásia, Salvador, n. 14, 1983. p.3. Disponível em: <https://periodicos.ufba.br/index.php/afroasia/article/view/20824/13425>. Acesso em: jul. 2024.

Em suma, vale depreender também que “a distribuição racializada das cidades brasileiras é resultado tanto do acúmulo convergente de inúmeras decisões e incidências da desigualdade e racismo quanto da adoção de ideologias racistas nas cidades planejadas.”¹²

Tratando-se ainda do Brasil, um país que enfrenta grandes problemas de inclusão digital e profundas desigualdades sociais e econômicas, entre as pessoas que não acessam a internet, 24 milhões estão em áreas urbanas, 17 milhões se declararam pretas ou pardas e 17 milhões pertencem às classes D-E, o que aponta uma exclusão digital nas periferias urbanas do país¹³. Assim, o conceito de *Smart Cities* está sendo incorporado de forma limitada, embora alguns segmentos, como a segurança pública, receba investimentos robustos já pensando nesse modelo de realidade¹⁴. Ainda está longe de ser uma realidade plena pensar na implantação completa de recursos tecnológicos no desenvolvimento urbano, sendo mais uma política megalomaniaca sem conhecimento empírico de suas consequências.

Essa questão também é abordada por Teresa Cristina, que corrobora:

Embora com discursos inclusivos, constata-se que a questão da desigualdade ainda se faz presente em boa parte das iniciativas (notadamente nos países menos desenvolvidos), pois de potencial atuação ativa, os habitantes são definidos como meros consumidores das soluções tecnológicas.¹⁵

A falta de infraestrutura adequada, os altos custos de implementação e a ausência de políticas públicas eficazes agravam essa situação. Isso sem mencionar também a gravidade de replicabilidade de um modelo – mesmo que tenha sido eficiente em um outro contexto, especialmente se ele levar em conta o norte global. Além disso, as desigualdades regionais e a concentração de investimentos em áreas urbanas mais ricas intensificam a exclusão das populações periféricas e rurais. Para que o Brasil se aproxime de uma verdadeira cidade inteligente, é essencial implementar políticas que promovam a inclu-

12. SILVA, Tarcízio. *Racismo algorítmico: inteligência artificial e discriminação nas redes digitais*. São Paulo: Edições Sesc São Paulo, 2022. p. 141.

13. CAMARGO, Bianca. *Cerca de 84% dos lares brasileiros têm acesso à internet, diz pesquisa*. CNN, São Paulo, 16 novembro, 2023. Disponível em: <https://www.cnnbrasil.com.br/nacional/cerca-de-84-dos-lares-brasileiros-tem-acesso-a-internet-diz-pesquisa/>. Acesso em: ago. 2024.

14. O Governador do Rio de Janeiro, Cláudio Castro investiu um montante de R\$236,5 milhões de reais na compra de equipamentos de reconhecimento facial. SANTO, Thaís Espírito. RJ anuncia câmeras com reconhecimento facial e leitura de placas em viaturas da PM. *G1*, Rio de Janeiro, 03 abril, 2021. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2024/04/03/rj-anuncia-cameras-com-reconhecimento-facial-e-leitura-de-placas-em-viaturas-da-pm.ghtml> Acesso em: jul. 2024.

15. MENDES, Teresa Cristina M. *Smart Cities: Solução para as cidades ou aprofundamento das desigualdades sociais?*. Rio de Janeiro, 2020. p.6. Disponível em: https://www.observatoriodasmegacidades.net.br/wp-content/uploads/2020/01/TD-011-2020_Teresa-Mendes_Final.pdf Acesso em: jul. de 2024.

são digital, assegurem o acesso equitativo às novas tecnologias e promovam a participação cidadã nas decisões sobre o desenvolvimento urbano.

Imprescindível constatar que a citada participação cidadã traz consigo a ideia de que os territórios periféricos têm conhecimento empírico acerca da realidade que vivenciam, ainda mais se tratando do processo de formulação, monitoramento da execução e avaliação de uma política pública, mas que necessita de esforços multissetoriais para, por exemplo, participar de fóruns populares, seminários, oficinas e outros mecanismos de co-construção, nos quais se garanta o conhecimento informado e a autonomia para deliberar sobre a temática em questão¹⁶. Sem esses esforços, as tecnologias podem acabar aprofundando as divisões existentes e perpetuando a marginalização das comunidades mais vulneráveis.¹⁷

2. “Dadificação” da vida e os direitos fundamentais na era digital

Stefano Rodotà¹⁸, em palestra-aula intitulada “Transformações do Corpo”, realizada em 06 de novembro de 2015, na Universidade do Estado do Rio de Janeiro (UERJ), acompanhada *in loco* pelo autor da obra, discorreu sobre as profundas transformações pelas quais o corpo humano estava passando, fato que é ainda extremamente atual, especialmente na era da informação e da tecnologia. Rodotà observou que o corpo, antes visto como uma entidade física inviolável, agora se transforma em dados e informações que podem ser manipulados e usados por terceiros. A era digital introduziu o conceito de “corpo eletrônico”, onde elementos biométricos como impressões digitais, íris, retinas e até mesmo expressões faciais, são também “dadificados”, sendo utilizados para identificar e controlar indivíduos.

Este controle se estende a tecnologias como microchips subcutâneos e incluindo ainda celulares *smartphones*, que permitem a localização constante

16. A exemplo do Fórum Popular de Segurança Pública, que foi lançado em 2022, no Rio de Janeiro, segundo o Observatório de Favelas. Evento este que é recente do ponto de vista histórico, mas que já abre margem para se pensar em uma iniciativa nacional e na construção de um espaço no qual os governantes e tomadores de decisão possam também tomar decisões melhor informadas sobre uma questão tão sensível. VELLASCO, Ramon. Fórum Popular de Segurança Pública é lançado no Rio de Janeiro. *Observatório de Favelas*. Rio de Janeiro. 29 jun, 2023. Disponível em: <https://observatoriodefavelas.org.br/forum-popular-de-seguranca-publica-e-lancado-no-rio-de-janeiro/>. Acesso em: ago. 2024.

17. Nesse sentido, também conclui Clarissa Nassar Tambelli: “Nesse sentido, é importante que as oportunidades de uma cidade inteligente não atropelem outras questões notáveis como a desigualdade social, os iletrados tecnológicos, as diferenças de acesso geracional e até mesmo por gênero. Pelo contrário, tais aspectos precisam ser levantados ao se pensar em uma solução que envolva a tecnologia, como também devem ser exploradas e aplicadas outras soluções, que não considerem apenas o uso dela.”. TAMBELLI, Clarice Nassar. *Smart Cities: uma breve investigação crítica sobre os limites de uma narrativa contemporânea sobre cidades e tecnologia*. Disponível em: https://itsrio.org/wp-content/uploads/2018/03/clarice_tambelli_smartcity.pdf. Acesso em: jul. 2024.

18. RODOTÁ, Stefano. *Corpo Eletrônico e Privacidade. Palestra-Aula apresentada na Universidade do Rio de Janeiro*, Rio de Janeiro, 06 de novembro de 2015.

de uma pessoa, gerando uma nova forma de vigilância que ameaça a privacidade e a dignidade humana. A vigilância massiva, exemplificada por câmeras de segurança que podem filmar uma pessoa centenas de vezes ao dia em grandes cidades, levanta questões sobre a expectativa de privacidade e o impacto dessas práticas sobre a vida pessoal e profissional dos indivíduos.

Diante disso, também observou Danilo Doneda:

A informação pessoal – que compreende toda informação que se refere a uma pessoa – assume, portanto, importância por pressupostos diversos. Podemos estabelecer, de início, dois fatores que estão quase sempre entre as justificativas para a utilização de informações pessoais: a eficiência e o controle. Uma série de interesses se articula em torno desses dois fatores, envolvendo o Estado como entes privados [...]¹⁹

A proteção dos dados emerge, portanto, como elemento fundamental no que se refere à temática em debate, singularmente considerando a referida era da informação. Conforme crescem os graus de exposição dos indivíduos e de sua sujeição a estruturas tecnológicas, pertencentes a Estados e grandes empresas, verifica-se a relevância de se desenvolverem não só instrumentos que coloquem os direitos à proteção de dados e à privacidade em posição de preeminência, em face de situação estritamente patrimoniais²⁰, mas também oferecer ferramentas a nível de conhecimento e informação aos cidadãos – especialmente aqueles pertencentes a grupos mais vulneráveis historicamente. Isso independentemente também de muní-los para que tenham consciência política, a fim de possivelmente questionarem determinados tipos de políticas públicas empregadas com fulcro apenas na supremacia do interesse público, a exemplo do emprego de tecnologias de reconhecimento facial na segurança pública.

Importante registrar também que o direito à privacidade, não obstante ao fato de ter surgido, em tese, como um desejo pelo isolamento (fora do contexto brasileiro e do sul global, diga-se), passa a não ser só um desejo, mas um direito oponível a terceiros, a partir do final do século XIX, com a consagração das Revoluções Burguesas, a partir ainda do artigo *The Right to Privacy*, em 15 de dezembro de 1980, desenvolvido respectivamente por Samuel Warren e

19. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: Fundamentos da Lei Geral de Proteção de Dados [e-book]*. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019. p 33.

20. TEFFÉ, Chiara Spadaccini de. *Dados pessoais sensíveis: qualificação, tratamento e boas práticas*. 1. ed. Indaiatuba, SP: Foco, 2022. E-book.

Louis Brandeis²¹. Essa foi a primeira construção jurídica sobre esse direito no globo. A privacidade nasce como um direito individualista, mas, atualmente, quando migra para um ecossistema baseado em dados pessoais, conecta as pessoas à sociedade, necessitando, ainda, de um regime seguro para que isso aconteça sem danos.

Em suma, a privacidade e a proteção de dados tem ordens diferentes, mas estão interligadas. A proteção de dados não substitui a privacidade, mas a complementa. Por tais motivos é que se encontram cristalizadas em nossa Carta Maior²², a qual tutela a intimidade e a vida privada como direitos fundamentais na forma do art. 5º, X, além do próprio direito a proteção de dados, inclusive em meios digitais, conforme dispõe o art. 5º, inciso LXXIX, também da CRFB/88, sendo esta última normativa inserida em um contexto mais recente, através da Emenda Constitucional nº 115, de 2022.

Além disso, surge a Lei Geral de Proteção de Dados, primeira normativa e também a mais específica que versa sobre a proteção de dados pessoais que foi aprovada no ano de 2018, na forma da Lei nº 13.709, de 14 de agosto de 2018 e com entrada em vigor em 18 de setembro de 2020²³. A normativa desponta em um cenário no qual se busca definir diretrizes para a consolidação da regulação de um ecossistema de proteção dos direitos à privacidade e de dados pessoais. A referida lei visa também, dentre outros objetivos, (i) garantir a igualdade material e a liberdade das pessoas naturais; (ii) assegurar o livre desenvolvimento da personalidade do ser humano; (iii) impedir discriminações ilícitas e/ou abusivas; (iv) evitar que determinados grupos sofram restrições indevidas a bens e cenários de preconceito e estigmatização.

Tal contextualização é imprescindível para que não se compreenda o modelo de *Smart Cities* como um fenômeno isolado de outros, como aparente simbolismo do progresso, principalmente quando analisada sob o aspecto da segurança pública em um território tão acidentado quanto o brasileiro, sobre-

21. Samuel Warren e Louis Brandeis, “*The right to privacy*”, in: 4 Harvard Law Review 193 (1890).

22. Nesse aspecto, no que concerne a prevalência da sistemática do direito civil-constitucional, no que se refere ao viés protetivo ao ser humano na controvérsia não só entre particulares, mas também desses com o próprio Estado, conforme os ensinamentos da obra coletiva organizada pelos mestres Anderson Schreiber e Carlos Nelson Konder: “Vale dizer são as normas constitucionais que devem guiar o processo hermenêutico, de modo que não cabe às partes optar pela fonte prevalente. Esta prevalência será fruto da interpretação da Constituição Federal e da legislação ordinária à sua luz.”. SOARES, Felipe Ramos Ribas; MATIELI, Louise Vago; DUARTE, Luciana da Mota Gomes de Souza. *Unidade do ordenamento na pluralidade das fontes: uma crítica à teoria dos microssistemas*. In: SCHREIBER, Anderson; KONDER, Carlos Nelson (Coords.). *Direito civil constitucional*. e-book. São Paulo: Atlas, 2016. p.79.

23. No entanto, como leciona Chiara de Teffé, a tutela dos direitos concernentes à proteção de dados era pleiteada com base em determinadas previsões estabelecidas, para além da Constituição Federal, em algumas normas setoriais, que direta ou indiretamente tratam de questões relacionadas tanto a privacidade quanto dos dados pessoais, em si, como por exemplo o Código de Defesa do Consumidor (Lei nº 8.078/90), o Marco Civil da Internet (Lei nº 12.965/14), para além da Lei de Acesso à Informação (Lei nº 12.527/11) e a Lei do Cadastro Positivo (Lei nº 12.414/11). Todavia, esse arcabouço regulatório mostrava-se pouco preciso e não oferecia garantias adequadas às pessoas (...). TEFFÉ, Chiara Spadaccini de. *Dados pessoais sensíveis: qualificação, tratamento e boas práticas*. 1. ed. Indaiatuba, SP: Foco, 2022. E-book.

tudo porque deve se considerar o valor inestimável do direito à privacidade e proteção de dados como fundamentais e inerentes aos cidadãos. A ideia de progresso trazida por aquela dinâmica passa a ser vista como relativa diante disso.

Em estudo que resultou do projeto de pesquisa do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas, ligada ao curso de Direito no Estado do Rio de Janeiro (CTS-FGV)²⁴, realizado entre 2017 e 2019 em três cidades brasileiras: Salvador, Rio de Janeiro e Campinas, três pesquisadores examinaram tanto o escopo, quanto a escala de práticas de vigilância estatais associadas à segurança pública no Brasil, a partir da observação de três ferramentas de videovigilância – reconhecimento facial, reconhecimento automático de placas e câmeras. Ao final, constataram que: o entusiasmo pela incorporação de novas tecnologias ao portfólio de autoridades estatais não necessariamente se traduz em avanços na segurança pública; depois, que as limitações materiais e de recursos humanos podem levar à discriminação de pessoas e grupos já tradicionalmente perseguidos por autoridades policiais, particularmente negros e pobres, que circulam em espaços onde essas tecnologias estão em pleno funcionamento; e que dessa forma, em vez de ampliada, a segurança dos cidadãos é potencialmente ameaçada pelo aumento da repressão a direitos fundamentais.²⁵

As reflexões de Stefano Rodotà e, posteriormente, as de Danilo Doneda trazem à tona questões cruciais sobre a transformação do conceito de corpo e privacidade na era digital. A noção de “corpo eletrônico” revela como a individualidade está cada vez mais sujeita à manipulação de dados, representando uma ameaça à privacidade, à proteção de dados e à própria dignidade humana. Os referidos autores alertam para a necessidade de um arcabouço jurídico que proteja a integridade dos dados pessoais, mas adicionalmente a isso, é crucial oferecer ferramentas que também busquem empoderar os cidadãos com conhecimento e instrumentos para defender seus direitos em um cenário de vigilância crescente em oposição tanto aos particulares, quanto ao próprio Estado. Ressalta-se, nesse ponto, a incessante contribuição das Organizações da Sociedade Civil para fazer valer os direitos mais básicos dos cidadãos brasileiros.

24. Ver mais em: <https://diretorio.fgv.br/pesquisa/centro-de-tecnologia-e-sociedade>.

25. REIA, Jess; BELLI, Luca. *Smart Cities no Brasil: regulação, tecnologia e direitos*. Belo Horizonte, MG : Casa do Direito, 2021. p.112. Disponível em: <https://repositorio.fgv.br/server/api/core/bitstreams/390c1729-357b-4c4f-ba30-e236419debf1/content>. Acesso em: jul. 2024.

A LGPD emerge como uma resposta impreterível para regular a utilização de informações pessoais, garantindo a liberdade e igualdade material dos indivíduos em face do aporte sem precedentes nos modelos de *Smart Cities*. Para que haja uma efetiva proteção de dados, vale pensar numa perspectiva mais prática em que se considere a participação cidadã, em uma ótica na qual se possa co-construir, ou seja, não apenas construir em relação ao outro, devemos nos colocar como parte do problema para gerar uma solução efetiva, dentro da realidade da conexão direta com os anseios de políticas sociais mais latentes em respeito aos direitos básico-fundamentais. Inclusive, esse elemento de participação é que tem o potencial de conferir cidadania de modo mais concreto, garantindo o protagonismo a um grupo sub-representado dentro do modelo democrático ao qual estamos inseridos.

Essa abordagem é primordial para garantir que as inovações tecnológicas não escalem desigualdades, mas promovam um desenvolvimento urbano inclusivo que respeite a dignidade humana.

3. Do Colonialismo à Era Digital: A Persistência da Vigilância e do Controle Social no Brasil

Uma análise da história brasileira, desde a chegada dos portugueses, em 1500²⁶, até o “fim” da escravidão, com a assinatura da Lei Áurea, nos demonstra que até hoje ainda encontramos políticas que refletem aspectos dessa época. Apesar dos significativos avanços jurídicos e sociais, o controle, vigilância e genocídio de vidas e corpos de pessoas negras e periféricas, ainda é uma tônica da organização estatal mais recente²⁷.

Não por acaso, é o próprio Estado quem define quais bens jurídicos recebem maior ou menor grau de tutela, algo que reflete diretamente na definição de políticas públicas. Nesse sentido, tende a privilegiar indivíduos integrantes das classes dominantes e com maiores possibilidades e oportunidades de acúmulo de capital, “dando a máxima ênfase à proteção do patrimônio privado

26. Cf. <https://brasil500anos.ibge.gov.br/>.

27. Exemplo disso, foi a reafirmação da institucionalização da política propagada e executada pelo ex-Governador, também impeachado no Rio de Janeiro, Wilson Witzel, sob as diretrizes do “mirar na cabecinha”. Isso, ao passo que desde sua eleição, em 2018, o número de operações policiais nas favelas do RJ também cresceram indiscriminadamente sob o Governo de seu sucessor Cláudio Castro, o qual também investiu massivamente em tecnologias de reconhecimento facial, sem qualquer avaliação de impacto dessa medida, não se levando em conta ainda aspectos estruturais do território, sendo posto que o que mais se pode observar, foram balas e mais balas “perdidas” nas pessoas pertencentes às comunidades cariocas, a exemplo da chacina ocorrida na favela do Jacarezinho ocorrida em 6 de maio de 2021, que resultou em um total de 28 pessoas mortas, incluindo um policial. Ao não tutelar as vidas, de fato, o Estado já está falhando profundamente, diga-se, tendo em visto que não houve melhorias significativas nos índices de segurança pública do estado do Rio de Janeiro. MENA, Fernanda. ‘Mirar na cabecinha’ é errar o alvo. *Folha de São Paulo*. 7 nov, 2018. Disponível em: <https://www1.folha.uol.com.br/colunas/fernanda-mena/2018/11/mirar-na-cabecinha-e-errar-o-alvo.shtml>. Acesso em: ago. 2024.

para atingir as formas de desvio típicas dos grupos socialmente mais débeis e marginalizados”^{28 29}. No entanto, nesse aspecto, tal ator não leva em consideração tais processos sociais que são inerentes à sua história.

Achille Mbembe tem significativa contribuição com essa literatura diante da construção do conceito da necropolítica, que se consubstancia na ideia de que a soberania é a faculdade de exercer controle sobre a mortalidade e definir a vida como a implantação e manifestação de poder³⁰, pensando inicialmente na atuação do Estado. Levando-se em conta que dados também estão em um espectro da relação de poder, os modelos de *Smart Cities*, quando pensados sem a participação cidadã, estão basicamente expressando um ato de poder, unicamente, servindo de ferramenta de automatização de opressões sistemáticas, sendo ainda prejudicial àqueles que historicamente já não usufruem plenamente de seus direitos fundamentais e que também tradicionalmente foram subjugados e controlados.

O poder social e político do Estado para ditar como algumas pessoas podem viver e como outras devem morrer, um dos aspectos do conceito da necropolítica de Mbembe, leva-nos a considerar não só a morte de corpos, em si, do ponto de vista biológico, fato que por si só, é de extrema relevância. Há também, atos que desumanizam, silenciam e cerceiam direitos fundamentais³¹, como a privacidade e proteção de dados, em atos explicados pelo racismo estrutural, sendo propagados pelos modelos de *Smart Cities*, levando pessoas negras a terem suas “mortes em vida”, em analogia ao que Mbembe também entende por “matanças invisíveis”³².

28. BARATTA, Alessandro. *Criminologia crítica e crítica do direito penal: introdução à sociologia do direito*. Tradução de Juarez Cirino dos Santos. Rio de Janeiro: Instituto Carioca de Criminologia/Revan, 3a ed., 2002. p. 176.

29. Instituições do Estado se valem de dados como o uso de publicações em redes sociais como estopim para inquéritos que culminam em operações policiais, a exemplo da Chacina do Jacarezinho ocorrida em 6 de maio de 2021 na cidade do Rio de Janeiro. Evento que é tido como o mais letal da história do Rio de Janeiro, dado por uma operação policial que resultou na morte de 28 pessoas, incluindo 1 policial. Essa ação levantou várias suspeitas de ilegalidades e violações de direitos humanos e, apesar da gravidade e da consequente necessidade de transparência no caso, o relatório da operação foi colocado sob sigilo de cinco anos. Cf. BARREIRA, Gabriel; BRASIL, Filipe. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2021/05/06/operacao-no-jacarezinho-rio-tem-numero-recorde-de-mortes.ghtml>. Acesso em julho de 2024. Cf. NUNES, Pablo; SILVA, Mariah Rafaela; OLIVEIRA, Samuel R. de. *Um Rio de câmeras com olhos seletivos: uso do reconhecimento facial pela polícia fluminense*. Rio de Janeiro: CeSec, 2022, p. 14. Disponível em: https://cesecseguranca.com.br/wp-content/uploads/2022/05/PANOPT_riodecameras_mar22_0404b.pdf. Acesso em agosto de 2024.

30. MBEMBE, Achille. *Necropolítica. Biopoder, soberania, estado de exceção, política da morte (ebook)*. São Paulo: N-1 edições, 2018. p.7.

31. Nesse sentido, vale registrar o depoimento de João Antônio, jovem negro, torcedor que sofreu vasto constrangimento, que jamais deve ser naturalizado, ao ser detido em um estádio de futebol em Sergipe, após “falha” no sistema de reconhecimento policial utilizado pela polícia: “Na final do Campeonato Sergipano passei uma uma situação que nunca imaginei que fosse possível e venho com vergonha e indignação compartilhar para que algo aconteça e isso não se repita. Fiquei altamente constrangido, tentando esconder meu rosto, não sabia o que fazer pois tava a torcida do Confiança inteira me olhando, conhecidos e desconhecidos”. Após o incidente, o governo de Sergipe suspendeu o uso do sistema, e anunciou que vai revisar as abordagens, para evitar constrangimentos como os de João Antônio. Torcedor é detido por engano em Sergipe após falha da ferramenta de reconhecimento facial. *O Dia*, Rio de Janeiro, 28 abr. 2024. Disponível em: <https://odia.ig.com.br/esporte/2024/04/6828699-torcedor-e-detido-por-engano-em-sergipe-apos-falha-da-ferramenta-de-reconhecimento-facial.html>. Acesso em: ago. 2024.

32. MBEMBE, Achille. *Necropolítica. Biopoder, soberania, estado de exceção, política da morte (ebook)*. São Paulo: N-1 edições, 2018. p. 38.

Inclusive, esta é uma considerável preocupação da Autoridade Nacional de Proteção de Dados (ANPD) – órgão responsável pela fiscalização e regulação da LGPD, e que também é um aliado na luta pela efetividade da consecução do gozo plena dos direitos à privacidade e proteção de dados dos cidadãos brasileiros:

Dados coletados por governos e empresas em diversas instâncias das cidades podem gerar informações, categorizações e relatórios detalhados sobre a vida pessoal dos residentes, agravando a assimetria de informações e poder.³³

Diante do cenário exposto, nota-se a importância do investimento na educação, direito que funciona como um aspecto fundamental para o desenvolvimento social. A não observância desse quesito, em vista disso, segundo o patrono da educação brasileira, Paulo Freire, contribui para a manutenção das estruturas opressoras, fundada em uma ordem injusta e também responsável pela violência àqueles indivíduos historicamente vulnerabilizados e que, não à toa, habitam as comunidades e periferias da cidade. Fato que encandece ainda mais as desigualdades sociais.³⁴

Não obstante, é urgente garantir a participação cidadã nos processos de tomada de decisão, seja a partir de consultas públicas, avaliação de impacto, nos quais, via de regra, as Organizações da Sociedade Civil (como algumas aqui referenciadas) têm contribuído significativamente com base em suas pesquisas metodológicas para avaliar os impactos da inserção de um modelo de vigilância extrema. Por outro lado, vale também pensar acerca da ausência de diversidade no que tange a composição que abrange os tomadores de decisão, perpassando por setores desde os governos até as instituições da sociedade e empresas³⁵. Tal quesito é fundamental para que se possa construir uma cultura que promova um maior diálogo entre diferentes grupos sociais e suas múltiplas facetas, principalmente para se ter um olhar de fato humanizado para as populações mais vulnerabilizadas, igualmente titulares de dados.

Considerações Finais

33. GOB.BR AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Cidades Inteligentes. Disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/publicacao_radar_tecnologico_jan_2024.pdf. Acesso em julho de 2024.

34. FREIRE, Paulo. *Pedagogia do Oprimido*. 78. ed. Rio de Janeiro: Paz e Terra, 2021.

35. Apesar disso, cita-se pesquisa Desigualdades sociais por cor ou raça no Brasil, realizada pelo IBGE, a qual identificou que 69% dos cargos gerenciais no país são ocupados por pessoas brancas, enquanto apenas 29,5% são ocupados por pessoas pretas ou pardas. Cf. IBGE – Instituto Brasileiro de Geografia e Estatística, 2022 (Segunda Edição). Desigualdades sociais por cor ou raça no Brasil. Disponível em: https://static.poder360.com.br/2022/11/IBGE-DESIGUALDADES-11.NV_.pdf. Acesso em agosto de 2024.

A crescente urbanização e digitalização das cidades, sob o rótulo do modelo *Smart Cities*, promete melhorias significativas na qualidade de vida por meio da aplicação de tecnologias avançadas. No entanto, a realidade enfrentada por diversas cidades brasileiras revela uma complexa teia de desigualdades sociais e econômicas que não pode ser ignorada na importação e implementação dessas tecnologias, sob pena de automatizarmos (ainda mais) opressões históricas.

Nesta obra, discutimos como o avanço das Cidades Inteligentes pode tanto reforçar quanto atenuar desigualdades sociais existentes, a depender da contextualização do cenário histórico-social do território e do setor da economia ao qual será empregado os insumos tecnológicos, em especial a segurança pública. A importância da participação cidadã é substancial: sem a inclusão ativa de todas as vozes, especialmente das comunidades e grupos marginalizados, as inovações tecnológicas correm o risco de perpetuar práticas de exclusão histórica e discriminação. Como evidenciado pela análise do conceito de necropolítica de Achille Mbembe, a tecnologia pode ser utilizada como ferramenta de extrema vigilância, controle social, morte biológica e “em vida” agravando a vulnerabilidade das populações que já enfrentam opressões sistêmicas.

A tutela dos direitos à privacidade e dos dados pessoais emergem como um pilar central na discussão sobre direitos fundamentais na era da informação. A LGPD representa, no Brasil, um avanço significativo na regulamentação do tratamento de dados pessoais, buscando garantir a privacidade e a autonomia dos indivíduos. No entanto, a efetiva implementação dessas proteções depende também de uma conscientização abrangente e do fortalecimento de uma cultura de proteção de dados, que deve ser amplamente acessível a todos os cidadãos, independentemente de seu contexto socioeconômico.

O modelo de *Smart Cities*, se implementado sem uma estrutura de governança inclusiva, pode amplificar desigualdades preexistentes, transformando-se em mais uma camada de controle social. Para que as cidades inteligentes realmente contribuam para um futuro mais justo e equitativo, é essencial integrar políticas que promovam a equidade digital, a justiça social e racial, assegurando que todas as comunidades tenham acesso igualitário aos benefícios oferecidos pela tecnologia, desde que esta seja centrada no ser humano.

Finalmente, é crucial que o desenvolvimento de cidades inteligentes seja guiado por princípios de transparência, inclusão e respeito aos direitos fundamentais. A participação cidadã não deve ser apenas um componente adicional,

mas sim a base sobre a qual as políticas de urbanização e digitalização devem ser construídas. Somente através de uma abordagem verdadeiramente participativa poderemos avançar para cidades que não apenas utilizem tecnologia para inovar, mas também para promover a dignidade e o bem-viver de todos os seus habitantes.

Referências

BARATTA, Alessandro. *Criminologia crítica e crítica do direito penal: introdução à sociologia do direito*. Tradução de Juarez Cirino dos Santos. Rio de Janeiro: Instituto Carioca de Criminologia/Revan, 3a ed., 2002. p. 176.

BARREIRA, Gabriel; BRASIL, Filipe. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2021/05/06/operacao-no-jacarezinho-rio-tem-numero-recorde-de-mortes.ghtml>. Acesso em: jul. 2024.

BOLLA, Carla. Como a França popularizou o uso de talheres. *Forbes*. 15 set, 2022. Disponível em: <https://forbes.com.br/forbeslife/2022/09/carla-bolla-como-a-franca-popularizou-o-uso-de-talheres/> Acesso em: jul. 2024.

BRASIL: 500 anos de Povoamento. Instituto Brasileiro de Geografia Estatística (IBGE). Disponível em: <https://brasil500anos.ibge.gov.br/>.

CAMARGO, Bianca. Cerca de 84% dos lares brasileiros têm acesso à internet, diz pesquisa. *CNN*, São Paulo, 16 nov, 2023. Disponível em: <https://www.cnnbrasil.com.br/nacional/cerca-de-84-dos-lares-brasileiros-tem-acesso-a-internet-diz-pesquisa/>. Acesso em: ago. 2024.

CENTRO DE TECNOLOGIA E SOCIEDADE. Disponível em: <https://diretorio.fgv.br/pesquisa/centro-de-tecnologia-e-sociedade>.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: Fundamentos da Lei Geral de Proteção de Dados [e-book]*. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019. p 33.

FREIRE, Paulo. *Pedagogia do Oprimido*. 78. ed. Rio de Janeiro: Paz e Terra, 2021.

GOB.BR. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Cidades Inteligentes. Disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/publicacao_radar_tecnologico_jan_2024.pdf. Acesso em: jul. 2024.

Instituto de Tecnologia e Sociedade do Rio de Janeiro do Rio. *Big data no Sul Global. Relatório sobre estudos de caso*. Instituto de Tecnologia & Sociedade do Rio. Rio de Janeiro, 2016. Disponível em: https://itsrio.org/wp-content/uploads/2017/02/ITS_Big-Data_PT-BR_v4.pdf. Acesso em: jul. 2024.

Instituto Brasileiro de Geografia e Estatística, 2022 (Segunda Edição). Desigualdades sociais por cor ou raça no Brasil. Disponível em: https://static.poder360.com.br/2022/11/IBGE-DESIGUALDADES-11.NV_.pdf. Acesso em: ago. 2024.

MBEMBE, Achille. *Necropolítica. Biopoder, soberania, estado de exceção, política da morte (ebook)*. São Paulo: N-1 edições, 2018. p.7.

MENA, Fernanda. 'Mirar na cabecinha' é errar o alvo. *Folha de São Paulo*. 7 nov, 2018. Disponível em: <https://www1.folha.uol.com.br/colunas/fernanda-mena/2018/11/mirar-na-cabecinha-e-errar-o-alvo.shtml> Acesso em: ago. 2024.

MENDES, Teresa Cristina M. *Smart Cities: Solução para as cidades ou aprofundamento das desigualdades sociais?*. Rio de Janeiro, 2020. Disponível em: https://www.observatoriodasmotropoles.net.br/wp-content/uploads/2020/01/TD-011-2020_Teresa-Mendes_Final.pdf Acesso em: jul. 2024.

MOURA, Clóvis. *Escravidão, colonialismo, imperialismo e racismo*. Afro-Ásia, Salvador, n. 14, 1983. Disponível em: <https://periodicos.ufba.br/index.php/afroasia/article/view/20824/13425>. Acesso em: jul. 2024.

NUNES, Pablo; SILVA, Mariah Rafaela; OLIVEIRA, Samuel R. de. *Um Rio de câmeras com olhos seletivos: uso do reconhecimento facial pela polícia fluminense*. Rio de Janeiro: CeSec, 2022, p. 14. Disponível em: https://cesecseguranca.com.br/wp-content/uploads/2022/05/PANOPT_riodecameras_mar22_0404b.pdf. Acesso em: ago. 2024.

O Dia, Rio de Janeiro, 28 abr. 2024. Disponível em: <https://odia.ig.com.br/esporte/2024/04/6828699-torcedor-e-detido-por-engano-em-sergipe-apos-falha-da-ferramenta-de-reconhecimento-facial.html>. Acesso em: ago. 2024.

PROJETO DE LEI Nº 976/2021. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1977843&filename=PL%20976/2021. Acesso em: jul. 2024.

REIA, Jess; BELLI, Luca. *Smart Cities no Brasil: regulação, tecnologia e direitos*. Belo Horizonte, MG: Casa do Direito, 2021. p.112. Disponível em: <https://repositorio.fgv.br/server/api/core/bitstreams/390c1729-357b-4c4f-ba30-e236419debf1/content>. Acesso em: jul. 2024.

RIBEIRO, Laura Talho. *Tecnologias inteligentes de vigilância: percepções sobre segurança nos centros urbanos*. Disponível em: https://itsrio.org/wp-content/uploads/2018/03/laura_talho_smart-surveillance.pdf. Acesso em: jul. 2024.

RODOTÁ, Stefano. *Corpo Eletrônico e Privacidade. Palestra-Aula apresentada na Universidade do Rio de Janeiro*, Rio de Janeiro, 06 de novembro de 2015.

SANTO, Thaís Espírito. RJ anuncia câmeras com reconhecimento facial e leitura de placas em viaturas da PM. *G1*, Rio de Janeiro, 03 abril, 2021. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2024/04/03/rj-anuncia-cameras-com-reconhecimento-facial-e-leitura-de-placas-em-viaturas-da-pm.ghtml> Acesso em: jul. 2024.

Samuel Warren e Louis Brandeis, “*The right to privacy*”, in: 4 Harvard Law Review 193 (1890).

SOARES, Felipe Ramos Ribas; MATIELI, Louise Vago; DUARTE, Luciana da Mota Gomes de Souza. Unidade do ordenamento na pluralidade das fontes: uma crítica à teoria dos microsistemas. In: SCHREIBER, Anderson; KONDER, Carlos Nelson (Coords.). *Direito civil constitucional*. e-book. São Paulo: Atlas, 2016.

SILVA, Tarcízio. *Racismo algorítmico: inteligência artificial e discriminação nas redes digitais*. São Paulo: Edições Sesc São Paulo, 2022.

TAMBELLI, Clarice Nassar. *Smart Cities: uma breve investigação crítica sobre os limites de uma narrativa contemporânea sobre cidades e tecnologia*. Disponível em: https://itsrio.org/wp-content/uploads/2018/03/clarice_tambelli_smartcity.pdf. Acesso em: jul. 2024.

TEFFÉ, Chiara Spadaccini de. *Dados pessoais sensíveis: qualificação, tratamento e boas práticas*. 1. ed. Indaiatuba, SP: Foco, 2022. E-book.

VELLASCO, Ramon. Fórum Popular de Segurança Pública é lançado no Rio de Janeiro. *Observatório de Favelas*. Rio de Janeiro. 29 jun, 2023. Disponível em: <https://observatoriodefavelas.org.br/forum-popular-de-seguranca-publica-e-lancado-no-rio-de-janeiro/>. Acesso em: ago. 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

12

Implementação de cidades inteligentes e sandbox regulatório: Desafios e oportunidades na lei de inovação de Juiz de Fora

DANIEL SANTIAGO DINIZ

Sumário: Introdução. 1. História, Tecnologia e Governança nas Cidades Inteligentes. 2. Bases Legislativas para Inovação no Brasil. 3. A Lei de Inovação de Juiz de Fora: Estrutura, Mecanismos e Impactos. 4. Implementação e Regulamentação do sandbox em Juiz de Fora. Considerações finais. Referências.

Introdução

O conceito de cidades inteligentes tem sido amplamente discutido nos últimos anos, destacando-se como uma solução promissora para os desafios urbanos contemporâneos. A utilização de tecnologias da informação e comunicação (TICs) para otimizar a eficiência dos serviços urbanos, melhorar a qualidade de vida dos cidadãos e promover o desenvolvimento sustentável são objetivos centrais dessas iniciativas. No entanto, a implementação prática desses conceitos varia significativamente, levando a debates sobre a verdadeira eficácia e inclusão dessas estratégias.

No Brasil, um conjunto de marcos legislativos e regulamentações estabelece as bases para o avanço tecnológico no ambiente urbano, com destaque para o Marco Legal da Inovação e o Marco Legal das Startups. Esses instrumentos legislativos promovem a criação de ecossistemas de inovação e experimentação em diferentes esferas governamentais, incentivando a cooperação entre o setor público e o privado. Nesse contexto, a Lei de Inovação de Juiz de Fora (Lei nº 14.746/2023) representa um exemplo de como uma cidade brasileira pode adaptar essas diretrizes nacionais para fomentar a inovação local, introduzindo mecanismos como o sandbox regulatório, um ambiente controlado onde é possível testar inovações em conformidade com a regulamentação específica municipal².

Este artigo busca responder à questão: “Como a Lei de Inovação de Juiz de Fora, por meio de seu arcabouço regulatório e do sandbox, implementa os princípios de cidades inteligentes, e quais são os desafios e as oportunidades dessa abordagem?”. Para isso, a estrutura do trabalho percorre desde as bases teóricas e históricas das cidades inteligentes, incluindo a visão crítica

1. Advogado e Gestor Público, formado em Direito pela Universidade Federal de Juiz de Fora (UFJF), pós-graduando em Direito Digital pela Universidade do Estado do Rio de Janeiro (UERJ) e Instituto de Tecnologia e Sociedade do Rio (ITS Rio)

2. JUIZ DE FORA. Lei nº 14.746, de 04 de dezembro de 2023. Institui o Sistema de Inovação de Juiz de Fora; define os polos de desenvolvimento do Município; dispõe sobre as atribuições do Conselho Municipal de Desenvolvimento, Tecnologia e Inovação (Comdeti) e dá outras providências. Diário Oficial do Município de Juiz de Fora, Juiz de Fora, MG, 05 dez. 2023.

de autores como Robert G. Hollands³, Evgeny Morozov e Francesca Bria⁴, até a análise das bases legislativas brasileiras que facilitam essa transformação urbana.

O estudo se aprofunda na Lei de Inovação de Juiz de Fora, examinando sua estrutura, mecanismos e impactos esperados, com atenção ao Decreto nº 16.734/2024⁵, que detalha o funcionamento do sandbox regulatório. A análise explora como a regulamentação busca equilibrar a inovação com a responsabilidade social, promovendo uma governança urbana alinhada com os interesses da comunidade. Por fim, nas considerações finais, são apresentados os principais achados e sugestões para aprimorar a aplicação dos conceitos de cidades inteligentes, enfatizando a importância de uma governança que sustente o desenvolvimento urbano justo, sustentável e inovador.

1. História, Tecnologia e Governança nas Cidades Inteligentes

As cidades inteligentes, conforme discutido por Robert G. Hollands⁶, são caracterizadas pela utilização de tecnologias da informação e comunicação (TICs) para melhorar a eficiência dos serviços urbanos e a qualidade de vida dos cidadãos. No entanto, Hollands argumenta que o conceito de cidades inteligentes é multifacetado e sujeito a diversas interpretações, o que pode levar a um entendimento superficial ou distorcido do que realmente constitui uma cidade inteligente. Ele destaca que o termo “smart” é frequentemente associado a inovações tecnológicas urbanas positivas, mas alerta que esse rótulo pode esconder problemas subjacentes e criar suposições não questionadas sobre o desenvolvimento urbano.

Uma das críticas centrais de Hollands é que o termo “smart cities” pode ser usado de forma retórica, sem uma definição precisa, levando à auto-congratulação e falta de questionamento crítico. Muitas cidades que se autodenominam inteligentes fazem isso como uma estratégia de marketing urbano, sem necessariamente implementar mudanças estruturais ou sustentáveis. Hollands questiona a suposição de que a tecnologia por si só pode resolver

3. HOLLANDS, Robert G. *Will the real smart city please stand up? Intelligent, progressive or entrepreneurial? City*, v. 12, n. 3, p. 303-320, 2008. DOI: 10.1080/13604810802479126.

4. MOROZOV, Evgeny; BRIA, Francesca. *A cidade inteligente: tecnologias urbanas e democracia*. Traduzido por Humberto do Amaral. São Paulo: Ubu Editora, 2019. 192 p. ISBN: 978-85-7126-046-7.

5. JUIZ DE FORA. Decreto nº 16.734, de 20 de agosto de 2024. Regulamenta o funcionamento do sandbox regulatório em Juiz de Fora e especifica as condições para sua implementação e supervisão. Diário Oficial do Município de Juiz de Fora, Juiz de Fora, MG, 21 ago. 2024.

6. HOLLANDS, Robert G. *Will the real smart city please stand up? Intelligent, progressive or entrepreneurial? City*, v. 12, n. 3, p. 303-320, 2008. DOI: 10.1080/13604810802479126.

problemas urbanos complexos e sugere que é necessário um entendimento mais profundo e crítico das implicações sociais e políticas das TICs nas cidades, enfatizando a importância de considerar a justiça social e a inclusão nas discussões sobre cidades inteligentes.

De acordo com a Organização para a Cooperação e Desenvolvimento Econômico (OCDE)⁷, as cidades inteligentes envolvem o uso eficaz da digitalização para aprimorar a qualidade de vida dos moradores, proporcionando serviços urbanos e ambientes mais eficientes, sustentáveis e inclusivos.

Morozov e Bria discutem as implicações sociais e democráticas das tecnologias urbanas⁸. Embora as TICs prometam tornar as cidades mais eficientes e seguras, há um risco significativo de que essas tecnologias sejam utilizadas para beneficiar principalmente interesses privados em vez de servir ao bem comum. Os autores destacam que a “smart city” muitas vezes se torna uma marca associada a serviços oferecidos por grandes empresas de tecnologia, como Google, IBM e Cisco, que priorizam a otimização e o controle em detrimento da participação cidadã e da justiça social.

A virada tecnológica promovida pelas grandes corporações transformou os dados em um elemento essencial da economia neoliberal. As cidades inteligentes, repletas de sensores e sistemas algorítmicos, tornam-se espaços de extração permanente de dados, controle e modulação de comportamentos. Para evitar que as cidades inteligentes se tornem máquinas de precarizar trabalhadores e beneficiar apenas interesses privados, Morozov e Bria propõem uma gestão cooperativa das tecnologias urbanas, que deve ser democrática e inclusiva, enfatizando a necessidade de retomar o controle sobre tecnologias, dados e infraestruturas para garantir uma governança que promova a participação cidadã e a equidade social.

A implementação de tecnologias urbanas, segundo Morozov e Bria, deve ser acompanhada por políticas que garantam a participação democrática e a inclusão social. Eles sugerem a criação de uma infraestrutura compartilhada e a promoção da soberania tecnológica, onde a governança dos dados e as práticas colaborativas são essenciais. Isso significa que as cidades devem adotar abordagens que permitam aos cidadãos deliberarem sobre o uso de seus dados e participar ativamente no desenvolvimento das tecnologias que moldam seu ambiente urbano.

7. OCDE. *Smart Cities and Inclusive Growth*. 2020. Disponível em: https://www.oecd.org/cfe/cities/OECD_Policy_Paper_Smart_Cities_and_Inclusive_Growth.pdf.

8. MOROZOV, Evgeny; BRIA, Francesca. *A cidade inteligente: tecnologias urbanas e democracia*. Traduzido por Humberto do Amaral. São Paulo: Ubu Editora, 2019. 192 p. ISBN: 978-85-7126-046-7.

Ao discutir as implicações sociais e democráticas das cidades inteligentes, é crucial reconhecer os desafios e as oportunidades que surgem com a transformação digital das cidades. Por um lado, há o potencial de melhorar significativamente a qualidade de vida urbana através da eficiência e da inovação. Por outro lado, há o risco de exacerbar desigualdades sociais e criar novas formas de exclusão, se a implementação dessas tecnologias não for cuidadosamente regulada e orientada para o bem comum. Portanto, a legislação inovadora desempenha um papel fundamental ao garantir que as cidades inteligentes não apenas utilizem tecnologias avançadas, mas também promovam um desenvolvimento urbano justo e inclusivo.

O desenvolvimento do governo eletrônico é uma parte crucial da evolução das cidades inteligentes. Segundo Jon Agar⁹, a história do governo eletrônico pode ser traçada desde os primeiros esforços para mecanizar e informatizar os processos governamentais. A integração de tecnologias de informação nos processos administrativos teve um impacto profundo na eficiência e na capacidade de resposta das instituições governamentais. A revolução do governo eletrônico começou com a introdução de tecnologias básicas de escritório, como máquinas de escrever e sistemas de arquivamento, e evoluiu para a implementação de computadores e redes digitais.

No contexto das cidades inteligentes, o governo eletrônico representa a aplicação de tecnologias digitais para melhorar a gestão urbana e a prestação de serviços públicos. Agar argumenta que a informatização do governo foi um passo crucial para a implementação de tecnologias inteligentes nas cidades, permitindo a automação de tarefas administrativas e a melhoria da comunicação entre diferentes departamentos governamentais. A introdução de sistemas computacionais nas administrações públicas transformou a forma como os dados são coletados, armazenados e utilizados, facilitando a tomada de decisões e a prestação de serviços mais eficientes e transparentes.

A interação entre tecnologia e governança é outro aspecto importante na evolução das cidades inteligentes. Eden Medina¹⁰ discute como a implementação de sistemas cibernéticos no Chile de Allende é um exemplo precoce de como a tecnologia pode ser integrada à governança urbana para criar cidades mais inteligentes. Durante o governo de Salvador Allende, foram implementados sistemas cibernéticos para gerenciar a economia nacional, uma tenta-

9. AGAR, Jon. *The Government Machine: a Revolutionary History of the Computer*. Cambridge, MA: MIT Press, 2003.

10. MEDINA, Eden. *Cybernetic Revolutionaries: Technology and Politics in Allende's Chile*. Cambridge: The MIT Press, 2011. ISBN: 978-0-262-01649-0.

tiva pioneira de utilizar tecnologias avançadas para melhorar a eficiência e a transparência da administração pública.

Medina enfatiza que a integração de tecnologias na governança urbana pode trazer benefícios significativos, como a melhoria da eficiência administrativa, a transparência nas operações governamentais e a participação cidadã. No entanto, também alerta para os desafios e riscos associados, como a centralização do poder e a potencial exclusão de grupos marginalizados. A experiência chilena demonstra a necessidade de uma abordagem equilibrada, onde a tecnologia seja utilizada para empoderar cidadãos e promover uma governança mais inclusiva e participativa.

A evolução do governo eletrônico e a interação entre tecnologia e governança ilustram como as cidades podem se tornar mais inteligentes e eficientes através da integração tecnológica. A história do governo eletrônico, conforme descrita por Agar, e o exemplo chileno de sistemas cibernéticos discutido por Medina, mostram que a implementação bem-sucedida de tecnologias nas cidades depende de uma abordagem que considere tanto os benefícios quanto os desafios dessas inovações.

Nesse contexto, a inclusão de sandboxes regulatórios representa um avanço significativo na abordagem experimentalista da administração pública para promover a inovação. Segundo Quirino, Hocayen e Cunha¹¹, o sandbox regulatório é um ambiente controlado onde normas aplicáveis a produtos ou serviços inovadores são temporariamente suspensas para testar seu impacto no mercado. Essa ferramenta permite que a administração pública local experimente e ajuste suas regulações com base em evidências, promovendo um desenvolvimento econômico mais alinhado com as necessidades locais.

O sandbox regulatório é uma ferramenta estratégica que permite à Administração Pública criar ambientes experimentais em que normas regulatórias são temporariamente flexibilizadas, facilitando o desenvolvimento e a testagem de produtos ou serviços inovadores sem as restrições impostas pelas regulamentações tradicionais. Segundo Quirino, Hocayen e Cunha, essa abordagem experimentalista é particularmente vantajosa para administrações locais, pois oferece um campo de testes seguro onde a Administração Pública pode observar os impactos das inovações em condições controladas e com supervisão contínua, promovendo um desenvolvimento econômico mais dinâmico e adaptado às necessidades específicas de cada localidade.

11. QUIRINO, Carina de Castro; HOCAYEN, Helena Gouvêa de Paula; CUNHA, Marcella Brandão Flores da. *Sandbox regulatório: instrumento experimentalista à disposição da Administração Pública local como suporte ao desenvolvimento econômico*. R. de Dir. Público da Economia – RDPE, Belo Horizonte, v. 21, n. 84, p. 9-33, out./dez. 2023.

O potencial de um sandbox regulatório se dá pela flexibilidade que oferece aos governos locais na implementação de tecnologias urbanas emergentes e na testagem de soluções inovadoras que podem transformar a administração pública e a vida nas cidades. No entanto, essa flexibilidade vem acompanhada de desafios consideráveis. Para que um sandbox regulatório cumpra seu papel de maneira efetiva, é essencial que haja uma colaboração interinstitucional sólida e que o ambiente regulatório experimental conte com uma governança abrangente e inclusiva. Isso significa que a participação de múltiplos setores, como transporte, segurança pública e infraestrutura digital, é imprescindível para integrar as inovações de forma harmoniosa às políticas urbanas e garantir que os resultados atendam aos objetivos coletivos.

Um desafio crítico para a implementação eficaz dos sandboxes regulatórios reside na definição de critérios e limites rigorosos para a participação das empresas. Sem uma regulamentação detalhada que estabeleça limites de atuação, há o risco de que o sandbox funcione mais como uma brecha regulatória do que como um espaço de experimentação responsável. Hollands e Morozov e Bria¹² alertam sobre esse risco, discutindo como, muitas vezes, o conceito de cidades inteligentes é utilizado de forma retórica, promovendo a tecnologia urbana sem uma análise profunda dos impactos sociais e da necessidade de inclusão. Eles destacam que, sem diretrizes claras, inovações urbanas podem acabar favorecendo grandes corporações, promovendo a extração de dados e o controle comportamental, em detrimento do bem-estar coletivo e da justiça social.

Além disso, a transparência no processo de seleção e acompanhamento das empresas participantes é fundamental. Os sandboxes regulatórios devem possuir diretrizes de supervisão e monitoramento, assegurando que as empresas cumpram com as responsabilidades estabelecidas e que os riscos emergentes sejam identificados e mitigados prontamente. Segundo Quirino et al., é necessário que o sandbox regulatório funcione como um campo de testes onde há um ciclo de feedback constante entre a Administração Pública e as empresas participantes, ajustando os regulamentos com base em dados reais e nas demandas sociais. A supervisão contínua é crucial para prevenir abusos e garantir que o sandbox contribua para a promoção de tecnologias urbanas de forma ética e inclusiva.

Outro ponto crítico para o sucesso dos sandboxes regulatórios é a adaptação às mudanças rápidas no contexto urbano e tecnológico. A abordagem experimental oferecida pelo sandbox permite que a Administração Pública ajus-

12. HOLLANDS, Robert G. *Will the real smart city please stand up? Intelligent, progressive or entrepreneurial? City*, v. 12, n. 3, p. 303-320, 2008; MOROZOV, Evgeny; BRIA, Francesca. *A cidade inteligente: tecnologias urbanas e democracia*. Traduzido por Humberto do Amaral. São Paulo: Ubu Editora, 2019.

te as normas conforme o desenvolvimento das tecnologias testadas, mas isso requer um compromisso com a governança adaptativa e a inovação responsável. Morozov e Bria defendem que a implementação de tecnologias urbanas deve ser acompanhada de mecanismos de soberania tecnológica, que garantam aos cidadãos o controle sobre seus dados e uma participação ativa na construção do ambiente urbano inteligente. Isso é especialmente importante em cidades inteligentes, onde a aplicação de novas tecnologias pode impactar diretamente a vida urbana e criar novos desafios éticos, sociais e políticos.

Em síntese, o sandbox regulatório é uma ferramenta com potencial para promover uma inovação urbana sustentável e inclusiva, ao oferecer um espaço controlado para que novas tecnologias sejam testadas e avaliadas antes de sua aplicação em larga escala. Os desafios de governança, definição de critérios e transparência na supervisão destacam a necessidade de uma abordagem cautelosa e de uma regulamentação robusta. Dessa forma, o sandbox regulatório não apenas permite a experimentação de soluções inovadoras, mas também contribui para uma administração pública mais responsiva e comprometida com a promoção de uma transformação digital ética e responsável.

2. Bases Legislativas para Inovação no Brasil

O Brasil, em resposta às crescentes demandas por desenvolvimento tecnológico e sustentabilidade, tem consolidado um arcabouço legislativo inovador que serve como base para o avanço da ciência, tecnologia e inovação em diversos níveis. Esse conjunto de normas, que chamamos de “bases legislativas para inovação no Brasil,” inclui marcos legais significativos e suas regulamentações específicas, como o Marco Legal da Inovação (Lei nº 13.243/2016)¹³, o Marco Legal das Startups (Lei Complementar nº 182/2021)¹⁴ e diretrizes estratégicas como a Carta Brasileira para Cidades Inteligentes¹⁵. Essas legislações e orientações são fundamentais para criar ambientes propícios ao desenvolvimento de ecossistemas inovadores, desde a esfera federal até o nível municipal.

O Marco Legal da Inovação, sancionado em 2016, aprimora a Lei de Inovação de 2004 (Lei nº 10.973/2004)¹⁶ ao estabelecer mecanismos para simplifi-

13. BRASIL. *Lei nº 13.243*, de 11 de janeiro de 2016. Dispõe sobre estímulos ao desenvolvimento científico, à pesquisa, à capacitação científica e tecnológica e à inovação, e altera diversas leis. *Diário Oficial da União*: seção 1, Brasília, DF, p. 1, 12 jan. 2016.

14. BRASIL. *Lei Complementar nº 182*, de 1º de junho de 2021. Institui o marco legal das startups e do empreendedorismo inovador e altera a Lei Complementar nº 123, de 14 de dezembro de 2006. *Diário Oficial da União*: seção 1, Brasília, DF, p. 2, 2 jun. 2021.

15. Ministério do Desenvolvimento Regional. *Carta Brasileira para Cidades Inteligentes*. Brasília, 2021.

16. BRASIL. *Lei nº 10.973*, de 2 de dezembro de 2004. Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, p. 2, 3 dez. 2004.

car a colaboração entre o setor privado e as instituições públicas de pesquisa, visando descentralizar o fomento à inovação para estados e municípios. Esse marco legal reformula nove leis federais e introduz medidas independentes que facilitam o desenvolvimento da ciência e tecnologia no país. O Decreto nº 9.283/2018¹⁷ complementa a regulamentação do Marco Legal da Inovação, instituindo incentivos como subvenções econômicas e encomendas tecnológicas, que fortalecem a transferência de tecnologias das Instituições Científicas, Tecnológicas e de Inovação (ICTs) para o mercado. Esse decreto permite que a administração pública direta e indireta, incluindo ICTs, participem minoritariamente do capital social de empresas inovadoras, fomentando a criação de produtos e processos inovadores.

A regulamentação também incentiva a cooperação entre entes públicos e privados para a execução de projetos de Pesquisa, Desenvolvimento e Inovação (PD&I), garantindo maior segurança jurídica nas parcerias e facilitando a implementação de políticas de inovação. Esta cooperação é exemplificada por programas de parceria público-privada que financiam projetos de energia renovável e tecnologias verdes.

Na temática da Internet das Coisas (IoT), a publicação do Decreto nº 9.854/2019¹⁸, que instituiu o “Plano Nacional de Internet das Coisas,” fez o país avançar no objetivo de implementar e desenvolver a IoT, promovendo a livre concorrência e a livre circulação de dados, respeitando as diretrizes de segurança da informação e proteção de dados pessoais. Este plano foi desenvolvido por meio de uma parceria entre o Ministério da Ciência, Tecnologia e Inovação e o Banco Nacional de Desenvolvimento Econômico e Social (BNDES), incentivando a criação de cidades inteligentes que utilizam sensores e redes IoT para melhorar serviços públicos como transporte e segurança.

A Lei Complementar nº 182/2021, conhecida como Marco Legal das Startups, complementa as iniciativas de inovação ao estabelecer um ambiente regulatório favorável para startups e empreendedores. Esta lei define diretrizes específicas para fomentar o ecossistema de startups no Brasil, incluindo a criação de ambientes regulatórios experimentais, conhecidos como sandboxes regulatórios, que permitem o teste de inovações com flexibilidade regulatória.

17. BRASIL. Decreto nº 9.283, de 7 de fevereiro de 2018. Regulamenta a Lei nº 10.973, de 2 de dezembro de 2004, e a Lei nº 13.243, de 11 de janeiro de 2016, sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo. *Diário Oficial da União*: seção 1, Brasília, DF, p. 1, 8 fev. 2018.

18. BRASIL. Decreto nº 9.854, de 25 de junho de 2019. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas. *Diário Oficial da União*: seção 1, Brasília, DF, p. 5, 26 jun. 2019.

Entre os principais pontos da Lei Complementar nº 182/2021 estão a definição clara do que constitui uma startup, facilitando o acesso a programas de incentivo e financiamento, o estabelecimento de mecanismos de contratação pública que favorecem a participação de startups, como a modalidade de contratação por meio de desafios tecnológicos, incentivos fiscais e acesso facilitado a investimentos para startups em estágios iniciais. A criação de sandboxes regulatórios permite a experimentação de novas tecnologias e modelos de negócios em um ambiente controlado, mitigando riscos regulatórios e promovendo a inovação. Um exemplo prático é o sandbox regulatório do Banco Central do Brasil, que permitiu que startups financeiras desenvolvessem e testassem novas soluções de pagamento digital¹⁹.

Em 2020, o Governo Federal lançou um guia essencial para o desenvolvimento urbano sustentável e inovador no Brasil, a Carta Brasileira para Cidades Inteligentes²⁰. Elaborada de forma colaborativa, a Carta busca integrar a transformação digital com o desenvolvimento urbano sustentável, abordando questões como redução de desigualdades, inclusão digital, governança urbana inovadora e desenvolvimento econômico local.

A Carta estabelece diretrizes fundamentais que orientam o desenvolvimento de cidades inteligentes. Entre essas diretrizes, destaca-se a importância de uma legislação específica que vise à implementação de tecnologias inteligentes nas cidades brasileiras. A legislação deve ser robusta e capaz de integrar as TICs de maneira que promovam a sustentabilidade, a inclusão social e a eficiência urbana.

A legislação desempenha um papel crucial na criação de um ambiente propício à adoção e ao desenvolvimento de tecnologias inteligentes. Ela fornece uma base legal necessária para que as cidades possam integrar TICs em seus processos urbanos, facilitando a gestão de recursos, a prestação de serviços públicos e a promoção da inclusão digital.

Para enfrentar os desafios urbanos e sociais, a Carta destaca que é fundamental que a transformação digital seja acompanhada por políticas públicas que garantam a equidade e a sustentabilidade. Isso inclui a promoção de acessibilidade à internet, a proteção de dados pessoais, a participação cidadã e a governança transparente. A Carta integra as agendas de desenvolvimento urbano e de transformação digital, para definir um conceito brasileiro para

19. AMATO, Lucas Fucci; MISSAGIA, Caio Rezende. Ambientes regulatórios experimentais: o sandbox no sistema financeiro brasileiro. *RBSD – Revista Brasileira de Sociologia do Direito*, v. 10, n. 3, p. 143-171, set./dez. 2023.

20. Ministério do Desenvolvimento Regional. *Carta Brasileira para Cidades Inteligentes*. Brasília, 2021.

idades inteligentes, apresentar uma agenda pública articulada e apoiar os municípios em suas ações locais.

Desde 2021, está em tramitação o Projeto de Lei (PL) nº 976, que visa instituir uma Política Nacional de Cidades Inteligentes (PNCI). Esse projeto visa melhorar a qualidade de vida nos municípios e estabelece os princípios e diretrizes que orientam essa política, além de definir seus objetivos, ações a serem realizadas e recursos alocáveis. O projeto foi enviado à Comissão de Constituição, Justiça e Cidadania da Câmara dos Deputados em 11 de julho de 2022, onde permanece aguardando parecer do relator.

Conforme a norma ABNT baseada na ISO 37122 (ABNT, 2021)²¹, uma cidade inteligente é definida como uma cidade que acelera a obtenção de resultados sustentáveis nos âmbitos social, econômico e ambiental. Além disso, melhora significativamente o engajamento social, aplica liderança colaborativa, integra disciplinas e sistemas municipais e utiliza dados e tecnologias modernas para oferecer melhores serviços e qualidade de vida aos seus habitantes (residentes, empresas e visitantes), tanto no presente quanto no futuro, evitando injustiças e a degradação ambiental.

São José dos Campos (SP) foi a primeira cidade a receber essa certificação, em 16 de março de 2022. Para obter a certificação, a cidade passou por um processo rigoroso que avaliou até 252 indicadores, entre eles sustentabilidade, mobilidade, saúde, educação e segurança pública.

A importância de uma legislação inovadora reside na sua capacidade de estabelecer um marco regulatório que não apenas apoie, mas também promova a transformação digital das cidades de maneira sustentável e inclusiva. O crescimento populacional global, especialmente nas áreas urbanas, traz desafios importantes nas esferas econômicas, sociais, organizacionais e estruturais. Nesse cenário, as cidades inteligentes serão fundamentais para resolver os diversos desafios e atender às demandas das grandes áreas urbanas.

Ao seguir as diretrizes previstas na Carta Brasileira para Cidades Inteligentes e nas legislações mencionadas, as cidades brasileiras podem se desenvolver de forma mais equilibrada, enfrentando os desafios do século XXI com soluções tecnológicas que melhoram a qualidade de vida de todos os cidadãos. Nesse contexto, destaca-se o papel das regulamentações municipais, como a Lei nº 14.746/2023 e o Decreto nº 16.734/2024, que atuam de maneira

21. ABNT NBR ISO 37122:2021. Cidades e comunidades sustentáveis – Indicadores para cidades inteligentes. Associação Brasileira de Normas Técnicas, 2021.

complementar aos marcos federais, promovendo um ecossistema de inovação local robusto e aplicando as diretrizes nacionais no nível municipal.

3. A Lei de Inovação de Juiz de Fora: Estrutura, Mecanismos e Impactos

A Lei nº 14.746/2023, que institui o Sistema de Inovação de Juiz de Fora, estabelece uma série de objetivos e diretrizes para promover a inovação tecnológica, o desenvolvimento sustentável e a competitividade econômica na cidade. Esta legislação visa criar um ambiente propício para o crescimento de startups, empresas tecnológicas e cooperativas de base tecnológica, fornecendo o suporte financeiro, estrutural e regulatório necessário para o desenvolvimento de novas tecnologias e modelos de negócios.

Entre os principais objetivos da lei, destaca-se a necessidade de estimular, organizar e apoiar ecossistemas e mecanismos de inovação em Juiz de Fora e região. A Lei nº 14.746/2023 foi regulamentada por três decretos principais: o Decreto nº 16.372/2024²², que dispõe sobre a composição e as atribuições do Conselho Municipal de Desenvolvimento, Tecnologia e Inovação (COMDETI); o Decreto nº 16.448/2024²³, que define as diretrizes para a criação e funcionamento do Sistema Municipal de Inovação (Simi-JF); e o Decreto nº 16.734/2024²⁴, que aborda aspectos complementares não previstos nos decretos anteriores, incluindo detalhes sobre fundos de coinvestimento, participação minoritária em sociedades de propósito específico, capital semente e o ambiente regulatório experimental do sandbox.

A missão da lei, conforme especificado no Art. 1º, é promover startups, empresas sustentáveis, negócios de baixo impacto socioambiental, redes de produção local e cooperativas de base tecnológica, com o objetivo de potencializar a competitividade, a cooperação e o crescimento dessas organizações, focando na geração de produtos, processos e serviços inovadores e na transferência e difusão de tecnologias.

Para alcançar esses objetivos, a lei institui o Sistema Municipal de Inovação de Juiz de Fora (Simi-JF) e o Fundo Municipal de Desenvolvimento da

22. JUIZ DE FORA. Decreto nº 16.372, de 30 de janeiro de 2024. Regulamenta os arts. 39, 40 e 41 da Lei Municipal nº 14.746, de 04 de dezembro de 2023, que dispõem sobre a composição e atribuições do Conselho Municipal de Desenvolvimento, Tecnologia e Inovação (COMDETI) e dá outras providências. *Diário Oficial do Município de Juiz de Fora*, Juiz de Fora, MG, 31 jan. 2024.

23. JUIZ DE FORA. Decreto nº 16.448, de 11 de março de 2024. Regulamenta os arts. 1º, 2º (inciso I) e 6º da Lei Municipal nº 14.746, de 04 de dezembro de 2023, que dispõem sobre a criação, composição e finalidades do Sistema Municipal de Inovação em Juiz de Fora. *Diário Oficial do Município de Juiz de Fora*, Juiz de Fora, MG, 12 mar. 2024.

24. JUIZ DE FORA. Decreto nº 16.734, de 11 de setembro de 2024. Dispõe sobre o sistema de inovação do município e outras providências. *Diário Oficial do Município de Juiz de Fora*, Juiz de Fora, MG, 12 set. 2024.

Inovação (FMDI) como principais instrumentos de suporte, conforme detalhado no Art. 2º. Esses mecanismos são fundamentais para fornecer suporte financeiro e estrutural às iniciativas de inovação, garantindo que os projetos tenham os recursos necessários para seu desenvolvimento e implementação. A capacitação e a inclusão social também são prioridades da lei, com o Art. 3º enfatizando a importância de dotar o sistema produtivo municipal com recursos humanos adicionais e tecnologias específicas. Além disso, a lei visa atender a programas e projetos que promovam a inovação, a inclusão social, a energia renovável, a preservação ambiental e a mitigação de impactos socioambientais, fomentando modelos de cidades sustentáveis.

O FMDI, conforme previsto no Art. 2º, II, é um instrumento financeiro fundamental para apoiar projetos de inovação no município. Este fundo é destinado a atender projetos de fomento à ciência, tecnologia e inovação, fornecendo recursos para o desenvolvimento de novos produtos, processos e serviços inovadores. Os recursos do FMDI são utilizados para subsidiar bônus tecnológicos, bolsas de pesquisa em inovação, encomendas tecnológicas, aquisição de sistemas de gestão inovadores, projetos de capacitação científico-tecnológica, e organização e participação em eventos relacionados à ciência, tecnologia e inovação, conforme art. 21.

A Lei introduz a possibilidade de participação da Prefeitura de Juiz de Fora e suas autarquias, fundações e empresas controladas em fundos de investimento e sociedades de propósito específico. Esses fundos são registrados na Comissão de Valores Mobiliários (CVM) e têm como objetivo apoiar empresas inovadoras, principalmente aquelas com sede em Juiz de Fora e com foco em tecnologia. A legislação permite a participação minoritária do capital social de sociedades de propósito específico e cooperativas de base tecnológica, ampliando o suporte ao desenvolvimento de projetos científicos e tecnológicos no município, conforme especificado no Art. 4º da lei. Esse mecanismo possibilita um alinhamento com as prioridades estratégicas de inovação da cidade, favorecendo uma conexão mais sólida entre o setor público e o setor privado.

Além dos fundos de investimento, a Lei regulamenta a possibilidade de aporte de capital semente para empresas inovadoras realizadas em parceria com Instituições de Ciência, Tecnologia e Inovação (ICTs), seguindo diretrizes financeiras e de impacto tecnológico. Esse capital é direcionado para empresas formalmente incluídas em áreas estratégicas de inovação, que apresentam um plano de negócios robusto e alinhado com as prioridades econômicas e sociais do município. A gestão e acompanhamento desses fundos e a partici-

pação do município são coordenados pela Secretaria Municipal de Desenvolvimento Sustentável e Inclusivo, da Inovação e Competitividade (SEDIC) e pela Secretaria de Fazenda.

Outro aspecto regulamentado pela Lei refere-se aos ambientes promotores de inovação (APIs), definidos pela lei como espaços financeiros ou virtuais destinados a fomentar a inovação e o empreendedorismo em Juiz de Fora. Entre os principais ambientes promotores de inovação, destacam-se aceleradoras, incubadoras, parques tecnológicos, ecossistemas de inovação e Living Labs. As aceleradoras de empresas, conforme descrito no Art. 5º, são ambientes que participam, acompanham e investem recursos materiais e financeiros em startups, recebendo contrapartidas como participação no capital social, royalties e outras receitas. As incubadoras, por sua vez, são ambientes que abrigam e acompanham startups, oferecendo orientação e suporte para suas graduações, além de infraestrutura necessária para seu desenvolvimento.

Parques tecnológicos e ecossistemas de inovação públicos são descritos em lei como áreas que possibilitam a integração de pesquisa científica e tecnológica, negócios e organizações governamentais, fornecendo suporte às inter-relações entre esses grupos para o desenvolvimento de produtos e processos inovadores. Esses ambientes de inovação ainda são regulamentados pelo decreto para que atendam a critérios de segurança, previsões econômicas e de impacto ambiental.

O regulamento do Decreto nº 16.734/2024 também apresenta disposições previstas para o ambiente regulatório experimental (sandbox regulatório), originalmente introduzidas na Lei nº 14.746/2023. O sandbox regulatório permite que as empresas desenvolvam e testem inovações tecnológicas em um ambiente controlado, com autorização temporária, facilitando a experimentação enquanto gerenciam os riscos associados a novas tecnologias. O Decreto estabelece critérios claros para a criação e operação do sandbox, exigindo que as empresas submetam propostas fundamentadas com planejamento específico da inovação, objetivos, metodologias de teste, cronograma e avaliação de riscos. Essa regulamentação é essencial para garantir que o sandbox regulador funcione como um espaço experimental seguro e que incentive a inovação.

No âmbito da governança, o Decreto nº 16.734/2024 estipula que o COM-DETI e a SEDIC serão responsáveis pela supervisão dos projetos no sandbox regulatório, incluindo auditorias e monitoramento contínuo, garantindo o cumprimento das metas de desempenho e das medidas de mitigação de riscos. A autorização para participar do sandbox tem validade de até 12 meses, po-

dendo ser prorrogada mediante justificativa técnica. A administração pública também promove a transparência por meio da divulgação de editais, chamamentos públicos e resultados de avaliações de projetos inovadores.

A governança do sistema de inovação em Juiz de Fora é estruturada para garantir a transparência, eficácia e supervisão dos projetos financiados e incentivados pela lei. COMDETI desempenha um papel central na governança do sistema. O Conselho Gestor do Fundo Municipal de Desenvolvimento da Inovação (FMDI) é responsável pelo planejamento e aplicação dos recursos do fundo, conforme especificado nos arts. 22 a 24. Este conselho é composto por representantes de diversas secretarias municipais e da sociedade civil, garantindo uma representação ampla e diversificada.

Entre suas competências estão a aprovação da programação orçamentária e financeira dos recursos do FMDI, a avaliação e aprovação de projetos nas áreas de Desenvolvimento Econômico, Tecnologia e Inovação que serão financiadas com recursos do FMDI, a elaboração do Plano Anual de Aplicação dos Recursos, a criação e publicação do relatório anual de atividades, e a fiscalização da aplicação dos recursos, garantindo a legalidade e transparência na aplicação dos recursos concedidos pelo fundo, além da avaliação dos indicadores e metas alcançadas.

Os incentivos fiscais previstos na lei, detalhados no Art. 25 ao 36, incluem isenções de ITBI, ISSQN e IPTU para empresas instaladas nas áreas designadas como Polos de Desenvolvimento e Inovação. Esses incentivos são destinados a fomentar a atração e a expansão de empreendimentos tecnológicos no município, criando um ambiente favorável à inovação e ao crescimento econômico. O Decreto nº 16.734/2024 complementa esses incentivos, estabelecendo condições e procedimentos específicos para a concessão de benefícios fiscais, com um processo de análise de impacto econômico e social das empresas beneficiadas.

A Lei nº 14.746/2023, em conjunto com os três decretos regulamentadores, em especial o Decreto nº 16.734/2024, estabelece uma estrutura robusta de mecanismos de fomento e ambientes promotores de inovação que são essenciais para promover o desenvolvimento tecnológico e a competitividade econômica no município. Com investimentos financeiros, parcerias estratégicas e uma infraestrutura de suporte abrangente, a legislação em Juiz de Fora cria um ambiente favorável para o crescimento de startups, empresas tecnológicas e cooperativas de base tecnológica. Esses esforços são alinhados com as diretrizes nacionais e internacionais, como a Carta Brasileira para Cidades Inteligentes, promovendo um desenvolvimento urbano sustentável e inovador.

4. Implementação e Regulamentação do Sandbox em Juiz de Fora

Com a publicação do Decreto nº 16.734/2024, o regulamento da Lei de Inovação de Juiz de Fora avança significativamente na implementação do sandbox regulatório, detalhando as condições necessárias para a criação, funcionamento e monitoramento desse ambiente regulatório experimental. O Decreto nº 16.734/2024 destaca-se por oferecer diretrizes específicas e definidas para que empresas e instituições de inovação possam desenvolver e testar novas tecnologias em um ambiente seguro e controlado, com a supervisão da administração pública.

O Capítulo VI do Decreto nº 16.734/2024 define o sandbox regulatório como um conjunto de condições especiais simplificadas e temporárias, que permite que empresas e instituições desenvolvam, testem e implementem inovações tecnológicas mediante autorização específica dos órgãos reguladores. Esse decreto estabelece o processo de submissão das propostas para o sandbox, incluindo tanto os casos de exigência direta das empresas quanto aquelas realizadas por meio de chamado público. As propostas devem ser apresentadas com especificações da tecnologia, justificativa para a criação do sandbox, objetivos esperados, planos de teste, cronograma, metodologia e avaliação de riscos, garantindo que a administração pública possa avaliar cuidadosamente cada projeto antes da autorização.

O processo de seleção no sandbox é baseado em critérios estabelecidos pelo decreto, como o grau de inovação e originalidade, o impacto potencial econômico, social e ambiental, a viabilidade técnica e econômica do projeto, a experiência da equipe proponente e o alinhamento com as prioridades estratégicas do município. A avaliação das propostas é realizada por uma comissão técnica designada pela COMDETI, composta por representantes da administração pública e especialistas nas áreas pertinentes. Esse sistema de seleção visa garantir que somente projetos com alto potencial de impacto sejam admitidos, minimizando os riscos associados à experimentação de tecnologias emergentes em um ambiente urbano.

Durante o período de participação, que tem validade inicial de até 12 meses e pode ser prorrogado por igual período mediante justificativa técnica, as empresas deverão apresentar relatórios periódicos de progresso, incluindo resultados parciais, desafios enfrentados e recomendações para eventuais ajustes. A supervisão contínua é realizada pela Secretaria Municipal de Desenvolvimento Sustentável e Inclusivo, da Inovação e Competitividade (SE-

DIC), em conjunto com a Secretaria de Fazenda e a Secretaria de Transformação Digital e Administrativa (STDA). Esse monitoramento constante, incluindo a possibilidade de auditorias e visitas técnicas, visa garantir que os projetos cumpram os requisitos de segurança e mitigação de riscos, promovendo a inovação de maneira alinhada aos interesses públicos.

A regulamentação estabelece ainda as responsabilidades de manutenção e suporte das tecnologias durante o período de teste, a cargo das empresas participantes. A infraestrutura necessária para a implementação das soluções será disponibilizada pelo município, conforme acordado nos termos de colaboração, e os termos de confidencialidade e propriedade intelectual serão definidos para garantir a segurança dos dados e das informações geradas. Ao final do período de teste, as empresas participantes deverão apresentar um relatório final detalhado, documentando os resultados, a avaliação dos impactos e as possíveis recomendações para a adoção ou expansão da solução.

Essa regulamentação detalhada representa um avanço significativo para o ecossistema de inovação de Juiz de Fora. Diferentemente da crítica anterior, que apontava a ausência de diretrizes para o sandbox regulatório, o Decreto nº 16.734/2024 oferece uma estrutura robusta e transparente para a realização de experimentos regulatórios. A regulamentação responde às preocupações levantadas por autores como Hollands, Morozov e Bria, Agar e Medina, que alertam para os riscos de iniciativas tecnológicas não reguladas e sua possível instrumentalização por interesses privados. Através do processo de supervisão, monitoramento e controle de qualidade, o decreto busca garantir que as iniciativas no sandbox regulatório sejam realizadas de forma inclusiva, com participação cidadã e responsabilidade social, minimizando o risco de que o espaço de experimentação beneficie exclusivamente empresas privadas ou resulte na centralização do poder.

No entanto, a implementação prática do regulamento sandbox não está isenta de desafios. A necessidade de uma supervisão contínua, além do rigor nos critérios de seleção e na definição de indicadores de desempenho, levanta questões sobre a capacidade de recursos humanos e técnicos para monitorar de perto todos os projetos aprovados. A dependência de estruturas municipais de fiscalização, mesmo com a atuação de múltiplas secretarias, pode limitar a abrangência e o alcance do sandbox, especialmente à medida que o volume de projetos aumenta. Essa restrição pode afetar a eficiência e a segurança dos testes de inovação no ambiente urbano, caso a supervisão não seja estruturada para o crescimento das iniciativas.

Outro ponto que merece atenção é a temporalidade da autorização. Embora a possibilidade de prorrogação permita flexibilidade para projetos que necessitem de mais tempo para a realização de testes, ela também pode gerar riscos caso o controle de qualidade e a conformidade com as regulamentações não sejam mantidos durante todo o período de experimentação. O decreto visa mitigar esses riscos através da exigência de relatórios periódicos e auditorias, mas a eficácia dessas medidas depende da capacidade administrativa de atuar de forma responsiva às particularidades de cada projeto.

A regulamentação também permite que o município avalie, ao final do período de teste, a adoção ou expansão das inovações testadas no sandbox, considerando os resultados obtidos e as recomendações apresentadas. Essa flexibilidade é uma característica importante para o desenvolvimento urbano, pois possibilita que Juiz de Fora adote soluções tecnológicas comprovadas como eficazes e seguras. Contudo, é essencial que as decisões de adoção sejam embasadas não apenas nos resultados técnicos, mas também nos impactos sociais e ambientais, garantindo que a tecnologia renovada contribua para o bem-estar coletivo e não apenas para benefícios privados.

A regulamentação do sandbox regulatório em Juiz de Fora, conforme o Decreto nº 16.734/2024, fornece a estrutura necessária para a experimentação controlada de inovações tecnológicas no ambiente urbano. A regulamentação atende a diversas demandas de segurança e inclusão, proporcionando um espaço de inovação que promove a responsabilidade social e a sustentabilidade. No entanto, para que esse ambiente regulador experimental realize plenamente o seu potencial, é fundamental que a administração pública esteja preparada para implementar controles rigorosos, garantir a transparência e assegurar que o desenvolvimento tecnológico atenda aos interesses da população, evitando exclusões ou marginalizações.

Considerações finais

Ao longo deste estudo, revisou-se o conceito e a evolução das cidades inteligentes, considerando suas múltiplas interpretações e os desafios para implementar tecnologias urbanas inclusivas e eficazes. Os modelos globais de inovação e os marcos legais brasileiros foram contextualizados para identificar o papel essencial da legislação na promoção de ambientes urbanos sustentáveis e tecnologicamente avançados. A análise da Lei de Inovação de Juiz de Fora posiciona essa estrutura legislativa como um catalisador para o de-

envolvimento econômico e tecnológico local, integrando a cidade aos princípios de uma governança inteligente.

A análise da Lei de Inovação de Juiz de Fora, juntamente com sua regulamentação específica, revela um esforço coordenado para implementar os princípios de cidades inteligentes, centrados na eficiência, na sustentabilidade e na inclusão social. Por meio do Sistema Municipal de Inovação (Simi-JF) e do Fundo Municipal de Desenvolvimento da Inovação (FMDI), a lei oferece um arcabouço regulatório robusto que visa criar um ambiente favorável ao desenvolvimento tecnológico e econômico. Esse ecossistema busca transformar a cidade em um centro de inovação, promovendo a criação de produtos e serviços que respondam às necessidades urbanas contemporâneas.

A introdução do sandbox regulatório, estruturado pelo Decreto nº 16.734/2024, representa uma inovação significativa nesse contexto. Ao permitir que empresas e instituições testem novas tecnologias em um ambiente controlado e supervisionado, o sandbox materializa o princípio experimentalista fundamental para as cidades inteligentes. Esta abordagem experimentalista permite que Juiz de Fora explore inovações tecnológicas de maneira segura e alinhada com os interesses públicos, proporcionando uma base para avaliar os impactos de novas soluções antes de sua implementação em larga escala. Dessa forma, o sandbox contribui para que a cidade avance em direção à gestão urbana eficiente, impulsionando o uso responsável e ético das tecnologias digitais.

No entanto, os desafios dessa abordagem são substanciais. A necessidade de critérios rigorosos de seleção e de governança inclusiva destaca a complexidade de gerenciar o sandbox de maneira que promova benefícios coletivos e evite a concentração de poder. A supervisão contínua dos projetos experimentais e a definição de métricas de desempenho específicas são fundamentais para assegurar que as tecnologias testadas no sandbox realmente contribuam para o bem-estar urbano e a justiça social. Sem uma governança robusta, o risco é que essas inovações favoreçam interesses privados em detrimento dos objetivos de inclusão e sustentabilidade que norteiam o conceito de cidades inteligentes.

Em termos de oportunidades, o sandbox regulatório posiciona Juiz de Fora como uma cidade pioneira no Brasil, criando um modelo para outras localidades que buscam integrar tecnologia e governança urbana de forma responsável. Ao adotar práticas experimentais e promover a transparência e a participação cidadã, a cidade pode garantir que suas políticas de inovação atendam

às demandas da população e reflitam os princípios de uma cidade verdadeiramente inteligente. O ambiente regulatório experimental também incentiva a criação de um ciclo de feedback constante entre o setor público e o setor privado, permitindo ajustes regulatórios com base em evidências e promovendo um desenvolvimento econômico mais alinhado às necessidades locais.

Por fim, para que Juiz de Fora realize plenamente o potencial de seu arcabouço regulatório e do sandbox, será essencial manter um compromisso com a adaptabilidade regulatória e com o monitoramento dos impactos sociais e ambientais das inovações testadas. A Lei de Inovação de Juiz de Fora e sua regulamentação fornecem as bases para uma cidade que concilia avanços tecnológicos com justiça social, mas o sucesso dessa jornada dependerá da capacidade de aprimorar continuamente esses mecanismos e de assegurar que a inovação esteja a serviço de um desenvolvimento urbano inclusivo e sustentável.

Referências

ABNT NBR ISO 37122:2021. *Cidades e comunidades sustentáveis – Indicadores para cidades inteligentes*. Associação Brasileira de Normas Técnicas, 2021.

AGAR, Jon. *The Government Machine: a Revolutionary History of the Computer*. Cambridge, MA: MIT Press, 2003. viii + 554 p. ISBN: 0-262-01202-2.

AMATO, Lucas Fucci; MISSAGIA, Caio Rezende. Ambientes regulatórios experimentais: O sandbox no sistema financeiro brasileiro. *RBSD – Revista Brasileira de Sociologia do Direito*, v. 10, n. 3, p. 143-171, set./dez. 2023.

ANTONIELLI, Dennys Marcelo; KIRA, Beatriz. Planejamento Urbano do Futuro, Dados do Presente: A Proteção da Privacidade no Contexto das Cidades Inteligentes. *Revista Brasileira de Estudos Urbanos e Regionais (RBEUR)*, v. 22, e202003, 2020. DOI: <https://doi.org/10.22296/2317-1529.rbeur.202003>.

DUARTE, Fábio; FIRMINO, Rodrigo José. *Unplugging the City: The Urban Phenomenon and its Sociotechnical Controversies*. 1st Edition. New York: Routledge, 2017. eBook. DOI: <https://doi.org/10.4324/9781315523255>. eISBN: 9781315523255.

HOLLANDS, Robert G. Will the real smart city please stand up? Intelligent, progressive or entrepreneurial? *City*, v. 12, n. 3, p. 303-320, 2008. DOI: 10.1080/13604810802479126.

JUIZ DE FORA. Lei nº 14.746, de 04 de dezembro de 2023. Institui o Sistema de Inovação de Juiz de Fora; define os polos de desenvolvimento do Município; dispõe sobre as atribuições do Conselho Municipal de Desenvolvimento, Tecnologia e Inovação (Comdeti) e dá outras providências. *Diário Oficial do Município de Juiz de Fora*, Juiz de Fora, MG, 05 dez. 2023.

JUIZ DE FORA. Decreto nº 16.372, de 30 de janeiro de 2024. Regulamenta os arts. 39, 40 e 41 da Lei Municipal nº 14.746, de 04 de dezembro de 2023, que dispõem sobre a composição e atribui-

ções do Conselho Municipal de Desenvolvimento, Tecnologia e Inovação (COMDETI) e dá outras providências. *Diário Oficial do Município de Juiz de Fora*, Juiz de Fora, MG, 31 jan. 2024.

JUIZ DE FORA. Decreto nº 16.448, de 11 de março de 2024. Regulamenta os arts. 1º, 2º (inciso I) e 6º da Lei Municipal nº 14.746, de 04 de dezembro de 2023, que dispõem sobre a criação, composição e finalidades do Sistema Municipal de Inovação em Juiz de Fora. *Diário Oficial do Município de Juiz de Fora*, Juiz de Fora, MG, 12 mar. 2024.

JUIZ DE FORA. Decreto nº 16.734, de 11 de setembro de 2024. Dispõe sobre o sistema de inovação do município e outras providências. *Diário Oficial do Município de Juiz de Fora*, Juiz de Fora, MG, 12 set. 2024.

MINISTÉRIO DO DESENVOLVIMENTO REGIONAL. *Carta Brasileira para Cidades Inteligentes*. Brasília, 2021.

MEDINA, Eden. *Cybernetic Revolutionaries: Technology and Politics in Allende's Chile*. Cambridge: The MIT Press, 2011. ISBN: 978-0-262-01649-0.

MOROZOV, Evgeny; BRIA, Francesca. *A cidade inteligente: tecnologias urbanas e democracia*. Traduzido por Humberto do Amaral. São Paulo: Ubu Editora, 2019. 192 p. ISBN: 978-85-7126-046-7.

OCDE. *Smart Cities and Inclusive Growth*. 2020. Disponível em: https://www.oecd.org/cfe/cities/OECD_Policy_Paper_Smart_Cities_and_Inclusive_Growth.pdf.

QUIRINO, Carina de Castro; HOCAYEN, Helena Gouvêa de Paula; CUNHA, Marcella Brandão Flores da. Sandbox regulatório: instrumento experimentalista à disposição da Administração Pública local como suporte ao desenvolvimento econômico. *R. de Dir. Público da Economia – RDPE*, Belo Horizonte, v. 21, n. 84, p. 9-33, out./dez. 2023.

REIA, Jess; BELLI, Luca (orgs.). *Smart Cities no Brasil: Regulação, Tecnologia e Direitos*. Belo Horizonte, MG: Casa do Direito, 2021. ISBN: 978-85-9530-274-7.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

13

**Da Segurança Jurídica à
Segurança Técnica: Temas
Decodificadores do Avanço
Tecnológico no Registro
Eletrônico de Imóveis**

LUÍS HENRIQUE DE MENEZES ACIOLY

Sumário: Introdução. 1. Desenvolvimento do Registro Eletrônico de Imóveis no Cenário Jurídico Brasileiro. 2. Primeiro decodificador: A assinatura eletrônica e atos digitais que envolvam bens imóveis no registro público. 2.1. Assinatura eletrônica: conceituação e relação com o ordenamento jurídico brasileiro. 2.2. Aceitabilidade das assinaturas eletrônicas perante o Registro de Imóveis. 3. Segundo decodificador: a segurança do armazenamento digital de documentos e a possibilidade de uso da Tecnologia *Blockchain*. 3.1. *Blockchain*: elementos conceituais e aplicações. 3.2. Aplicabilidade da *Blockchain* ao Repositório Confiável de Documentos Eletrônicos. Considerações finais.

Introdução

No que se refere ao ambiente regulatório das novas tecnologias, pode-se observar o direcionamento de medidas regulatórias às novas ferramentas e à renovação de dinâmicas sociais, tal como ocorre com a *Internet* das Coisas (*IoT*), a plataformização de serviços e a inteligência artificial generativa. No entanto, não se pode deixar de lado que a evolução tecnológica apresenta implicações em setores exaustivamente sistematizados, trazendo questionamentos sobre como balizar as antigas normas com o cenário atual.

Essa preocupação é muito bem externada pela professora Lyria Bennett Moses², para quem a normalização incidente à tecnologia é matéria também afeta ao problema de desconexão regulatória, quando novas técnicas se apresentam em um espaço regulado de maneira que se modifica a própria feição da atividade, promovendo a necessidade de adequação normativa. Esse é o caso do mercado imobiliário e o registro de imóveis.

As serventias extrajudiciais e o sistema do fôlio real apresentam de vital importância para a segurança jurídica e publicidade dos direitos reais, contribuindo para a pacificação social, e como tal, também foram inseridas à era digital. Nasce, assim, o desafio da forma adequada de viabilizar uma segurança jurídica, objeto do registro de imóveis, em compatibilização com a segurança técnica na utilização de novas tecnologias.

Para tanto, dois temas são decodificadores do avanço tecnológico no registro imobiliário: a aceitabilidade de diferentes espécies de assinaturas ele-

1. Pós-Graduando em Direito Digital (Especialização) junto ao Instituto de Tecnologia e Sociedade (ITS) e Centro de Estudos e Pesquisas no Ensino do Direito (CEPED) da UERJ. Graduado em Direito pelo Centro Universitário Ruy Barbosa - UniRuy. Coordenador de Pesquisa do Grupo de Estudos em Tecnologia, Informação e Sociedade - GETIS/CNPq. Advogado. Contato em: acioly10@gmail.com.

2. MOSES, Lyria Bennett. How to Think About Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target. *Law, Innovation and Technology*, v. 5, n. 1, p. 1-20, 2013.

trônicas para garantia a autenticidade dos documentos nato-digitais; e os parâmetros de segurança dos documentos arquivados eletronicamente, especialmente no Repositório Confiável de Documento Eletrônico (RCDE), sendo a *blockchain* uma possível tecnologia auxiliar relevante. Tem-se como problema de pesquisa a delimitação técnico-jurídica dos quesitos de autenticidade e elementos de confluência do registro eletrônico de imóveis com a *Blockchain*.

O presente estudo busca, assim, traçar o panorama jurídico atual da inserção do registro de imóveis no ambiente digital, com ênfase no Sistema do Registro Eletrônico de Imóveis (SREI) e sob a ótica dos temas decodificados. Para tanto, é imprescindível compreender o quadro evolutivo do SREI, o horizonte das assinaturas eletrônicas para atos envolvendo bens imóveis nos registros públicos e a moldura técnica em que a *Blockchain* se funda. A presente pesquisa consolida dois raciocínios construtivos: analisar-se-á o primeiro decodificador a com foco na estrutura normativa existente; e avaliar-se-á o segundo decodificador a partir da sua confluência com possibilidades tecnológicas, isto é, a *Blockchain*.

Para tanto, procedeu-se, metodologicamente, a partir da revisão crítica da literatura de referência no tema, à materialização em uma pesquisa bibliográfica e documental de cunho descritivo, natureza qualitativa e caráter exploratório, em que se preconizou o diálogo entre autores das diferentes áreas das ciências sociais. Empreendeu-se aqui uma revisão literária, materializada por meio de uma pesquisa bibliográfica, cuja coleta de dados se deu por livros, dissertações e artigos, depositados em bases de dados eletrônicas – *Scientific Electronic Library Online (Scielo)*, *Index Law Journals* e *Google Scholar* –, tendo como descritores: “assinatura eletrônica”; “registro eletrônico”; “sistema do registro eletrônico de imóveis”; “*blockchain*”; “*smart contracts*”.

1. Desenvolvimento do Registro Eletrônico de Imóveis no Cenário Jurídico Brasileiro

Diferente de outras atividades, em que a regulamentação vem a reboque, o registro imobiliário brasileiro, em sua maior parte, teve o seu desenvolvimento decorrente do avanço normativo, em atenção ao constante aperfeiçoamento das técnicas jurídicas e arquivísticas. Foi assim com a Lei Federal n. 6.015, de 1973, que instituiu o sistema de fôlio real, em que se deu preponderância à matrícula com cerne da atividade registral³.

3. RIBEIRO, Moacyr Petrocelli de Ávila. A Matrícula: Paradigmas para o Sistema do Registro Eletrônico de Imóveis. *Revista de Direito Imobiliário*, a. 42, v. 86, p. 215-262, jan./jun. 2019.

Esse aprimoramento técnico e jurídico ocorreu como reação ao sistema de transcrições que, conforme assevera Fioranelli⁴, tornava obrigatória a repetição da caracterização do bem registrado a cada vez que sua propriedade era transmitida ou de qualquer outra forma era onerado. Com o sistema de matrículas, os imóveis passaram a ter um registro concentrado, fazendo-se constar toda a cadeia dominial do bem⁵, assim como sua realidade, observando-se a devida qualificação objetiva e modificações estruturais⁶.

A eficiência e eficácia desse sistema deu embasamento à ampliação do registro de imóveis, dando ao oficial registrador o protagonismo na proteção do direito de propriedade a partir da qualidade da informação vinculado à matrícula imobiliária⁷. No entanto, na contemporânea sociedade da *hiperinformação*⁸, a *Internet* tem assumido o lugar de protagonista das relações sociais, promovendo mudanças em termos culturais, econômicos, jurídicos e governamentais⁹.

Sem embargo de ressaltar a profundidade do tema “Governo como Plataforma”¹⁰, a remodelagem da prestação de serviços públicos por meio da *Internet* também alcançou o registro imobiliário, notadamente a partir da Lei Federal n. 11.977, de 2009. Esse diploma deu luz à possibilidade de recepção e emissão de documentos eletrônicos, desde que observados os requisitos da Infraestrutura de Chaves Públicas Brasileira – ICP Brasil e a arquitetura e-PING.

A Lei Federal n. 11.977, de 2009, também se arvorou a estabelecer o dever de os serviços de registros públicos instituírem um “sistema do registro eletrônico”, conforme regulamentação própria. Seguindo essas linha, o Conselho Nacional de Justiça editou a sua Recomendação n. 14, de 2014, para orientar as Corregedorias Gerais de Justiça, das respectivas Unidades da Federação,

4. FIORANELLI, Ademar. Matrícula no registro de imóveis: questões práticas. In: YOSHIDA, Consuelo Yatsuda Moromizato Yoshida; FIGUEIREDO, Marcelo. AMADEI, Vicente de Abreu (coords). *Direito notarial e registral avançado*. São Paulo: Revista dos Tribunais, 2014.

5. CASTRO, Manuella Santos. *Registro de Imóveis na Era Digital: Impactos das novas tecnologias no sistema registral brasileiro*. 2021, 306 f. Tese (Doutorado) - Faculdade de Direito, USP, São Paulo, 2021.

6. RIBEIRO, Moacyr Petrocelli de Ávila. A Matrícula: Paradigmas para o Sistema do Registro Eletrônico de Imóveis. *Revista de Direito Imobiliário*, a. 42, v. 86, p. 215-262, jan./jun. 2019.

7. RIBEIRO, Moacyr Petrocelli de Ávila. A Matrícula: Paradigmas para o Sistema do Registro Eletrônico de Imóveis. *Revista de Direito Imobiliário*, a. 42, v. 86, p. 215-262, jan./jun. 2019.

8. MADALENA, Juliano. Regulação das Fronteiras da Internet: um primeiro passo para uma Teoria Geral do Direito Digital. In: MARTINS, G. M.; LONGHI, J. V. R. (coords.). *Direito Digital: Direito Privado e Internet*. 2. ed. Indaiatuba: Foco, 2019. p. 183-206.

9. CASTELLS, Manuel. *A sociedade em rede*. Trad. Roneide Venâncio Majer. 6. ed. São Paulo: Paz e Terra, 2002.

10. Conforme Faleiros Júnior elucida, a teoria do “Governo como Plataforma” se fundamenta em estudo desenvolvido por O’Reilly e refere-se ao “dever estatal de fomento à implementação de infraestrutura tecnológica voltada a facilitar a interação entre diversos agentes, com finalidades variadas” (FALEIROS JÚNIOR, José Luiz de Moura. Inovação, desenvolvimento e a Lei do Governo Digital (Lei nº 14.129/2021): perspectivas quanto às estruturas de governo como plataforma. *Inova Jur - Revista Jurídica da UEMG*, Belo Horizonte, v. 1, n. 1, p. 1-29, jan./jun. 2022, p. 6; O’REILLY, Tim. Government as platform. *Innovations: Technology, Governance, Globalization*, Cambridge, v. 6, n. 1, p. 13-40, 2011).

na implementação de um “sistema do registro eletrônico de imóveis”¹¹. A Recomendação n. 14, de 2014, estabeleceu que fossem observados os parâmetros definidos pela Associação do Laboratório de Sistemas Integráveis Tecnológicos, na implementação desse sistema, sem trazer maiores definições¹².

No entanto, a Corregedoria Geral de Justiça de São Paulo (CGJ-SP) já havia editado, em 2012, o seu Provimento n. 42, fornecendo diretrizes para a implantação do Sistema do Registro Eletrônico de Imóveis (SREI) naquele Estado, dando forma à Central de Serviços Eletrônicos Compartilhados dos Registradores de Imóveis como ponto de acesso a serviços do registro imobiliário através da *Internet*¹³⁻¹⁴. À luz dessa norma, o desenvolvimento, a operação e administração do SREI no estado paulista seria de responsabilidade da ARISP – Associação de Registradores Imobiliários de São Paulo¹⁵⁻¹⁶.

Não muito distante, o Conselho Nacional de Justiça editou o Provimento n. 47, de 2015, para traçar as diretrizes técnicas e jurídicas que deveriam ser observadas na implementação do Sistema do Registro Eletrônico de Imóveis (SREI) no âmbito de cada Estados e Distrito Federal¹⁷. A partir dessa norma, promoveu-se a criação das centrais de serviço eletrônico compartilhados, administradas de forma local, mediante ato normativo promovido por cada Corregedoria Geral de Justiça¹⁸. O Provimento n. 47, de 2015, do CNJ, trouxe a necessidade de uniformidade das centrais eletrônicas em cada um dos Es-

11. GRUBER, Rafael Ricardo. Registro Eletrônico de Imóveis, Cadastros e SINTER: Interconexão sem Submissão. *Revista de Direito Imobiliário*, a. 39, v. 81, p. 253-287, jul./dez. 2016; CASTRO, Manuella Santos. *Registro de Imóveis na Era Digital: Impactos das novas tecnologias no sistema registral brasileiro*. 2021, 306 f. Tese (Doutorado) - Faculdade de Direito, USP, São Paulo, 2021.

12. ASSAD, Frederico Jorge Vaz de Figueiredo. Registro de imóveis eletrônico e governança fundiária. *Revista de Direito Imobiliário*, a. 39, v. 81, p. 215-234, jul./dez. 2016; TAVARES, Ramos André. O Operador Nacional do Sistema de Registro Eletrônico de Imóveis: Resposta à Exigência Constitucional de um Eficiente Sistema Registral. *Jornal Eletrônico Migalhas*, v. 136, p. 23-42, 2018.

13. À luz do referido diploma, os módulos que deveriam ser ofertados pela Central de Registradores seriam: I - Ofício Eletrônico; II - Penhora Eletrônica de Imóveis (Penhora Online); III - Certidão Digital; IV - Matrícula Online; V - Pesquisa Eletrônica; VI - Protocolo Eletrônico de Títulos (e-Protocolo); VII - Repositório Confiável de Documento Eletrônico (RCDE); VIII - Acompanhamento Registral Online; IX - Monitor Registral; X - Correção Online (Acompanhamento, controle e fiscalização); e XI - Cadastro de Regularização Fundiária Urbana. Essa mesma estrutura se manteve no Serviço de Atendimento Eletrônico Compartilhado (SAEC), com os aperfeiçoamentos e inclusões pertinentes, constituindo o esqueleto do “front-end” de todo o Registro Eletrônico de Imóveis.

14. ASSAD, Frederico Jorge Vaz de Figueiredo. Registro de imóveis eletrônico e governança fundiária. *Revista de Direito Imobiliário*, a. 39, v. 81, p. 215-234, jul./dez. 2016; CASTRO, Manuella Santos. *Registro de Imóveis na Era Digital: Impactos das novas tecnologias no sistema registral brasileiro*. 2021, 306 f. Tese (Doutorado) - Faculdade de Direito, USP, São Paulo, 2021.

15. *In verbis*: “258. O Serviço de Registro Eletrônico de Imóveis (SREI) será prestado aos usuários externos por meio de plataforma única na *Internet* que funcionará no Portal Eletrônico da Central de Serviços Eletrônicos Compartilhados dos Registradores de Imóveis (Central Registradores de Imóveis), desenvolvido, operado e administrado pela Associação dos Registradores Imobiliários de São Paulo (ARISP) (...)”.

16. ASSAD, Frederico Jorge Vaz de Figueiredo. Registro de imóveis eletrônico e governança fundiária. *Revista de Direito Imobiliário*, a. 39, v. 81, p. 215-234, jul./dez. 2016; CASTRO, Manuella Santos. *Registro de Imóveis na Era Digital: Impactos das novas tecnologias no sistema registral brasileiro*. 2021, 306 f. Tese (Doutorado) - Faculdade de Direito, USP, São Paulo, 2021.

17. GRUBER, Rafael Ricardo. Registro Eletrônico de Imóveis, Cadastros e SINTER: Interconexão sem Submissão. *Revista de Direito Imobiliário*, a. 39, v. 81, p. 253-287, jul./dez. 2016.

18. *In verbis*: “Art. 3º. O intercâmbio de documentos eletrônicos e de informações entre os escritórios de registro de imóveis, o Poder Judiciário, a Administração Pública e o público em geral estará a cargo de centrais de serviços eletrônicos compartilhados que se criarão em cada um dos Estados e no Distrito Federal. § 1º. As centrais de serviços eletrônicos compartilhados serão criadas pelos respectivos oficiais de registro de imóveis, mediante ato normativo da Corregedoria Geral de Justiça local.”

tados e Distrito Federal, demandando também a coordenação entre si, para que uniformização da prestação do serviço registral¹⁹.

A pulverização das centrais eletrônicas estaduais foi, contudo, contrastada pela necessidade de consolidação de um ponto de acesso universal pela *Internet*, assim como de interoperabilidade inerente às diversas camadas técnicas que envolvem a prestação do serviço registral imobiliário em âmbito nacional. Aliado à necessidade de prover efetividade à política de regularização fundiária, esse contexto fez surgir no texto da Lei Federal n. 14.365, de 2017, o Operador Nacional do Sistema de Registro Eletrônico de Imóveis (ONR) como responsável por implementar e operar o SREI em âmbito nacional²⁰.

O diploma trouxe a estrutura geral para a formação²¹, sustentação financeira²² e regulação²³ do ONR, que seria constituído como entidade privada com vinculação obrigatória de todos os oficiais de registro imobiliário²⁴. Não compõem, assim, a administração pública federal, mas ostenta natureza jurídica *sui generis*²⁵. Coube à Corregedoria Geral do CNJ editar o Provimento n. 89, de 2019, com as diretrizes específicas para os fins estatutários do ONR e para sua atuação, designando a implantação e operação do Serviço de Atendimento Eletrônico Compartilhado – SAEC²⁶.

Com o Provimento n. 89, do CNJ, o SREI passa a ser composto por: (i) todos os oficiais de registro de imóveis do Brasil; (ii) o Serviço de Atendimento Eletrônico Compartilhado (SAEC); e (iii) as centrais de serviços eletrônicos compartilhados. Aos poucos, as centrais estaduais perderam protagonismo em relação ao SAEC, que agasalhou de forma horizontal uma gama de atividades implicadas ao registro imobiliário, integralizando serventias extrajudiciais em caráter nacional a partir de um único ponto de acesso na *Internet*²⁷.

19. *In verbis*: “Art. 3º (...). § 2º. Haverá uma única central de serviços eletrônicos compartilhados em cada um dos Estados e no Distrito Federal. (...) § 5º. As centrais de serviços eletrônicos compartilhados coordenar-se-ão entre si para que se universalize o acesso ao tráfego eletrônico e se prestem os mesmos serviços em todo o País”.

20. TAVARES, Ramos André. O Operador Nacional do Sistema de Registro Eletrônico de Imóveis: Resposta à Exigência Constitucional de um Eficiente Sistema Registral. *Jornal Eletrônico Migalhas*, v. 136, p. 23-42, 2018.

21. *In verbis*: “Art. 76. (...) 2º O ONR será organizado como pessoa jurídica de direito privado, sem fins lucrativos”.

22. *In verbis*: “Art. 76 (...) § 9º Fica criado o fundo para a implementação e custeio do SREI, que será gerido pelo ONR e subvencionado pelas unidades do serviço de registro de imóveis dos Estados e do Distrito Federal referidas no § 5º deste artigo”.

23. *In verbis*: “Art. 76. (...) § 4º Caberá à Corregedoria Nacional de Justiça do Conselho Nacional de Justiça exercer a função de agente regulador do ONR e zelar pelo cumprimento de seu estatuto”.

24. *In verbis*: “Art. 76. (...) § 5º As unidades do serviço de registro de imóveis dos Estados e do Distrito Federal integram o SREI e ficam vinculadas ao ONR”.

25. CASTRO, Manuella Santos. *Registro de Imóveis na Era Digital: Impactos das novas tecnologias no sistema registral brasileiro*. 2021, 306 f. Tese (Doutorado) - Faculdade de Direito, USP, São Paulo, 2021.

26. CASTRO, Manuella Santos. *Registro de Imóveis na Era Digital: Impactos das novas tecnologias no sistema registral brasileiro*. 2021, 306 f. Tese (Doutorado) - Faculdade de Direito, USP, São Paulo, 2021.

27. VALERIO, Alexandre Scigliano; BONFATTI, Fabio Fernandes Neves. Possibilidade de Assinatura, Registro e Protesto Eletrônico dos Títulos de Crédito do Agronegócio. *Revista Brasileira de Direito Empresarial*, v. 7, n. 2, p. 17-38, jul./dez. 2021.

A integralização de todas as serventias de registro de imóveis ao SAEC²⁸, e a sua prevalência frente à fragmentação das centrais estaduais, deu novos contornos ao SREI. Impulsionou-se a promoção de atos essencialmente digitais, como a emissão de certidões eletrônicas e a recepção de documentos nato-digitais, vinculando uma cadeia complexa de oficiais de Registro de Imóveis à promoção de um novo patamar tecnológico²⁹. Essa convergência de ações para o fomento ao serviço extrajudicial de caráter eletrônico foi consolidada com a Lei Federal n. 14.382, de 2022, que dispôs sobre o Sistema Eletrônico dos Registros Públicos (SERP), com fito de realizar a integralização dos demais ofícios de registros públicos, em moldes da governança semelhantes à coordenação do SREI³⁰.

O SERP – assim como o SREI em relação ao registro imobiliário – se propõe a construir um sistema eletrônico que efetive a interoperabilidade entre as bases de dados das serventias de registro, sua interconexão e a universalidade do atendimento ao usuário, utilizando-se das estruturas tecnológicas baseadas na *Internet*. Para tanto, a construção de parâmetros técnicos, balizados em sólido arcabouço normativo, se mostra essencial para viabilizar um ambiente seguro para o desenvolvimento do registro eletrônico de imóveis.

2. Primeiro decodificador: A assinatura eletrônica e atos digitais que envolvam bens imóveis no registro público

A validade do ato registral eletrônico depende da garantia de autenticidade dos emissores da vontade ali documentada, o que conduz ao reconhecimento da assinatura eletrônica como pilar da era digital dos cartórios. O protocolo eletrônico de documentos pelo usuário do serviço extrajudicial está condicionado ao cumprimento das regras técnicas e jurídicas específicas. A construção desse arcabouço normativo é, por sua vez, um termômetro para a medição da fluidez do binômio desburocratização – segurança no mercado imobiliário.

28. Importa ressaltar que a integralização de todas as serventias de registro de imóveis ao SAEC foi objeto de normalização promovida pela Corregedoria Nacional do CNJ que, com o seu Provimento n. 124, de 2021, estabeleceu a data de 15 de fevereiro de 2022 como limite para a completude desse processo.

29. MIRANDA, Caleb Matheus Ribeiro de. Comentários ao Sistema Eletrônico de Registros Públicos (SERP) – artigos 1º ao 9º. In: KÜMPEL, Vitor (Coord). *Breves comentários à Lei nº 14.382/2022*. 2 ed. São Paulo: YK, 2023, p. 11-48.

30. A Lei Federal n. 14.382, de 2022, estabeleceu que deveria ser constituído operador nacional, na forma de entidade privada administrada pelos oficiais de registro, conforme regulamentação do CNJ. Com o Provimento n. 139, de 2024, o CNJ trouxe à luz o Operador Nacional do Sistema Eletrônico do Registro Público (ONSERP), composto pelo Operador Nacional do Registro Civil das Pessoas Naturais (ON-RCPN), o Operador Nacional do Registro de Títulos e Documentos e Civil das Pessoas Jurídicas (ON-RTDPJ), também nascidos dessa normativa, e o ONR. O Provimento n. 139 teve suas diretrizes inseridas no Provimento n. 149, de 2023, do CNJ. Nesse ponto, o art. 212, § 2º, deste último, consolidou a estrutura de gestão compartilhada: “A gestão do ONSERP ficará a cargo do Comitê Executivo de Gestão, composto pelos presidentes dos operadores nacionais de registros públicos, que funcionará sob a orientação e a fiscalização da Corregedoria Nacional de Justiça”.

2.1 Assinatura eletrônica: conceituação e relação com o ordenamento jurídico brasileiro

Os contratos eletrônicos não constituem nova espécie de acordo, mas forma específica de sua conclusão, em que se emprega meios de tecnologia da informação para construção do documento³¹. No entanto, para validade técnica de um documento eletrônico, devem ser observados alguns elementos formativos: (i) a autenticidade, no sentido de garantia de que seu originador é quem diz ser; (ii) a integridade, isto é, a garantia de que o documento recebido é idêntico ao documento formado originalmente; (iii) a confidencialidade, isto é, a garantia de que nenhuma pessoa não autorizada possa acessar seu conteúdo; e (iv) o não repúdio, isto é, a impossibilidade de que o emissor possa negar que produziu o documento³².

A assinatura eletrônica³³ desempenha, nesse contexto, o papel de dar autenticidade e integridade ao documento, de forma que o não-repúdio decorre de presunção dada pelo Ordenamento jurídico, validando o ato conforme o nível exigido para a assinatura³⁴. O ordenamento jurídico brasileiro agasalhou a aceitabilidade das assinaturas eletrônicas com a Medida Provisória n. 2.200-2, de 2001, que incorporou diretrizes da Lei Modelo da *United Nations Commission on International Trade Law – UNCITRAL*³⁵.

A Lei Modelo da UNCITRAL estabelece duas partes necessárias ao funcionamento das Chaves Públicas de Identificação: (i) o signatário (“*signatory*”), pessoa responsável por criar a assinatura eletrônica; e (ii) a parte confiável (“*relying party*”), pessoa responsável pela verificação e aceitação ou não desta

31. MENKE, Fabiano. A forma dos contratos eletrônicos. *Revista de Direito Civil Contemporâneo*, São Paulo: Revista dos Tribunais, a. 8, v. 26, p. 85-113, jan./mar. 2021.

32. PINHEIRO, Patrícia Peck; WEBER, Sandra Tomazi; OLIVEIRA NETO, Antonio Alves de. *Fundamentos dos Negócios e Contratos Digitais*. 2. ed. São Paulo: Revista dos Tribunais, 2021; SOTTANO, Augusto; LAGO, Ivan Jacopetti. As assinaturas eletrônicas e o registro de imóveis: estado atual da questão. In: GALHARDO, Flaviano; PARO, João P.; NALINI, José R.; BRANDELLI, Leonardo (org.). *Direito Registral e Novas Tecnologias*. Rio de Janeiro: Forense, 2021.

33. Entende-se por assinatura eletrônica o resumo matemático computacionalmente calculado a partir de tecnologia de chaves assimétricas. Na Criptografia de Chaves Assimétricas, um par de chaves trabalha em conjunto, de forma que uma chave cifra e outra a decifra. A chave privada é mantida em controle, conhecimento e uso exclusivo do signatário e a chave pública é distribuída livremente. O *hashing*, por sua vez, transforma dados de qualquer tamanho em um bloco de dados de tamanho fixo, de forma que ao alterar qualquer informação dos dados originais do documento, obtém-se um novo *hash*, completamente distinto do anterior. O emissor da assinatura, neste caso, envia o documento original e o *hash* do documento criptografado pela chave privada, ao passo que o receptor utiliza a chave pública para descriptografar o *hash*, calcular o *hash* do documento e validar os dois *hash* por comparação. Existindo identidade entre os dois *hash*, tem-se uma assinatura eletrônica válida, denotando autenticidade ao documento digital. Esse procedimento é capaz de realizar autenticação da assinatura conferindo integridade ao documento nato-digital. Após sua realização, é possível conferir uma camada adicional de segurança a partir de um certificado digital, com verificação por Autoridade Certificadora, que apõe um Certificado Digital (PINHEIRO, Patrícia Peck; WEBER, Sandra Tomazi; OLIVEIRA NETO, Antonio Alves de. *Fundamentos dos Negócios e Contratos Digitais*. 2. ed. São Paulo: Revista dos Tribunais, 2021).

34. LEITE, Clarisse Frechiani Lara. Assinatura eletrônica. *Revista de Processo*, São Paulo: Revista dos Tribunais, a. 48, v. 345, p. 79-121, nov. 2023.

35. MENKE, Fabiano. A forma dos contratos eletrônicos. *Revista de Direito Civil Contemporâneo*, São Paulo: Revista dos Tribunais, a. 8, v. 26, p. 85-113, jan./mar. 2021; SOTTANO, Augusto; LAGO, Ivan Jacopetti. As assinaturas eletrônicas e o registro de imóveis: estado atual da questão. In: GALHARDO, Flaviano; PARO, João P.; NALINI, José R.; BRANDELLI, Leonardo (org.). *Direito Registral e Novas Tecnologias*. Rio de Janeiro: Forense, 2021; LEITE, Clarisse Frechiani Lara. Assinatura eletrônica. *Revista de Processo*, São Paulo: Revista dos Tribunais, a. 48, v. 345, p. 79-121, nov. 2023.

assinatura. A norma descreveu, ainda, uma terceira parte, de caráter opcional, concernente a um agente responsável por certificar o titular dessa assinatura, podendo esse terceiro ser agente público ou não (“*certification authority*” ou “*certification services provider*”)³⁶.

A Medida Provisória n. 2200-2, de 2001, ao incorporar a Lei Modelo da UNCITRAL, previu paralelamente a convivência de dois modelos de reconhecimento da validade da assinatura³⁷. O primeiro modelo com as três partes³⁸, concerne à Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), cujo papel de Autoridade Certificadora Raiz é atribuído ao Instituto Nacional de Tecnologia da Informação (ITI). O segundo modelo³⁹, com apenas duas figuras, concerne aos certificados não são emitidos no âmbito da Infraestrutura de Chaves Públicas Brasileira⁴⁰.

A amplitude de possibilidades oportunizadas em razão deste dispositivo, contudo, trazia dúvidas e insegurança pelo cidadão na aplicação de assinaturas eletrônicas, especialmente nas relações que envolvessem a apresentação de documentos eletrônicos perante o Poder Público⁴¹. Apontando direcionamentos para suprir essa lacuna, a Lei Federal n. 14.063, de 2020, consolidou três espécies de assinaturas eletrônicas: (i) assinatura simples⁴²; (ii) assinatura avançada⁴³; e (iii) assinatura qualificada⁴⁴.

36. SOTTANO, Augusto; LAGO, Ivan Jacopetti. As assinaturas eletrônicas e o registro de imóveis: estado atual da questão. In: GALHARDO, Flaviano; PARO, João P.; NALINI, José R.; BRANDELLI, Leonardo (org.). *Direito Registral e Novas Tecnologias*. Rio de Janeiro: Forense, 2021.

37. ALVIM, Arruda; CUNHA, Igor Martins da. As assinaturas eletrônicas no ordenamento jurídico brasileiro e a relevância da autonomia privada: uma breve análise da validade dos documentos eletrônicos à luz da MP 2.200-2/2001 e da Lei 14.063/2020. *Revista de Processo*, São Paulo: Revista dos Tribunais, a. 48, v. 337, p. 83-114, São Paulo: RT, mar. 2023.

38. *In verbis*: “Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória. § 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1o de janeiro de 1916 - Código Civil”.

39. *In verbis*: “Art. 10. (...) § 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento”.

40. PINHEIRO, Patrícia Peck; WEBER, Sandra Tomazi; OLIVEIRA NETO, Antonio Alves de. *Fundamentos dos Negócios e Contratos Digitais*. 2. ed. São Paulo: Revista dos Tribunais, 2021.

41. ALVIM, Arruda; CUNHA, Igor Martins da. As assinaturas eletrônicas no ordenamento jurídico brasileiro e a relevância da autonomia privada: uma breve análise da validade dos documentos eletrônicos à luz da MP 2.200-2/2001 e da Lei 14.063/2020. *Revista de Processo*, São Paulo: Revista dos Tribunais, a. 48, v. 337, p. 83-114, São Paulo: RT, mar. 2023; LEITE, Clarisse Frechiani Lara. Assinatura eletrônica. *Revista de Processo*, São Paulo: Revista dos Tribunais, a. 48, v. 345, p. 79-121, nov. 2023.

42. *In verbis*: “Art. 4º Para efeitos desta Lei, as assinaturas eletrônicas são classificadas em: I - assinatura eletrônica simples: a) a que permite identificar o seu signatário; b) a que anexa ou associa dados a outros dados em formato eletrônico do signatário”.

43. *In verbis*: “Art. 4º (...) II - assinatura eletrônica avançada: a que utiliza certificados não emitidos pela ICP-Brasil ou outro meio de comprovação da autoria e da integridade de documentos em forma eletrônica, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento, com as seguintes características: a) está associada ao signatário de maneira unívoca; b) utiliza dados para a criação de assinatura eletrônica cujo signatário pode, com elevado nível de confiança, operar sob o seu controle exclusivo; c) está relacionada aos dados a ela associados de tal modo que qualquer modificação posterior é detectável”.

44. *In verbis*: “Art. 4º (...) III - assinatura eletrônica qualificada: a que utiliza certificado digital, nos termos do § 1º do art. 10 da Medida Provisória nº 2.200-2, de 24 de agosto de 2001”.

2.2 Aceitabilidade das assinaturas eletrônicas perante o Registro de Imóveis

Ao disciplinar as hipóteses de aceitabilidade de assinaturas baseadas em certificados não baseados na ICP-Brasil perante o Poder Público, a Lei Federal n. 14.063, de 2020 também trouxe os casos em que essa infraestrutura seria exigida⁴⁵. Consignou, assim, que para atos de transferência e registro de imóveis seria exigida a modalidade qualificada de assinatura, salvo exceções legais⁴⁶⁻⁴⁷. Isso foi revisto pela Lei Federal n. 14.382, de 2022, que alterou a Lei de Registros Públicos para permitir a adoção de assinatura avançada nos atos do registro público que envolvam bens imóveis, conforme regulamentação da Corregedoria Nacional do CNJ⁴⁸⁻⁴⁹.

A superação da restrição imposta pela Lei Federal n. 14.063, de 2020, não ocorre apenas em razão da incompatibilidade de suas disposições com a Lei Federal n. 14.382, de 2022, mas também e especialmente em razão da aplicação do critério de solução de aparentes antinomias entre normas de mesmo grau hierárquico. Nesse sentido, tem-se que a norma mais recente, quando incompatível com a anterior, opera a sua revogação tácita, como reza a Lei de Introdução às Normas do Direito Brasileiro (Decreto-Lei n. 4.657, de 1942)⁵⁰.

Nessa esteira, a Corregedoria Nacional do CNJ apresentou robusta regulamentação do manejo de assinaturas eletrônicas sob responsabilidade do Operador Nacional do Registro Civil das Pessoas Naturais (ON-RCPN), a partir do Provimento n. 157, de 2023, que alterou o Código Nacional de Normas do Foro Extrajudicial para agasalhar: (i) o Sistema de Autenticação Eletrônica com dados biográficos e biométricos para identificação de usuários internos

45. ALVIM, Arruda; CUNHA, Igor Martins da. As assinaturas eletrônicas no ordenamento jurídico brasileiro e a relevância da autonomia privada: uma breve análise da validade dos documentos eletrônicos à luz da MP 2.200-2/2001 e da Lei 14.063/2020. *Revista de Processo*, São Paulo: Revista dos Tribunais, a. 48, v. 337, p. 83-114, São Paulo: RT, mar. 2023.

46. As exceções previstas no próprio texto da Lei Federal n. 14.063, de 2020, foram para o registro de atos nas juntas comerciais (art. 5º, § 1º, II, “c”), e no caso de os atos serem praticados por instituições financeiras que atuem com crédito imobiliário autorizadas a celebrar instrumentos particulares com caráter de escritura pública (art. 17-A).

47. SOTTANO, Augusto; LAGO, Ivan Jacopetti. As assinaturas eletrônicas e o registro de imóveis: estado atual da questão. In: GALHARDO, Flaviano; PARO, João P.; NALINI, José R.; BRANDELLI, Leonardo (org.). *Direito Registral e Novas Tecnologias*. Rio de Janeiro: Forense, 2021.

48. *In verbis*: “Art. 17. Qualquer pessoa pode requerer certidão do registro sem informar ao oficial ou ao funcionário o motivo ou interesse do pedido. § 1º O acesso ou o envio de informações aos registros públicos, quando realizados por meio da internet, deverão ser assinados com o uso de assinatura avançada ou qualificada de que trata o art. 4º da Lei nº 14.063, de 23 de setembro de 2020, nos termos estabelecidos pela Corregedoria Nacional de Justiça do Conselho Nacional de Justiça. § 2º Ato da Corregedoria Nacional de Justiça do Conselho Nacional de Justiça poderá estabelecer hipóteses de uso de assinatura avançada em atos que envolvam imóveis”.

49. LEITE, Clarisse Frechiani Lara. Assinatura eletrônica. *Revista de Processo*, São Paulo: Revista dos Tribunais, a. 48, v. 345, p. 79-121, nov. 2023.

50. *In verbis*: “Art. 2º Não se destinando à vigência temporária, a lei terá vigor até que outra a modifique ou revogue. § 1º A lei posterior revoga a anterior quando expressamente o declare, quando seja com ela incompatível ou quando regule inteiramente a matéria de que tratava a lei anterior”.

e externos de todas as especialidades do Serp⁵¹; e (ii) uma Infraestrutura de Chaves Públicas do Registro Civil (ICP-RC), baseada na assinatura eletrônica avançada⁵².

Realizou-se, nesse sentido, a consolidação de uma Lista de Serviços Eletrônicos Confiáveis do Registro Civil do Brasil⁵³ (LSEC-RCPN), incluindo-se nela o ICP-RC, que reconhece a validade de assinaturas eletrônicas avançadas para os atos inerentes a documentos eletrônicos apresentados aos serviços de registros públicos, para atos envolvendo bens imóveis, e para celebrar instrumentos particulares com caráter de escritura pública por instituições financeiras que atuem com crédito imobiliário.

Ressalta-se, contudo, que o protocolo de documentos no registro de imóveis, bem como a condução de procedimentos registraes específicos⁵⁴, pode estar condicionado à formalidade exigida por lei. Nos casos que se depende de escritura pública⁵⁵, a atuação do tabelião de notas é imprescindível. Em relação aos atos notariais eletrônicos, há específica diretriz que dá validade aos documentos subscritos mediante certificado notariado (espécie de assinatura avançada) ou certificação ICP-Brasil em relação aos demais signatários⁵⁶.

O movimento de desburocratização da atividade registral imobiliária pela aceitabilidade de assinatura eletrônicas baseados em certificados digitais não emitidos pela ICP-Brasil resulta, em última instância, na maior adesão da sociedade ao serviço extrajudicial⁵⁷. Isso em razão de menor custo associado aos certificados digitais não baseados na ICP-Brasil, bem como na maior di-

51. *In verbis*: “Art. 228-C. O IdRC será considerado válido para identificação e autenticação de usuários em todas as plataformas e serviços do Serp, inclusive pelas demais especialidades de registro (...)”.

52. *In verbis*: “Art. 228-E. A ICP-RC será utilizada para a gestão do ciclo de vida de chaves públicas de assinaturas eletrônicas avançadas, em conformidade com o disposto no art. 38 da Lei n. 11.977, de 7 de julho de 2009, e art. 4º, II, da Lei n. 14.063, de 23 de setembro de 2020. § 1º A ICP-RC não integra a cadeia hierárquica da ICP-Brasil”.

53. *In verbis*: “Art. 228-F. A LSEC-RCPN conterá dados que descrevem os serviços aceitos como confiáveis pelo ON-RCPN. (...) § 3º A ICP-RC integra a LSEC-RCPN. § 4º É válida a utilização de assinaturas eletrônicas cuja raiz estiver registrada na LSEC-RCPN para os atos descritos nos art. 38 da Lei n. 11.977, de 7 de julho de 2009, art. 17 da Lei n. 6.015, de 31 de dezembro de 1973, e no art. 17-A da Lei n. 14.063, de 14 de julho de 2023”.

54. Além do registro dos documentos listados no inciso I do art. 167, da Lei Federal n. 6.015, de 1973, há também as averbações constantes no inciso II do mesmo dispositivo, assim como procedimentos especiais, como, v.g. a usucapião (art. 216-A), a retificação de área (art. 213) e a intimação para regularização de pagamento decorrente de compromisso de compra e venda (art. 251-A).

55. À luz do art. 108 do Código Civil, os atos que visem à constituição, transferência, modificação ou renúncia de direitos reais sobre imóveis de valor superior a trinta vezes o maior salário mínimo vigente no País deverão ser feitos mediante escritura pública. Essa regra, no entanto, é relativizada para as operações realizadas por entes vinculados ao Sistema Financeiro Habitacional (SFH), conforme art. 61 da Lei Federal n. 4.380 de 1964, e Sistema Financeiro Imobiliário (SFI), cf. art. 38 da Lei Federal n. 9.514, de 1997.

56. ALVARES, Luís Ramon. *O Papel dos Cartórios Extrajudiciais na Dinâmica da Desjudicialização no Brasil*. 2022, 61 f. Dissertação (Mestrado) - Programa de Pós-graduação em Direito Curso de Mestrado Profissional, Universidade de Araraquara (UNIARA), Araraquara, 2022.

57. FARIA, Bianca Castellar de; LACERDA, Naurican Ludovico. A eficiência do Registro Imobiliário brasileiro e os impactos da Medida Provisória 1.085/2021. *In*: FIUZA, César Augusto de Castro; MARTOS, Frederico Thales; BORGES, Maria Creusa de Araújo. *Direito Civil Contemporâneo*. Florianópolis: CONPEDI, 2022.

versidade de fatores de autenticação que proporciona diversas camadas de segurança e impedem o obsolescimento⁵⁸.

Trata-se de chave decodificadora do avanço do registro eletrônico de imóveis, que promove maior desburocratização ao mesmo tempo que garante uma segurança jurídica pautada em um arcabouço normativo que reconhece a confiabilidade inerente a essa espécie de assinatura eletrônica, nos termos regulamentados.

3. Segundo Decodificador: a segurança do armazenamento digital de documentos e a possibilidade de uso da Tecnologia Blockchain

Um segundo pilar para a inserção dos cartórios na era digital é a segurança do armazenamento de documentos nato-digitais. Trata-se, aqui, não somente de prevenção a acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, como preconizado pela Lei Federal n. 13.709, de 2018, mas de específica construção de um panorama técnico que promova a confidencialidade, a integridade e a disponibilidade das informações em registro⁵⁹.

Essas regras acabaram sendo desenvolvidas com ênfase no Provimento n. 74, de 2018, do Conselho Nacional de Justiça, direcionadas às serventias extrajudiciais divididas em três classes, conforme montante de faturamento. Há, nesse sentido, uma lacuna normativa quanto às regras de segurança das atividades desenvolvidas no âmbito do SREI e ao Repositório Confiável de Documentos Eletrônicos (RCDE).

Trata-se, no entanto, de abordagem associada ao sistema de governança do ONR, a quem cabe a instituição de diretrizes técnicas para implantação e coordenação do SREI⁶⁰. O presente estudo parte, então, para investigar a possibilidade de utilização da tecnologia *Blockchain* como possível aliada à segurança técnica do arquivamento de documentos nato-digitais no Registro Eletrônico de Imóveis.

58. PINHEIRO, Patrícia Peck; WEBER, Sandra Tomazi; OLIVEIRA NETO, Antonio Alves de. *Fundamentos dos Negócios e Contratos Digitais*. 2. ed. São Paulo: Revista dos Tribunais, 2021.

59. HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. *Fundamentos de Segurança da Informação*: Com base na ISO 27001 e na ISO 27002. São Paulo: Brasport, 2018.

60. Constitui como atribuição do ONR apresentar “sugestões à Corregedoria Nacional de Justiça para edição de instruções técnicas de normalização aplicáveis ao SREI para propiciar a operação segura do sistema, a interoperabilidade de dados e documentos e a longevidade de arquivos eletrônicos, como também a adaptação eletrônica dos requisitos jurídico-formais implicados nos serviços, visando garantir a autenticidade e segurança das operações realizadas com documentos informáticos” (art. 31, II, “d”, do Provimento n. 89, de 2019, do CNJ).

3.1 Blockchain: elementos conceituais e aplicações

Comumente associado às “criptomoedas” e aos “*Non-Fungible Tokens*”, a tecnologia *Blockchain* representa inegável avanço na segurança e integridade da informação, principalmente quando se põe em foco o contexto sociotécnico no qual o elevado fluxo informacional performa as diversas dimensões da sociedade⁶¹. A *Blockchain* é um mecanismo tecnológico que se viabiliza a partir da descentralização do registro de dados em uma rede encadeada, procedimento também denominado de *decentralised ledger technology*⁶², em contraposição à centralização do registro de informação que é comum aos fluxos de dados.

Barbosa⁶³ traz à luz um conceito de *Blockchain* como uma lista de blocos, que cresce continuamente, que se relacionam de forma segura por meio de criptografia, em uma rede *peer-to-peer*. Faleiros Júnior e Roth⁶⁴, por sua vez, apresentam o conceito de Tapscott e Tapscott⁶⁵, reverberando que a *Blockchain* se baseia em um conjunto de regras, na forma de cálculos distribuídos, que asseguram a integridade dos dados em fluxo, mantendo-se um registro compartilhado em consonância por inúmeros validadores. Cada unidade dessa rede armazena informações, conforme sua configuração, como créditos, débitos ou propriedades, que são verificadas por meio do consenso com outros pontos⁶⁶.

A descentralização de registro é dada por um livro-razão, ou “*ledger*”, que recebe a informação e a multiplica ao longo de uma rede complexa de pontos-chave⁶⁷, sem um registro centralizado, ou unificado⁶⁸. Não há hierarquia entre as unidades da cadeia, nem se realiza a gestão a partir de um nó central, mas através de uma distribuição espacial de convergência linear⁶⁹. Cada nó dessa rede constitui um participante, que aumenta a confiança pelo comparti-

61. O'SHIELDS, Reggie. Smart Contracts: Legal Agreements for the Blockchain. *North Carolina Banking Institute*, v. 21, p. 177-194, 2017.

62. ZETSCHE, Dirk; BUCKLETY, Ross; ARNER, Douglas. The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *SSRN - European Banking Institute Working Paper Series 14*, 2017.

63. BARBOSA, Mafalda Miranda. Blockchain e responsabilidade civil. In: BARBOSA, M. M.; BRAGA NETTO, F.; SILVA, M.C.; FALEIROS JÚNIOR, J. L. M. (coords.). *Direito Digital e Inteligência Artificial: Diálogos entre Brasil e Europa*. Indaiatuba: Foco, 2021, p. 797-824.

64. FALEIROS JÚNIOR, José Luiz de Moura; ROTH, Gabriela. Como a utilização do Blockchain pode afetar Institutos Jurídicos Tradicionais?. *Revista Jurídica do Ministério Público Catarinense*, Florianópolis, v. 14, n. 30, p. 39-59, jun./nov. 2019.

65. TAPSCOTT, Don; TAPSCOTT, Alex. *Blockchain Revolution: como a tecnologia por trás do bitcoin está mudando o dinheiro, os negócios e o mundo*. São Paulo: SENAI-SP, 2016.

66. RASKIN, Max. The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, v. 1, n. 2, p. 305-341, 2017.

67. A ideia de uma rede complexa, formada por unidades específicas é o que dá forma à conceituação de *Blockchain*, de forma que o presente estudo utiliza os termos “bloco”, “pontos”, ou “pontos-chave” de forma indistinta, considerando-se que no contexto aqui apresentado, ambos podem servir à mesma compreensão.

68. BARBOSA, Mafalda Miranda. Blockchain e responsabilidade civil. In: BARBOSA, M. M.; BRAGA NETTO, F.; SILVA, M.C.; FALEIROS JÚNIOR, J. L. M. (coords.). *Direito Digital e Inteligência Artificial: Diálogos entre Brasil e Europa*. Indaiatuba: Foco, 2021, p. 797-824.

69. ZETSCHE, Dirk; BUCKLETY, Ross; ARNER, Douglas. The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *SSRN - European Banking Institute Working Paper Series 14*, 2017.

lhamento dos mesmos dados. Nessa circunstância, o acréscimo de participantes enseja igualmente a adição de validadores da informação registrada no *ledger*⁷⁰. Nessa esteira, a *Blockchain* consagra a descentralização da informação em consonância com a necessidade de consenso.

A doutrina consagra cinco atributos para a tecnologia *Blockchain*: (i) distributividade, pois cada integrante da rede pode inferir a totalidade dos dados em fluxo e seu histórico; a (ii) irreversibilidade, pois os registros não podem ser alterados, ficando imutavelmente ligados a cada transação registrada que tenha ocorrido anteriormente; o (iii) *peer-to-peer*, ante a viabilização direta entre os *pontos-chave* da rede, sendo dispensada a figura do intermediário; a (iv) programação lógica, por conta do processamento via codificação computacional; e (v) a transparência, pois cada bloco fica disponível para qualquer integrante da rede, ainda que os dados sejam anonimizados⁷¹. É a irreversibilidade que viabiliza uma autenticidade do conteúdo grafado no livro-razão, em atenção à onerosidade técnica para sua modificação⁷².

No contexto relacional, a utilização da *Blockchain* se associa à realização de transações, mediante aposição de um *hash* à informação apontada, de maneira que cada ponto-chave mantém em registro o fluxo de dado, em referência ao ponto anterior⁷³. A sincronização entre as informações registradas no ponto anterior e no seguinte mantém a integridade dos dados em fluxo, viabilizando a transação⁷⁴. Especificamente no contexto dos criptoativos, os blocos em cadeia mantêm, além da titularidade associada, o registro de data e hora de cada transação realizada, consolidando-se uma cadeia de propriedade⁷⁵.

Aqui, a validação da informação constante no livro-razão é resultado da convergência e consenso de todos os pontos-chave da cadeia, em contraposição à centralização do *ledger* em um intermediário confiável, tal como ocorrer nas transações bancárias⁷⁶. Isso implica em considerar que, para que uma modificação não

70. O'SHIELDS, Reggie. Smart Contracts: Legal Agreements for the Blockchain. *North Carolina Banking Institute*, v. 21, p. 177-194, 2017.

71. CHITTENDEN, Tara. *Blockchain: The Legal Implications of Distributed Systems*. The Law Society: London, 2017; BARBOSA, Mafalda Miranda. Blockchain e responsabilidade civil. In: BARBOSA, M. M.; BRAGA NETTO, F.; SILVA, M.C.; FALEIROS JÚNIOR, J. L. M. (coords.). *Direito Digital e Inteligência Artificial: Diálogos entre Brasil e Europa*. Indaiatuba: Foco, 2021, p. 797-824.

72. NALIN, Paulo; NAGAROLI, Rafaella. Inteligência artificial, blockchain e smart contracts: breves reflexões sobre o novo desenho jurídico do contrato na sociedade da informação. In: BARBOSA, M. M.; BRAGA NETTO, F.; SILVA, M.C.; FALEIROS JÚNIOR, J. L. M. (coords.). *Direito Digital e Inteligência Artificial: Diálogos entre Brasil e Europa*. Indaiatuba: Foco, 2021, p. 753-773.

73. DIVINO, Sthéfano Bruno Santos. Smart Contracts: Conceitos, Limitações, Aplicabilidade e Desafios. *Revista Jurídico Luso-Brasileira*, a. 4, n. 6, p. 2771-2808, nov./dez. 2018.

74. WRIGHT, Aaron; DE FILIPPI, Primavera. Decentralized Blockchain Technology and the Rise of Lex Cryptographia, *SSRN*, 10 de março de 2015; CANTALI, Rodrigo Ustároz. Smart Contracts e Direito Contratual: Primeiras Impressões sobre suas Vantagens e Limites. *Revista Jurídico Luso-Brasileira*, a. 8, n. 3, p. 1529-1599, maio/jun. 2022.

75. RASKIN, Max. The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, v. 1, n. 2, p. 305-341, 2017.

76. ZETSCHE, Dirk; BUCKLETY, Ross; ARNER, Douglas. The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *SSRN - European Banking Institute Working Paper Series 14*, 2017.

autorizada ocorra, é necessária que a ação seja coordenada para com todos os blocos da cadeia, simultaneamente, o que torna o procedimento mais dificultoso⁷⁷.

Esse panorama se amplia quando em foco a diferenciação entre *Blockchain* pública e privada. Na cadeia de blocos pública há liberdade de agregação por qualquer usuário, independentemente de permissão, passando a integrar a rede de validação e contribuir para a convergência⁷⁸. Esse modelo, também conhecido como *Blockchain* não permissionada, viabiliza o anonimato dos seus usuários, ao mesmo tempo que não se define a quantidade de pontos-chave nessa cadeia⁷⁹. Por sua vez, a cadeia de blocos privada mantém pré-determinado o parâmetro de quem poderá lhe agregar, a quantidade de usuários e quais efetivamente podem contribuir com o consenso⁸⁰. Nesse sistema – chamado por Zetsche *et al.*⁸¹ como *permissionado*, – inexistente anonimato, de maneira que as permissões de cada usuário e sua autenticidade podem ser definidas a partir da aposição de um certificado digital⁸².

A aplicação da tecnologia *Blockchain* aos “*Smart Contracts*”, tem resultado na sua franca expansão, na medida em que serve como subsídio técnico para uma robusta segurança na autoexecutoriedade de sua programação⁸³. Os *Smart Contracts* não é figura específica do direito contratual, mas forma de execução automática das disposições de um acordo por meio de engenharia computacional, ou um *software*⁸⁴⁻⁸⁵. É um programa de computador, escrito

77. GUIMARÃES, Luíza Resende; CASTRO, Maria Clara Versiani de. Afinal, smart contracts são contratos? Natureza jurídica a partir de uma leitura sociológica. In: CHAVES, N. C.; COLOMBI, H. (Orgs). *Direito e Tecnologia: novos modelos e tendências*. Porto Alegre: Fi, 2021, p. 36-64.

78. ZETSCHE, Dirk; BUCKLETY, Ross; ARNER, Douglas. The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *SSRN - European Banking Institute Working Paper Series 14*, 2017; ALEXANDRE, Marcos Gaspar. *Sharing Economy e Blockchain: Problemas e Possíveis Soluções*, 2018, 105f. Dissertação de Mestrado em Gestão - Faculdade de Economia da Universidade de Coimbra, Coimbra, 2018.

79. VUKOLIC, Marko. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. *Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*, v. 9591, p. 112-126, 2016; ALEXANDRE, Marcos Gaspar. *Sharing Economy e Blockchain: Problemas e Possíveis Soluções*, 2018, 105f. Dissertação de Mestrado em Gestão - Faculdade de Economia da Universidade de Coimbra, Coimbra, 2018.

80. PILKINGTON, Marc. Blockchain Technology: Principles and Applications. In: OLLEROS, F. X.; ZHEGU, M. (eds). *Research Handbook on Digital Transformations*, Cheltenham: Edward Edgar Publishing, 2016.

81. ZETSCHE, Dirk; BUCKLETY, Ross; ARNER, Douglas. The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *SSRN - European Banking Institute Working Paper Series 14*, 2017

82. ALEXANDRE, Marcos Gaspar. *Sharing Economy e Blockchain: Problemas e Possíveis Soluções*, 2018, 105f. Dissertação de Mestrado em Gestão - Faculdade de Economia da Universidade de Coimbra, Coimbra, 2018.

83. O'SHIELDS, Reggie. Smart Contracts: Legal Agreements for the Blockchain. *North Carolina Banking Institute*, v. 21, p. 177-194, 2017; CANTALI, Rodrigo Ustároz. Smart Contracts e Direito Contratual: Primeiras Impressões sobre suas Vantagens e Limites. *Revista Jurídico Luso-Brasileira*, a. 8, n. 3, p. 1529-1599, 2022.

84. Interessa ressaltar que, segundo Florani, os *Smart Contracts* são uma terceira fase na contratação digital. A primeira fase diz respeito aos contratos eletrônicos, em que há mera transposição do suporte em que se registra o acordo de vontades. A segunda etapa concerne aos contratos orientados por dados, que se posicionam como um híbrido entre os acordos tradicionais e o preenchimento automático de informações por meio digital (FLORANI, Lara Bonemer Rocha. *Smart contracts nos contratos empresariais: um estudo sobre possibilidade e viabilidade econômica de sua utilização*. 2020. 163 f. Tese (doutorado) – Pontifícia Universidade Católica do Paraná, 2020).

85. CANTALI, Rodrigo Ustároz. Smart Contracts e Direito Contratual: Primeiras Impressões sobre suas Vantagens e Limites. *Revista Jurídico Luso-Brasileira*, a. 8, n. 3, p. 1529-1599, maio/jun. 2022.

em linguagem de código, que é estruturado em algoritmos⁸⁶ para produzir um resultado pré-determinado. Esse conceito foi idealizado por Nick Szabó⁸⁷, ao buscar dar autoexecutoriedade aos deveres contratuais a partir da ocorrência de um evento desencadeador⁸⁸. Esse produto fornece uma rápida resposta às condições em que se programou o software, dando maior racionalidade às negociações.

A *Blockchain* não é essencial para a concepção de um *Smart Contract*, mas é a partir dela que se fornece segurança suficiente para que a execução dos deveres contratuais siga a forma anteriormente planejada⁸⁹. O registro das transações no livro-razão descentralizado promove uma coesa validação dos dados em fluxo, impedindo a modificação das obrigações pré-determinadas⁹⁰. Essa programação de obrigações contratuais transforma um *ledger* estático em um sistema dinâmico capaz de executar a dialética de negócios de um contrato⁹¹. Essa lógica é o que dá subsídio para as transações envolvendo criptomoedas, a partir do registro do fluxo de saída e de entrada do ativo em carteiras protegidas por criptografia por chaves assimétricas⁹². A segurança inerente a essa operação converge com as principais demandas no fluxo de informações na era digital.

86. Destaca-se que “algoritmo”, embora seja rapidamente associado aos sistemas de inteligência artificial, constitui conceito diferente. Os algoritmos podem ser conceituados como um conjunto de instruções, organizadas de forma sequencial, que determina um comando, uma ordem a ser executada (MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. *Revista de Direito Público*, v. 16, n. 90, p. 39-64, nov./dez. 2019). Trata-se da própria programação de comandos a serem executados por um organismo, seja mecânico ou computacional (ACIOLY, Luis Henrique de Menezes. Reflexões sobre a Utilização da Inteligência Artificial e Algoritmos nas Relações Consumeristas à Luz da Lei Geral de Proteção de Dados. *Revista Brasileira de Direito Comercial, Concorrência, Empresarial e do Consumidor*. Porto Alegre: Lex Magister. v. 48, p. 165-187, ago./set. 2022). Inteligência Artificial, por sua vez, pode ser trazido como o campo de estudo voltado à construção de sistemas capazes de exibir comportamentos humanos, através do aprendizado (BIGONHA, Carolina. Inteligência Artificial em Perspectiva. *Panorama Setorial da Internet*, a. 10, n. 2, p. 1-9, jul./out. 2018). No contexto da IA é o algoritmo que estrutura a lógica para construção do aprendizado de máquina (ACIOLY, Luis Henrique de Menezes. Reflexões sobre a Utilização da Inteligência Artificial e Algoritmos nas Relações Consumeristas à Luz da Lei Geral de Proteção de Dados. *Revista Brasileira de Direito Comercial, Concorrência, Empresarial e do Consumidor*. Porto Alegre: Lex Magister. v. 48, p. 165-187, ago./set. 2022).

87. SZABO, Nick. Formalizing and Securing Relationships on Public Networks. *First Monday*, v. 2, n. 9, 1997.

88. Um exemplo dado por Szabó (SZABO, Nick. Formalizing and Securing Relationships on Public Networks. *First Monday*, v. 2, n. 9, 1997), apresentado pela doutrina é a máquina de venda automática, que recebe o valor do usuário e lhe entrega o produto escolhido, de forma simples (RASKIN, Max. The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, v. 1, n. 2, p. 305-341, 2017; FLORANI, Lara Bonemer Rocha. *Smart contracts nos contratos empresariais: um estudo sobre possibilidade e viabilidade econômica de sua utilização*. 2020. 163 f. Tese (doutorado) – Pontifícia Universidade Católica do Paraná, 2020; CANTALI, Rodrigo Ustároz. *Smart Contracts e Direito Contratual: Primeiras Impressões sobre suas Vantagens e Limites*. *Revista Jurídico Luso-Brasileira*, a. 8, n. 3, p. 1529-1599, maio/jun. 2022).

89. O'SHIELDS, Reggie. Smart Contracts: Legal Agreements for the Blockchain. *North Carolina Banking Institute*, v. 21, p. 177-194, 2017; ACIOLY, Luis Henrique de Menezes; OLIVEIRA, Micael Araújo de Souza. Espectro de Aplicação dos *Smart Contracts* à Luz do Direito Contratual Brasileiro: Breves considerações no contexto da boa-fé objetiva. *Revista Conversas Civilísticas*, Salvador, v. 2, n. 2, p. 98-121, 2022.

90. ACIOLY, Luis Henrique de Menezes; OLIVEIRA, Micael Araújo de Souza. Espectro de Aplicação dos *Smart Contracts* à Luz do Direito Contratual Brasileiro: Breves considerações no contexto da boa-fé objetiva. *Revista Conversas Civilísticas*, Salvador, v. 2, n. 2, p. 98-121, 2022.

91. FLORANI, Lara Bonemer Rocha. *Smart contracts nos contratos empresariais: um estudo sobre possibilidade e viabilidade econômica de sua utilização*. 2020. 163 f. Tese (doutorado) – Pontifícia Universidade Católica do Paraná, 2020.

92. NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2009. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 01 jul. 2024; FOLLADOR, Guilherme Broto. Criptomoedas e competência tributária. *Revista Brasileira de Políticas Públicas*, Brasília, v. 7, n. 3, p. 79-104, 2017.

3.2 Repositório Confiável de Documentos Eletrônicos e o armazenamento digital

Promovendo um pequeno salto de raciocínio, a inserção da *Blockchain* na estrutura do Poder Público brasileiro ganhou destaque com a *Notarchain*, no âmbito da plataforma e-Notariado, para veiculação via *Internet* dos serviços notariais, associada ao Provimento n. 100, de 2020, do Conselho Nacional de Justiça. A *Notarchain* foi desenvolvida em parceria com a IBM, por meio de uma tecnologia denominada “*Hyperledger Fabric*” (Santos, 2022), e se constitui como espécie de *Blockchain* privada. A *Notarchain* viabiliza diferentes níveis de acesso, conforme permissão inerente ao tipo de usuário mediante certificado digital que garante autenticidade⁹³. Por sua vez, o acesso é restrito aos usuários previamente autorizados, limitando-se o número de pontos-chave aos notários.

Trata-se de parâmetros técnicos coesos que dão sustentabilidade à atuação do delegatário no ambiente digital, promovendo uma segurança compartilhada por todos os blocos de uma cadeia restrita de agentes. Em outro giro, o Repositório Confiável de Documentos Eletrônicos (RCDE), módulo específico do SAEC, possui função semelhante, consistente em viabilizar o armazenamento de documentos eletrônicos, *i.e.* arquivos nato digitais ou desmaterializados de procurações, certidões, contratos, cancelamentos de hipoteca, escrituras públicas, para suporte aos atos registrais⁹⁴. Esses arquivos estariam, então, acessíveis para qualquer Oficial de Registro de Imóveis, evitando-se novos pedidos de documentos quando o usuário indicar sua submissão à plataforma.

O RCDE surgiu no âmbito do Serviço de Atendimento Eletrônico Compartilhado como iniciativa associada ao cumprimento das disposições do art. 10 da Portaria n. 1.248, de 2023, do Ministério das Cidades, que trata da declaração de quitação dos contratos celebrados com recursos do Fundo de Arrendamento Residencial (FAR) e do Fundo de Desenvolvimento Social (FDS), no âmbito do Programa Nacional de Habitação Urbana (PNHU), administrados pela Caixa Econômica Federal⁹⁵. A partir do RCDE podem ser feitos o armazenamento do Termo de Quitação e Procuração desses contratos, viabilizando um acesso facilitado aos oficiais de registro.

93. SANTOS, Gabriel Gonçalves. *Smart Contracts: Conceitos, limitações e potencialidades*. 2022, 138f. il. Dissertação (Mestrado) - Universidade Federal de Minas Gerais, Faculdade de Direito, Belo Horizonte, 2022.

94. OPERADOR NACIONAL DO SISTEMA DO REGISTRO ELETRÔNICO DE IMÓVEIS - ONR. *Comunicado nº 2, de 2024*. Declaração de Quitação. Disponível em: https://www.irib.org.br/app/webroot/files/downloads/files/CAMPAIGN_334%5B1%5D.pdf. Acesso em: 01 jul. 2024.

95. OPERADOR NACIONAL DO SISTEMA DO REGISTRO ELETRÔNICO DE IMÓVEIS - ONR. *Comunicado nº 2, de 2024*. Declaração de Quitação. Disponível em: https://www.irib.org.br/app/webroot/files/downloads/files/CAMPAIGN_334%5B1%5D.pdf. Acesso em: 01 jul. 2024.

Entretanto, a funcionalidade de consolidação de meio de arquivamento de documentos nato-digitais promove o reenquadramento da ferramenta, para lhe dar importância singular no contexto do armazenamento de arquivos e livre acesso ao Oficial de Registro de Imóveis, servindo como um suporte amplo para os atos eletrônicos registrais. Para tanto, a *Blockchain* privada pode ser utilizada como tecnologia de arquivamento que congrega a segurança da inalterabilidade do conteúdo com a validação distribuída entre os oficiais de registro, como pontos-chave de uma cadeia complexa.

Considerações Finais

No presente artigo foram apresentadas questões sensíveis ao contexto de um avanço tecnológico decorrente do panorama normativo. Foi necessário investigar o ambiente normativo para compreender o contexto técnico em que o desenvolvimento do Registro Eletrônico de Imóveis se realiza. Para tanto, os temas analisados foram pontos-chave para compreender a dinâmica de condução do registro de imóveis digital.

Ao se investigar o desenvolvimento normativo do Sistema do Registro Eletrônico de Imóveis (SREI), pôde-se compreender que seu delineamento não foi uniforme, previsível e sistematizado desde a sua concepção na Lei Federal n. 11.977, de 2009, mas decorreu de um conjunto normas que sucessivamente foram dando estrutura e modelando a atividade. Observou-se que o SREI, no formato atual, apresenta uma sólida estrutura de governança e sustentabilidade que viabiliza a sua operação em âmbito nacional, interconectando serventias de registro imobiliário de todo o país e concentrando a prestação digital dos serviços em único ponto de acesso na *Internet*, o Serviço de Atendimento Eletrônico Compartilhado (SAEC).

Passou-se então à análise dos temas decodificadores. A assinatura eletrônica, como forma de dar autenticidade e integridade aos documentos nato-digitais, tiveram o desenvolvimento de sua aceitabilidade de forma semelhante ao próprio SREI, isto é, a partir de um complexo normativo que foram dando forma à sua utilização perante atos do registro público que envolvam bens imóveis. Nesse escopo, a prevalência da modalidade qualificada da assinatura, baseada na Infraestrutura de Chaves Públicas Brasileira, tem dado espaço à convivência simultânea desse modelo com a aceitabilidade da assinatura eletrônica avançada. Isso fomenta a desburocratização e a democratização do registro imobiliário, na medida em que os modelos de assinatura avançada possibilitam diversificados fatores de autenticação, garantindo a segurança das operações.

Por sua vez, o arquivamento digital de documentos é matéria pouco baseada em normas regulamentadoras, seja em razão da inconveniência de uma regulação técnica do assunto, por claro risco de obsolescência jurídica, seja por já haver um conjunto técnico de segurança da informação baseado em padrões e boas práticas. Nesse sentido, o aperfeiçoamento do modelo de arquivamento digital reside na incorporação da tecnologia *Blockchain*, especialmente no contexto do Repositório Confiável de Documentos Eletrônicos junto ao SAEC, de utilização compartilhada por registradores e usuários.

Referências Bibliográficas

ACIOLY, Luis Henrique de Menezes. Reflexões sobre a Utilização da Inteligência Artificial e Algoritmos nas Relações Consumeristas à Luz da Lei Geral de Proteção de Dados. *Revista Brasileira de Direito Comercial, Concorrência, Empresarial e do Consumidor*. Porto Alegre: Lex Magister. v. 48, p. 165-187, ago./set. 2022.

ACIOLY, Luis Henrique de Menezes; OLIVEIRA, Micael Araújo de Souza. Espectro de Aplicação dos *Smart Contracts* à Luz do Direito Contratual Brasileiro: Breves considerações no contexto da boa-fé objetiva. *Revista Conversas Civilísticas*, Salvador, v. 2, n. 2, p. 98-121, 2022.

ALEXANDRE, Marcos Gaspar. *Sharing Economy e Blockchain: Problemas e Possíveis Soluções*, 2018, 105f. Dissertação de Mestrado em Gestão – Faculdade de Economia da Universidade de Coimbra, Coimbra, 2018.

ALVARES, Luís Ramon. *O Papel dos Cartórios Extrajudiciais na Dinâmica da Desjudicialização no Brasil*. 2022, 61 f. Dissertação (Mestrado) – Programa de Pós-graduação em Direito Curso de Mestrado Profissional, Universidade de Araraquara (UNIARA), Araraquara, 2022.

ALVIM, Arruda; CUNHA, Igor Martins da. As assinaturas eletrônicas no ordenamento jurídico brasileiro e a relevância da autonomia privada: uma breve análise da validade dos documentos eletrônicos à luz da MP 2.200-2/2001 e da Lei 14.063/2020. *Revista de Processo*, São Paulo: Revista dos Tribunais, a. 48, v. 337, p. 83-114, São Paulo: RT, mar. 2023.

ASSAD, Frederico Jorge Vaz de Figueiredo. Registro de imóveis eletrônico e governança fundiária. *Revista de Direito Imobiliário*, a. 39, v. 81, p. 215-234, jul./dez. 2016.

BARBOSA, Mafalda Miranda. Blockchain e responsabilidade civil. In: BARBOSA, M. M.; BRAGA NETTO, F.; SILVA, M.C.; FALEIROS JÚNIOR, J. L. M. (coords.). *Direito Digital e Inteligência Artificial: Diálogos entre Brasil e Europa*. Indaiatuba: Foco, 2021, p. 797-824.

BIGONHA, Carolina. Inteligência Artificial em Perspectiva. *Panorama Setorial da Internet*, a. 10, n. 2, p. 1-9, jul./out. 2018.

CANTALI, Rodrigo Ustároz. Smart Contracts e Direito Contratual: Primeiras Impressões sobre suas Vantagens e Limites. *Revista Jurídico Luso-Brasileira*, a. 8, n. 3, p. 1529-1599, maio/jun. 2022.

CASTELLS, Manuel. *A sociedade em rede*. Trad. Roneide Venâncio Majer. 6. ed. São Paulo: Paz e Terra, 2002.

CASTRO, Manuella Santos. *Registro de Imóveis na Era Digital: Impactos das novas tecnologias no sistema registral brasileiro*. 2021, 306 f. Tese (Doutorado) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021.

CHITTENDEN, Tara. *Blockchain: The Legal Implications of Distributed Systems*. The Law Society: London, 2017.

DIVINO, Sthéfano Bruno Santos. Smart Contracts: Conceitos, Limitações, Aplicabilidade e Desafios. *Revista Jurídico Luso-Brasileira*, a. 4, n. 6, p. 2771-2808, nov./dez. 2018.

FALEIROS JÚNIOR, José Luiz de Moura. Inovação, desenvolvimento e a Lei do Governo Digital (Lei nº 14.129/2021): perspectivas quanto às estruturas de governo como plataforma. *Inova Jur – Revista Jurídica da UEMG*, Belo Horizonte, v. 1, n. 1, p. 1-29, jan./jun. 2022.

FALEIROS JÚNIOR, José Luiz de Moura; ROTH, Gabriela. Como a utilização do Blockchain pode afetar Institutos Jurídicos Tradicionais?. *Revista Jurídica do Ministério Público Catarinense*, Florianópolis, v. 14, n. 30, p. 39-59, jun./nov. 2019.

FARIA, Bianca Castellar de; LACERDA, Naurican Ludovico. A eficiência do Registro Imobiliário brasileiro e os impactos da Medida Provisória 1.085/2021. In: FIUZA, César Augusto de Castro; MARTOS, Frederico Thales de Araújo; BORGES, Maria Creusa de Araújo. *Direito Civil Contemporâneo*. Florianópolis: CONPEDI, 2022.

FIORANELLI, Ademar. Matrícula no registro de imóveis: questões práticas. In: YOSHIDA, Consuelo Yatsuda Moromizato Yoshida; FIGUEIREDO, Marcelo. AMADEI, Vicente de Abreu (coords). *Direito notarial e registral avançado*. São Paulo: Revista dos Tribunais, 2014.

FLORANI, Lara Bonemer Rocha. *Smart contracts nos contratos empresariais: um estudo sobre possibilidade e viabilidade econômica de sua utilização*. 2020. 163 f. Tese (doutorado) – Pontifícia Universidade Católica do Paraná, 2020.

FOLLADOR, Guilherme Broto. Criptomoedas e competência tributária. *Revista Brasileira de Políticas Públicas*, Brasília, v. 7, n. 3, p. 79-104, 2017. Disponível em: <https://www.publicacoes.uniceub.br/RBPP/article/view/4925/0>. Acesso em: 01 jul. 2024.

GRUBER, Rafael Ricardo. Registro Eletrônico de Imóveis, Cadastros e SINTER: Interconexão sem Submissão. *Revista de Direito Imobiliário*, a. 39, v. 81, p. 253-287, jul./dez. 2016.

GUIMARÃES, Luíza Resende; CASTRO, Maria Clara Versiani de. Afinal, smart contracts são contratos? Natureza jurídica a partir de uma leitura sociológica. In: CHAVES, N. C.; COLOMBI, H. (Orgs). *Direito e Tecnologia: novos modelos e tendências*. Porto Alegre: Fi, 2021, p. 36-64.

HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. *Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002*. São Paulo: Brasport, 2018.

LEITE, Clarisse Frechiani Lara. Assinatura eletrônica. *Revista de Processo*, São Paulo: Revista dos Tribunais, a. 48, v. 345, p. 79-121, nov. 2023.

MADALENA, Juliano. Regulação das Fronteiras da Internet: um primeiro passo para uma Teoria Geral do Direito Digital. In: MARTINS, G. M.; LONGHI, J. V. R. (coords.). *Direito Digital: Direito Privado e Internet*. 2. ed. Indaiatuba: Foco, 2019. p. 183-206.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. *Revista de Direito Público*, v. 16, n. 90. p. 39-64, nov./dez. 2019.

MENKE, Fabiano. A forma dos contratos eletrônicos. *Revista de Direito Civil Contemporâneo*, São Paulo: Revista dos Tribunais, a. 8, v. 26, p. 85-113, jan./mar. 2021.

MIRANDA, Caleb Matheus Ribeiro de. Comentários ao Sistema Eletrônico de Registros Públicos (SERP) – artigos 1º ao 9º. In: KÜMPEL, Vitor (Coord). *Breves comentários à Lei nº 14.382/2022*. 2 ed. São Paulo: YK, 2023, p. 11-48.

MOSES, Lyria Bennett. How to Think About Law, Regulation and Technology: Problems with ‘Technology’ as a Regulatory Target. *Law, Innovation and Technology*, v. 5, n. 1, p. 1-20, 2013. Disponível em: <http://ssrn.com/abstract=2464750>. Acesso em: 11 jun. 2023.

NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2009. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 01 jul. 2024.

NALIN, Paulo; NAGAROLI, Rafaella. Inteligência artificial, blockchain e smart contracts: breves reflexões sobre o novo desenho jurídico do contrato na sociedade da informação. In: BARBOSA, M. M.; BRAGA NETTO, F.; SILVA, M.C.; FALEIROS JÚNIOR, J. L. M. (coords.). *Direito Digital e Inteligência Artificial: Diálogos entre Brasil e Europa*. Indaiatuba: Foco, 2021, p. 753-773.

OPERADOR NACIONAL DO SISTEMA DO REGISTRO ELETRÔNICO DE IMÓVEIS – ONR. *Comunicado nº 2, de 2024*. Declaração de Quitação. Disponível em: https://www.irib.org.br/app/webroot/files/downloads/files/CAMPAIGN_334%5B1%5D.pdf. Acesso em: 01 jul. 2024.

O'REILLY, Tim. Government as platform. *Innovations: Technology, Governance, Globalization*, Cambridge, v. 6, n. 1, p. 13-40, 2011. Disponível em: <https://direct.mit.edu/itgg/article/6/1/13/9649/Government-as-a-Platform>. Acesso em: 15 jun. 2024.

O'SHIELDS, Reggie. Smart Contracts: Legal Agreements for the Blockchain. *North Carolina Banking Institute*, v. 21, p. 177-194, 2017.

PILKINGTON, Marc. Blockchain Technology: Principles and Applications. In: OLLEROS, F. X.; ZHEGU, M. (eds). *Research Handbook on Digital Transformations*, Cheltenham: Edward Edgar Publishing, 2016.

PINHEIRO, Patrícia Peck; WEBER, Sandra Tomazi; OLIVEIRA NETO, Antonio Alves de. *Fundamentos dos Negócios e Contratos Digitais*. 2. ed. São Paulo: Revista dos Tribunais, 2021.

RASKIN, Max. The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, v. 1, n. 2, p. 305-341, 2017.

RIBEIRO, Moacyr Petrocelli de Ávila. A Matrícula: Paradigmas para o Sistema do Registro Eletrônico de Imóveis. *Revista de Direito Imobiliário*, a. 42, v. 86, p. 215-262, jan./jun. 2019.

SANTOS, Gabriel Gonçalves. *Smart Contracts: Conceitos, limitações e potencialidades*. 2022, 138f. il. Dissertação (Mestrado) – Universidade Federal de Minas Gerais, Faculdade de Direito, Belo Horizonte, 2022. Disponível em: <http://hdl.handle.net/1843/57345>. Acesso em: 01 jul. 2024.

SOTTANO, Augusto; LAGO, Ivan Jacopetti. As assinaturas eletrônicas e o registro de imóveis: estado atual da questão. In: GALHARDO, Flaviano; PARO, João P.; NALINI, José R.; BRANDELLI, Leonardo (org.). *Direito Registral e Novas Tecnologias*. Rio de Janeiro: Forense, 2021.

SZABO, Nick. Formalizing and Securing Relationships on Public Networks. *First Monday*, v. 2, n. 9, 1997. Disponível em: <https://doi.org/10.5210/fm.v2i9.548>. Acesso em: 01 jul. 2024.

TAPSCOTT, Don; TAPSCOTT, Alex. *Blockchain Revolution: como a tecnologia por trás do bitcoin está mudando o dinheiro, os negócios e o mundo*. São Paulo: SENAI-SP, 2016.

TAVARES, Ramos André. O Operador Nacional do Sistema de Registro Eletrônico de Imóveis: Resposta à Exigência Constitucional de um Eficiente Sistema Registral. *Jornal Eletrônico Migalhas*, v. 136, p. 23-42, 2018. Disponível em: <https://www.migalhas.com.br/arquivos/2018/8/art20180821-03.pdf>. Acesso em: 01. jul. 2024.

VALERIO, Alexandre Scigliano; BONFATTI, Fabio Fernandes Neves. Possibilidade de Assinatura, Registro e Protesto Eletrônico dos Títulos de Crédito do Agronegócio. *Revista Brasileira de Direito Empresarial*, v. 7, n. 2, p. 17-38, jul./dez. 2021.

VUKOLIC, Marko. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. *Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*, v. 9591, p. 112-126, 2016.

WRIGHT, Aaron; DE FILIPPI, Primavera. Decentralized Blockchain Technology and the Rise of Lex Cryptographia, *SSRN*, 10 de março de 2015. Disponível em: <http://dx.doi.org/10.2139/ssrn.2580664>. Acesso em: 01 jul. 2024.

ZETSCHE, Dirk; BUCKLETY, Ross; ARNER, Douglas. The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *SSRN – European Banking Institute Working Paper Series 14*, 2017. Disponível em: <http://dx.doi.org/10.2139/ssrn.3018214>. Acesso em: 01 jul. 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

14

O papel do Banco Central do Brasil na regulação das fintechs de pagamento

VICTOR CHAME ALVIM

Sumário: Introdução. 1. A Evolução das Fintechs de Pagamento no Brasil. 2. O Papel do Banco Central do Brasil na Regulação das Fintechs de Pagamento 2.1. Principais Regulações e Normas para Fintechs de Pagamento 3. Desafios e Oportunidades na Regulação das Fintechs de Pagamento. Considerações finais. Referências.

Introdução

Desde o seu surgimento, as fintechs têm desempenhado um papel revolucionário no cenário financeiro global, catalisando transformações significativas através da aplicação de tecnologia inovadora. Com a capacidade de romper paradigmas estabelecidos, essas empresas têm não apenas redefinido a maneira como os serviços financeiros são acessados e consumidos, mas também têm proporcionado inclusão econômica a segmentos anteriormente marginalizados. Este contexto destaca a importância de compreender não apenas o crescimento exponencial das fintechs, mas também os desafios regulatórios e as oportunidades para a inovação que este setor emergente enfrenta.

A justificativa para este estudo reside na necessidade premente de explorar o impacto das fintechs no ambiente financeiro brasileiro. Em um país marcado por uma significativa bancarização e uma rápida adoção de tecnologias digitais, compreender como as fintechs estão moldando e sendo moldadas pelo contexto regulatório e econômico é crucial. Este trabalho visa contribuir para um entendimento mais profundo das dinâmicas entre inovação tecnológica, regulação financeira e inclusão financeira, fornecendo contribuições relevantes para formuladores de políticas, acadêmicos e profissionais do setor financeiro.

O problema de pesquisa central deste estudo é: como as fintechs de pagamento estão sendo regulamentadas no Brasil, e de que maneira essas regulamentações influenciam sua capacidade de promover inclusão financeira e inovação tecnológica? Esta questão busca investigar não apenas os desafios enfrentados pelas fintechs no contexto regulatório brasileiro, mas também as oportunidades que surgem com uma regulação eficaz e adaptável. Ao delimitar este problema, o estudo se propõe a oferecer respostas claras e objetivas que contribuam para um debate informado e fundamentado sobre o futuro das fintechs no país.

1. Bacharel em Direito pela Universidade Federal Fluminense - UFF e pós-graduando em direito digital pelo ITS Rio em parceria com a Universidade do Estado do Rio de Janeiro - UERJ. Legal Counsel na dLocal Instituição de Pagamento.

Os objetivos deste estudo incluem investigar a evolução das fintechs de pagamento no Brasil, abordando os fatores econômicos, tecnológicos e regulatórios que impulsionaram seu crescimento. Será realizado um exame das diferentes fases dessa evolução e como essas empresas têm influenciado o cenário financeiro nacional. Além disso, o estudo visa analisar os desafios regulatórios enfrentados pelas fintechs, explorando as normas e regulamentações que afetam suas operações no país. Serão destacadas as exigências de compliance e os dilemas enfrentados pelas fintechs ao adaptar-se a um ambiente regulatório em constante mudança, buscando compreender seu impacto no desenvolvimento e na inovação do setor.

A metodologia adotada neste estudo consistirá em uma revisão bibliográfica abrangente e analítica. Serão consultadas fontes acadêmicas, relatórios de instituições financeiras, documentos regulatórios e artigos de periódicos especializados para mapear e analisar criticamente o estado atual do conhecimento sobre o tema. Esta abordagem permitirá uma síntese integrada das informações disponíveis, proporcionando uma base sólida para as análises e conclusões apresentadas neste artigo científico.

1. A Evolução das Fintechs de Pagamento no Brasil

Fintech é um termo que se refere a empresas que utilizam tecnologia inovadora para oferecer produtos e serviços financeiros de forma mais eficiente, acessível e adaptada às necessidades dos consumidores e empresas². Essas empresas operam em diversos segmentos do mercado financeiro, como pagamentos eletrônicos, empréstimos peer-to-peer, gestão financeira pessoal, investimentos automatizados, seguros digitais, entre outros. O conceito de fintech destaca-se pela sua capacidade de disruptura no setor financeiro tradicional, geralmente caracterizado por estruturas mais burocráticas e menos ágeis. As fintechs buscam transformar a experiência financeira dos usuários através de soluções tecnológicas inovadoras, aproveitando avanços como inteligência artificial, blockchain e análise de big data para oferecer serviços mais eficientes, transparentes e acessíveis.

O surgimento e desenvolvimento das fintechs de pagamento representam um marco significativo na evolução do setor financeiro global. Originadas da convergência entre tecnologia e finanças, as fintechs emergiram como alternativas disruptivas aos modelos tradicionais de serviços financeiros. No contex-

2. WÓJCIK, D. Financial Geography I: Exploring FinTech – Maps and concepts. *Progress in Human Geography*, 45(3), 566-576. 2021.

to brasileiro e internacional, diversas foram as forças impulsionadoras desse crescimento, destacando-se fatores econômicos, tecnológicos e regulatórios³.

O surgimento e a evolução das fintechs no Brasil representam um capítulo fascinante na história recente do setor financeiro. Inicialmente, as fintechs ganharam destaque no país no início dos anos 2000, com a crescente penetração da internet e o avanço das tecnologias móveis. Empresas como PagSeguro e Moip (atualmente parte do grupo Wirecard) foram pioneiras ao oferecer soluções de pagamentos eletrônicos e processamento de transações online, permitindo a pequenos comerciantes e empreendedores digitais acesso facilitado ao mercado financeiro⁴.

A partir de meados da década de 2010, o cenário das fintechs no Brasil expandiu significativamente. Startups voltadas para serviços financeiros começaram a surgir em diversas áreas, incluindo gestão financeira pessoal, crédito online, investimentos automatizados e seguros digitais. Esse crescimento foi impulsionado pela demanda por soluções mais acessíveis e eficientes, especialmente entre os consumidores que buscavam alternativas aos bancos tradicionais⁵.

O ambiente regulatório também desempenhou um papel crucial na evolução das fintechs brasileiras⁶. O Banco Central do Brasil, por exemplo, introduziu medidas como a Resolução nº 4.282, de 2013, que estabelece requisitos para a operação de instituições de pagamento, e mais recentemente, em 2020, a criação do sistema de pagamentos instantâneos PIX, que revolucionou a maneira como as transações financeiras são realizadas no país, abrindo novas oportunidades para as fintechs.

Hoje, as fintechs no Brasil estão cada vez mais integradas ao ecossistema financeiro nacional, competindo de igual para igual com os bancos tradicionais em muitos aspectos. Elas não apenas democratizaram o acesso aos serviços financeiros, mas também promoveram uma maior eficiência e inovação no mercado, contribuindo para um sistema financeiro mais dinâmico e inclusivo para todos os brasileiros⁷.

3. SILVA, Lucas Leão. LISBOA, Erika Farias. FERREIRA, Luciene Braz. VERSIANI, Ângela França. SOUSA, Paulo Renato. CORDEIRO, Marcelo Lisboa. As instituições financeiras e sua relação com as fintechs no Brasil. *Revista Economia & Gestão*, v. 20, n. 55, 2020.

4. BASTOS, Luiz Felipe Pereira. *Cronologia das fintechs no brasil: um olhar sobre a transformação do setor financeiro*, 2023. Trabalho de conclusão de Curso Superior de Tecnologia em Gestão Empresarial. Fatec São Carlos, São Carlos, 2023.

5. MILIAN, Eduardo Z.; SPINOLA, Mauro de M.; CARVALHO, Marly M. Fintechs: A literature review and research agenda. *Electronic Commerce Research and Applications*, v. 34, p. 100833, 2019

6. LIMA, Talison Layala Praxedes de. *Análise do cenário regulatório das fintechs no Brasil*. Universidade Federal Rural do Semi-árido Centro de Ciências Sociais Aplicadas e Humanas curso de Direito 2020. Disponível em: <https://repositorio.ufersa.edu.br/server/api/core/bitstreams/754509b9-d274-415f-be7d-c84861ac2bb2/content> Acesso em 18 jul. 2024.

7. BASTOS, Luiz Felipe Pereira. *Cronologia das fintechs no brasil: um olhar sobre a transformação do setor financeiro*, 2023. Trabalho de conclusão de Curso Superior de Tecnologia em Gestão Empresarial. Fatec São Carlos, São Carlos, 2023.

Economicamente, o surgimento das fintechs foi motivado pela necessidade de eficiência e acessibilidade nos serviços financeiros, especialmente entre os segmentos da população anteriormente excluídos do sistema bancário tradicional. Tecnicamente, avanços em plataformas digitais, computação em nuvem, análise de big data e inteligência artificial possibilitaram a criação de soluções financeiras ágeis, personalizadas e acessíveis. Essas tecnologias não apenas viabilizaram novos modelos de negócios, como também transformaram a experiência do usuário, permitindo transações mais rápidas e seguras⁸.

Além disso, o ambiente regulatório desempenhou um papel crucial na configuração do cenário das fintechs. Em muitos casos, regulamentações inovadoras como o sandbox regulatório, que oferece um ambiente controlado para testar novos produtos e serviços, têm sido fundamentais para o desenvolvimento e a validação das soluções propostas pelas fintechs. Por outro lado, regulamentações tradicionais muitas vezes apresentam desafios, exigindo adaptações significativas das fintechs para cumprir com requisitos de segurança, proteção ao consumidor e prevenção à lavagem de dinheiro⁹.

Ao longo das principais fases de desenvolvimento das fintechs, observa-se uma progressão desde startups emergentes até integrantes estabelecidos do ecossistema financeiro. Inicialmente focadas em nichos específicos como pagamentos móveis e transferências internacionais, as fintechs expandiram suas operações para áreas como empréstimos peer-to-peer, gestão financeira pessoal, investimentos automatizados e seguros digitais. Esta diversificação reflete a capacidade adaptativa das fintechs em responder às demandas do mercado e explorar novas oportunidades de crescimento.

2. O Papel do Banco Central do Brasil na Regulação das Fintechs de Pagamento

O Banco Central do Brasil foi instituído em 31 de dezembro de 1964, mediante a promulgação da Lei nº 4.595, com a missão de garantir a estabilidade do poder de compra da moeda nacional, manter um sistema financeiro sólido e eficiente e promover o bem-estar econômico da população. Ao longo dos anos, a missão do BCB evoluiu, abrangendo o controle da inflação, a

8. LIMA, Talison Layala Praxedes de. Análise do cenário regulatório das fintechs no Brasil. Universidade Federal Rural do Semi-árido Centro de Ciências Sociais Aplicadas e Humanas curso de Direito 2020. Disponível em: <https://repositorio.ufersa.edu.br/server/api/core/bitstreams/754509b9-d274-415f-be7d-c84861ac2bb2/content> Acesso em 18 jul. 2024

9. DINIZ, Bruno. O fenômeno Fintech: tudo sobre o movimento que está transformando o mercado financeiro no Brasil e no mundo. Rio de Janeiro: Alta Books, 2019, p. 31.

regulação do sistema financeiro e a implementação de políticas monetárias eficazes¹⁰.

A estrutura do Banco Central do Brasil é composta por diversas áreas e departamentos, cada qual com funções específicas que contribuem para a missão geral da instituição. A organização interna do BCB é delineada da seguinte forma: o Conselho Monetário Nacional (CMN), órgão superior do sistema financeiro nacional, responsável pela formulação da política da moeda e do crédito, é composto pelo Ministro da Fazenda, pelo Ministro do Planejamento, Desenvolvimento e Gestão e pelo Presidente do Banco Central. A Diretoria Colegiada, formada pelo Presidente do Banco Central e pelos Diretores, cada um responsável por uma área específica, define e implementa políticas para alcançar os objetivos estabelecidos pelo CMN¹¹.

Os departamentos e áreas funcionais do BCB incluem, entre outros: o Departamento de Operações Bancárias e de Sistema de Pagamentos (Deban), encarregado da gestão das operações de bancos e do sistema de pagamentos; o Departamento de Supervisão Bancária (Desup), responsável pela supervisão das instituições financeiras para assegurar a solidez e a conformidade com as regulamentações; o Departamento Econômico (Depec), que realiza análises econômicas e acompanha os indicadores macroeconômicos; e o Departamento de Operações de Mercado Aberto (Demab), incumbido da execução das operações de mercado aberto e do controle da liquidez do sistema financeiro¹².

Para alcançar seus objetivos, o Banco Central do Brasil utiliza diversos instrumentos de política monetária. A taxa Selic, taxa básica de juros da economia, influencia todas as outras taxas de juros e é utilizada para controlar a inflação e estabilizar a moeda. As operações de mercado aberto, que envolvem a compra e venda de títulos públicos, são empregadas para controlar a quantidade de dinheiro em circulação e manter a liquidez do sistema financeiro em níveis adequados. As reservas compulsórias, que correspondem ao percentual dos depósitos que os bancos comerciais são obrigados a manter no Banco Central, são utilizadas para regular a oferta de crédito e a liquidez do sistema bancário. Ademais, as intervenções no mercado de câmbio visam

10. BANCO CENTRAL DO BRASIL. Estabilidade financeira: fintechs. Brasília, DF: Banco Central do Brasil, 2020a. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/fintechs>. Acesso em 15 jul. 2024.

11. MENDONÇA, Saulo Bichara; DE PAULA IVO, Felipe. Conselho Administrativo de Defesa Econômica e Banco Central do Brasil: análise do conflito de competência. *Revista de Direito*, v. 12, n. 1, p. 4, 2020.

12. MISSAGIA, Caio Rezende; AMATO, Lucas Fucci. Ambientes regulatórios experimentais: o sandbox no sistema financeiro brasileiro. *Revista Brasileira de Sociologia do Direito*, v. 10, n. 3, p. 143-171, 2023.

influenciar a taxa de câmbio e estabilizar a moeda, protegendo a economia de choques externos e flutuações cambiais¹³.

O Banco Central do Brasil desempenha um papel vital na economia do país, sendo responsável por assegurar a estabilidade econômica e financeira por meio de uma estrutura organizacional bem definida e do uso eficaz de diversos instrumentos de política monetária. A missão do BCB e suas funções são essenciais para promover um ambiente econômico estável e favorável ao desenvolvimento sustentável do Brasil.

2.1 Principais Regulações e Normas para Fintechs de Pagamento

O Banco Central do Brasil tem adotado diversas iniciativas regulatórias que desempenham um papel crucial na supervisão das fintechs de pagamento. Entre as principais iniciativas, destaca-se a Resolução nº 4.282, de 2013¹⁴, que estabelece critérios para a autorização e o funcionamento de instituições de pagamento. Esta resolução define os requisitos mínimos de capital, governança corporativa, controles internos e gestão de riscos que devem ser observados pelas fintechs para obterem e manterem sua autorização de funcionamento¹⁵.

Adicionalmente, o Banco Central instituiu a Circular nº 3.682, de 2013¹⁶, que regulamenta a prestação de serviços de pagamento, estabelecendo diretrizes específicas para a operação de instituições de pagamento. Esta norma abrange aspectos como a prestação de informações aos usuários, a proteção dos fundos dos clientes, a transparência nas tarifas e a prevenção à lavagem de dinheiro e ao financiamento do terrorismo. A Circular nº 3.682, ao promo-

13. SILVA, Christian Feliciano da. Disque 100 – Implementação de políticas regulatórias: o caso do Open Finance a partir do Banco Central do Brasil. 2023. 42 f., il. Trabalho de Conclusão de Curso (Bacharelado em Gestão de Políticas Públicas) – Universidade de Brasília, Brasília, 2023.

14. BRASIL. Ministério da Fazenda. Banco Central do Brasil. Resolução nº 4.282, de 4 de novembro de 2013. Estabelece as diretrizes que devem ser observadas na regulamentação, na vigilância e na supervisão das instituições de pagamento e dos arranjos de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB), de que trata a Lei nº 12.865, de 9 de outubro de 2013. Diário Oficial da União: seção 1, Brasília, DF, ano 150, n. 216, p. 16, 6 nov. 2013c. Disponível em: <https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=06/11/2013&jornal=1&pagina=16>. Acesso em: 18 jul. 2024.

15. OIOLI, Erik Frederico; SILVA, Rafael Toni; ZILIOTI, Matheus. Fintechs e a regulação do sistema financeiro nacional. In: OIOLI, Erik Frederico (coord.). Manual de direito para startups. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 187-210.

16. BRASIL. Ministério da Fazenda. Banco Central do Brasil. Circular nº 3.682, de 4 de novembro de 2013. Aprova o regulamento que disciplina a prestação de serviço de pagamento no âmbito dos arranjos de pagamentos integrantes do Sistema de Pagamentos Brasileiro (SPB), estabelece os critérios segundo os quais os arranjos de pagamento não integrarão o SPB e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, ano 150, n. 216, p. 18-20, 6 nov. 2013b. Disponível em: <https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=06/11/2013&jornal=1&pagina=18>. Acesso em: 18 jul. 2024.

ver maior transparência e segurança nas operações, reforça a confiança dos usuários nos serviços prestados pelas fintechs de pagamento¹⁷.

Outro marco regulatório importante é a criação do Sistema de Pagamentos Brasileiro (SPB), instituído pela Lei nº 12.865, de 2013¹⁸. O SPB estabelece a infraestrutura necessária para a realização de transações financeiras no país, incluindo pagamentos eletrônicos e transferências de fundos. As fintechs de pagamento, ao integrarem o SPB, passam a operar dentro de um sistema seguro e eficiente, que facilita a interoperabilidade entre diferentes instituições financeiras e promove a inclusão financeira.

O Banco Central também implementou o conceito de sandbox regulatório, conforme disposto na Resolução nº 29, de 2020¹⁹. O sandbox regulatório permite que fintechs de pagamento testem inovações tecnológicas em um ambiente controlado, com supervisão e acompanhamento do BCB. Esta iniciativa visa fomentar a inovação no setor financeiro, ao mesmo tempo em que assegura a proteção dos consumidores e a estabilidade do sistema financeiro. O sandbox regulatório proporciona um espaço para que novas tecnologias e modelos de negócios sejam experimentados e avaliados antes de sua plena implementação no mercado.

O termo geral “sandbox” é utilizado nas estratégias de desenvolvimento de software e representa um ambiente isolado da interação com outros sistemas que permite que se opere um novo sistema sem que a interação com o ambiente externo atrapalhe seu desenvolvimento. Trazido pelas fintechs ao ambiente financeiro, sandbox

17. Art. 18. As instituições financeiras somente poderão funcionar no País mediante prévia autorização do Banco Central da República do Brasil ou decreto do Poder Executivo, quando forem estrangeiras.” (BRASIL. Lei nº 4.595, de 31 de dezembro de 1964. Dispõe sobre a Política e as Instituições monetárias, Bancárias e Creditícias, Cria o Conselho Monetário Nacional e dá outras providências. Brasília, DF: Presidência da República, [2017], art. 18. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L4595compilado.htm. Acesso em: 18 jul. 2024).

18. “Art. 6º Para os efeitos das normas aplicáveis aos arranjos e às instituições de pagamento que passam a integrar o Sistema de Pagamentos Brasileiro (SPB), nos termos desta Lei, considera-se: I - arranjo de pagamento - conjunto de regras e procedimentos que disciplina a prestação de determinado serviço de pagamento ao público aceito por mais de um receptor, mediante acesso direto pelos usuários finais, pagadores e recebedores;” (BRASIL. Lei nº 12.865, de 9 de outubro de 2013. Dispõe sobre os arranjos de pagamento e as instituições de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB), entre outros. Brasília, DF: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato20112014/2013/lei/l12865.htm. Acesso em: 18 jul. 2024.)

19. No Brasil, o principal marco regulatório que permitiu a criação do sandbox regulatório para fintechs foi a Resolução Conjunta nº 1, de 4 de fevereiro de 2021. Esta resolução foi emitida em conjunto pelo Conselho Monetário Nacional (CMN), Banco Central do Brasil (Bacen), Comissão de Valores Mobiliários (CVM) e pela Superintendência de Seguros Privados (Susep). A resolução estabelece as diretrizes para a implementação do ambiente regulatório experimental, conhecido como sandbox regulatório.

A Resolução Conjunta nº 1/2021 define os critérios e procedimentos para a seleção e acompanhamento das empresas participantes do sandbox, bem como os requisitos para a entrada e saída deste ambiente regulatório controlado. A iniciativa visa promover a inovação no setor financeiro, permitindo que as fintechs testem novos produtos e serviços sob a supervisão dos reguladores, garantindo a proteção dos consumidores e a integridade do sistema financeiro.

Além desta resolução, o Banco Central do Brasil também emitiu a Resolução BCB nº 29, de 26 de outubro de 2020, que estabelece as condições específicas para a criação e operação do sandbox regulatório no âmbito do Bacen. Esta resolução detalha os critérios para a admissão das fintechs no sandbox, as obrigações das empresas participantes e os mecanismos de supervisão e controle.

passa a definir um ambiente de teste onde produtos e serviços financeiros são testados isoladamente e avaliados em sua segurança e eficácia antes de serem oferecidos ao público²⁰

Em termos de segurança e compliance, o Banco Central estabelece normas rigorosas para a proteção dos dados dos clientes e a prevenção de atividades ilícitas. A Lei Geral de Proteção de Dados (LGPD), promulgada em 2018, e as diretrizes do BCB sobre segurança cibernética e gestão de riscos, conforme a Resolução nº 4.658, de 2018,²¹ impõem obrigações às fintechs de pagamento para garantir a confidencialidade, integridade e disponibilidade das informações dos usuários. Estas normas de segurança são essenciais para mitigar riscos e assegurar a confiança dos consumidores nos serviços prestados pelas fintechs.

3. Desafios e Oportunidades na Regulação das Fintechs de Pagamento

Os desafios regulatórios e de compliance enfrentados pelas fintechs de pagamento são substanciais e multifacetados. Em um ambiente financeiro em constante evolução, as fintechs necessitam adaptar-se a um quadro regulatório que, embora vise garantir a segurança e a estabilidade do sistema financeiro, pode também impor barreiras significativas à inovação e ao crescimento. A necessidade de cumprir com rigorosos requisitos legais e regulamentares impõe um ônus considerável sobre estas empresas, que frequentemente operam com estruturas mais ágeis e menos robustas do que as instituições financeiras tradicionais²².

Um dos principais desafios regulatórios reside na necessidade de conformidade com a legislação vigente, que inclui normas complexas e detalhadas sobre prevenção à lavagem de dinheiro, proteção de dados e segurança cibernética. As fintechs de pagamento devem implementar políticas e procedimentos robustos para garantir que suas operações estejam em conformidade com a Lei nº 9.613/1998, que dispõe sobre os crimes de “lavagem” ou ocultação de bens,

20. SQUASSONI, Christian. O Sandbox Regulatório e o novo papel do regulador financeiro. In: EROLES, Pedro (coord.). Fintechs, Bancos Digitais e Meios de Pagamento: Aspectos Regulatórios das novas Tecnologias Financeiras. São Paulo: Quartier Latin, 2019. p. 157-178.

21. RESOLUÇÃO Nº 4.658, DE 26 DE ABRIL DE 2018 Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

22. PELLEGRINO, Maria Beatriz. A evolução dos subcredenciadores no Sistema de Pagamentos Brasileiro (SPB). In: EROLES, Pedro (coord.). Fintechs, bancos digitais e meios de pagamento: aspectos regulatórios das novas tecnologias financeiras. São Paulo: Quartier Latin, 2019, p. 109.

direitos e valores, bem como com a Lei Geral de Proteção de Dados (LGPD), que estabelece diretrizes para o tratamento de dados pessoais. Estas exigências demandam investimentos significativos em tecnologia e recursos humanos, além de um contínuo monitoramento e atualização dos processos internos²³.

Ademais, a regulação impõe desafios relacionados à transparência e à prestação de contas. As fintechs de pagamento devem manter registros detalhados de suas operações e estar preparadas para fornecer informações precisas e tempestivas às autoridades regulatórias. A Circular nº 3.682, de 2013, do Banco Central do Brasil, por exemplo, estabelece obrigações de prestação de informações periódicas, o que requer a adoção de sistemas de gestão eficientes e confiáveis. A falha em cumprir estas obrigações pode resultar em sanções severas, incluindo multas substanciais e, em casos extremos, a revogação da autorização para operar²⁴.

Outro desafio relevante é a necessidade de gestão de riscos e de implementação de controles internos adequados. As fintechs de pagamento operam em um ambiente dinâmico e suscetível a diversas formas de risco, incluindo riscos operacionais, de crédito e de mercado. A Resolução nº 4.658, de 2018, do Conselho Monetário Nacional, que dispõe sobre a política de segurança cibernética e os requisitos para a contratação de serviços de processamento e armazenamento de dados, impõe às fintechs a responsabilidade de adotar medidas para mitigar riscos e proteger a integridade e a confidencialidade das informações dos clientes. A implementação de um programa de compliance efetivo, que inclua a realização de auditorias internas regulares e a capacitação contínua dos colaboradores, é essencial para a mitigação destes riscos²⁵.

Além disso, o ambiente regulatório pode ser um fator de incerteza para as fintechs de pagamento. A evolução constante das tecnologias financeiras e as mudanças nas expectativas dos consumidores frequentemente antecedem a atualização das normas regulatórias. Esta lacuna entre inovação e regulação pode criar incertezas jurídicas e operacionais, dificultando a previsibilidade e o planejamento estratégico das fintechs. A criação de um marco regulatório flexível e adaptável, que permita a experimentação e o teste de novos modelos de negócios em um ambiente controlado, como o sandbox regulatório imple-

23. SQUASSONI, Christian. O Sandbox Regulatório e o novo papel do regulador financeiro. In: EROLES, Pedro (coord.). *Fintechs, Bancos Digitais e Meios de Pagamento: Aspectos Regulatórios das novas Tecnologias Financeiras*. São Paulo: Quartier Latin, 2019. p. 157-178.

24. OIOLI, Erik Frederico; SILVA, Rafael Toni; ZILIOTI, Matheus. *Fintechs e a regulação do sistema financeiro nacional*. In: OIOLI, Erik Frederico (coord.). *Manual de direito para startups*. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 187-210.

25. DINIZ, Bruno. *O fenômeno Fintech: tudo sobre o movimento que está transformando o mercado financeiro no Brasil e no mundo*. Rio de Janeiro: Alta Books, 2019.

mentado pelo Banco Central, é uma resposta positiva a este desafio, embora a sua efetiva implementação e o seu alcance ainda estejam em processo de desenvolvimento²⁶.

Considerações finais

As fintechs de pagamento apresentam inúmeras oportunidades para impulsionar a inovação e promover a inclusão financeira no Brasil. A regulação adequada, embora desafiadora, também abre caminho para um ambiente mais seguro e confiável, onde a inovação pode florescer e novos modelos de negócios podem ser testados e implementados, beneficiando tanto as empresas quanto os consumidores.

A inovação tecnológica é uma das maiores oportunidades proporcionadas pelo crescimento das fintechs de pagamento. Com a digitalização dos serviços financeiros, as fintechs podem oferecer soluções mais eficientes, acessíveis e convenientes. A utilização de tecnologias avançadas como inteligência artificial, machine learning e blockchain permite a criação de produtos e serviços inovadores que atendem às necessidades específicas dos consumidores, melhorando a experiência do usuário e aumentando a competitividade no mercado financeiro. A introdução de carteiras digitais, pagamentos por aproximação e plataformas de pagamento integradas são exemplos de como as fintechs estão revolucionando o setor.

Ainda, as fintechs desempenham um papel crucial na promoção da inclusão financeira. No Brasil, um significativo percentual da população ainda é desbancarizado ou sub-bancarizado, enfrentando dificuldades para acessar serviços financeiros tradicionais. As fintechs de pagamento, com suas soluções digitais, têm a capacidade de alcançar essas populações marginalizadas, oferecendo-lhes acesso a serviços financeiros básicos, como contas de pagamento, transferências de fundos e microcrédito. Esta inclusão financeira é essencial para o desenvolvimento econômico e social, proporcionando às pessoas maior autonomia e capacidade de gestão de suas finanças.

O ambiente regulatório também oferece oportunidades significativas para as fintechs. A implementação do open banking no Brasil, por exemplo, é uma iniciativa que visa fomentar a inovação e a competição no setor financeiro. O open banking permite o compartilhamento seguro de dados financeiros entre diferen-

26. SQUASSONI, Christian. O Sandbox Regulatório e o novo papel do regulador financeiro. In: EROLES, Pedro (coord.). Fintechs, Bancos Digitais e Meios de Pagamento: Aspectos Regulatórios das novas Tecnologias Financeiras. São Paulo: Quartier Latin, 2019. p. 157-178.

tes instituições, com o consentimento do cliente, promovendo a criação de novos serviços personalizados e integrados. As fintechs podem aproveitar esta infraestrutura para desenvolver soluções mais competitivas e adaptadas às necessidades dos consumidores, melhorando a eficiência e a transparência do mercado.

Outra oportunidade importante é o sandbox regulatório, uma iniciativa do Banco Central que permite que fintechs testem inovações tecnológicas em um ambiente controlado e supervisionado. Este espaço experimental possibilita que novas ideias sejam avaliadas e ajustadas antes de serem plenamente implementadas no mercado, reduzindo riscos e aumentando as chances de sucesso. O sandbox regulatório não apenas incentiva a inovação, mas também facilita a adaptação das fintechs às exigências regulatórias, promovendo um diálogo construtivo entre reguladores e inovadores.

A crescente demanda por soluções sustentáveis e socialmente responsáveis também apresenta oportunidades para as fintechs de pagamento. As fintechs podem desenvolver produtos financeiros que promovam a sustentabilidade ambiental e o impacto social positivo, alinhando-se às expectativas dos consumidores e investidores modernos. Exemplos incluem plataformas de investimento em projetos sustentáveis, serviços de microcrédito para pequenas empresas e iniciativas de educação financeira. Ao integrar critérios de responsabilidade social em suas operações, as fintechs podem conquistar a confiança dos consumidores e contribuir para um desenvolvimento mais equitativo e sustentável.

Em conclusão, as fintechs de pagamento no Brasil têm diante de si um vasto leque de oportunidades para impulsionar a inovação e promover a inclusão financeira. A digitalização dos serviços financeiros, a promoção do open banking, o uso do sandbox regulatório e o desenvolvimento de soluções sustentáveis são apenas algumas das maneiras pelas quais as fintechs podem transformar o mercado financeiro. A regulação adequada, longe de ser um obstáculo, pode ser um catalisador para a inovação e o crescimento, criando um ambiente onde as fintechs possam prosperar e oferecer benefícios significativos à sociedade.

Referências

BANCO CENTRAL DO BRASIL. Estabilidade financeira: fintechs. Brasília, DF: Banco Central do Brasil, 2020a. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/fintechs>. Acesso em 15 jul. 2024.

BASTOS, Luiz Felipe Pereira. Cronologia das fintechs no brasil: um olhar sobre a transformação do setor financeiro. Trabalho de conclusão de Curso Superior de Tecnologia em Gestão Empresarial. Fatec São Carlos, São Carlos, 2023.

BRASIL. Lei nº 12.865, de 9 de outubro de 2013. Dispõe sobre os arranjos de pagamento e as instituições de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB), entre outros. Brasília, DF: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato20112014/2013/lei/l12865.htm. Acesso em: 18 jul. 2024.)

BRASIL. Lei nº 4.595, de 31 de dezembro de 1964. Dispõe sobre a Política e as Instituições monetárias, Bancárias e Creditícias, Cria o Conselho Monetário Nacional e dá outras providências. Brasília, DF: Presidência da República, [2017], art. 18. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L4595compilado.htm. Acesso em: 18 jul. 2024).

BRASIL. Ministério da Fazenda. Banco Central do Brasil. Circular nº 3.682, de 4 de novembro de 2013. Aprova o regulamento que disciplina a prestação de serviço de pagamento no âmbito dos arranjos de pagamentos integrantes do Sistema de Pagamentos Brasileiro (SPB), estabelece os critérios segundo os quais os arranjos de pagamento não integrarão o SPB e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, ano 150, n. 216, p. 18-20, 6 nov. 2013b. Disponível em: <https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=06/11/2013&jornal=1&pagina=18>. Acesso em: 18 jul. 2024.

BRASIL. Ministério da Fazenda. Banco Central do Brasil. Resolução nº 4.282, de 4 de novembro de 2013. Estabelece as diretrizes que devem ser observadas na regulamentação, na vigilância e na supervisão das instituições de pagamento e dos arranjos de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB), de que trata a Lei nº 12.865, de 9 de outubro de 2013. Diário Oficial da União: seção 1, Brasília, DF, ano 150, n. 216, p. 16, 6 nov. 2013c. Disponível em: <https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=06/11/2013&jornal=1&pagina=16>. Acesso em: 18 jul. 2024.

LIMA, Talison Layala Praxedes de. Análise do cenário regulatório das fintechs no Brasil. Universidade Federal Rural do Semiárido. Centro de Ciências Sociais Aplicadas e Humanas Curso de Direito 2020. Disponível em: <https://repositorio.ufersa.edu.br/server/api/core/bitstreams/754509b-9-d274-415f-be7d-c84861ac2bb2/content> Acesso em 18 jul. 2024.

MISSAGIA, Caio Rezende; AMATO, Lucas Fucci. Ambientes regulatórios experimentais: o sandbox no sistema financeiro brasileiro. Revista Brasileira de Sociologia do Direito, v. 10, n. 3, p. 143-171, 2023.

MENDONÇA, Saulo Bichara; DE PAULA IVO, Felipe. Conselho Administrativo de Defesa Econômica e Banco Central do Brasil: análise do conflito de competência. Revista de Direito, v. 12, n. 1, p. 4, 2020.

MILIAN, Eduardo Z.; SPINOLA, Mauro de M.; CARVALHO, Marly M. Fintechs: A literature review and research agenda. Electronic Commerce Research and Applications, v. 34, p. 100833, 2019

OIOLI, Erik Frederico; SILVA, Rafael Toni; ZILIOTI, Matheus. Fintechs e a regulação do sistema financeiro nacional. In: OIOLI, Erik Frederico (coord.). Manual de direito para startups. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 187-210.

PELLEGRINO, Maria Beatriz. A evolução dos subcredenciadores no Sistema de Pagamentos Brasileiro (SPB). In: EROLES, Pedro (coord.). Fintechs, bancos digitais e meios de pagamento: aspectos regulatórios das novas tecnologias financeiras. São Paulo: Quartier Latin, 2019, p. 109.

RESOLUÇÃO Nº 4.658, DE 26 DE ABRIL DE 2018 Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de

dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

SILVA, Lucas Leão. LISBOA, Erika Farias. FERREIRA, Luciene Braz. VERSIANI, Ângela França. SOUSA, Paulo Renato. CORDEIRO, Marcelo Lisboa. As instituições financeiras e sua relação com as fintechs no Brasil. *Revista Economia & Gestão*, v. 20, n. 55, 2020.

SILVA, Christian Feliciano da. Disque 100 – Implementação de políticas regulatórias: o caso do Open Finance a partir do Banco Central do Brasil. 2023. 42 f., il. Trabalho de Conclusão de Curso (Bacharelado em Gestão de Políticas Públicas) – Universidade de Brasília, Brasília, 2023.

SQUASSONI, Christian. O Sandbox Regulatório e o novo papel do regulador financeiro. In: EROLES, Pedro (coord.). *Fintechs, Bancos Digitais e Meios de Pagamento: Aspectos Regulatórios das novas Tecnologias Financeiras*. São Paulo: Quartier Latin, 2019. p. 157-178.

WÓJCIK, D. Financial Geography I: Exploring FinTech – Maps and concepts. *Progress in Human Geography*, 45(3), 566-576. 2021.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

15

**Blockchain como
substantivo feminino: uma
análise de gênero quanto
ao uso em ascensão da
tecnologia blockchain**

CAROLINA FREITAS GOMIDE DE ARAUJO

Sumário: Introdução. 1. Quais serão os valores da tecnologia de valor? 2. O quão distribuído é o sistema distribuído de finanças? 3. Podemos confiar o futuro das mulheres para a tecnologia da confiança? Considerações finais. Referências.

Introdução

Para o Dicionário Priberam da Língua Portuguesa (DPLP), blockchain, substantivo masculino, é “tecnologia que usa um banco de dados não centralizado, com informações provenientes de uma grande rede, ligadas por algoritmos de encriptação, geralmente usada para transações em criptomoedas.”²

A escolha de uma tradução no dicionário para o masculino, embora seja dúvida gramatical interessante, serve como um ponto de partida para uma questão mais profunda: o quão masculina é a tecnologia blockchain?

Ao que se parece, a escolha gramatical confirma uma realidade, blockchain é um sistema, até o momento, construído em uma perspectiva masculina. O artigo, no entanto, busca destacar possíveis aplicações para que a tecnologia possa reduzir, e não contribuir com a intensificação de desigualdades de gênero.

Assim, o objetivo deste artigo é analisar como essa tecnologia emergente interage com as desigualdades de gênero em diversos contextos. Ao abordar essas questões, o artigo visa ampliar a compreensão sobre a interseção entre gênero e tecnologia na era digital, trazendo à tona possíveis aplicações da tecnologia. Para isso, será utilizada uma abordagem que inclui revisão bibliográfica, análise documental e estudo de casos já documentados.

A tecnologia blockchain emergiu como uma inovação revolucionária, prometendo transformar diversos setores, desde o financeiro até o governamental. Contudo, apesar de sua crescente adoção e impacto potencial, questões de gênero relacionadas a essa tecnologia permanecem amplamente inexploradas. Na literatura, uma revisão bibliográfica feita por pesquisadores da FGV sobre a aplicação de blockchain em perspectiva de gênero encontrou apenas 21 artigos nas bases de dados Scopus, Web of Science, Scielo, Ebsco e Google Scholar até agosto de 2023, sendo apenas um focado no caso brasileiro.³

1. Mestra 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 do livro “Cortes Constitucionais Digitais” e do livro “Poder Constituinte Originário das Mulheres no Brasil”.

2. DICIONÁRIO PRIBERAM. *Blockchain*. Disponível em: <https://dicionario.priberam.org/blockchain>. Acesso em: 20 jul. 2024.

3. SANTOS, Vanessa Martins dos; DINIZ, Eduardo Henrique; MORAES, Tricia Karla Lacerda; CERNEV, Adrian Kemmer; LOURENÇO, Carlos Eduardo. *Blockchain e (des)igualdade de gênero: uma revisão sistemática da literatura*. AMCIS 2024 Proceedings, 2024. Disponível em: https://aisel.aisnet.org/amcis2024/span_lacais/span_lacais/5. Acesso em: 7 jul. 2024.

Dessa forma, a escolha do tema é justificada pela ainda incipiente literatura acadêmica sobre o assunto. Isto é, embora a tecnologia blockchain seja cada vez mais importante e tenha potencial para transformar diversos setores da sociedade, ainda são raras as análises que consideram suas implicações de gênero.

O artigo está estruturado em três tópicos. O primeiro tópico discute como as estruturas de poder masculinas vêm moldando o acesso às tecnologias desde sua origem e o possível impacto de uma ausência de perspectiva de gênero na aplicação de novas tecnologias, como a blockchain. No segundo tópico, serão apresentados exemplos de iniciativas que usam blockchain para promover a igualdade de gênero no acesso à propriedade e a recursos financeiros, com o objetivo de explorar como essa tecnologia pode impactar as desigualdades de gênero nos sistemas econômicos globais. No último tópico, por sua vez, serão apresentadas soluções baseadas em blockchain para enfrentar as desigualdades de gênero em escala global e em diferentes contextos sociais.

1. Quais são os valores da tecnologia de valor?

A internet, tal como a conhecemos hoje, é um reflexo de um mundo historicamente moldado por estruturas patriarcais. A arquitetura inicial da internet foi construída em um ambiente cultural onde as vozes masculinas predominavam, influenciando tanto o desenvolvimento técnico quanto o conteúdo acessível. Como resultado, as plataformas online frequentemente reproduzem e amplificam as dinâmicas de poder existentes, perpetuando estereótipos de gênero e marginalizando as vozes femininas. Isso cria um espaço digital que, em muitos casos, não é seguro nem inclusivo para as mulheres.

O advento da blockchain promete uma revolução nas trocas de valores e propriedade online. No entanto, a promessa de um sistema mais justo e inclusivo enfrenta desafios significativos relacionados à reprodução das mesmas desigualdades de gênero observadas na sociedade e replicadas e intensificadas no desenvolvimento da internet.

Se a internet cresceu rapidamente e trouxe consigo os problemas sociais da realidade física para o espaço digital, a tendência é que a tecnologia blockchain siga um caminho semelhante, mas em um ritmo mais acelerado. Isso é preocupante, considerando que as dinâmicas de exclusão de gênero podem se intensificar em um ambiente onde a distribuição de valores e propriedade é central.

Como será trabalhado nesse tópico, embora a blockchain seja frequentemente promovida como uma tecnologia neutra, a realidade é que sua implementação e desenvolvimento ocorrem em um contexto social que ainda carre-

ga profundas disparidades de gênero. Além disso, a indústria de blockchain e criptomoedas ainda é predominantemente masculina, com uma representação feminina significativamente baixa em posições de liderança e desenvolvimento tecnológico. Essa desigualdade pode resultar em produtos e soluções que não consideram adequadamente as necessidades e perspectivas das mulheres.

O universo da blockchain é amplamente reconhecido por sua dominância masculina, muitas vezes caracterizado pelo termo “Bitcoin bros”. Essa realidade é evidente em eventos relacionados ao setor, que frequentemente acabam desencorajando a participação feminina.

Um exemplo notório ocorreu em 2018, durante a Conferência Norte-Americana de Bitcoin, onde 85 dos palestrantes eram homens e apenas três eram mulheres. O evento foi amplamente criticado após os organizadores convidarem os 5.000 participantes para uma oportunidade oficial de networking noturno em um grande clube de strip-tease em Miami. Até às 23h, quando o evento tecnicamente terminou, os convidados foram servidos por mulheres vestindo lingerie. Mulheres que participaram da conferência disseram ter deixado o clube quando as *strippers* apareceram e criticaram o evento online. Jeff Scott, um trader de criptomoedas de Nova York presente na conferência, comentou: “Somos um grupo de caras na casa dos 20 anos com muito dinheiro. Gostamos de garotas peladas. Se você não gosta, tudo bem, mas não espere que mudemos.”⁴

Em 2022, na Conferência de Bitcoin em Miami, que atraiu mais de 25.000 participantes, Rachel Siegel, conhecida online como @CryptoFinally, viveu um caso de assédio que destacou o sexismo persistente na comunidade. Durante o evento, Siegel, que estava interagindo com outros participantes, teve sua foto tirada sem permissão por um participante identificado como @bitcoin_fuckboi. A imagem, postada nas redes sociais, apresentava um ângulo desfavorável de Siegel e foi acompanhada de comentários sexualmente agressivos e insultos sobre seu corpo. Quando Siegel tentou relatar o incidente à organização da conferência, encontrou resistência e uma resposta insuficiente. Mesmo após identificar o assediador nas redes sociais e descobrir que ele havia tirado selfies com outros participantes proeminentes, a organização não tomou medidas significativas. Um dos organizadores, que usava o pseudônimo @Chairforce, chegou a curtir alguns dos tweets ofensivos.⁵

4. MURDOCK, Jason. *We like naked girls': Bitcoin bros slammed as major crypto conference uses strip club*. 2018. Disponível em: <https://www.ibtimes.co.uk/we-like-naked-girls-bitcoin-bros-slammed-major-crypto-conference-uses-strip-club-1658353>. Acesso em: 6 ago.2024

5. PARDES, Arielle. *Miami's Bitcoin Conference Left a Trail of Harassment*. 2022. Disponível em: <https://www.wired.com/story/bitcoin-2022-conference-harassment/> Acesso em: 6 ago. 2024

Para tentar contornar o cenário, iniciativas focadas na educação e na criação de redes de mulheres na blockchain vêm sendo desenvolvidas. Em 2022, Gwyneth Paltrow e Mila Kunis promoveram um evento para apresentar o novo clube de criptomoedas, chamado BFF. Iniciativas como o Women in Blockchain e o Black Women Blockchain Council também têm como objetivo apoiar mulheres no amplo ecossistema das criptomoedas. Outro exemplo é o Ladies in Bitcoin, que organiza eventos e workshops destinados a educar mulheres interessadas em Bitcoin⁶

Analisar a tecnologia blockchain através de uma lente de gênero é crucial para compreender como essa inovação pode ser utilizada para promover a igualdade ou, alternativamente, reforçar as disparidades existentes.

No estágio atual de exploração do potencial da blockchain, a literatura destaca ao menos quatro áreas específicas de riscos relacionados à aplicação da tecnologia por uma perspectiva de gênero. São elas: (i) a falta de análise de gênero nas fases de planejamento de projetos que utilizam blockchain; (ii) o acesso desigual à tecnologia; (iii) a ausência de representação e participação de mulheres e meninas no design e na implementação das aplicações; e (iv) as preocupações com a proteção dos direitos humanos, incluindo a violência baseada em gênero.⁷

Primeiramente, no que tange à análise de gênero, a utilização da tecnologia blockchain não pode ser considerada isoladamente, mas deve refletir as limitações subjacentes dos contextos específicos onde será aplicada. Assim, seria necessário realizar uma análise de impacto de gênero para qualquer uso proposto da tecnologia blockchain para prever algumas das principais áreas de preocupação e riscos que precisam ser abordados antes de sua introdução.

No que tange ao acesso desigual à tecnologia, a disparidade no acesso a smartphones e conectividade é um problema com uma forte influência de gênero. As mulheres frequentemente enfrentam maiores dificuldades para acessar informações e meios de comunicação e o hiato digital de gênero faz com que mulheres em países de baixa e média renda sejam 10% menos propensas a possuir um celular e 23% menos propensas a usar a internet móvel. Em locais como o campo de refugiados de Kakuma, no Quênia, embora a posse de smartphones e o acesso à internet estejam crescendo, apenas 12% das mulheres possuem smartphones, comparado a 37% dos homens. Isso faz

6. PARDES, Arielle. *Miami's Bitcoin Conference Left a Trail of Harassment*. 2022. Disponível em: <https://www.wired.com/story/bitcoin-2022-conference-harassment/> Acesso em: 6 ago. 2024

7. THYLIN, T., DUARTE, M. F. N. Leveraging blockchain technology in humanitarian settings – opportunities and risks for women and girls. *Gender & Development*, p. 317-336. 2019.

com que as mulheres muitas vezes dependam dos smartphones dos homens ao invés de terem o seu, limitando o acesso das mulheres a serviços online e aplicativos.⁸

Quanto à ausência de representação e participação de mulheres e meninas no design e na implementação da tecnologia, é essencial ouvir e considerar as diversas perspectivas, necessidades, aspirações e preocupações de mulheres e meninas para garantir que elas não apenas tenham acesso e se beneficiem da tecnologia, mas também possam exercer sua autonomia e utilizar a tecnologia blockchain de maneiras que as empoderem. Os dados, no entanto, demonstram a disparidade das mulheres nesse mercado.

No que tange à quem sejam os donos de startups relacionadas com o uso de blockchain, pesquisa da corretora Bitget identificou que apenas 8% das startups são lideradas por mulheres.⁹

Uma pesquisa conduzida pela Forex revela dados preocupantes sobre a disparidade de gênero no setor de cripto e blockchain, evidenciando o predomínio masculino nos cargos de liderança. De acordo com o estudo, 94% dos CEOs no setor são homens, com 47 CEOs masculinos e apenas 3 mulheres ocupando essa posição. Essa diferença ilustra claramente o domínio masculino na indústria.¹⁰

Além de analisar os CEOs, a pesquisa da Forex examinou posições de liderança em geral, constatando que, dos 259 cargos de liderança identificados, 201 eram ocupados por homens e 58 por mulheres. Isso representa 78% dos cargos ocupados por homens e apenas 22% por mulheres. Outro ponto de destaque é a análise dos 50 principais influenciadores de cripto no Twitter, onde a Forex constatou que apenas 14% eram mulheres.¹¹

Por fim, no que em relação ao quarto aspecto e às eventuais violências de gênero ocasionadas pela tecnologia, Thylin e Duarte apontam que qualquer aplicação humanitária da tecnologia blockchain deve estar em conformidade com o direito humanitário internacional, o que pode ser desafiador quando interesses das empresas privadas entram em conflito com os interesses humanitários. Uma preocupação central com as novas tecnologias é a questão

8. THYLIN, T., DUARTE, M. F. N. Leveraging blockchain technology in humanitarian settings— opportunities and risks for women and girls. *Gender & Development*, p. 317-336. 2019.

9. BITGET. *Bitget Report: Blockchain Market Funding Shows Limited Gender Diversity, Female-led Startups Raise Only 6% Of Overall Funds*. Disponível em: <https://www.bitget.com/blog/articles/bitget-report-the-gender-gap-in-blockchain-startup-funding>. Acesso em 3 ago. 2024.

10. FOREX. *Women in Crypto: What role are women playing in crypto in 2024?* Disponível em: <https://forexsuggest.com/women-in-crypto/> Acesso em 11 jul.2024

11. FOREX. *Women in Crypto: What role are women playing in crypto in 2024?* Disponível em: <https://forexsuggest.com/women-in-crypto/> Acesso em 11. jul.2024

da proteção de dados e privacidade, que pode levar a violações severas dos direitos humanos. Se a gama completa de possíveis violações ainda não está clara, a manutenção das informações na blockchain de forma privada e segura contra possíveis ataques é uma das questões mais preocupantes sobre a tecnologia blockchain e as dimensões de gênero desses riscos de proteção de dados e privacidade precisam ser exploradas.¹²

Diante dos indícios de impactos desproporcionais de gênero relacionados à implantação de sistemas com blockchain, é essencial que essa nova tecnologia, que se espera reformular a troca de valores, tenha como um de seus princípios fundamentais a igualdade de gênero. Portanto, é imperativo que a academia analise os possíveis riscos e aplicações da blockchain, conforme seu alcance se expande, e iniciando essa agenda de pesquisa nos próximos tópicos passa-se a destacar algumas aplicações possíveis já registradas na literatura.

2. O quão distribuído é o sistema distribuído de finanças?

“Mulheres, considerem as criptomoedas. Do contrário, os homens irão ficar com toda riqueza de novo”. Esse famoso alerta foi feito pela investidora Alexia Bonatsos, no Twitter.¹³

De fato, no mundo offline, as mulheres historicamente enfrentam barreiras significativas em relação à propriedade e ao acesso a recursos financeiros. Durante séculos, as leis de muitos países negaram às mulheres o direito à propriedade, restringindo sua autonomia econômica e social. Mesmo após conquistas legais que garantem às mulheres o direito de possuir bens, persistem desigualdades substanciais que dificultam o acesso feminino a financiamentos e investimentos.

A promessa da tecnologia blockchain é democratizar o acesso à propriedade e valores, porém, dados demonstram que não existe distribuição de gênero no sistema distribuído de finanças. Isso pode ser analisado por alguns aspectos, como o número de mulheres com investimento em criptomoedas ou o número de mulheres que conseguem alavancar o seu patrimônio utilizando tecnologias relacionadas com blockchain.

Segundo dados disponibilizados pela Receita Federal, entre 2021 e 2023 as operações com criptoativos realizadas por mulheres oscilaram em média

12. THYLIN, T., DUARTE, M. F. N. Leveraging blockchain technology in humanitarian settings—opportunities and risks for women and girls. *Gender & Development*, p. 317-336. 2019.

13. ÉPOCA NEGÓCIOS. *Mulheres buscam seu espaço na indústria do Blockchain*. Disponível em: < <https://epocanegocios.globo.com/Carreira/noticia/2018/02/mulheres-buscam-seu-espaco-na-industria-do-blockchain.html> > Acesso em: 6 jul. 2024

entre 10% e 20%. No melhor cenário, registrado no mês de dezembro de 2022, os homens ainda representavam mais de 70% das operações.¹⁴

No que tange ao recebimento de investimentos, estudo realizado pela corretora Bitget demonstra existir uma clara correlação entre o gênero do fundador e os volumes de investimento, pois as estatísticas indicam que as startups de blockchain lideradas por mulheres arrecadaram apenas 6% do valor total dos investimentos do mercado, comprovando a existência de um viés de gênero.¹⁵

Esse histórico desigual reforça a importância de estudar a tecnologia blockchain sob uma perspectiva de gênero para que essa tecnologia se desenvolva de forma a incluir e empoderar mulheres e minorias de gênero. Neste capítulo, discute-se o potencial da aplicação da blockchain como um instrumento financeiro capaz de mitigar as desigualdades de gênero no mercado financeiro.

Um exemplo brasileiro de aplicação da tecnologia blockchain com impacto de gênero é a plataforma *Moeda Seeds*. Esta plataforma facilita o acesso a microfinanças para empreendedoras que têm projetos com impacto social. Utilizando blockchain e tokens digitais próprios, *Moeda Seeds* cria um ecossistema onde investidores de todo o mundo podem contribuir de forma rápida e transparente para o crescimento sustentável. A plataforma é projetada para apoiar a inclusão financeira e a igualdade de gênero, especialmente para mulheres que enfrentam dificuldades para acessar crédito em bancos tradicionais. Além do suporte financeiro, os projetos selecionados recebem assistência em gestão para otimizar suas operações e promover práticas sustentáveis a longo prazo.¹⁶

Outro exemplo é o *VipiCash*, um aplicativo que usa a tecnologia blockchain para permitir transferências seguras de dinheiro entre mulheres, garantindo que elas tenham controle total sobre seus próprios recursos financeiros, independentemente de membros masculinos da família. Olivier Mukuta e sua equipe desenvolveram essa solução e foram premiados no primeiro hackathon de blockchain co-organizado pelo *UN Women e Innovation Norway* em julho de 2017, com o objetivo de empoderar mulheres em situações de crise humanitária.¹⁷

14. RECEITA FEDERAL. *Criptoativos: Relatório de Dados abertos e informações gerais*. Disponível em: https://www.gov.br/receitafederal/pt-br/assuntos/orientacao-tributaria/declaracoes-e-demonstrativos/criptoativos/arquivos/criptoativos_dados_abertos_25092023.pdf Acesso em: 25 jul.2024

15. BITGET. *Bitget Report: Blockchain Market Funding Shows Limited Gender Diversity, Female-led Startups Raise Only 6% Of Overall Funds*. Disponível em: < <https://www.bitget.com/blog/articles/bitget-report-the-gender-gap-in-blockchain-startup-funding> > Acesso em 3 ago.2024.

16. KANEGAE, L. C.; CERNEV, A. K.; DINIZ, E. *Moeda Seeds: E-Commerce and Crypto Solutions for Development*. *Revista de Administração Contemporânea*, v. 25, n. spe, p. e200224, 2021.

17. UN WOMEN. *From where I stand: Using blockchain technology to empower women*. 2018. Disponível em: <https://www.unwomen.org/en/news/stories/2018/2/from-where-i-stand-olivier-mukuta> Acesso em: 6 jul.2024

Para mulheres em crises humanitárias, a falta de acesso a sistemas financeiros e a incapacidade de transferir ativos representam questões críticas. Esse problema está frequentemente associado à ausência de documentos de identificação, pois em países de baixa renda, por exemplo, mais de 45% das mulheres não possuem uma identificação básica, em comparação com 30% dos homens. Além disso, a maioria dos adultos sem acesso a bancos são mulheres, representando 56% dos desbancarizados, em contraste com 44% dos homens. Em países afetados por crises humanitárias, as mulheres têm 30% menos probabilidade de possuir uma conta financeira individual do que os homens, como no Líbano, em que 62% dos homens e 33% das mulheres têm uma conta bancária.¹⁸

Quando uma crise ocorre, a capacidade de enviar e receber fundos rapidamente pode ser crucial. A tecnologia blockchain pode apoiar os esforços humanitários para aumentar o uso de transferências de dinheiro em respostas emergenciais e já está sendo explorada em programas humanitários.¹⁹

Um exemplo é o *Building Blocks*, um projeto do Programa Mundial de Alimentos (WFP) considerado o maior sistema de distribuição de dinheiro baseado em blockchain do setor humanitário, utilizado para oferecer assistência eficiente e segura a refugiados e pessoas em situação de vulnerabilidade. Atuando em países como Bangladesh, Jordânia, Líbano e Ucrânia, o projeto permite a distribuição de ajuda financeira através de uma rede colaborativa que reúne diversas organizações humanitárias. Desde o seu início, o projeto processou mais de 555 milhões de dólares em transferências de dinheiro, economizando 3,5 milhões de dólares em taxas bancárias, que podem ser redirecionadas para atender mais pessoas em necessidade.²⁰

Através de hubs de blockchain operados por várias organizações, a plataforma permite a coordenação da distribuição de ajuda, atendendo necessidades como alimentação e saúde reprodutiva de forma simultânea. Famílias recebem vouchers que podem ser usados em pontos de venda locais, simplificando o processo e eliminando a necessidade de visitar diferentes locais para obter ajuda. Isso libera recursos para outras necessidades, como educação, e proporciona proteção contra doenças comuns em ambientes sem saneamento adequado.²¹

18. THYLIN, T., DUARTE, M. F. N. Leveraging blockchain technology in humanitarian settings– opportunities and risks for women and girls. *Gender & Development*, p. 317-336. 2019.

19. THYLIN, T., DUARTE, M. F. N. Leveraging blockchain technology in humanitarian settings– opportunities and risks for women and girls. *Gender & Development*, p. 317-336. 2019.

20. WORLD FOOD PROGRAMME. *Building Blocks: Blockchain network for humanitarian assistance*. Disponível em: https://innovation.wfp.org/project/building-blocks?_ga=2.191649962.1216090504.1723029544-45489905.1723029543 Acesso em 4 ago.2024

21. MATAK, Vincent. *How blockchain can power efforts to empower women and girls in Bangladesh*. 2022. Disponível em: <https://www.wfp.org/stories/how-blockchain-can-power-efforts-empower-women-and-girls-bangladesh> Acesso em 4 jul.2024.

A ONU mulheres fez também uma parceria com a WFP com o objetivo de inovar na utilização da blockchain para apoiar mulheres refugiadas sírias que participam dos programas de trabalho remunerado nos campos de refugiados de Za'atari e Azraq, na Jordânia. Na iniciativa conjunta, as mulheres beneficiárias que anteriormente recebiam seu benefício mensal nos centros Oasis da ONU mulheres em forma de dinheiro em uma data específica agora podem retirar dinheiro conforme sua conveniência em vários supermercados, como cashback do caixa.

No programa, uma carteira virtual é criada na para cada beneficiária, constando o valor do dinheiro devido a ela pelo trabalho e, uma vez que uma compra é feita, a blockchain registra o valor a ser debitado. Ademais, em vez de exigir qualquer documento de identificação adicional, as mulheres podem fazer isso com uma leitura da íris que valida sua identidade no supermercado. Isso torna as transações para as mulheres nos campos de refugiados muito mais rápidas e seguras para monitorar.²²

Além disso, a ONU mulheres está fortalecendo sua programação para aprimorar a alfabetização digital e financeira das mulheres refugiadas beneficiárias. Em seus quatro centros Oasis, a ONU está oferecendo treinamentos adicionais e seminários sobre rastreamento de despesas e orçamento para que as beneficiárias possam visualizar suas contas e histórico do Building Blocks online.²³

É necessário destacar, no entanto, que existem ressalvas para adoção do programa. Em primeiro lugar, críticas foram feitas no sentido de que, por ser uma blockchain privada, o seu potencial transformador seria restrito. Fato é que, antes da parceria com a ONU mulheres, o WFP gerenciava todos os nós do sistema, diminuindo sua credibilidade. A ONU mulheres passou a operar um nó independente, o que permite a validação mútua das transações, e a expectativa é que, ao demonstrar uma colaboração efetiva em torno de uma rede blockchain neutra, outras organizações humanitárias percebam os benefícios e se integrem à rede comum, aproximando o sistema das características de uma rede pública.²⁴

Ademais, a tecnologia blockchain enfrenta vários desafios, incluindo alta complexidade técnica, falta de regulamentação e altos custos ambientais associados ao seu uso. A blockchain ainda exige considerável infraestrutura e

22. THYLIN, T., DUARTE, M. F. N. Leveraging blockchain technology in humanitarian settings– opportunities and risks for women and girls. *Gender & Development*, p. 317-336. 2019.

23. THYLIN, T., DUARTE, M. F. N. Leveraging blockchain technology in humanitarian settings– opportunities and risks for women and girls. *Gender & Development*, p. 317-336. 2019.

24. THYLIN, T., DUARTE, M. F. N. Leveraging blockchain technology in humanitarian settings– opportunities and risks for women and girls. *Gender & Development*, p. 317-336. 2019.

recursos, o que pode ser problemático em contextos humanitários. Além disso, países menos envolvidos na exploração da tecnologia e pequenos atores humanitários podem não se beneficiar plenamente da blockchain, exacerbando desigualdades globais.²⁵

Assim, de diferentes maneiras, algumas iniciativas que utilizam da tecnologia blockchain para incentivar o acesso de mulheres ao sistema bancário e financeiro já podem ser mapeadas. A tecnologia, no entanto, também possui o condão de influenciar em outras relações sociais, como se passa a destacar.

3. Podemos confiar o futuro das mulheres para a tecnologia da confiança?

A blockchain é conhecida como tecnologia da confiança, pois as transfe-rências nela registrada podem ser consideradas confiáveis e imutáveis. Utilizando dessa analogia, esse tópico busca explorar se é possível confiar que a tecnologia blockchain poderá ter boas aplicações no que diz respeito ao acesso das mulheres a serviços e políticas. Nesse tópico, apresentam-se algumas aplicações possíveis da tecnologia.

No que tange à ascensão de carreiras, a escassez de mulheres em cargos de liderança em startups de blockchain, como já apontado, demanda a criação de estratégias com o objetivo de promover a igualdade de gênero nos espaços tecnológicos. E as próprias plataformas de blockchain apresentam-se como instrumentos viáveis para aumentar a participação feminina no mercado, desde o processo de contratação, eliminando vieses e permitindo avaliações imparciais com base nas qualificações dos candidatos, até a gestão de carreira, promovendo a participação e o avanço das mulheres.²⁶

Na literatura, por exemplo, já se defende a possibilidade de se criar uma plataforma de recrutamento na qual cada candidato tenha uma identidade única, eliminando a possibilidade de preconceitos e permitindo que os candidatos sejam avaliados apenas com base em suas qualificações. No estudo de Obu et al. foi projetado praticamente uma plataforma de contratação baseada

25. THYLIN, T., DUARTE, M. F. N. Leveraging blockchain technology in humanitarian settings—opportunities and risks for women and girls. *Gender & Development*, p. 317-336. 2019.

26. SANTOS, Vanessa Martins dos; DINIZ, Eduardo Henrique; MORAES, Tricia Karla Lacerda; CERNEV, Adrian Kemmer; LOURENÇO, Carlos Eduardo. *Blockchain e (des)igualdade de gênero: uma revisão sistemática da literatura*. AMCIS 2024 Proceedings, 2024.

em blockchain, que foi ajustada intencionalmente para impedir contratações baseadas em gênero e outros fatores discriminatórios.²⁷

Para além de incentivar a ascensão de mulheres em carreiras, a blockchain pode desempenhar um papel vital na proteção de mulheres contra violência e abusos, oferecendo soluções tecnológicas que permitem a denúncia anônima e segura de assédios e violência de gênero. Essas soluções não apenas aumentam a confiança das vítimas em denunciar, mas também garantem que as evidências sejam preservadas de forma segura e imutável.

A tecnologia blockchain está sendo utilizada em aplicativos móveis para registrar e denunciar casos de assédio sexual de forma anônima. Esses aplicativos garantem que as denúncias sejam tratadas com confidencialidade e que as evidências digitais sejam preservadas de forma segura.

O aplicativo *Hehop* na França, redução de *Help for Hope*, usa blockchain para permitir que vítimas de violência doméstica colem e armazenem evidências digitais de abusos, que podem ser usadas em processos legais. A tecnologia garante que as evidências sejam seguras e não adulteráveis, proporcionando uma ferramenta poderosa para que as vítimas possam acessar o Poder Judiciário.²⁸

No Brasil, têm-se como exemplo o Projeto Glória, em que a blockchain é integrada com inteligência artificial e analytics para melhorar a coleta, análise e disponibilização de dados sobre a violência contra a mulher. Com esses dados, pretende-se desenvolver conteúdos educacionais, implementar políticas públicas e estabelecer uma rede de apoio equipada com ferramentas necessárias para alcançar melhorias sociais.²⁹

Uma terceira aplicação seria para incentivar mulheres no setor cultural por meio da utilização de tokens não-fungíveis (NFTs) no mercado das artes. Os NFTs são ativos digitais que existem na blockchain com uma assinatura única e, entre outras possibilidades, permitem promover a arte digital. Com o potencial dos NFTs para transformar o mundo da arte, a falta de representação feminina no espaço dos NFTs e na blockchain começou a ocupar a agenda de artistas voltados para missões sociais e levando algumas artistas a começarem a ocupar estrategicamente seu espaço em

27. OBU, U.; AMBEKAR, Y.; LINGAM, R.; BORIKAR, Y.; YADAV, R.; DONGRE, S. *Blockchain system against gender bias and other discriminatory practices in workplaces*. Anais da 2023 IEEE 3rd International Conference on Technology, Engineering, Management for Societal Impact using Marketing, Entrepreneurship and Talent (TEMSMET), p. 1-6, 2023.

28. WELSH, Chris. *An app to put domestic abusers on trial*. 2021. Disponível em: <https://www.eib.org/en/stories/domestic-violence-evidence-app> Acesso em 5 jul.2024.

29. VICENTE, Beatriz de Freitas Alves. *A tecnologia blockchain a favor da mulher*. 2022. Disponível em: <https://www.conjur.com.br/2022-abr-04/beatriz-vicente-blockchain-favor-mulher/> Acesso em: 3 jul.2024

um mercado dominado por homens, por meio de diferentes iniciativas e projetos.³⁰

Um exemplo é *World of Women* (WoW), projeto de arte NFT lançado em 2021. Ele apresenta uma coleção de tokens femininos diversos, com a primeira coleção chamada WoW e uma expansão lançada em 2022, denominada *WoW Galaxy*. O WoW visa criar uma Web 3.0 inclusiva e diversificada, promovendo a participação igualitária no espaço NFT. A equipe do projeto apoia causas relacionadas ao empoderamento feminino, inicialmente doando 7,5% das vendas de sua primeira coleção para instituições como *She's The First*, *Too Young to Wed* e *Strange Cintia*.³¹

De forma semelhante, o projeto *Women Rise* é um projeto de arte NFT criado pela artista visual Maliha Abidi e lançado 2021. A coleção *Women Rise* é composta por 10.000 tokens digitais únicos gerados aleatoriamente. Para ajudar na busca da igualdade de gênero, 2,5% das vendas são doadas ao *Malala Fund* e 7,5% a organizações que apoiam a igualdade de gênero, educação de mulheres e saúde mental em comunidades marginalizadas. Além disso, o *Women Rise* é um dos primeiros projetos NFT a se comprometer com a Agenda 2030 para o Desenvolvimento Sustentável, integrando os Objetivos de Desenvolvimento Sustentável (ODS) em suas obras de arte e doações.³²

Outro uso de NFT é proposto pela literatura para modificar a segurança na prática *sexting* e no compartilhamento não autorizado de fotos íntimas, que afeta principalmente meninas e mulheres. Franco et al. exploram o uso de tecnologia blockchain e especificamente NFTs para combater a disseminação não consensual de imagens íntimas geradas pelos usuários e destacam que as aplicações de mensagens tradicionais utilizadas para *sexting* são inseguras, pois permitem o compartilhamento fácil de conteúdos pessoais. Ao implementar soluções descentralizadas baseadas em blockchain, os autores visam criar um ambiente mais seguro e confiável, onde a presença de nós maliciosos é mitigada, garantindo melhor desempenho, escalabilidade e privacidade em comparação com sistemas centralizados.³³

Um risco sobre dados relacionados à gênero e a sua inserção em tecnologia blockchain, por sua vez, é levantado por Shahaab et al. que advogam que se

30. SYULEYMANOGLU, B. *Call for diversity in Web 3.0: case study of NFT art projects World of Women (WoW) and Women Rise*. Malmö University, Faculty of Culture and Society (KS), School of Arts and Communication (K3). 2022.

31. SYULEYMANOGLU, B. *Call for diversity in Web 3.0: case study of NFT art projects World of Women (WoW) and Women Rise*. Malmö University, Faculty of Culture and Society (KS), School of Arts and Communication (K3). 2022.

32. SYULEYMANOGLU, B. *Call for diversity in Web 3.0: case study of NFT art projects World of Women (WoW) and Women Rise*. Malmö University, Faculty of Culture and Society (KS), School of Arts and Communication (K3). 2022.

33. FRANCO, M.; GAGGI, O.; GUIDI, B.; MICHIEZI, A.; PALAZZI, C. E. A decentralised messaging system robust against the unauthorised forwarding of private content. *Future Generation Computer Systems*, v. 145, p. 211-222, 2023.

a blockchain pode desempenhar um papel crucial na construção de identidade digital e na proteção de dados pessoais online, no entanto, dados pessoais não devem ser considerados “estáticos” e nunca devem ser armazenados de forma imutável, pois poderiam ter consequências graves para pessoas trans.³⁴

Assim, esse tópico buscou destacar que, para além das típicas aplicações relacionadas com o mercado financeiro, já existe na literatura discussões sobre possíveis aplicações e riscos da tecnologia blockchain em diversos contextos sociais.

Considerações finais

Este artigo explorou as diversas maneiras pelas quais a tecnologia blockchain pode ser alavancada para abordar questões de desigualdade de gênero, considerando a inexpressividade de trabalhos acadêmicos que abordam o tema, em especial em português.

No primeiro tópico, destacou-se como a promessa de democratização da tecnologia blockchain ainda enfrenta desafios significativos para cumprir totalmente seu potencial transformador em termos de igualdade de gênero.

No segundo tópico, discutiu-se a distribuição de gênero no sistema financeiro distribuído. A análise dos dados revelou que as mulheres ainda enfrentam barreiras significativas no acesso e uso de criptoativos e investimentos, demonstradas pela disparidade de gênero em startups de blockchain e a menor participação feminina nas operações de criptomoedas. No entanto, através de exemplos como a *Moeda Seeds* e o *VipiCash*, demonstrou-se que a tecnologia pode proporcionar às mulheres um maior controle sobre seus recursos financeiros e facilitar o acesso a microfinanças. Ademais, iniciativas como a *Building Blocks* demonstram como a blockchain pode ser utilizada para oferecer soluções inovadoras em contextos humanitários.

No último tópico, apresentou-se soluções de blockchain para recrutamento imparcial, NFTs no mercado de arte e aplicações para denúncias de violência que oferecem um vislumbre de como a tecnologia pode ser utilizada de maneira inovadora para abordar questões sociais.

Se existe um potencial para uso da tecnologia sob uma perspectiva de gênero, é crucial garantir que essas soluções sejam implementadas com atenção às considerações éticas e às necessidades das mulheres, reconhecendo

34. SHAHAAB, A.; MAUDE, R.; HEWAGE, C.; KHAN, I. Managing gender change information on immutable blockchain in context of GDPR. *The Journal of British Blockchain Association*, p. 1-8, 2020.

que a tecnologia por si só não resolverá desigualdades sistêmicas. Conclui-se que é essencial que os desenvolvimentos tecnológicos sejam acompanhados por uma abordagem holística que inclua políticas públicas, educação e conscientização para criar um ambiente mais inclusivo.

Somente através da colaboração entre governos, setor privado e sociedade civil será possível maximizar o impacto positivo da tecnologia blockchain na vida das mulheres, garantindo que ela se torne um verdadeiro substantivo feminino.

Referências

BITGET. Bitget Report: Blockchain Market Funding Shows Limited Gender Diversity, Female-led Startups Raise Only 6% Of Overall Funds. Disponível em: <https://www.bitget.com/blog/articles/bitget-report-the-gender-gap-in-blockchain-startup-funding>. Acesso em 3 ago. 2024.

DICIONÁRIO PRIBERAM. Blockchain. Disponível em: <https://dicionario.priberam.org/blockchain>. Acesso em: 20 jul. 2024.

ÉPOCA NEGÓCIOS. Mulheres buscam seu espaço na indústria do Blockchain. Disponível em: <https://epocanegocios.globo.com/Carreira/noticia/2018/02/mulheres-buscam-seu-espaco-na-industria-do-blockchain.html>. Acesso em: 6 jul. 2024.

FOREX. Women in Crypto: What role are women playing in crypto in 2024? Disponível em: <https://forexsuggest.com/women-in-crypto/>. Acesso em: 11 jul. 2024.

FRANCO, M.; GAGGI, O.; GUIDI, B.; MICHIEZI, A.; PALAZZI, C. E. A decentralised messaging system robust against the unauthorised forwarding of private content. *Future Generation Computer Systems*, v. 145, p. 211-222, 2023.

KANEGAE, L. C.; CERNEV, A. K.; DINIZ, E. Moeda Seeds: E-Commerce and Crypto Solutions for Development. *Revista de Administração Contemporânea*, v. 25, n. spe, p. e200224, 2021.

MATAK, Vincent. How blockchain can power efforts to empower women and girls in Bangladesh. 2022. Disponível em: <https://www.wfp.org/stories/how-blockchain-can-power-efforts-empower-women-and-girls-bangladesh>. Acesso em: 4 jul. 2024.

MURDOCK, Jason. 'We like naked girls': Bitcoin bros slammed as major crypto conference uses strip club. 2018. Disponível em: <https://www.ibtimes.co.uk/we-like-naked-girls-bitcoin-bros-slammed-major-crypto-conference-uses-strip-club-1658353>. Acesso em: 6 ago. 2024.

OBU, U.; AMBEKAR, Y.; LINGAM, R.; BORIKAR, Y.; YADAV, R.; DONGRE, S. Blockchain system against gender bias and other discriminatory practices in workplaces. *Anais da 2023 IEEE 3rd International Conference on Technology, Engineering, Management for Societal Impact using Marketing, Entrepreneurship and Talent (TEMSMET)*, p. 1-6, 2023.

PARDES, Arielle. Miami's Bitcoin Conference Left a Trail of Harassment. 2022. Disponível em: <https://www.wired.com/story/bitcoin-2022-conference-harassment/>. Acesso em: 6 ago. 2024.

RECEITA FEDERAL. Criptoativos: Relatório de Dados abertos e informações gerais. Disponível em: https://www.gov.br/receitafederal/pt-br/assuntos/orientacao-tributaria/declaracoes-e-demonstrativos/criptoativos/arquivos/criptoativos_dados_abertos_25092023.pdf. Acesso em: 25 jul. 2024.

SANTOS, Vanessa Martins dos; DINIZ, Eduardo Henrique; MORAES, Tricia Karla Lacerda; CERNEV, Adrian Kemmer; LOURENÇO, Carlos Eduardo. Blockchain e (des)igualdade de gênero: uma revisão sistemática da literatura. AMCIS 2024 Proceedings, 2024. Disponível em: https://aisel.aisnet.org/amcis2024/span_lacais/span_lacais/5. Acesso em: 7 jul. 2024.

SHAHAAB, A.; MAUDE, R.; HEWAGE, C.; KHAN, I. Managing gender change information on immutable blockchain in context of GDPR. The Journal of British Blockchain Association, p. 1-8, 2020.

SYULEYMANOGLU, B. Call for diversity in Web 3.0: case study of NFT art projects World of Women (WoW) and Women Rise. Malmö University, Faculty of Culture and Society (KS), School of Arts and Communication (K3). 2022.

THYLIN, T.; DUARTE, M. F. N. Leveraging blockchain technology in humanitarian settings—opportunities and risks for women and girls. Gender & Development, p. 317-336, 2019.

UN WOMEN. From where I stand: Using blockchain technology to empower women. 2018. Disponível em: <https://www.unwomen.org/en/news/stories/2018/2/from-where-i-stand-olivier-mukuta>. Acesso em: 6 jul. 2024.

VICENTE, Beatriz de Freitas Alves. A tecnologia blockchain a favor da mulher. 2022. Disponível em: <https://www.conjur.com.br/2022-abr-04/beatriz-vicente-blockchain-favor-mulher/>. Acesso em: 3 jul. 2024.

WELSH, Chris. An app to put domestic abusers on trial. 2021. Disponível em: <https://www.eib.org/en/stories/domestic-violence-evidence-app>. Acesso em: 5 jul. 2024.

WORLD FOOD PROGRAMME. Building Blocks: Blockchain network for humanitarian assistance. Disponível em: https://innovation.wfp.org/project/building-blocks?_ga=2.191649962.1216090504.1723029544-45489905.1723029543. Acesso em: 4 ago. 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

EIXO III

Proteção de dados e segurança digital

AUTORES

Giovana Sant'Anna

Lígia Maria de Souza Lopes Reis

Maíra Lima de Souza

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

16

Risco e Cibersegurança no Brasil: uma análise regulatória visando a proteção de dados

GIOVANA SANT'ANNA

Sumário: Introdução. 1. A Sociedade de Risco e a Sociedade da Informação. 2. Fragilidades cibernéticas e a cibersegurança. 3. Panorama Legislativo Atual. Considerações finais. Referências Bibliográficas.

Introdução

Não se pode dizer que a preocupação com o uso da internet é uma novidade da geração atual. Desde a década de 1980 e a constante e gradativa democratização dos computadores, o termo vírus² já se tornava popular entre os usuários, administradores de sistemas e, de modo geral, dentro das organizações. Os riscos decorrentes do uso da internet já existiam à época, mas atualmente os ataques cibernéticos se mostram cada vez mais sofisticados e de difícil detecção, restando a nós encontrarmos as mais variadas maneiras de mitigá-los, principalmente de forma preditiva³.

A evolução social decorrente da crescente utilização das tecnologias trouxe para as relações pessoais um viés vinculado a estruturas digitais, que, por sua vez, demanda a utilização constante de numerosos dados pessoais e sensíveis⁴. Isso atraiu atenção à temática da Segurança da Informação⁵ e da segurança digital⁶, temas que se tornaram frequentes focos de debates e discussões fomentados pela perspectiva midiática principalmente após inci-

1. Advogada graduada em Direito pela Faculdade de Direito de São Bernardo do Campo em 2018. Pós-Graduada pelo Instituto de Tecnologia do Rio de Janeiro (ITS Rio).

2. Um vírus de computador é um *malware*, ou seja, um software ou um código invasivos e criados com o objetivo de infectar, deteriorar ou acessar arquivos do computador, autorreplicando-se e infectando outros arquivos e documentos. Para mais detalhes ver: LATTO, Nica. *O que é e como funciona um vírus de computador?* Avast Academy, 2020. Disponível em: <https://www.avast.com/pt-br/c-computer-virus#:~:text=Um%20v%C3%A9rus%20de%20computador%20%C3%A9,a%20outros%20arquivos%20ou%20documentos>. Acesso em: 17 jul. 2024.

3. ALMEIDA, João Emílio de. *Cibersegurança: da prevenção do risco à gestão de incidentes*. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, Porto, ed. 43, p. 1-4, 30 set. 2021. p. 1-4. Disponível em: <https://scielo.pt/pdf/rist/n43/1646-9895-rist-43-1.pdf>. Acesso em: 2 maio 2024.

4. Em suma, conforme a Lei 13.709/2018, considera-se dado pessoal toda informação relacionada a pessoa que a torne identificada ou identificável e dado pessoal sensível todo aquele que verse sobre a origem étnica ou racial, religião, opinião política, filiação sindicatos ou a organizações religiosas, filosóficas ou políticas, saúde ou vida sexual, genético ou biométrico. Para mais detalhes ver: BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*. Brasília: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

5. Para Belli et al a segurança da informação é uma dimensão da cibersegurança. Para mais detalhes ver: BELLI, Luca; FRANQUEIRA, Bruna; BAKONYI, Erica; CHEN, Larissa; COUTO, Natalia; CHANG, Sofia; HORA, Nina da; GASPARD, Walter B. *Cibersegurança: Uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano*. 1. ed. Rio de Janeiro: Rio de Janeiro: FGV Direito Rio, Ag. 2023. Disponível em: <https://diretorio.fgv.br/publicacao/ciberseguranca-uma-visao-sistematica-rumo-uma-proposta-de-marco-regulatorio-para-um-brasil>. Acesso em: 24 jun. 2024.

6. SHIRA, Fer; JANCZ, Carla. *Barricadas estratégias e coletividade: uma cartilha de segurança digital para organizações*. Marialab, São Paulo, 1 dez. 2022. p. 3. Disponível em: <https://www.marialab.org/wp-content/uploads/2020/12/Barricadas-estrategias-coletividade.pdf>. Acesso em: 13 jul. 2024.

dentes envolvendo grandes vazamentos de informações, colocando em risco os direitos de milhares de usuários ao redor do mundo⁷.

Hoje os alvos não se limitam a empresas privadas ou a pessoas particulares. Os ataques virtuais destinam-se às organizações governamentais e até mesmo diretamente a países, sendo um exemplo disso a polêmica eleição presidencial dos Estados Unidos em 2016, que trouxe à baila os termos “ciberterrorismo” e “ataque militar” através de meios cibernéticos. Ou seja, o avanço tecnológico trouxe consigo um enorme peso: a valoração pecuniária da informação e a sua utilização como uma influente arma de controle social, político e econômico⁸.

Beck⁹ destaca que a globalização traz à tona novos riscos. O risco não se restringe a ameaças físicas, mas a perigos sociais e ambientais decorrentes do progresso tecnológico e podem variar de acidentes nucleares à privacidade e segurança de dados. São riscos globais e transcendentais capazes de afetar indivíduos e sociedades e desafiar as estruturas tradicionais que obrigatoriamente terão de partir para descoberta de novos métodos de gestão de riscos, os digitais.

Portanto, a intensa transformação decorrente das últimas décadas de desenfreado avanço tecnológico culminou no surgimento de uma nova era para a humanidade, caracterizada pela atraente tecnologia¹⁰. Assim, a Teoria do Direito se viu obrigada a repensar seus fundamentos a fim de incorporar os impactos tecnológicos tecendo fronteiras e regras capazes de frear o - até então - desconhecido desenvolvimento tecnológico e acompanhar a ressignificação humana e social, garantindo a proteção dos direitos dos usuários titulares de dados¹¹.

Teffé¹² entende que cabe ao Direito atuar preventivamente na proteção dos dados, sem deixar de refletir a autonomia dos indivíduos e a imposição de deveres aos agentes. Desta forma origina-se o termo “Direito Digital”, advindo do próprio Direito, que engloba suas mais variadas áreas, os impasses da cha-

7. FICHTNER, Laura. What kind of cyber security? Theorising cyber security and mapping approaches. *Internet Policy Review*, Germany, v. 7, p. 1-19, 15 maio 2018. DOI 10.14763/2018.2.788. Disponível em: <https://policyreview.info/articles/analysis/what-kind-cyber-security-theorising-cyber-security-and-mapping-approaches>. Acesso em: 3 jun. 2024.

8. ALMEIDA, João Emílio de. Cibersegurança: da prevenção do risco à gestão de incidentes. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, Porto, ed. 43, p. 1-4, 30 set. 2021. P. 1-4. Disponível em: <https://scielo.pt/pdf/rist/n43/1646-9895-rist-43-1.pdf>. Acesso em: 2 maio 2024.

9. BECK, Ulrich. *Sociedade de Risco rumo a uma outra modernidade*. São Paulo: Editora 34, 2014, p. 25-28.

10. LUCCA, Newton de. Dignidade da pessoa humana e os riscos eletrônicos. *Galileu - Revista de Economia e Direito*, v. XVII, n.1. 2012. p. 283.

11. BITTAR, Eduardo C.B. A Teoria do Direito, a Era Digital e o Pós-Humano: o novo estatuto do corpo sob um regime tecnológico e a emergência do Sujeito Pós-Humano de Direito. *Direito e Praxis*, v. 10, n. 2, 2019, p. 935.

12. TEFFÉ, Chiara de. *Dados pessoais sensíveis: Qualificação, tratamento e boas práticas*. Indaiatuba, São Paulo, 2022. n.p. Disponível em: https://www.google.com.br/books/edition/Dados_Pessoais_Sens%C3%ADveis/atCLEAAQBAJ?hl=ptBR&-gbpv=1. Acesso em: 28 jun.2024.

mada sociedade da informação e a expansão tecnológica atual¹³. Vê-se que a temática da regulamentação para o mundo virtual e o advento do direito digital se traduzem muito mais numa visão política do que jurídica, já que a internet representa um domínio direto para o desenvolvimento econômico e social¹⁴.

No cenário interno verificamos a existência de alguns marcos legislativos que buscam a proteção dos direitos individuais e de dados dos usuários da internet, dentre eles destacam-se: A Lei de Crimes Cibernéticos (Lei 12.737/2012), o Marco Civil da Internet (Lei 12.965/2014) e a Lei Geral de Proteção de Dados (Lei 13.709/2018)¹⁵. Contudo, a regulamentação de medidas de cibersegurança ainda se apresenta obscura e segmentada. É dentro desta seara que o presente artigo se desenvolverá, buscando elucidar o conceito de risco na sociedade digital, a importância da atuação preventiva através de medidas de governança e quais são as regulamentações atuais aplicáveis à temática da cibersegurança e proteção de dados no Brasil até a publicação da inédita - e recente - Política Nacional de Segurança da Informação, promulgada pelo Decreto nº 11.856 em dezembro de 2023.

1. A Sociedade de Risco e a Sociedade da Informação

A era digital impõe desafios inéditos à Ciência do Direito em razão das intensas transformações sociais, da imposição dos “algoritmos” e da operacionalização digital, ou seja, da atribuição de uma nova dinâmica social (tecnológica) que traçou processos necessários de adaptação da matéria jurídica, visando a garantia efetiva na proteção de direitos dos titulares de dados¹⁶. O direito digital advém da própria necessidade de regulamentação incitada pelos entraves tecnológicos e dilemas característicos da Sociedade da Informação¹⁷. Na sociedade atual a informação é tida como produto valioso, ativo financeiro, e deve ser entendida como tal, portanto, deve ser tratada, cuidada e protegida. Os sistemas de informação são fundamentais para organizar esses dados e desempenham um papel importante na análise de riscos e na mitigação de possíveis incidentes de vazamento de informações¹⁸.

13. PIMENTEL, José E. S. Introdução ao Direito Digital. *Revista Jurídica ESMP-SP*, v. 13, 2018, p. 18.

14. LUCCA, Newton. Dignidade da pessoa humana e os riscos eletrônicos. *Galileu – Revista de Economia e Direito*, v. XVII, n.1, 2012. p. 283.

15. GOLDONI, Luiz R. F.; RODRIGUES, K.F.; MEDEIROS, B.P. Qual é o futuro da governança de cibersegurança no Brasil. *Brasil contemporâneo*. São Paulo, v. 29., 2024. p. 4.

16. BITTAR, Eduardo C.B. A Teoria do Direito, a Era Digital e o Pós-Humano: o novo estatuto do corpo sob um regime tecnológico e a emergência do Sujeito Pós-Humano de Direito. *Direito e Praxis*, v. 10, n. 2, 2019, p. 935.

17. PIMENTEL, José E. S. Introdução ao Direito Digital. *Revista Jurídica ESMP-SP*, v. 13, 2018, p. 18.

18. SAMPAIO, Dhiêgo R.L. *Um estudo sobre riscos de segurança da informação no campus da UFC em Quixadá com base na norma ISO/IEC 27005*. 2014. 45 f. Monografia (Bacharelado em Ciências de Informação) – Universidade Federal do Ceará, Quixadá, 2014.

Em visão ampla, o Direito Digital surge com o objetivo de disciplinar o ambiente virtual, as interações decorrentes desse meio, o armazenamento e o tratamento dos dados digitais para proteger ativamente a sociedade contra violações de seus direitos subjetivos. De Lucca¹⁹ conceitua que, se fosse plausível o paralelismo entre as duas eras (Revolução Industrial e Revolução Digital), a diferença se consubstanciaria a partir da velocidade das transformações ocasionadas pela era digital. Enquanto a Revolução Industrial se baseia na quantidade de trabalho investida nos produtos e serviços, a Revolução Digital se pauta na quantidade de informações e conhecimento de produtos e serviços. A elevada quantidade e a velocidade de transmissão dessas informações são marcos da era digital, que possui como modelo produtivo a massificação de informações, a velocidade de disseminação e a descentralização das fontes dessas informações²⁰.

Uma informação presente num ambiente perigoso ou incerto ocasiona riscos²¹, portanto gera insegurança. A insegurança digital deve ser combatida com a implementação de controles que possam ser implementados para garantir que os riscos sejam reduzidos até que cheguem a um nível aceitável²². Há também de se pensar que o tratamento de dados pelo Estado, por meio do uso de tecnologias digitais, pode ocasionar violência institucional contra coletividades. Os usuários são considerados a parte fraca em qualquer sistema digital, logo, a capacitação social é – sem dúvidas – considerada primordial, uma vez que se enquadra como um dos meios hábeis de coibir essas novas formas de violência social e fragilidade dos direitos individuais²³. Ressalta-se que a grande quantidade de dados decorrentes do uso da internet se tornou uma moeda de troca extremamente valiosa na sociedade atual, o que evidencia um severo risco à privacidade dos titulares²⁴.

O sociólogo alemão Ulrich Beck²⁵ propõe com a “Teoria da Sociedade (Industrial) de Risco” uma ruptura no cerne da sociedade como consequência do

19. LUCCA, Newton. Dignidade da pessoa humana e os riscos eletrônicos. *Galileu – Revista de Economia e Direito*, v. XVII, n.1. 2012. p. 283-285.

20. PIMENTEL, José E. S. Introdução ao Direito Digital. *Revista Jurídica ESMP-SP*, v. 13, 2018, p. 19-20.

21. Segundo a ISO/IEC 27005, risco em segurança da informação é previsto em função da possibilidade de um incidente e de suas consequências e, ao ser administrado, é possível alterar sua possibilidade e suas consequências.

22. SAMPAIO, Dhiêgo R.L. *Um estudo sobre riscos de segurança da informação no campus da UFC em Quixadá com base na norma ISO/IEC 27005*. 2014. 45 f. Monografia (Bacharelado em Ciências de Informação) – Universidade Federal do Ceará, Quixadá, 2014.

23. BELLI, Lucca; Bakonyi Erica; Chen Larissa, et al. Cibersegurança: uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. Rio de Janeiro: *FGV Direito Rio*, 2023, p. 15-16.

24. LORENZON, Laila N. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement. *Revista do Programa de Direito da União Europeia*, 2021, p. 40.

25. BECK, Ulrich. *Sociedade de Risco rumo a uma outra modernidade*. São Paulo: Editora 34, 2014, p. 17.

desenvolvimento industrial e científico e, inerente a estes, os riscos. O autor determina que a Sociedade de risco é intrinsecamente catastrófica, pois nela o estado excepcional de insegurança e ameaça são normalizados. Ainda, define que os riscos atuais são impactos diretos da modernização e os difere dos riscos industriais do século XIX e XX, uma vez que estes eram limitados a determinadas áreas e grupos específicos, mas os riscos decorrentes da modernização são transnacionais e inevitavelmente atingirão as barreiras fronteiriças e, inclusive, aqueles que os produziu ou lucra com eles.

Beck²⁶ menciona que esses riscos contém um efeito *boomerang*, ou seja, nem mesmo a camada social mais poderosa está efetivamente segura e blindada deles. O sociólogo ainda propõe que os riscos, assim como as riquezas, são objetos de distribuição e essa distribuição não ocorre de maneira igualitária. Enquanto as riquezas se mostram como produtos, os riscos ou ameaças se qualificam como o subproduto da modernização²⁷. Portanto, é necessário se atentar à distribuição dos riscos na sociedade atual para que não nos coloquemos numa estrutura desleal e descompensada de distribuição de riscos, ameaçando diretamente os direitos fundamentais dos titulares de dados. Neste sentido, Gomes²⁸ destaca a assimetria entre o Estado, os Agentes de Tratamento e os Titulares de Dados na distribuição de riscos, sublinhando a necessidade de repensar essa distribuição para melhorar a proteção de dados. Historicamente, houve abusos de direitos relacionados ao uso de dados para vigilância estatal, intensificando a já existente assimetria e tornando a proteção de dados extremamente frágil para os titulares.

Niklas Luhmann²⁹ preleciona que o conceito de risco já estava presente desde meados do século XVI. Seu surgimento teria ocorrido a partir da invenção do seguro marítimo, sendo visto como uma probabilidade de perdas e ganhos ao longo das viagens. Assim, ele envolveria a interação entre os sistemas, a sociedade e as incertezas decorrentes dessa relação, sendo inerente, portanto, a uma construção social complexa. Luhmann³⁰ ainda estabelece que conforme a área social envolvida, o risco será diferente e acarretará desafios e resultados diversos. Como exemplo, o aspecto político demandará um risco e resultados diversos das áreas econômicas e jurídicas na sociedade. Quanto ao risco tecnológico, podemos entender como resultado do próprio desenvol-

26. BECK, Ulrich. *Sociedade de Risco rumo a uma outra modernidade*. São Paulo: Editora 34, 2014, p. 25-30.

27. *Ibid.*

28. GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In *Temas atuais de proteção de dados*. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, p. 255.

29. LUHMANN, Niklas. *A Sociological Theory*. Nova Iorque: Editora Routledge, 2017, p. 8-9.

30. *Ibid.* p. 30-35.

vimento sistêmico, capaz de envolver riscos de falhas técnicas, ataques cibernéticos e até desdobramentos sociais e ambientais ainda não mapeados. Contudo, os riscos devem ser avaliados e mitigados, ou seja, administrados, visando garantir a segurança da sociedade geral na utilização da internet.

Lhumann³¹ distingue os conceitos de risco, segurança e perigo. Os dois primeiros são vistos por ele como antagônicos, sendo o risco associado às decisões tomadas no dia a dia e a segurança ao estado que constantemente buscamos socialmente, mesmo que no cenário mundial contemporâneo seja praticamente impossível mitigar totalmente todos os tipos de riscos. Já para o perigo, o autor relaciona esse conceito a uma situação de dano que não é causada pelo agente que sofre as consequências, como no caso de desastres naturais.

Neste sentido, é relevante uma reflexão histórica: antes do antropocentrismo, os eventos eram frequentemente atribuídos a forças externas à vontade humana. Contudo, após o Renascimento, houve uma mudança significativa com a racionalização das tomadas de decisões, quando passamos a gradualmente assumir a responsabilidade pelos resultados dessas decisões³². Logo, os riscos digitais estarão presentes enquanto as mudanças sociais e tecnológicas produzirem consequências não previstas. Podemos, portanto, considerar os riscos como o lado incerto da modernidade. Isso não significa que a vida atual é mais arriscada do que em épocas anteriores, mas que para a sociedade atual, tanto leigos quanto especialistas deverão realizar a tarefa diária e permanente de ponderação e administração de riscos³³.

Com o passar dos anos, observou-se um avanço gradativo da sociedade estabelecendo cálculos racionais de riscos. Inicialmente o cálculo de riscos se dava numa visão dualista de falha *versus* sucesso, mas posteriormente esse cálculo foi mais bem desenvolvido com métricas robustas a partir da matemática e da probabilidade, gerando maior controle sobre os resultados dos riscos. Porém, ao abordarmos a temática de risco temos sempre que nos lembrar que estamos diante de um vasto leque de experiências humanas, o que nos coloca frente a um eterno desconhecido e faz com que, mesmo com os métodos mais robustos desenvolvidos até o momento, seja impossível de prever ou controlar todos os riscos³⁴. Ademais, a ciência e a tecnologia trazem consigo diversos

31. Ibd. p. 19.

32. GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, p. 252.

33. GIDDENS, Anthony. *Modernidade e Identidade*. Rio de Janeiro: Jorge Zahar, 2002, p. 32.

34. GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, p. 252.

benefícios e facilidades, apesar de nos impor o enfrentamento de riscos e perigos. Assim, é vantajoso que avaliemos e administremos os riscos de maneira racional para podermos colher os benefícios da sociedade pós-moderna³⁵.

No início dos anos 2000 os casos de invasão de dados e lesão a privacidade dos usuários se tornaram mais frequentes em decorrência do surgimento de *spams*³⁶ de bancos de dados de sites, que vendiam e compartilhavam informações dos usuários³⁷. Essa rápida transformação social ocasionada pela alta digitalização, com o foco para os dados como modelo de riqueza, trouxe à tona a necessidade de maiores investimentos em cibersegurança. Na medida em que há um mercado tecnológico em expansão, com profissionais qualificados na área, há também uma crescente criminalidade exigindo uma constante atualização sobre o tema. Assim, a demanda de proteção jurídica dos dados advém da importância econômica que os dados desempenham na realidade atual, e a alta volumetria de dados armazenados pelas entidades públicas e privadas evidencia o elevado risco à privacidade dos usuários, tornando nítida a necessidade de atualização legislativa para garantir a proteção dos direitos fundamentais da sociedade civil³⁸.

2. Fragilidades cibernéticas e a cibersegurança

Conforme já mencionado, a grande quantidade de pessoas conectadas culminou num significativo aumento de crimes cibernéticos e numa maior atenção por parte da sociedade sobre a necessidade premente de elaborar regras de conduta e limitar a atuação estatal e privada no controle das informações que tratam e armazenam³⁹. Em primeira análise, a cibersegurança é um ecossistema multifacetário que demanda a implementação de um mecanismo de governança e de um conjunto normativo hábil que conversem entre si e com os diferentes setores da sociedade, a fim de assegurar uma aplicação eficiente e eficaz. Para isso é necessário um alinhamento nacional formalizado por meio

35. GIDDENS, Anthony. *Modernidade e Identidade*. Rio de Janeiro: Jorge Zahar, 2002, p. 32.

36. Spam é advindo do termo em inglês “*Sending and Posting Advertisement in Mass*”, ou seja, pode ser interpretado como o envio e a postagem de propagandas em massa. Para mais detalhes ver: LINKNACIONAL. O que é spam? Link Nacional, 20 out. 2023. Disponível em: <https://www.linknacional.com.br/blog/o-que-e-spam/>. Acesso em: 24 jun. 2024.

37. BRAGA, Noelson Araújo. *Ciberegurança e o Direito à Privacidade: Um estudo sobre a construção cibernética no Brasil e na União Europeia na ótica realista*. 2021. 35 f. Monografia (Bacharel em Relações Internacionais) – Universidade de Brasília UNB, Brasília, 2021.

38. LORENZON, Laila N. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement. *Revista do Programa de Direito da União Europeia*, 2021, p. 40.

39. BRAGA, Noelson Araújo. *Ciberegurança e o Direito à Privacidade: Um estudo sobre a construção cibernética no Brasil e na União Europeia na ótica realista*. 2021. 35 f. Monografia (Bacharel em Relações Internacionais) – Universidade de Brasília UNB, Brasília, 2021.

de uma regulação capaz de estabelecer padrões operacionais mínimos, princípios e o sistema de governança com mitigação de riscos⁴⁰.

A cibersegurança deve ser considerada uma preocupação real para traçar um plano de enfrentamento de desafios e poder prevenir que os riscos e ameaças ocorram. A ação reativa – tomada de decisões após os acidentes – pode causar perdas substanciais e enormes danos financeiros, legais e reputacionais às empresas e ao poder público⁴¹. No cenário das organizações privadas é inevitável aumentar os sistemas de defesa e antecipar os frequentes ataques digitais. Esses ataques geralmente consistem em roubo ou sequestro de informações⁴², como ocorre no *ransomware*⁴³. Podemos, portanto, entender a cibersegurança como um conjunto normativo que estabelece procedimentos e práticas visando a segurança de sistemas, informações e riscos digitais, sendo a segurança da informação apenas uma das camadas da cibersegurança.

Os incidentes de cibersegurança, embora muitas vezes estejam ligados a falhas ou a ataques diretos, também se referem a comportamentos inseguros de desenvolvedores ou usuários de tecnologias, que podem comprometer os princípios basilares da confidencialidade, integridade, autenticidade, autenticação e acesso⁴⁴. Há casos recentes e marcantes que afetaram diretamente o provimento de serviços públicos no Brasil, com destaque ao incidente envolvendo o controle vacinal da população brasileira e ataques a sistemas de tribunais que forçam a dilação de prazos e a paralização de prestação de serviços públicos aos cidadãos⁴⁵.

Em 2021, dois casos emblemáticos marcaram a realidade brasileira a nível de cibersegurança: a invasão do aplicativo ConectSUS⁴⁶ e a venda de dados da Controladoria Geral da União em fóruns da internet. O aplicativo ConectSUS foi invadido em dezembro de 2021 e ocasionou, além da impossibilidade

40. BELLI, Luca; FRANQUEIRA, Bruna; BAKONYI, Erica; CHEN, Larissa; COUTO, Natalia; CHANG, Sofia; HORA, Nina da; GASPAR, Walter B. Cibersegurança: Uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. 1. ed. Rio de Janeiro: Rio de Janeiro: FGV *Direito Rio*, Ag. 2023. p. 22. Disponível em: <https://direitorio.fgv.br/publicacao/ciberseguranca-uma-visao-sistematica-rumo-uma-proposta-de-marco-regulatorio-para-um-brasil>. Acesso em: 24 jun. 2024.

41. *Ibdi*.

42. ALMEIDA, João E. de. Cibersegurança: da prevenção do risco à gestão de incidentes. *RISTI – Revista Ibérica de Sistemas e Tecnologias de Informação*. Porto, 2021, p.2.

43. Uma forma de ataque que consiste no bloqueio ou sequestro de informações ou sistemas de organizações em que a liberação somente ocorre mediante pagamento de resgate. Para mais detalhes ver: *ibdi*. p. 19.

44. BELLI, Luca; FRANQUEIRA, Bruna; BAKONYI, Erica; CHEN, Larissa; COUTO, Natalia; CHANG, Sofia; HORA, Nina da; GASPAR, Walter B. Cibersegurança: Uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. 1. ed. Rio de Janeiro: Rio de Janeiro: FGV *Direito Rio*, Ag. 2023. p. 24-25. Disponível em: <https://direitorio.fgv.br/publicacao/ciberseguranca-uma-visao-sistematica-rumo-uma-proposta-de-marco-regulatorio-para-um-brasil>. Acesso em: 24 jun. 2024.

45. *Ibid.*. p. 19.

46. *Problemas no ConecteSUS: antes de ataque hacker, sistema teve polêmica com alteração de dados e falhas*. Disponível em: <https://g1.globo.com/saude/noticia/2021/12/10/problemas-no-conectesus-antes-de-ataque-hacker-sistema-teve-polemica-com-alteracao-de-dados-e-falhas.ghtml>.

de emissão dos comprovantes de vacinação, a alteração dos dados de diversos usuários. Algumas doses de vacinas simplesmente sumiram do sistema e usuários relataram que tiveram seus dados (nome, nome da mãe e nacionalidade) modificados. O Ministério da Saúde informou na ocasião que tomou as medidas cabíveis e chegou a derrubar o acesso ao aplicativo ConectSUS⁴⁷. Ainda em 2021 houve uma invasão generalizada a serviços públicos do governo brasileiro, credenciais da Administração Federal foram encontradas à venda em fóruns da *dark web*, logins e senhas da Controladoria Geral da União e do Ministério da Saúde foram vazadas⁴⁸.

Além disso, em novembro de 2020 o Superior Tribunal de Justiça vivenciou um ataque cibernético⁴⁹ que ficou conhecido pela própria Corte como o pior ataque cibernético já realizado contra uma instituição pública brasileira⁵⁰. O ataque impediu que milhões de pessoas acessassem a plataforma do STJ, inclusive dos próprios Ministros, ocasionando um verdadeiro caos no judiciário e a suspensão de prazos processuais por quase uma semana inteira. Os anos de 2020 e 2021, portanto, ficaram marcados por grandes vazamentos de dados no Brasil, vazamentos esses capazes de afetar um número maior do que a própria população nacional, uma vez que expuseram dados de mais de 220 milhões de pessoas⁵¹. Esse fato traduz uma importante característica atual: a dependência das organizações públicas e privadas à internet⁵².

Isso mostra que, no cenário atual, em que estar conectado se mostra um ato essencial em diversas camadas sociais, a insegurança cibernética ameaça a sociedade como um todo, colocando em xeque até mesmo a perspectiva democrática⁵³. Empresas privadas, órgãos e entidades públicas ainda são o maior alvo de ataques, contudo a sociedade em geral deve sempre se preocupar e contribuir com a proteção dos seus direitos. Vale ressaltar que os ata-

47. *Problemas no ConecteSUS: antes de ataque hacker, sistema teve polêmica com alteração de dados e falhas*. Disponível em: <<https://g1.globo.com/saude/noticia/2021/12/10/problemas-no-conectesus-antes-de-ataque-hacker-sistema-teve-polemica-com-alteracao-de-dados-e-falhas.ghtml>>.

48. *CRIMINOSOS vendem dados do CGU e Ministério da Saúde na dark web*. [S. l.], 21 dez. 2021. Disponível em: <https://canaltech.com.br/seguranca/criminosos-vendem-dados-do-cgu-e-ministerio-da-saude-na-dark-web-204985/>. Acesso em: 27 jun. 2024.

49. G1. STJ aciona PF para apurar possível ataque de hackers ao sistema do tribunal. *G1*, 4 nov. 2020. Disponível em: <https://g1.globo.com/politica/noticia/2020/11/04/stj-aciona-pf-para-apurar-possivel-ataque-de-hackers-ao-sistema-do-tribunal.ghtml>. Acesso em: 2 jul. 2024.

50. MARCON, Daniele Verza. *Seguro contra Riscos Cibernéticos: desafios para delimitar a garantia e promover a cibersegurança na era digital*. 2023. Dissertação (Mestrado em Ciências Jurídicas e Sociais) - Universidade Federal do Rio Grande do Sul, [S. l.], 2023. Disponível em: <https://lume.ufrgs.br/handle/10183/267969>. Acesso em: 3 jul. 2024.

51. Ibid.

52. Ibid.

53. BELLI, Luca; FRANQUEIRA, Bruna; BAKONYI, Erica; CHEN, Larissa; COUTO, Natalia; CHANG, Sofia; HORA, Nina da; GASPAR, Walter B. *Cibersegurança: Uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano*. 1. ed. Rio de Janeiro: Rio de Janeiro: FGV *Direito Rio*, Ag. 2023.p. 19. Disponível em: <https://direitorio.fgv.br/publicacao/ciberseguranca-uma-visao-sistematica-rumo-uma-proposta-de-marco-regulatorio-para-um-brasil>. Acesso em: 24 jun. 2024.

ques cibernéticos não ocorrem apenas em decorrência de ataques ativos, mas também se dão de maneira passiva, em virtude da fragilidade ou da ausência de medidas básicas de segurança e falta de capacitação dos usuários⁵⁴.

Em 2023 o Brasil liderou o *ranking* de países com maior volume de dados vazados, superando a Índia, Estados Unidos e a Indonésia em volume de informações comprometidas. Dentre as informações vazadas destacam-se nomes, e-mails, endereços e senhas arquivadas pelos *cookies*⁵⁵ salvos nos navegadores dos usuários brasileiros⁵⁶. Tais incidentes demonstram que a sociedade brasileira ainda padece de controle das próprias informações, o que pode ser interpretado como uma rusga ao direito de privacidade do titular do dado, que não consegue exercer o seu poder de decisão, tratamento e transmissão das suas informações⁵⁷.

Tendo em vista o alto risco das organizações públicas federais, em 2022 o Tribunal de Contas da União publicou uma cartilha destacando cinco medidas de controle em cibersegurança que precisariam ser implementadas com urgência pela administração pública brasileira, quais sejam: inventário e controles de ativos corporativos de tecnologia da informação; inventário e controles de ativos de *software*; gestão contínua de vulnerabilidades; conscientização sobre segurança e treinamento de competências; e gestão de respostas a incidentes⁵⁸.

Isso fez parte de uma série de medidas tomadas em resposta aos episódios aqui evidenciados, visto que eles trouxeram à tona a vulnerabilidade de alto risco da administração pública nacional. Além da cartilha publicada pelo Tribunal de Contas da União, esses eventos também incentivaram a publicação de um novo marco em matéria de cibersegurança em dezembro de 2023, a Política Nacional de Cibersegurança (PNCiber) - Decreto Presidencial nº 11.856. Esse Decreto, que se comporta como uma resposta imediata ao preocupante cenário atual⁵⁹, será analisado no próximo capítulo.

54. SHIRA, Fer; JANCZ, Carla. *BARRICADAS ESTRATÉGIAS E COLETIVIDADE: Uma cartilha de segurança digital para organizações*. Marialab, São Paulo, 1 dez. 2022. Disponível em: <https://www.marialab.org/wp-content/uploads/2020/12/Barricadas-estrategias-coletividade.pdf>. Acesso em: 13 jul. 2024.

55. *Cookies* são arquivos criados pelos sites a fim de coletar informações da navegação dos usuários na internet, podem ser utilizados para fins de comodidade do usuário, armazenando logins e senhas e itens adicionados a carrinhos virtuais, por exemplo. Para mais detalhes ver: G1. *O que são cookies na internet e como eles funcionam*. G1, 09 jun. 2024. Disponível em: <https://g1.globo.com/tecnologia/noticia/2024/06/09/o-que-sao-cookies-na-internet-e-como-eles-funcionam.ghtml>. Acesso em: 24 jun. 2024.

56. *CRIMINOSOS vendem dados do CGU e Ministério da Saúde na dark web*. [S. l.], 21 dez. 2021. Disponível em: <https://canaltech.com.br/seguranca/criminosos-vendem-dados-do-cgu-e-ministerio-da-saude-na-dark-web-204985/>. Acesso em: 27 jun. 2024.

57. TEFFÉ, Chiara de. *Dados pessoais sensíveis: Qualificação, tratamento e boas práticas*. Indaiatuba, São Paulo, 2022. n.p.

58. Tribunal de Contas da União. *Cinco controles de segurança cibernética para ontem* / Tribunal de Contas da União. – Brasília: TCU, 2022. 36 p. p.1. Disponível em: <https://portal.tcu.gov.br/5-controles-de-seguranca-cibernetica.htm>. Acesso em: 06 jul. 2024.

59. GOLDONI, Luiz R. F.; RODRIGUES, K.F.; MEDEIROS, B.P. Qual é o futuro da governança de cibersegurança no Brasil. *Brasil contemporâneo*. São Paulo, v. 29., 2024. p. 8-10.

3. Panorama Legislativo Atual

As políticas cibernéticas são indispensáveis numa abordagem de governança que demanda estruturas institucionais voltadas para solucionar problemas públicos num contexto indefinido de atribuições e responsabilidades. Nesse cenário de atuação de múltiplos atores, o papel da administração pública deve ser de direcionar e orientar as ações. Esses mecanismos deverão atuar definindo objetivos claros, atribuindo responsabilidades e desenvolvendo melhoria nas atuações e políticas de fomento à segurança da informação. Ou seja, necessária se faz a padronização orientativa pelo Governo Federal, o fomento a políticas públicas e a atribuição de responsabilidades aos órgãos e entidades competentes⁶⁰.

A Política Nacional de Cibersegurança (PNCiber) foi implementada justamente para responder reativamente ao cenário de insegurança atual a partir do desenvolvimento de mecanismos de regulação e fiscalização, estratégias de cooperação internacional, desenvolvimento de capacitação e educação em segurança cibernética, dentre outros⁶¹. No entanto, é imprescindível ressaltar que outras medidas foram adotadas antes da publicação da PNCiber, sendo necessário elucidá-las para possibilitar uma análise mais precisa desse cenário no Brasil.

Em primeiro lugar, destaca-se que no contexto de proteção de dados no Brasil evidenciam-se o artigo 5º da Constituição Federal, que prevê a inviolabilidade da vida privada, intimidade, honra e imagem das pessoas⁶²; o Código Civil, que dispõe sobre a inviolabilidade da vida privada⁶³; e o Marco Civil da Internet – Lei 12.965/2014 –, pioneiro na positivação de direitos e deveres para o uso da internet⁶⁴. Este último já previa como princípio do uso da internet a proteção dos dados pessoais no seu artigo 3º, incisos II e III⁶⁵. Porém, mesmo com sua promulgação ainda pairava sobre o Brasil a necessidade de uma regulamentação específica e consolidada sobre o tratamento de dados pessoais⁶⁶.

60. Ibid. 2-3.

61. Ibid. p. 10-11.

62. BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal, 2016. 496 p. Disponível em: planalto.gov.br/ccivil_03/constitucao/constitucao.htm. Acesso em 01 jun. 2024.

63. BRASIL. Lei 10.406, de 10 de janeiro de 2002. Institui o Código Civil Brasileiro. *Diário Oficial da União*. Brasília: Presidência da República. Disponível em: planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 05 jan. 2024.

64. LORENZON, Laila Neves. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement. *Revista do Programa de Direito da União Europeia*, [S. l.], p. 1-14, 15 mar. 2021. p. 41-42.

65. 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: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/ato2011-2014/2014/lei/l12965.htm. Acesso em: 07 jun. 2023.

66. MENDES, Laura Schertel. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. *Panorama Setorial da Internet*, [S. l.], ano 11, n. 2, p. 1-20, jun. 2019. p. 2-4. Disponível em: https://www.nic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano-xi_n_2_privacidade_e_dados_pessoais.pdf. Acesso em: jul. 2024.

Foi por conta disso que ocorreu o advento da Lei Geral de Proteção de Dados (LGPD) em 2018, com o intuito de estabelecer os padrões mínimos de segurança cibernética no Brasil (Pinheiro, 2024). Essa importante legislação, que antecedeu a PNCiber (Brasil, 2018a), se mostrou um grande instrumento precursor no cenário brasileiro ao estabelecer um padrão de condutas a serem adotadas por processadores de dados pessoais em prol da tutela de direitos fundamentais, da dignidade humana e do direito à privacidade dos titulares (Lóssio, 2020). Ela veio como o instrumento capaz de assegurar a proteção aos dados pessoais, que até então não eram efetivamente assegurados por outros instrumentos. Além disso, a LGPD apoiou o desenvolvimento de políticas públicas de controle dos tratamentos desses dados, uma vez que um cenário inseguro no meio digital se torna cada dia mais inaceitável, nacional ou internacionalmente. A mencionada legislação trouxe também como novidade característica a proteção da privacidade dos usuários contra as empresas com excessos de informações armazenadas (Braga, 2021).

Mesmo assim, a LGPD apresentou alguns problemas. Sua tardia implantação, por exemplo, resultou num nível considerável de circulação de dados, e pode-se dizer que a falta de atenção à cibersegurança no início do século XXI culminou numa defasagem que ainda não acompanha o exponencial crescimento tecnológico (Braga, 2021). Não obstante, ao estabelecer uma análise prática da análise de riscos na LGPD verifica-se muito mais uma prática de adequação regulatória visando atingir o *accountability*⁶⁷ e diminuir a probabilidade de imposição de sanções do que uma preocupação efetiva com possível lesão aos direitos dos usuários. Logo, é uma preocupação válida a sobreposição que ocorre durante a análise dos riscos de uma busca por adequação técnica e regulatória no lugar de proteção aos direitos fundamentais dos usuários⁶⁸.

Por conta disso, diversos Decretos se originaram no cenário brasileiro, dentre eles o E-Digital (Decreto 9.319/2018)⁶⁹; o Decreto nº 10.046/2019⁷⁰, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal; a Estratégia de Governo Digital para os anos de

67. Conjunto de práticas visando a responsabilização de toda a cadeia de tratamento de dados. Para mais detalhes ver: MENDES, Laura Schertel. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. *Panorama Setorial da Internet*, [S. l.], ano 11, n. 2, p. 1-20, jun. 2019. Disponível em: https://www.nic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano-xi_n_2_privacidade_e_dados_pessoais.pdf. Acesso em: jul. 2024.

68. GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In *Temas atuais de proteção de dados*. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271. p. 258.

69. BRASIL. Decreto nº 9.319, de 14 de março de 2018. Altera o Decreto nº 8.777, de 11 de maio de 2016, que institui a Política Nacional de Proteção e Defesa do Consumidor. *Diário Oficial da União*, Brasília, 15 mar. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9319.htm. Acesso em: 01 jun. 2024.

70. BRASIL. Decreto nº 10.046, de 30 de setembro de 2019. Altera o Decreto nº 9.203, de 22 de novembro de 2017, que regulamenta a Lei nº 13.334, de 13 de setembro de 2016. *Diário Oficial da União*, Brasília, 1º out. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10046.htm. Acesso em: 01 jun. 2024.

2020 a 2022 (Decreto nº 10.332/2020)⁷¹; a publicação da Estratégia Nacional de Segurança Cibernética, ou E-Ciber (Decreto 10.222/2020)⁷²; e a aprovação do Plano Nacional de Segurança e Infraestruturas Críticas, por meio do Decreto nº 11.200⁷³. O E-Digital é marcante na temática de cibersegurança, pois propõe melhorias significativas na infraestrutura cibernética brasileira⁷⁴. Promove o acesso adequado à tecnologia e a inclusão digital para todo território nacional, em áreas urbanas e rurais, propõe iniciativas de desenvolvimento e inovação, além de determinar a proteção dos direitos e privacidade dos usuários e fomentar a necessidade de segurança no meio digital, incentivando a educação e a capacitação profissional⁷⁵.

A PNCiber foi precedida também pela publicação do Decreto 9.637/2018 que instituiu a Política Nacional de Segurança da Informação (PNSI), atualizada em 2021 através do Decreto nº 10.641. A PNSI foi uma importante política a nível nacional, possuindo como escopo o fortalecimento da cultura da segurança da informação na sociedade e o incentivo à qualificação profissional na área da segurança da Informação⁷⁶. Podemos interpretá-la como a base da governança cibernética no Brasil, pois estabeleceu a segurança da informação em larga escala, incorporou os princípios da integridade, confidencialidade e garantia da disponibilidade das informações. Além do mais, estimulou a criação de uma política nacional de cibersegurança com a participação dos setores público e privado⁷⁷.

Neste sentido, a PNSI prevê a importância da criação de uma estratégia nacional de segurança da informação (E-Ciber)⁷⁸. A estratégia nacional, junto dos planos nacionais, constituiu os instrumentos da PNSI que estabeleceram a participação da sociedade, dos órgãos e das entidades públicas e atribuiu

71. BRASIL. Decreto nº 10.332, de 28 de abril de 2020. Dispõe sobre a criação do Programa Nacional de Apoio à Geração de Emprego e Renda. Diário Oficial da União, Brasília, 29 abr. 2020. Disponível em: [72. BRASIL. Decreto nº 10.222, de 05 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. Diário Oficial da União, Brasília, 2020. Disponível em: \[73. GOLDONI, Luiz R. F.; RODRIGUES, K.F.; MEDEIROS, B.P. Qual é o futuro da governança de cibersegurança no Brasil. *Brasil contemporâneo*. São Paulo, v. 29., 2024. p. 4-8.\]\(https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 07 jun. 2024.</p></div><div data-bbox=\)](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10332.htm#:~:text=DECRETO%20N%C2%BA%2010.332%2C%20DE%2028,fundacional%20e%20d%C3%A1%20outras%20provid%C3%AAs. Acesso em: 07 jun. 2024.</p></div><div data-bbox=)

74. Ibid.

75. Decreto n. 9.319, de 21 de março de 2018. (2018). Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital. Brasília, DF.

76. Ibid.

77. GOLDONI, Luiz R. F.; RODRIGUES, K.F.; MEDEIROS, B.P. Qual é o futuro da governança de cibersegurança no Brasil. *Brasil contemporâneo*. São Paulo, v. 29., 2024. p. 5.

78. BELLI, Luca; FRANQUEIRA, Bruna; BAKONYI, Erica; CHEN, Larissa; COUTO, Natalia; CHANG, Sofia; HORA, Nina da; GASPARELLO, Walter B. Cibersegurança: Uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. 1. ed. Rio de Janeiro: Rio de Janeiro: FGV Direito Rio, Ag. 2023. Disponível em: [2025](https://diretorio.fgv.br/publicacao/ciberseguranca-uma-visao-sistematica-rumo-uma-proposta-de-marco-regulatorio-para-um-brasil. Acesso em: 24 jun. 2024. p.12.</p></div><div data-bbox=)

como competência e responsabilidade do gabinete de segurança institucional da Presidência da República a elaboração e a publicação⁷⁹. O artigo 6º da PNSI determina a estrutura da Estratégia Nacional de Segurança da Informação, dividida nos seguintes módulos: defesa cibernética; segurança das infraestruturas críticas; segurança da informação sigilosa; e proteção contra vazamento de dados. Preocupou-se também a PNSI em garantir a proteção aos direitos fundamentais dos usuários contra os possíveis vazamentos de dados, estabelecendo como um de seus princípios a proteção de dados pessoais e à privacidade ao longo do seu artigo 3, inciso II⁸⁰.

O Plano Nacional de Segurança de Infraestruturas Críticas (Decreto nº 11.200/2022)⁸¹ aborda a imprescindibilidade da gestão de riscos para a segurança das infraestruturas críticas, com a determinação de metodologia sistêmica para identificar, avaliar e tratar os riscos. Em razão da quantidade de informações, estabelece a necessidade de monitoramento constante e a atuação tempestiva em cenários de crise para adoção de medidas adequadas. Também promoveu a necessidade de integração e cooperação entre os setores público e privado e estabeleceu um Sistema Integrado de Dados de Segurança e Infraestruturas Críticas, por meio do qual serão acompanhadas e monitoradas permanentemente a Segurança da Infraestrutura Crítica do Brasil, através de metodologias específicas para identificação, acompanhamento e fornecimento de dados sobre alertas e análises de riscos⁸².

Contudo, Belli et al⁸³ destaca que para que o Brasil se torne uma nação digitalmente soberana é imprescindível a criação de uma estratégia de soberania digital baseada na cibersegurança e em investimentos estratégicos. Por conta disso, em maio de 2023 foi publicada uma minuta pelo Gabinete de Segurança Institucional prevendo a criação da PNCiber. Essa minuta era extensa, mais do que o Decreto publicado, e trazia em seu conteúdo a necessidade de unificar a “colcha de retalhos” da realidade brasileira de regulamentação de cibersegurança⁸⁴.

79. Decreto n. 9.319, de 21 de março de 2018. (2018). Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital. Brasília, DF.

80. Ibid.

81. BRASIL. Decreto nº 11.200, de 30 de setembro de 2022. Dispõe sobre a regulamentação de políticas públicas. Diário Oficial da União: Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11200.htm#:~:text=DECRETO%20N%C2%BA%2011.200%2C%20DE%2015,de%20Seguran%C3%A7a%20de%20Infraestruturas%20Cr%C3%ADticas. Acesso em: 01 jun. 2024.

82. Ibid.

83. BELLI, Lucca; Bakonyi Erica; Chen Larissa, et al. Cibersegurança: uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. Rio de Janeiro: FGV *Direito Rio*, 2023, p. 13.

84. GOLDONI, Luiz R. F.; RODRIGUES, K.F.; MEDEIROS, B.P. Qual é o futuro da governança de cibersegurança no Brasil. *Brasil contemporâneo*. São Paulo, v. 29., 2024. p. 9.

Portanto, a PNCiber surgiu com o intuito de orientar as atividades de cibersegurança nacional a partir da instituição de métodos de governança, diretrizes e ações voltadas à segurança cibernética no Brasil⁸⁵. A parte principiológica da PNCiber se consubstancia na garantia de direitos fundamentais, na soberania e nos interesses nacionais, na resiliência das organizações públicas e privadas, na educação e no desenvolvimento tecnológico e na cooperação, tanto entre os entes públicos e privados quanto internacionalmente, acerca do assunto segurança cibernética⁸⁶.

Conforme já exposto, a própria LGPD corroborou preteritamente a proteção dos direitos fundamentais da sociedade civil no uso da internet ao estabelecer práticas a serem adotadas por todos aqueles que processam os dados dos usuários⁸⁷. Desta forma, a política em comento retificou a importância do protecionismo aos direitos fundamentais dos usuários, preocupando-se, além disso, com a necessidade de manutenção da soberania nacional, educação tecnológica e cooperação entre toda a camada social⁸⁸.

Entre os próprios objetivos da Política Nacional destacam-se ações preventivas com foco na capacitação e educação da sociedade em geral, o fomento à pesquisa científica, desenvolvimento tecnológico, inovação da temática da segurança cibernética, a necessidade de atuação coordenada e a troca de informações sobre segurança cibernética entre os três Poderes (Legislativo, Executivo e Judiciário), entre os Entes Federativos (Estados, União, Municípios e Distrito Federal), entre os setores público e privado e entre a sociedade em geral⁸⁹. Ou seja, a PNCiber tem um grande foco em ações preventivas a incidentes, não apenas para capacitação dos agentes públicos e das organizações privadas, mas da sociedade em geral, promovendo a educação e a capacitação técnica como formas de munir a sociedade de conhecimento em cibersegurança⁹⁰.

Assim, a PNCiber estabelece princípios objetivos e, também, institui em seu artigo 5º o Comitê Nacional de Cibersegurança (CNCiber) para promover

85. PINHEIRO, Patricia P.G. *Cibersegurança, Sociedade e Futuro*. Computação Brasil, [S. l.], p. 67-70, 1 jun. 2024, p. 69.

86. Decreto n. 11.856, de 26 de dezembro de 2023. (2023). *Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança*. Brasília, DF.

87. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Diário Oficial da União. Brasília: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 nov. 2023.

88. Decreto n. 11.856, de 26 de dezembro de 2023. (2023). *Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança*. Brasília, DF.

89. Ibid..

90. Ibid..

a unificação de medidas nesta seara⁹¹. Pinheiro⁹² destaca que a influência que a internet exerce sobre a economia global demanda a aplicação de padrões robustos de segurança cibernética, e foi essa necessidade que deu origem à intenção de criar um ecossistema de cibersegurança através do CNCiber. Esse comitê tem por objetivo implementar, fomentar e atualizar as medidas previstas na Política Nacional, visto que a cibersegurança precisa ser continuamente adequada e readequada através da aplicação de princípios éticos de desenvolvimento e da adoção de medidas preventivas⁹³. O Comitê, portanto, tem como competência a avaliação e proposição de medidas na temática de cibersegurança no Brasil, a formulação de propostas para a prevenção de incidentes cibernéticos, o fomento à educação e diálogos sobre cibersegurança e a cooperação internacional dentro dessa seara⁹⁴.

No entanto, é importante pontuar que a minuta que previa a criação da PNCiber não abordava os principais instrumentos já existentes, como a PNSI e o E-Ciber, e se demonstrava omissa com relação a pontos vitais para a implementação de medidas de governança para a cibersegurança brasileira. Isso é um sintoma da atual realidade legislativa brasileira em cibersegurança, que se mostra numerosa e regada de legislações e decretos esparsos, mas não necessariamente orientativa, clara e objetiva⁹⁵.

Ou seja, isso mostra que a atual legislação ainda não é capaz de relacionar expressamente os conteúdos regulamentares entre si em busca de um objetivo comum⁹⁶, evidenciando a importância do advento da PNCiber, que trouxe consigo um novo norte de atuação rápida e coordenada entre todos os responsáveis, com viés orientativo à cibersegurança no Brasil, a partir de diretrizes e métodos de governança e administração de riscos⁹⁷. Certo é que ainda se mostra imaturo qualquer diagnóstico acerca da Política Nacional de Cibersegurança, tendo em vista sua recente publicação, mas desde logo é possível observar que ela busca atingir uma padronização de atuação no cenário brasileiro de cibersegurança, atribui responsabilidades a órgãos e entidades competentes e fomenta a educação social e as ações preventivas a incidentes cibernéticos.

91. Ibid..

92. PINHEIRO, Patrícia P.G. *Cibersegurança, Sociedade e Futuro*. Computação Brasil, [S. l.], p. 67-70, 1 jun. 2024.p. 68.

93. Ibid. p. 69.

94. Decreto n. 11.856, de 26 de dezembro de 2023. (2023). *Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança*. Brasília, DF.

95. GOLDONI, Luiz R. F.; RODRIGUES, K.F.; MEDEIROS, B.P. Qual é o futuro da governança de cibersegurança no Brasil. *Brasil contemporâneo*. São Paulo, v. 29., 2024. p. 11.

96. Ibid.

97. PINHEIRO, Patrícia P.G. *Cibersegurança, Sociedade e Futuro*. Computação Brasil, [S. l.], p. 67-70, 1 jun. 2024.p. 69-70.

Considerações Finais

A partir de todo exposto é possível compreender que não existe uma receita pronta a ser seguida no âmbito da cibersegurança e da proteção de dados que possa ser aplicada indiscriminadamente e que assegurará a existência de um cenário de plena segurança digital, mesmo porque, tendo em vista o constante desenvolvimento tecnológico, a avaliação e administração dos riscos digitais se torna uma prática quase que ininterrupta. Contudo, a atuação geral deverá se dar a partir da conscientização das camadas sociais sobre a necessidade de seguir preceitos básicos de segurança cibernética, saber identificar adequadamente o que é risco, como mitigá-los e quais fundamentos devem ser observados e mandamentos legislativos ao tratar e armazenar dados, para não incorrerem num cenário de alto risco, com mais vulnerabilidade às valiosas informações na sociedade atual.

Na última década um verdadeiro ecossistema vem se construindo visando regular as tecnologias e ações no meio digital no Brasil. Desde a promulgação do Marco Civil da Internet -que este ano completa sua primeira década de vigência-, à LGPD, que se comportou como um verdadeiro marco na proteção de dados nacionalmente, até a publicação dos Decretos na seara da cibersegurança conforme já mencionados ao longo do terceiro capítulo, que culminaram na publicação da PNCiber. Ou seja, medidas que buscam, grosso modo, padronizar procedimentos, conscientizar as esferas pública e privada sobre a necessidade de capacitação profissional, da importância da união de esforços de todos os envolvidos na temática e da urgência de adoção de medidas preventivas, além de trazer à sociedade civil a ideia de premente acultramento e educação acerca do uso da internet no dia a dia, inclusive com ações preventivas de segurança cibernética e proteção de seus dados, mas que devem ser levados à prática com foco na verdadeira proteção de direitos ao invés de uma mera adequação procedimental e regulamentar.

Para que cheguemos a um cenário mais confortável a nível de cibersegurança imprescindível é que o próprio público tenha a consciência que existe uma ameaça real e iminente, já que cabe a cada um de nós enquanto usuários, desenvolvedores ou administradores de sistemas a adoção de ações preventivas, das boas práticas, da atenção às possíveis vulnerabilidades e mecanismos de governança capazes de apoiar na análise, monitoramento e contingenciamento dos riscos existentes. Não é à toa que todo arcabouço regulamentar brasileiro mencionado ao longo deste trabalho contém previsão acerca da promoção da educação e da capacitação dos usuários. Além disso, evidente

a necessidade contínua do desenvolvimento de mecanismos jurídicos, já que contribuem ativamente na prevenção de incidentes de segurança digital e a preocupação com a real aplicação da análise de risco pelos responsáveis, ultrapassando a esfera de mera adequação regulamentar.

Hoje somos capazes de enxergar a cibersegurança como uma pauta internacional, que busca mitigar os riscos inerentes a sua utilização e, em decorrência da tecnologia, transpassam fronteiras e atingem uma gama de disciplinas com impactos sérios a nível econômico, político, jurídico e social na mitigação de direitos fundamentais. Assim, a cibersegurança é apenas uma das camadas da governança da internet que se preocupa com as normas e regras tecnológicas, políticas e legais, outrossim é um processo contínuo e multidisciplinar. Em resumo, as significativas mudanças ocasionadas pelo acentuado uso da internet no século XXI proporcionaram importantes transformações nas interações humanas e implicou na necessidade de adaptação do conceito de risco e da regulamentação mundial para a proteção dos dados dos usuários, garantia de respaldo em caso de incidentes, atribuição de responsáveis e de medidas a serem adotadas continuamente para a mitigação de riscos digitais capazes de ocasionar graves danos à sociedade civil e aos setores público e organizações privadas.

Inegável o elevado número de regulamentos brasileiros sobre cibersegurança e proteção de dados, constituindo um verdadeiro cenário regulatório amplo, mas sem muita interrelação e assertividade na proteção dos direitos dos titulares de dados. Neste sentido, a Política Nacional recentemente publicada visa unificar diretrizes e orientações, a fim de garantir aplicações de boas práticas e ações preventivas aos possíveis incidentes e proporcionar uma efetiva tutela de direitos fundamentais. Por fim, não podemos olvidar a necessidade de que a avaliação de riscos seja realizada de maneira fiel à proteção daqueles que são inerentemente mais vulneráveis, os titulares de dados, obstando recair numa distribuição desleal desses riscos para a sociedade, o que pode ocasionar desastres sociais e lesão de direitos básicos dos usuários.

Referências Bibliográficas

ALMEIDA, João Emílio de. Cibersegurança: da prevenção do risco à gestão de incidentes. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, Porto, ed. 43, p. 1-4, 30 set. 2021. DOI 10.17013/risti.43.1-4. Disponível em: <https://scielo.pt/pdf/rist/n43/1646-9895-rist-43-1.pdf>. Acesso em: 2 maio 2024.

BECK, Ulrich; SEBASTIÃO NASCIMENTO. *Sociedade de risco: rumo a uma outra modernidade*. São Paulo: Editora 34, 2011.

BELLI, Luca; FRANQUEIRA, Bruna; BAKONYI, Erica; CHEN, Larissa; COUTO, Natalia; CHANG, Sofia; HORA, Nina da; GASPAR, Walter B. *Cibersegurança: Uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano*. 1. ed. Rio de Janeiro: Rio de Janeiro: FGV Direito Rio, Ag. 2023. Disponível em: <https://diretorio.fgv.br/publicacao/ciberseguranca-uma-visao-sistematica-rumo-uma-proposta-de-marco-regulatorio-para-um-brasil>. Acesso em: 24 jun. 2024.

BITTAR, E. C. B. A Teoria do Direito, a Era Digital e o Pós-Humano: o novo estatuto do corpo sob um regime tecnológico e a emergência do Sujeito Pós-Humano de Direito. *Revista Direito e Práxis*, v. 10, n. 2, p. 933–961, jun. 2019.

BRAGA, Noelson Araújo. *CIBERSEGURANÇA E O DIREITO À PRIVACIDADE: Um Estudo sobre a construção cibernética no Brasil e União Europeia na ótica realista*. 2021. Monografia (Bacharel em Relações Internacionais)-UNIVERSIDADE DE BRASÍLIA INSTITUTO DE RELAÇÕES INTERNACIONAIS, [S. l.], 2021. Disponível em: https://bdm.unb.br/bitstream/10483/30829/3/2021_NoelsonAraujoBraga_tcc.pdf. Acesso em: 3 jul. 2024.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 2016. 496 p. Disponível em: planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 01 jun. 2024.

BRASIL. Lei 10.406, de 10 de janeiro de 2002. Institui o Código Civil Brasileiro. *Diário Oficial da União*. Brasília: Presidência da República. Disponível em: planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 05 jan. 2024.

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: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 07 jun. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*. Brasília: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 nov. 2023.

CRIMINOSOS vendem dados do CGU e Ministério da Saúde na dark web. [S. l.], 21 dez. 2021. Disponível em: <https://canaltech.com.br/seguranca/criminosos-vendem-dados-do-cgu-e-ministerio-da-saude-na-dark-web-204985/>. Acesso em: 27 jun. 2024.

Decreto n. 9.319, de 21 de março de 2018. (2018). *Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital*. Brasília, DF.

Decreto n. 10.222, de 5 de fevereiro de 2020. (2020). *Aprova a Estratégia Nacional de Segurança Cibernética*. Brasília, DF.

Decreto n. 10.046, de 30 de setembro de 2019. *Altera o Decreto nº 9.203, de 22 de novembro de 2017, que regulamenta a Lei nº 13.334, de 13 de setembro de 2016*. Diário Oficial da União, Brasília, 1º out. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10046.htm. Acesso em: 01 jun. 2024.

Decreto n. 10.641, de 2 de março de 2021. (2021). Altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília, DF.

Decreto n. 11.200, de 15 de setembro de 2022. (2022). *Aprova o Plano Nacional de Segurança de Infraestruturas Críticas*. Brasília, DF.

Decreto n. 11.856, de 26 de dezembro de 2023. (2023). *Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança*. Brasília, DF.

FICHTNER, Laura. What kind of cyber security? Theorising cyber security and mapping approaches. *Internet Policy Review*, Germany, v. 7, p. 1-19, 15 maio 2018. DOI 10.14763/2018.2.788. Disponível em: <https://policyreview.info/articles/analysis/what-kind-cyber-security-theorising-cyber-security-and-mapping-approaches>. Acesso em: 3 jun. 2024.

G1. STJ aciona PF para apurar possível ataque de hackers ao sistema do tribunal. *G1*, 4 nov. 2020. Disponível em: <https://g1.globo.com/politica/noticia/2020/11/04/stj-aciona-pf-para-apurar-possivel-ataque-de-hackers-ao-sistema-do-tribunal.ghtml>. Acesso em: 2 jul. 2024.

G1. O que são cookies na internet e como eles funcionam. *G1*, 09 jun. 2024. Disponível em: <https://g1.globo.com/tecnologia/noticia/2024/06/09/o-que-sao-cookies-na-internet-e-como-eles-funcionam.ghtml>. Acesso em: 24 jun. 2024.

GIDDENS, A.; PLÍNIO DENTZIEN. *Modernidade e identidade*. Rio De Janeiro, RJ: Jorge Zahar, 2002.

GOLDONI, L. R. F.; RODRIGUES, K. F.; MEDEIROS, B. P. Qual é o futuro da governança de cibersegurança no Brasil? *Cadernos Gestão Pública e Cidadania*, v. 29, p. e90972–e90972, 17 abr. 2024.

GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In *Temas atuais de proteção de dados*. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271.

LATTO, Nica. *O que é um vírus de computador?* [S. l.], 12 fev. 2020. Disponível em: <https://www.avast.com/pt-br/c-computer-virus#:~:text=Um%20v%C3%ADrus%20de%20computador%20%C3%A9,a%20outros%20arquivos%20ou%20documentos>. Acesso em: 17 jul. 2024.

LHUMANN, Niklas. *Risk: A sociological Theory*. 1. ed. Nova Iorque: [s. n.], 2017. Disponível em: https://www.researchgate.net/publication/345677301_Risk_A_Sociological_Theory. Acesso em: 8 jun. 2024.

LINKNACIONAL. *O que é spam?* Link Nacional, 20 out. 2023. Disponível em: <https://www.linknacional.com.br/blog/o-que-e-spam/>. Acesso em: 24 jun. 2024.

LORENZON, Laila Neves. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (lgpd e gdpr) e seus respectivos instrumentos de enforcement. *Revista do Programa de Direito da União Europeia*, [S. l.], p. 1-14, 15 mar. 2021.

LÓSSIO, Cláudio Joel Brito. *O compliance digital e a proteção de dados: preservando direitos na sociedade da informação*. Dissertação (Mestrado em Direito) - Universidade Autônoma de Lisboa

Luís de Camões, Lisboa, 2020. Disponível em: <https://repositorio.ual.pt/handle/11144/4621>. Acesso em: 10 jul. 2024.

LUCCA, Newton de. Dignidade da pessoa humana e os riscos eletrônicos. *Galileu - Revista de Direito e Economia*, [s. l.], v. 7, p. 283-312, jan. 2012. Disponível em: <https://journals.ual.pt/galileu/wp-content/uploads/2019/02/Galileu-XVII-1-2-2012-Miolo-FINAL.pdf>. Acesso em: 17 jul. 2024.

MARCON, Daniele Verza. *Seguro contra Riscos Cibernéticos: desafios para delimitar a garantia e promover a cibersegurança na era digital*. 2023. Dissertação (Mestra em Ciências Jurídicas e Sociais) - Universidade Federal do Rio Grande do Sul, [S. l.], 2023. Disponível em: <https://lume.ufrgs.br/handle/10183/267969>. Acesso em: 3 jul. 2024.

MENDES, Laura Schertel. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. *Panorama Setorial da Internet*, [S. l.], ano 11, n. 2, p. 1-20, jun. 2019. Disponível em: https://www.nic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano-xi_n_2_privacidade_e_dados_pessoais.pdf. Acesso em: jul. 2024.

PIMENTEL, José Eduardo de Souza. Introdução ao Direito Digital. *Revista Jurídica da Escola Superior do Ministério Público de São Paulo*, v. 13, n. 1, p. 16-39, 17 set. 2018.

PINHEIRO, Patricia Peck Garrido. CIBERSEGURANÇA, SOCIEDADE E FUTURO. *Computação Brasil*, [S. l.], p. 67-70, 1 jun. 2024.

Problemas no ConecteSUS: antes de ataque hacker, sistema teve polêmica com alteração de dados e falhas. Disponível em: <https://g1.globo.com/saude/noticia/2021/12/10/problemas-no-conecte-sus-antes-de-ataque-hacker-sistema-teve-polemica-com-alteracao-de-dados-e-falhas.ghtml>.

SAMPAIO, Dhiêgo Rhubens Lima. *UM ESTUDO SOBRE RISCOS DE SEGURANÇA DA INFORMAÇÃO NO CAMPUS DA UFC EM QUIXADÁ COM BASE NA NORMA ISO/IEC 27005*. 2014. Monografia (Bacharelado em Sistemas de Informação) - Universidade Federal do Ceará, Quixadá, CE, 2014. Disponível em: <https://repositorio.ufc.br/handle/riufc/25039>. Acesso em: 7 jun. 2024.

SHIRA, Fer; JANCZ, Carla. BARRICADAS ESTRATÉGIAS E COLETIVIDADE: Uma cartilha de segurança digital para organizações. *Marialab*, São Paulo, 1 dez. 2022. Disponível em: <https://www.marialab.org/wp-content/uploads/2020/12/Barricas-estrategias-coletividade.pdf>. Acesso em: 13 jul. 2024.

Tribunal de Contas da União. *Cinco controles de segurança cibernética para ontem* / Tribunal de Contas da União. - Brasília: TCU, 2022. 36 p. Disponível em: <https://portal.tcu.gov.br/5-controles-de-seguranca-cibernetica.htm>. Acesso em: 06 jul. 2024.

TEFFÉ, Chiara de. *Dados Pessoais Sensíveis: Qualificação, Tratamento e Boas Práticas*. Indaiatuba, SP: Foco, 2022. 304 p. Disponível em: https://www.google.com.br/books/edition/Dados_Pessoais_Sens%C3%ADveis/atCLEAAQBAJ?hl=ptBR&gbpv=1&dq=inauthor:%22Chiara+Spadacini+de+Teff%C3%A9%22&printsec=frontcover. Acesso em: 28 jun. 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

17

Ciberinfância e cibersegurança social: em busca de aprimoramento da proteção de crianças e adolescentes na internet

LÍGIA MARIA DE SOUZA LOPES REIS

Sumário: Introdução. 1. Quadro geral: contexto e dados. 2. Quadro regulatório. 2.1. Coleta de dados diferenciada. 2.2. Exposição excessiva. 3. Quadro futuro. 3.1. Cibersegurança digital e futuro regulatório. Considerações finais. Referências Bibliográficas

Introdução

Este artigo pretende analisar como o Brasil tem avançado na construção de um arcabouço regulatório que se proponha a proteger crianças e adolescentes em ambientes digitais, buscando lançar luz sobre possíveis contribuições normativas para o aprimoramento da cibersegurança social. A partir do estudo das Leis 12.965/2014 (Marco Civil da Internet) e 13.709/2018 (Lei Geral de Proteção de Dados), apresenta avanços, lacunas e impactos desses regramentos no uso das plataformas digitais por esses grupos. Além disso, busca compreender o PL brasileiro 2628/2022 e a proposta legislativa americana *Kids Online Safety Act (Kosa)*, analisando se realmente oferecem o aprimoramento pretendido tanto da proteção digital quanto da segurança cibernética. Assim, a discussão se estrutura em três partes: o cenário atual de crianças e adolescentes nas redes sociais, o impacto dessas plataformas nas vidas deles e propostas regulatórias voltadas para um futuro digital mais seguro.

1. Quadro geral: contexto e dados

Crianças e adolescentes brasileiros têm acessado a internet cada vez mais cedo. De acordo com a TIC Kids Online Brasil 2023², 24% das crianças e adolescentes do país relatam ter começado a usar a rede mundial de computadores ainda na primeira infância, ou seja, até os seis anos de vida³. Somase a esse outro achado alarmante. Estudo realizado pela Nielsen⁴, a pedido

1. Comunicóloga e mestre em Políticas Regulatórias de Comunicação pela Universidade de Brasília (UnB). Especialista em Relações Internacionais, pela UnB, e Administração Pública, pela Escola Nacional de Administração Pública (Enap). Servidora pública federal do Conselho Nacional do Ministério Público da União (CNMP) desde 2011, cedida para atuar no Supremo Tribunal Federal (STF). Atualmente cursa pós-graduação em Direito Digital (parceria entre Instituto de Tecnologia e Sociedade do Rio e Centro de Estudos e Pesquisas em Direito da Universidade do Estado do Rio de Janeiro) e graduação em Direito.

2. Realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), ligado ao Comitê Gestor da Internet no Brasil (CGI.br), desde 2012. Para edição de 2023, a pesquisa ouviu, presencialmente, 2.704 crianças e adolescentes com idades entre 9 e 17 anos, além de pais ou responsáveis, em todo o território nacional no ano de 2022.

3. NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br). Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2023 [livro eletrônico]. ed. São Paulo: Comitê Gestor da Internet do Brasil, 2024.

4. Empresa americana que realiza medição, coleta de dados e análises globais de audiência das mídias tradicionais e digitais para avaliar tendências e comportamentos.

do Google, revela baixa adesão de pais e responsáveis ao controle parental⁵ no Brasil, garantido no ordenamento regulatório pátrio desde a edição da Lei 12.965/2014. Em 2023⁶, apenas 17% dos adultos ouvidos na pesquisa conheciam e utilizavam meios tecnológicos de controle de acesso.

A navegação online sem supervisão, a baixa literacia e a parca conscientização desses usuários envolve inúmeros riscos, alguns deles já mapeados por especialistas, como coleta excessiva de dados, superexposição da imagem e estímulo ao consumo. Essas ações incidem sobre usuários sem as habilidades digitais necessárias, como conhecimento de direitos e ferramentas de segurança cibernética⁷, algo essencial para o uso consciente e defensivo das redes. Afinal, crianças e adolescentes são pessoas em formação e, por isso, que contam com proteção constitucional específica no Brasil, enunciada no artigo 227, da CRFB. Diz o texto:

É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, *além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão*⁸.

Na tentativa de enfrentar os efeitos causados pela aceleração das mudanças contemporâneas, o Poder Público tem editado regramentos voltados especificamente para o ambiente digital, como a Lei 12.965/2014, mais conhecida como Marco Civil da Internet (MCI) e a Lei 13.709/2018, batizada de Lei Geral de Proteção de Dados (LGPD), apenas para citar alguns⁹. Adiciona-se a essas medidas a atuação de órgãos públicos, como a Secretaria Nacional dos Direitos da Criança e do Adolescente, do Ministério dos Direitos Humanos e Cidadania, a Autoridade Nacional de Proteção de Dados (ANPD), que em 2023 editou enunciado para uniformizar a interpretação da LGPD quanto às hipóteses legais que autorizam o tratamento de dados de crianças e adolescentes. Apesar dos esforços, percebe-se inconsistências e paradoxos.

5. Controle parental é um mecanismo utilizado pelos adultos para controlar o acesso que as crianças podem ter a diferentes sites, sistemas operativos ou computadores. Por meio disso, é possível monitorar a navegação, restringir conteúdos impróprios para menores, bloquear páginas ou usuários que possam representar ameaça para as crianças.

6. Disponível em <https://bit.ly/3VRHPyr>

7. Segundo o glossário do Gartner, segurança cibernética ou cibersegurança é a combinação de pessoas, políticas, processos e tecnologias empregados por uma organização para proteger seus ativos cibernéticos contra ataques e ameaças digitais.

8. BRASIL. Constituição Federal, art. 227, *caput*.

9. Em janeiro de 2024, editou-se a Lei 14.811/2024 cuja finalidade é proteger crianças e adolescentes contra a violência, especialmente em ambientes educacionais ou similares. O normativo inclui medidas específicas que visam aumentar a segurança dos mais jovens em ambientes virtuais, na medida em que acrescenta novos dispositivos sobre crimes digitais contra esses grupos no Código Penal.

De acordo com o *Relatório Global Digital 2024*¹⁰, o Brasil ocupa a segunda posição no *ranking* de países com usuários acima de 16 anos que passam mais tempo online e o quinto lugar global no uso do Instagram. O comportamento dos mais velhos é reproduzido pelos mais novos: além de iniciarem a vida digital cada vez mais cedo, as crianças brasileiras com menos de 13 anos preferem o TikTok¹¹.

O achado surpreende, uma vez que essa rede social está classificada com 12+anos nas lojas que fornecem o aplicativo para *download*. E esse limite não é, de modo algum, um corte aleatório. De acordo com o Estatuto da Criança e do Adolescente (ECA), considera-se criança toda pessoa com até doze anos incompletos e adolescentes, e, dessa idade até os 18 anos completos, passa-se a considerá-la adolescente.

O uso de redes sociais por crianças e adolescentes teve um crescimento notável no Brasil nos últimos anos. Segundo o CGI, em 2021, 78% dos jovens de 9 a 17 anos que usaram a internet acessaram as redes sociais, o que representa um aumento de dez pontos percentuais em relação a 2019, quando se registrou 68%. A título comparativo, estudo realizado no Reino Unido, em 2021, pela Ofcom - acrônimo em inglês para *The Office of Communications*¹² -, indicou que 33% das crianças de 5 a 7 anos possuem perfis próprios nas redes sociais. Esse número sobe para 60% entre as crianças de 8 a 11 anos, 89% entre aquelas de 12 a 15 anos e 94% entre os adolescentes de 16 a 17 anos.

2. Quadro regulatório

Falar que a internet não é regulada no Brasil é uma inverdade e um desconhecimento. Fato é que diferentes normas se aplicam ao ambiente digital, como a LGPD e o MCI. A depender da matéria, outras normas podem alcançar o ambiente digital, como a que trata de direitos autorais. No caso dos direitos de crianças e adolescentes, um importante conjunto de regramentos pode ser invocado para protegê-las.

2.1 Coleta de dados diferenciada

O avançar do século XXI e das novas tecnologias de comunicação trouxe não somente mudanças para o fluxo da informação e a produção do conheci-

10. WE ARE SOCIAL. Digital 2024: 5 billion social media users. Íntegra do conteúdo em inglês em <https://bit.ly/3VRTYUf>.

11. De acordo com a *TIC Kids Online Brasil 2023*, essa é a rede social preferida de 46% dentre os respondentes que têm de 11 a 12 anos (CETIC.BR, 2023).

12. Trata-se da agência reguladora de comunicações do Reino Unido, cujo conteúdo citado encontra-se em <https://bit.ly/Ofcom2024>.

mento, mas também alterou o comportamento das pessoas, incluindo o das crianças.

Vivendo em um mundo cada vez mais digital, os mais jovens têm encontrado nas redes digitais, nos jogos online, nas plataformas de *streaming*, outras formas de se distrair, informar e divertir, diferentes daquelas buscadas por seus pais. Ainda de acordo com a *TIC Kids Online Brasil 2023*, 95% da população, de 9 a 17 anos, declarou ser usuária de internet no país, o que representa 25 milhões de pessoas. O principal meio para isso é o celular, de acordo com a resposta de 97% desses usuários¹³.

No que se refere à coleta de dados na internet, a Lei Geral de Proteção de Dados pode ser entendida como norma geral e transversal, que perpassa diferentes agentes de tratamento e afeta diversas categorias de titulares de dados, dentre os quais estão aqueles que necessitam de regulamentação e proteção especial - crianças e adolescentes. A combinação dos artigos 5º, inciso X e LXXIX, e 227, da CRFB, com o artigo 17, do ECA, fez nascer um capítulo da LGPD inteiramente destacado para tratar desses grupos.

A Lei 13.709/2018 determina que o tratamento de dados pessoais de crianças e de adolescentes seja realizado em seu melhor interesse (art. 14). Aqui o melhor interesse remete à reflexão sobre a vulnerabilidade e a necessidade de cuidado, por parte da família, sociedade e Estado, de crianças e adolescentes (art. 227, *caput*, da Constituição Federal de 1988, combinado com art. 4º do ECA). Essa lei geral estabelece também que o controlador¹⁴, na coleta de dados desses grupos, atuará

somente por meio de práticas que promovam e protejam seus direitos, previstos no sistema jurídico nacional e internacional, com absoluta prioridade, abstendo-se de práticas exploratórias da vulnerabilidade infantojuvenil, inclusive as comerciais¹⁵.

O melhor interesse deve ser respeitado no âmbito da proteção de dados pessoais, uma vez que essa garantia se refere aos direitos da personalidade. Desse modo, “o seu uso [coleta de dados] indiscriminado é capaz de objetificar pessoas, afetar o desenvolvimento da personalidade, promover a manipulação

13. NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br). Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2023 [livro eletrônico]. ed. São Paulo: Comitê Gestor da Internet do Brasil, 2024.

14. Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, conforme informa o art. 5º, inciso VI, da LGPD.

15. HENRIQUES, I.; PITA, M.; HARTUNG, P. Proteção de dados pessoais e a vulnerabilidade infantil. São Paulo: Editora ABC, 2022, p. 213.

e gerar discriminações”¹⁶. E, quando os riscos envolvem as fases primordiais do desenvolvimento humano,

a questão deve ser tratada considerando, também, a proteção jurídica especial que assiste a crianças e adolescentes, os quais, por força constitucional, devem ter seus direitos assegurados com absoluta prioridade¹⁷.

Impõe, ainda, a LGPD que o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal (art. 14, § 1º). A doutrina esclarece que o consentimento parental deverá se dar como manifestação livre, informada, inequívoca e também atender ao princípio da finalidade, conforme estabelece o art. 5º, XII, do ordenamento, “independentemente de ser realizado por mães, pais ou responsáveis legais”¹⁸.

Há apenas duas hipóteses de tratamento de dados pessoais de crianças e adolescentes sem o consentimento de pelo menos um dos pais ou pelo responsável legal: 1) quando a coleta for necessária para contatá-los, mas isso poderá ocorrer uma única vez e sem armazenamento; e 2) quando se tratar de proteger a vida da criança e do adolescente. Contudo, em nenhum caso os dados poderão ser repassados a terceiro sem o consentimento de algum dos responsáveis mencionados (art. 14, §3º).

Estabelece ainda aquela lei geral que o controlador possui o dever de realizar todos os esforços razoáveis para verificar que o consentimento tenha sido dado pelo responsável pela criança, consideradas as tecnologias disponíveis (art. 14, § 5º). Adicionalmente, esse agente de tratamento deverá manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício pleno dos direitos desses titulares (art. 14, § 2º), o que atende ao princípio da transparência e finalidade, uma vez que oferece a eles plena consciência sobre os procedimentos e os usos daquilo que lhes pertence, a saber, seus dados.

Como se trata de pessoas em formação, as informações sobre o tratamento de dados deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário. Devem ser usados recursos audiovisuais quando

16. MENDES, SARLET, RODRIGUES JR. Tratado de Proteção de Dados Pessoais. São Paulo: Ed. ABDR, 2023, p.211.

17. *Ibidem*, p.211.

18. *Ibidem*, p.214.

adequado, de modo a proporcionar a informação necessária aos pais ou ao responsável legal e adequado ao entendimento da criança (art. 14, §6º). Ademais, os controladores não deverão condicionar a participação de crianças e adolescentes em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais, além das estritamente necessárias à atividade (art. 14, §4º).

No que se refere aos direitos dos titulares, constantes do art. 18 da LGPD e que também alcançam esse público, destacam-se cinco dos nove incisos enunciados na norma: 1) confirmação da existência de tratamento para completa e inequívoca ciência de pelo menos um dos pais ou pelo responsável legal; 2) correção de dados incompletos, inexatos ou desatualizados, considerando especialmente o desenvolvimento do titular; 3) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD, posto o aspecto da transitoriedade da relação; 4) eliminação dos dados pessoais tratados com o consentimento do titular; e 5) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

O exercício desses direitos precisa estar alinhado aos princípios da LGPD, dentre os quais se enumera cinco dos dez presentes na lei, por considerá-los especialmente importantes no tratamento de dados de crianças e adolescente: 1) adequação, que é a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; 2) finalidade, que visa atender a propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; 3) necessidade, que se refere à limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; 4) transparência, ou seja, a garantia oferecidas 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; e 5) responsabilização e prestação de contas, referente a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Vale observar que a doutrina mais atual defende regras mais restritivas para a gestão de dados pessoais desses grupos.

Interpretações restritivas, que fazem a proteção de dados de crianças equivaler ao ‘consentimento para o tratamento de dados’,

desoneram Estados, empresas e outras organizações da responsabilidade pelo uso prejudicial de dados pessoais e violações de privacidade. Há um desequilíbrio de poder entre o esforço dos coletores de dados para capturar maiores quantidades de dados e a capacidade das famílias e crianças de se protegerem em um mundo digital cada vez mais complexo¹⁹.

2.2 Exposição excessiva

A exposição não controlada de crianças a redes sociais gera fenômenos e comportamentos que exigem reflexão. Um deles é o perfilamento de preferências, que, em poucas palavras, significa a oferta de conteúdos e produtos de acordo com a navegação do usuário na plataforma. Um outro é o risco de isolamento dessa pessoa ainda em formação em bolhas de discussão, o que pode contribuir para o agravamento da polarização social e política, redução da diversidade de opiniões²⁰, aumento da intolerância, disseminação de desinformação, dentre outros efeitos sociais.

Muito além de aperfeiçoar estratégias econômicas já existentes, como as classificações e perfilizações (*profiling*) e como o *targeting marketing*, os dados processados têm implicações que podem levar à total modificação do cenário econômico, social e político²¹.

A presença não assistida desses usuários, desprovida de instrumentos e competências educacionais de reflexão e crítica, pode significar a abertura de portas virtuais a criminosos. Já há registros de novos métodos, como “sequestro digital”, que é o ocorre quando alguém furta fotos de crianças da internet e as publica como se fossem de seus próprios filhos. Dez anos atrás, esses crimes ainda não haviam se tornado questões a serem resolvidas quando da edição do primeiro e principal instrumento legal voltado para a internet, o Marco Civil da Internet (MCI). E não que devesse tratar de crimes, posto que o MCI é regulamento para as relações civis, como se infere. Contudo, trata-se da primeira lei brasileira específica sobre internet e, como tal, poderia ter olhado mais atentamente para o futuro, o que passa necessariamente pela tutela e

19. Tradução livre de texto retirado do documento *The Case for Better Governance of Children's Data: A Manifesto*, publicado pelo Fundo das Nações Unidas para a Infância (UNICEF, 2021). Disponível em <https://bit.ly/3RQXpJG>.

20. Especialistas têm chamado atenção para os conteúdos gerados por inteligência artificial (IA) voltados para o público infantil, que circulam nas redes sociais e são distribuídos pelos algoritmos. São produtos considerados de baixa qualidade, de conteúdo e pedagógica, e que contêm vieses e pouca diversidade.

21. FRAZÃO, A. In: FERNANDES, E.; TEFFÉ, C. S. de; BRANCO, S. (Coords.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021, p.87.

proteção da vida e do desenvolvimento de crianças e adolescentes. Mas não é o que se vê no texto.

A Lei 12.965/2014 é a primeira legislação a estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil. É composta por 32 artigos e estruturada em cinco capítulos, mas não há um específico para tratar de crianças, como na LGPD. Contudo, o MCI buscou, de certa forma, contribuir para a criação de um ambiente digital mais seguro para crianças e adolescentes. Diz o artigo 26 que o cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.

O MCI pode ser usado também para proteger crianças e adolescentes em caso de episódios de violências sexuais flagrantes, como imagens íntimas ou cenas de nudez. E não em razão da literalidade da norma, mas em consequência da interpretação, uma vez que para esses casos aplica-se o ECA em conjunto com o artigo 21 do MCI²². A jurisprudência considera que qualquer divulgação de imagens de crianças e adolescentes em situações de nudez ou com conotação sexual constitui crime grave, conforme dispõe o artigo 241-A do ECA. Entende também que é responsabilidade do provedor de internet a retirada do conteúdo infringente, mesmo que produzido por terceiros. É o que se lê na jurisprudência do Superior Tribunal de Justiça (STJ)²³.

É responsável civilmente o provedor de aplicação que, após ser notificado, não retira conteúdo ofensivo que envolva menor de idade, independentemente de ordem judicial, pois o princípio de proteção integral à criança e adolescente prevalece sobre o Marco Civil da Internet²⁴.

Outro dispositivo que merece menção é o artigo 19, cuja análise de constitucionalidade aguarda julgamento, no âmbito do Recurso Extraordinário (RE)

22. Diz o texto que o provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

23. Ver Jurisprudência em Teses, Edição nº 224. Disponível em <https://bit.ly/3WdtlVO>. De forma completar, vale destacar que, segundo o STJ, a exposição pornográfica sem consentimento, enunciada no Marco Civil da Internet, não se limita a nudez total, nem a atos sexuais que somente envolvam conjunção carnal, mas a conduta que possa gerar dano à personalidade da vítima.

24. O texto faz referência aos seguintes dispositivos: artigo 19 da Lei 12.965/2014; artigos 17 e 18 do ECA; e artigos 5º, X, e 227 da Constituição Federal. Ver REsp 1.783.269/MG, disponível em <https://bit.ly/3xO7Pmr>

1.037.396 do Supremo Tribunal Federal (STF)²⁵. Enuncia o dispositivo que, para 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. Essa base legal trata a responsabilidade do provedor como subjetiva, avaliando-a por sua omissão quando não retira do ar o conteúdo ofensivo, após a devida notificação judicial. Vale lembrar que o STJ já declarou que “a responsabilidade dos provedores de aplicações da internet por conteúdo gerado por terceiro é subjetiva e torna-se solidária quando, após notificação judicial, a retirada do material ofensivo é negada ou retardada”²⁶.

No que se refere à proteção dos grupos aqui estudados e a literalidade textual, diz o MCI que o usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios do ECA (Lei 12.965/2014, art. 29). Considerando que apenas 17% de todos os pais ouvidos no já citado estudo da Nielsen²⁷ terem declarado conhecer e utilizar meios tecnológicos de controle de acesso como forma de tornar a experiência dos menores mais segura, esse dispositivo sozinho parece ser insuficiente para dar conta dos desafios impostos à infância e à juventude na realidade atual.

Por fim, observa-se que o termo “criança” aparece apenas duas vezes no MCI e ocorre já nas disposições finais -quase como se, finalmente, o legislador tivesse se lembrado de olhar para o amanhã. Segundo o texto, cabe ao poder público, em conjunto com os provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e fornecer informações sobre o uso dos programas de computador previstos no *caput* do artigo 29, bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes. Um texto tão principiológico quanto vago, como se vê.

25. Trata-se do RE 1.037.396, Tema 987 da repercussão geral, de relatoria do ministro Dias Toffoli, e discute se o artigo 19 do Marco Civil da Internet é constitucional ou não. Esse artigo exige que uma ordem judicial específica seja emitida antes que sites, provedores de internet e aplicativos de redes sociais sejam responsabilizados por conteúdos prejudiciais publicados por outras pessoas.

26. Ver Jurisprudência em Teses, Edição nº 222. Disponível em <https://bit.ly/3RUyDYR>

27. Ver comentário da nota de rodapé nº 3.

3. Quadro futuro

Como se viu, o Brasil possui normas para a proteção de crianças e adolescentes no ambiente digital, mas ainda são necessários avanços. A construção de um ambiente seguro depende de decisões individuais e coletivas que protejam tanto os grupos quanto as estruturas sociais. A partir dessa perspectiva, passa-se a tratar de inovações regulatórias.

3.1 Cibersegurança digital e futuro regulatório

Uma das conceituações mais consensuais sobre a cibersegurança foi elaborada pelo Setor de Normatização das Telecomunicações, da União Internacional de Telecomunicações da ONU, conhecido pelo acrônimo inglês ITU-T. Segundo a agência especializada da Organização das Nações Unidas (ONU), o termo se refere ao conjunto de ferramentas, políticas, conceitos de segurança, diretrizes, abordagens de gestão de risco, ações, treinamentos, melhores práticas, garantias e tecnologias que podem ser utilizadas para proteger os ativos do ambiente cibernético, da organização e dos usuários²⁸.

Assim, quando compreendida a partir dos aspectos técnicos, a cibersegurança se refere à proteção de computadores, redes e aplicações de softwares e sistemas operacionais de possíveis ameaças digitais. Contudo, quando interpretado a partir de outros campos, como a ciências sociais aplicadas²⁹, o termo pode incluir acepções que englobam medidas de defesa da soberania (inclusive digital) dos países, respeito aos direitos humanos fundamentais, impactos no bem-estar e na saúde mental das pessoas.

A cibersegurança social seria, então, um campo emergente que surge em resposta às ameaças digitais e aos desafios da segurança cibernética, com foco em

caracterizar, compreender e prever mudanças no comportamento humano e nos resultados sociais, culturais e políticos mediadas por ambientes cibernéticos; e construir uma infraestrutura de cibersegurança social que permita que o caráter essencial de uma sociedade persista em um ambiente de informação mediado por meios cibernéticos, caracterizado por condições mutáveis, ameaças de

28. Do glossário da UIT-T, disponível em <https://encurtador.com.br/uEcAn>

29. Sandra Friberg, professora de direito civil na *Uppsala University*, defende que a segurança cibernética não se trata apenas de uma questão técnica e lembra que o tema está destacado em diferentes pontos da legislação da UE, incluindo o novo Ato de Inteligência Artificial (*AI Act*) e outras diversas legislações ao redor do mundo. A pesquisadora observa que essas regulações visam criar medidas e defesas a ameaças cibernéticas que desafiam a soberania dos países e o respeito aos direitos humanos fundamentais. Por essa razão, ela crê ser necessária uma ampla colaboração entre especialistas técnicos, advogados e outros cientistas sociais para compreender o tema. Disponível em <https://encurtador.com.br/o6D0u>

cibersegurança social reais ou iminentes, e ameaças mediadas por meios cibernéticos³⁰.

Trata-se de um subdomínio emergente, da cibersegurança e da segurança nacional, que surge em resposta ao impacto crescente da influência cibernética nas sociedades atuais, em que crenças, opiniões, comportamentos e tendências são moldados, de forma significativa, pelas dinâmicas e interações digitais³¹. A partir disso, a cibersegurança social conta com objetivos voltados à antecipação de fenômenos, como 1) caracterizar, entender e prever mudanças, mediadas por tecnologias, no comportamento humano e nas dinâmicas sociais, culturais e políticas e 2) construir uma *infraestrutura cibernética social (grifou-se)* que permita à sociedade preservar seu caráter essencial em um ambiente de informações mediado tecnologias³².

Outra acepção considera a cibersegurança como um amplo campo de estudo que abrange outros, além de incluir dimensões essenciais, como supervisão e governança, pesquisa, operação e manutenção, proteção e defesa, dedicando-se também à proteção da vida, da propriedade e da segurança da informação, como defendem Aguilar e Fonseca³³.

Ao estudar os impactos tecnológicos no contexto escolar, os autores defendem uma compreensão e uma formação em cibersegurança mais ampla, focada no uso consciente e saudável da internet, especialmente na infância e adolescência.

Essa ampliação conceitual é o que permite a atuação didática, informada e coordenada de pais e mães, comunidade escolar e demais integrantes do contexto. Baseia-se em ensino e apropriação de diretrizes de uso e segurança das redes, definição de tempos de navegação na escola e no lar, regras de segurança e de prevenção à ações de engenharia social e combate à violência online, dentre outras medidas.

Os atores do processo podem trabalhar com diferentes tipos de conhecimento, tanto teóricos, científicos e tecnológicos, quanto

30. BESKOW, D. M.; CARLEY, K. M. Social cybersecurity: an emerging science. 2019, p.1. O texto original em inglês diz o seguinte: "As noted by the National Academies of Science NAS (2019): Social cybersecurity is an applied computational social science with two objectives - 'characterize, understand, and forecast cyber-mediated changes in human behavior and in social, cultural, and political outcomes; and build a social cyber infrastructure that will allow the essential character of a society to persist in a cyber-mediated information environment that is characterized by changing conditions, actual or imminent social cyber-threats, and cyber-mediated threats'".

31. *Idem*, p.3.

32. *Ibidem*.

33. ASTORGA-AGUILAR, C.; SCHMIDT-FONSECA, I. Peligros de las redes sociales: Cómo educar nuestros hijos e hijas en ciberseguridad. *Educare* [online], v. 23, n. 3, p. 339-362, 2019. Epub 30 out. 2019.

aqueles fornecidos pelos grupos participantes do processo e pela própria sociedade. Em relação à didática e ao conhecimento, é necessário que crianças e adolescentes adquiram conhecimento sobre cibersegurança aplicada às redes sociais, mas, principalmente, que se apropriem e interiorizem esse aprendizado, de modo que essa informação passe para suas estruturas cognitivas, a fim de identificar perigos na rede³⁴.

De acordo com o *The Global Risk Report 2024 - 19th edition*³⁵, o risco cibernético será a quarta maior ameaça aos países nos próximos dois anos e a oitava, nos próximos dez. No contexto da sociedade contemporânea e de seus problemas complexos, a perspectiva da cibersegurança social oferece, por exemplo, a possibilidade de se utilizar “técnicas de ciência social computacional para identificar, combater e medir (ou avaliar) o impacto dos objetivos de comunicação”³⁶, sendo possível inclusive valer-se dela para analisar e promover ambientes digitais mais seguros e saudáveis para crianças e adolescentes.

É por isso que governos em todo o mundo estão cada vez mais interessados no desenvolvimento de estratégias nacionais de cibersegurança (ENC), que sejam aptas e eficazes para o enfrentamento e a prevenção, integrada e eficiente, de uma ampla gama de questões ligadas ao tema. De acordo com a Organização dos Estados Americanos (OEA), a elaboração de uma ENC é fundamental para lidar com ameaças cibernéticas e construir medidas desejáveis para preveni-las³⁷. No Brasil, a estratégia nacional de cibersegurança, criada em 2020, passa por revisão e, no apagar das luzes de 2023, foi incorporada ao Plano Nacional de Cibersegurança (PNCiber), com a publicação do Decreto 11.856/2023.

Há ainda pesquisadores que relacionam a cibersegurança social à proteção de sistemas de informação e redes contra ataques de criminosos, cujas técnicas de engenharia social³⁸ exploraram as vulnerabilidades humanas. Assim, essa nova área de investigação responderia a efeitos cibernéticos da atua-

34. *Idem*. Tradução livre do texto original em espanhol: *Los actores del proceso pueden trabajar con distintos tipos de conocimiento, tanto los teóricos, científicos y tecnológicos, así como los que aportan los grupos participantes del proceso y la sociedad misma. En relación con la didáctica y el conocimiento, se requiere que la niñez y la adolescencia obtengan conocimiento sobre ciberseguridad aplicada a redes sociales, pero que principalmente se apropien e interioricen con el aprendizaje, de manera que dicha información pase a sus estructuras cognitivas con el fin de identificar peligros en la red.*

35. WORLD ECONOMIC FORUM. *The Global Risks Report 2024* [livro eletrônico]. Cologny/Geneva: World Economic Forum, 2024.

36. BESKOW, D. M.; CARLEY, K. M. Social cybersecurity: an emerging science. 2019, p.2. No original, diz o texto: “Social cybersecurity uses computational social science techniques to identify, counter, and measure (or assess) the impact of communication objectives”.

37. Ver proposta de programa de segurança cibernética da OEA em <https://www.oas.org/ext/en/security/prog-cyber>

38. A engenharia social refere-se às táticas utilizadas para manipular pessoas a fim de revelar informações confidenciais ou realizar ações que comprometam a segurança. Exemplos incluem phishing, pretexting e outras formas de engano que visam influenciar o comportamento humano. Mais informações em <https://bit.ly/3L8llh8>

lidade valendo-se de pesquisa aplicada e diferentes áreas do conhecimento, como comunicação, ciência de dados, direito, economia comportamental, estatística, dentre outras, a fim de analisar as novas tecnologias e responder aos fenômenos da internet.

A cibersegurança social pode também investigar como se dão as operações de influência e manipulação de crenças, comportamentos e confiança pública dentro das plataformas digitais, e como é possível defender os grupos sociais disso. Métodos e resultados advindos deste domínio de pesquisa podem ser críticos para formuladores de políticas públicas e acadêmicos, na medida em que seus componentes teóricos aplicados contam com o potencial de se constituir em análises de redes de alta dimensionalidade³⁹, aprendizado de máquina, processamento de linguagem natural e simulação baseada em agentes⁴⁰.

Nessa linha, Wu *et al.* definem a cibersegurança social como um campo que estuda comportamentos e ameaças de segurança e privacidade em um ecossistema de interconectividade e influência social, reconhecendo o domínio das interações sociais e buscando criar sistemas de segurança que sejam mais alinhados com as práticas e necessidades sociais dos usuários. Dentre outras questões, explicam que famílias e lares exibem práticas complexas quando o assunto é compartilhamento de conteúdo, incluindo o de seus filhos. E que as concepções sobre o que é sensível ou não variam entre as famílias, as quais também divergem sobre mecanismos de controle de acesso para combater violações que alcancem a sensibilidade de crianças e adolescentes⁴¹.

No entanto, os usuários frequentemente adaptam iterativamente suas políticas ideais de controle de acesso, em vez de se conformarem com as inicialmente relatadas, sugerindo que políticas de controle de acesso, *a priori*, podem ser insuficientes no contexto doméstico⁴².

39. Análises de redes de alta dimensionalidade são técnicas e métodos utilizados para estudar e compreender redes complexas que envolvem múltiplas dimensões ou atributos. Essas redes não se limitam a simples conexões entre nós (como em uma rede social comum), mas consideram diversas camadas de dados e tipos de interações, além de suas complexidades e dimensionalidades. Valem-se de modelos matemáticos e algoritmos e podem ser aplicados a redes sociais e segurança cibernética.

40. No campo da regulação das tecnologias emergentes, cita-se o caso do *AI Act* Europeu que menciona cibersegurança 45 vezes em seu texto. Em um dos trechos a autoridade europeia afirma que *Cybersecurity plays a crucial role in ensuring that AI systems are resilient against attempts to alter their use, behaviour, performance or compromise their security properties by malicious third parties exploiting the system's vulnerabilities*. Disponível em https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf

41. U, Y. W.; EDWARDS, K.; DAS, S. SoK: Social Cybersecurity. In: 2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022, p. 1863-1879, p. 4. Eis o texto no original, em inglês: *However, users often iteratively adapt their ideal access control policies rather than settle on the initial ones they reported, suggesting that a priori access control policies may be insufficient within the household context.*

42. *Idem.*

Os autores concluem que ignorar os comportamentos sociais humanos quando se projeta sistemas e regramentos pode levar a comportamentos inadequados e reduzir a segurança, ao passo que a projeção e o aproveitamento dos comportamentos sociais humanos nestes contextos pode significar incremento de eficácia e ação desses sistemas e normas regulatórias.

Sobre esse tema, tramita no Congresso Nacional o PL 2628/2022, de autoria do Senador Alessandro Vieira, que propõe medidas mais protetivas para crianças e adolescentes em ambientes digitais. Dentre as mudanças sugeridas, destacam-se a exigência que plataformas digitais adotem, por padrão, configurações rígidas para a coleta de dados; a determinação que os serviços de tecnologia direcionados a crianças e adolescentes ofereçam mecanismos de controle parental simples e eficazes; a proibição à prática das caixas de recompensa (*loot boxes*) em jogos eletrônicos e à publicidade infantil - que já é proibida pelo Código de Defesa do Consumidor, mas o texto restringe elementos de comunicação que possam induzir o consumo; a previsão de se criar mecanismos para denúncias e retirada de conteúdo que viole direitos de crianças e adolescentes, independentemente de ordem judicial. A proposta enfrenta críticas sobre a viabilidade técnica de medidas como a verificação de idade nas redes sociais e o monitoramento de conteúdos, além de possíveis interferências na autonomia familiar.

Um outro exemplo é a proposta legislativa norte-americana *Kids Online Safety Act (Kosa)*, inédita e histórica proposição que defende o aprimoramento da segurança online de crianças e adolescentes por meio da modificação do *design* das plataformas, algo bastante aderente à cibersegurança social. Propõe ainda a não utilização de sistemas de recomendação baseados em algoritmos e a criação de uma nova responsabilidade ou um dever de cuidado⁴³ para aplicativos e plataformas digitais, no que se refere especificamente aos conteúdos inadequados para menores.

Em tramitação há mais de dois anos no parlamento norteamericano, o projeto de lei se divide entre forças apoiadoras no Senado e significativa oposição de organizações de direitos humanos e grupos de defesa da liberdade na internet. As emendas feitas ao projeto buscaram apaziguar detratores, mas não foram consideradas suficientes. Os críticos entendem que a lei ainda apresen-

43. Expressão que se refere à obrigação legal das plataformas digitais de tomar medidas razoáveis para proteger os usuários de danos, assegurando que suas operações não causem prejuízos e que qualquer conteúdo ou comportamento prejudicial seja devidamente monitorado e gerenciado. Isso inclui a prevenção de abusos, a proteção da privacidade, a segurança contra a exploração e a promoção de um ambiente digital seguro. O “dever de cuidado” também está contemplado no PL 2628/2022, na medida em que prevê configuração mais protetiva por padrão, monitoramento infantil, criação de mecanismos para denúncias e retirada de conteúdo que viole direitos de crianças e adolescentes sem necessidade de ordem judicial, dentre outras coisas.

ta riscos de censura e restrições excessivas, especialmente para comunidades marginalizadas⁴⁴. Opositores como o *Center for Democracy and Technology* e a *Electronic Frontier Foundation* dizem temer que uma linguagem vaga do projeto possa levar a uma moderação excessiva de conteúdo e, conseqüentemente, prejudicar comunidades vulneráveis⁴⁵, como jovens LGBTQ+.

Dito isso, afirma-se que o *Kosa* pode ser considerado um instrumento de cibersegurança social, posto que aborda tanto a segurança técnica quanto os aspectos sociais e comportamentais da segurança online para crianças e adolescentes. Dentre outros objetivos alinhados à cibersegurança social para proteger as interações humanas no ambiente digital, o documento aborda, por exemplo: 1) a regulação de conteúdo e de design, como já se mencionou, com vistas a ajudar na criação de um ambiente online mais seguro, cujo potencial conteúdo nocivo seja menos provável de ser promovido; 2) a educação e a conscientização, na medida em que propõe a inclusão de orientações de um conselho diversificado de atores, incluindo pais, especialistas acadêmicos, profissionais de saúde e jovens usuários de mídia social, além de reconhecer a necessidade de equipar os usuários com o conhecimento e as ferramentas para navegar de forma segura no ambiente digital⁴⁶; e 3) a proteção contra a manipulação e a desinformação, a partir da implementação de mecanismos de segurança e da exigência de que redes sociais adotem medidas específicas para proteger jovens usuários.

Considerações finais

A crescente integração de crianças e adolescentes ao universo digital exige uma abordagem transdisciplinar, multifacetada e multidimensional, que englobe educação, regulamentação, tecnologia, segurança cibernética, e outras dimensões que possibilitem a pavimentação de caminhos orientados à proteção e às experiências digitais mais saudáveis e humanas. Isso exige reforçar o ambiente regulatório, com normas, políticas e planos específicos, que

44. “The Kids Online Safety Act, if passed, would require social media platforms to reduce online dangers by changing their design or opting out of algorithm based recommendation systems.[5] It aims to create liability or a “duty of care” for apps and social networking platforms for specific content that may not be suitable for minors. If the entities behind these Internet platforms fail to filter said content from minors, they might be open for legal action against them”. Disponível em <https://abre.ai/katO>

45. “Rather than protecting children, this could impact access to protected speech, causing a chilling effect for all users and incentivizing companies to filter content on topics that disproportionately impact marginalized communities,” said Prem M Trivedi, policy director at the Open Technology Institute, which opposes *Kosa*. Em “New text, same problems: inside the fight over child online safety laws”. Disponível em <https://abre.ai/katP>

46. Por oportuno, chama-se atenção para a semelhança da proposta com o art. 29, parágrafo único, do Marco Civil da Internet. Diz o texto que “[c]abe ao poder público, em conjunto com os provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e fornecer informações sobre o uso dos programas de computador previstos no caput, bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes”.

não apenas proíbam práticas prejudiciais específicas, como a coleta excessiva de seus dados e o perfilamento realizado por algoritmos, mas que também promovam uma cultura digital mais favorável ao desenvolvimento humano.

Diante disso, ainda que sujeitas a críticas, inovações regulatórias como as propostas no PL 2628/2022 e no *Kosa* podem ser vistas como instrumentos de cibersegurança social, porque buscam abordar as ameaças digitais para além das questões tecnológicas. Contudo, não se deve perder de vista que a eficácia normativa dependerá da capacidade de implementação e fiscalização. Normas regulatórias específicas podem, certamente, contribuir para o aprimoramento da proteção desses públicos no ambiente digital, mas certamente carecerão de medidas, protocolos e políticas que auxiliem no desenvolvimento de conexões e ecossistemas favoráveis à presença dos jovens.

Nessa linha, há de se destacar a importância da colaboração entre governos, educadores, pais e provedores de serviços digitais para criar um ambiente digital mais seguro e enriquecedor para crianças e adolescentes, algo enunciado pelo Marco Civil da Internet, mas ainda não efetivado na realidade brasileira. Enquanto a tecnologia continua a evoluir, também devem evoluir a compreensão, os meios e os instrumentos de proteção ao bem-estar das pessoas, especialmente as mais vulneráveis, como são crianças e adolescentes. Somente essa articulação entre aqueles agentes sociais poderá oferecer, tanto os mais jovens quanto suas famílias, a segurança e a confiança necessárias às vivências digitais.

Integrar a cibersegurança social ao debate sobre ciberinfância é fundamental, pois crianças e adolescentes são particularmente vulneráveis a conteúdos, influências, manifestações no ecossistema digital. Estão frequentemente expostos a algoritmos, desinformação, manipulações digitais, de modo que estratégias de proteção para esses grupos devem incluir não apenas medidas técnicas, mas também sociais e comportamentais, além de iniciativas de educação digital que abordem a natureza social das ameaças cibernéticas. Programas educativos que priorizem a alfabetização digital e fomentem a conscientização sobre os riscos tecnológicos podem alcançar, de forma positiva, outros desafios emergentes para além das redes digitais, como uso e aplicações da inteligência artificial.

Assim, observou-se que a cibersegurança social, embora seja um campo emergente de pesquisa, deve ser estudado e explorado de modo a formular e propor combinação de lentes, conceitos, abordagens métodos das ciências sociais aplicadas e da engenharia computacional para construir infraestruturas

e instrumentos sociais mais resilientes, conscientes e aderentes ao comportamento dos usuários. Como resultado, é possível proteger mais eficazmente a sociedade e seus grupos, bem como a manter suas dinâmicas e instituições livres (ou menos vulneráveis) de riscos tecnológicos.

Referências

ASTORGA-AGUILAR, C.; SCHMIDT-FONSECA, I. *Peligros de las redes sociales: Cómo educar nuestros hijos e hijas en ciberseguridad*. Educare [online], v. 23, n. 3, p. 339-362, 2019. Epub 30 out. 2019. Disponível em: <https://bit.ly/PeligrosRedes2019>. Acesso em: jun. 2024.

BRASIL. *Constituição Federal*. Disponível em: <https://l1nk.dev/Qzkdl>. Acesso em: jun. 2024.

_____. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: jun. 2024.

_____. *Lei nº 8.098, de 11 de setembro de 1990*. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: jul. 2024.

_____. *Decreto nº 7.962, de 15 de março de 2013*. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm. Acesso em: jul. 2024.

_____. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: jul. 2024.

_____. *Lei nº 13.257, de 8 de março de 2016*. Marco Legal da Primeira Infância. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13257.htm. Acesso em: mai. 2024.

_____. *PL 2628/2022*. Proteção de crianças e adolescentes em ambientes digitais. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/154901>. Acesso em: jul. 2024.

_____. *PL 2630/2020*. Lei das Fake News. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/141944>. Acesso em: jul. 2024.

_____. *SUPERIOR TRIBUNAL DE JUSTIÇA*. Jurisprudência em Teses, Edição nº 222. Disponível em: https://scon.stj.jus.br/SCON/jt/doc.jsp?livre=%27222%27.tit.&_gl=1%2a1tyc6aj%2a_ga%2aMTU2MzYxNzg0OS4xNjQ2MzQ5MDAy%2a_ga_F31N0L6Z6D%2aMTY5NjQ1NTI4OS-40MTguMS4xNjk2NDU4NjUyLjYwLjAuMA. Acesso em: jun. 2024.

_____. *SUPERIOR TRIBUNAL DE JUSTIÇA*. Jurisprudência em Teses, Edição nº 224. Disponível em: <https://scon.stj.jus.br/SCON/jt/doc.jsp?livre=%27224%27.tit>. Acesso em: jun. 2024.

ALANA, Instituto. *Programa Criança e Consumo*. Disponível em: <https://criancaeconsumo.org.br/>. Acesso em: jun. 2024.

----- . *Sobre o Instituto Alana*. Disponível em: <https://alana.org.br/>.

ANGELINE, K.; BARBOSA, A.; SENNE, F.; DINO, L. A. *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. Disponível em: <https://d26k070p771odc.cloudfront.net/wp-content/uploads/2021/10/Privacidade-e-Protecao-de-Dados-de-Crian%C3%A7as-e-Adolescentes-ITS.pdf>. Acesso em: mai. 2024.

BELLI, L.; COUTO, N.; CHEN, L.; FRANQUEIRA, B.; BAKONYI, E.; CHANG, S.; DA HORA, N.; GASPAR, W. *Cibersegurança [recurso eletrônico]: uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano*. Rio de Janeiro: FGV, Direito Rio, 2023.

BESKOW, D. M.; CARLEY, K. M. *Social cybersecurity: an emerging science*. 2019. Disponível em: <https://apps.dtic.mil/sti/citations/AD1108494>. Acesso em: jun. 2024.

FGV, Fundação Getúlio Vargas. *Guia de Tratamento de Dados de Crianças e Adolescentes*. Disponível em: https://portal.fgv.br/sites/portal.fgv.br/files/criancas_e_adolescentes.pdf. Acesso em: [falta data de acesso].

FRAZÃO, A. In: FERNANDES, E.; TEFFÉ, C. S. de; BRANCO, S. (Coords.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. Disponível em: <https://bit.ly/3xGBo9v>.

HENRIQUES, I.; PITA, M.; HARTUNG, P. *Tratado de Proteção de Dados Pessoais*. São Paulo: Ed. ABDR, 2023.

LATERÇA, P. S.; FERNANDES, E.; TEFFÉ, C. S. de; BRANCO, S. (Coords.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. Disponível em: <https://d26k070p771odc.cloudfront.net/wp-content/uploads/2021/10/Privacidade-e-Protecao-de-Dados-de-Crian%C3%A7as-e-Adolescentes-ITS.pdf>.

MEIO & MENSAGEM. *Apenas 17% dos pais usam ferramentas para monitorar filhos na internet*. Disponível em: <https://www.meioemensagem.com.br/midia/apenas-17-dos-pais-usam-ferramentas-para-monitorar-filhos-na-internet>. Acesso em: mai. 2024.

NIELSEN. *Medição, coleta de dados e análises globais de audiência das mídias tradicionais e digitais para avaliar tendências e comportamentos*. Disponível em: <https://www.tiktok.com/business/pt-BR/blog/tiktok-funciona-meta-analise-nielsen>. Acesso em: mai. 2024.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br). *Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2023 [livro eletrônico] = Survey on Internet use by children in Brazil: ICT Kids Online Brazil 2023*. 1. ed. São Paulo: Comitê Gestor da Internet do Brasil, 2024. Disponível em: <https://bit.ly/TicKids2023>. Acesso em: jun. 2024.

PRINSKY, M. *Nativos Digitais*. Disponível em: https://pt.wikipedia.org/wiki/Nativo_digital. Acesso em: mai. 2024.

SOUZA, J.; NOVELLI, A.; CASTRO, J. *Quadro regulatório de enfrentamento às fake news no Brasil: uma análise das propostas legislativas*. Revista Ibero-Americana de Informação. Disponível em: <https://periodicos.unb.br/index.php/RICI/article/view/45659/35275>. Acesso em: mai. 2024.

TIKTOK. *Diretrizes da Comunidade*. Disponível em: <https://www.tiktok.com/creators/creator-portal/pt-br/community-guidelines-and-safety-pt-br/diretrizes-da-comunidade/>. Acesso em: mai. 2024.

UNICEF. *The Pulse Check on Digital Learning*. Disponível em: <https://www.unicef.org/media/132096/file/Pulse%20Check.pdf>. Acesso em: jun. 2024.

WORLD ECONOMIC FORUM. *The Global Risks Report 2024 [livro eletrônico]*. Cologny/Geneva: World Economic Forum, 2024. Disponível em: <https://www.weforum.org/publications/global-risks-report-2024/>. Acesso em: jul. 2024.

WU, Y. W.; EDWARDS, K.; DAS, S. *SoK: Social Cybersecurity*. In: 2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022, p. 1863-1879. Disponível em: <https://ieeexplore.ieee.org/abstract/document/9833757>. Acesso em: jul. 2024.

UNICEF. *The Case for Better Governance of Children's Data: A Manifesto*. Disponível em: <https://encurtador.com.br/mD60s>. Acesso em: jun. 2024.

WE ARE SOCIAL. *Digital 2024: 5 billion social media users*. Disponível em: <https://wearesocial.com/uk/blog/2024/01/digital-2024-5-billion-social-media-users/>. Acesso em: jun. 2024.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

18

**As bases legais no sistema
de coleta de informação
sobre a diversidade na Saúde
e na Saúde Digital**

MAÍRA LIMA DE SOUZA

Sumário: Introdução. 1. Os Sistemas de Informação em Saúde e a Saúde Digital. 2. As informações de diversidade. 2.1. A trajetória da diversidade como informação social. 3. Metodologia. 4. As bases legais e a incorporação da diversidade nos Sistemas em Saúde. 4.1. A trajetória da diversidade como informação social. 4.2. Etnia. 4.3. Lésbicas, Gays, Bissexuais, Travestis e Transexuais (LGBT). Considerações finais. Referências.

Introdução

O artigo aborda como as bases legais adotadas pelo governo brasileiro influenciam a coleta de informações sobre diversidade nos registros eletrônicos de saúde gerados pelos principais Sistemas de Informação (SIS) nacionais e como essa influência repercute na qualidade da informação no contexto da Saúde Digital. Além de influenciar a coleta, esses marcos legais também impactam o reconhecimento oficial de determinadas categorias sociais.

Informações sobre diversidade retratam a composição de uma população em relação a categorias como etnia/identidade racial, gênero, orientação sexual e migração/nacionalidade, entre outras. A palavra “diversidade” tem sido utilizada como um termo guarda-chuva, abrangente o suficiente para incluir minorias e populações vulneráveis, bem como para reconhecer as diferenças humanas².

Os dados de diversidade podem ser categorizados como culturais (por exemplo, normas compartilhadas e comportamentos), biológicos (por exemplo, idade, sexo) e definidos em termos pessoais (por exemplo, orientação sexual, religião)³.

Os sistemas de informação em saúde, por meio de formulários ou fichas de cadastro, recolhem essas informações. Contudo, esse registro não segue

1. Doutora em Difusão do Conhecimento (UFBA), mestre em Estudos Étnicos e Africanos (UFBA), graduada em Ciência da Computação (UNIFACS) e certificada em Privacidade e Proteção de Dados pela Data Privacy Brasil (2024). Atuo no campo da ciência, tecnologia e humanidades, trabalhando com os temas: política, governança e gestão de dados e decolonialidade. Sou também membro do grupo de pesquisa sobre Ciência e Teoria das Redes, intitulado *Fuxicos & Boatos* (<http://redesso-ciaisecomplexas.org>). Sou Curadora de Dados Sênior (*data steward*), com foco no tratamento de dados sensíveis e diversidade, e lidero o Núcleo de Curadoria de Dados do Centro de Integração de Dados e Conhecimentos para Saúde (Cidacs/Fiocruz BA), o centro com maior acervo de dados administrativos governamentais entre todos os países de baixa e média renda no mundo, vinculado à Fundação Oswaldo Cruz Bahia. Minha atuação abrange desde a supervisão de uma equipe multidisciplinar de curadores, o desenvolvimento de políticas e modelos sociotécnicos de curadoria de dados para projetos de saúde pública, até a curadoria de projetos de pesquisa em conformidade com a LGPD, definindo medidas que garantem o uso seguro de dados, de acordo com a ética e a legislação.

2. BALESTRA, C.; FLEISCHER, L. *Diversity statistics in the OECD: how do OECD countries collect data on ethnic, racial and indigenous identity?*. OECD Statistics Working Papers, No. 2018/09, Paris: OECD Publishing, 2018. Disponível em: <https://doi.org/10.1787/89bae654-en>. Acesso em: 21 abr. 2023.P.6.

3. BALESTRA, C.; FLEISCHER, L. *Diversity statistics in the OECD: how do OECD countries collect data on ethnic, racial and indigenous identity?*. OECD Statistics Working Papers, No. 2018/09, Paris: OECD Publishing, 2018. Disponível em: <https://doi.org/10.1787/89bae654-en>. Acesso em: 21 abr. 2023.P.7.

uma trajetória linear ou uniforme. Embora a definição dos campos presentes nesses formulários seja decisiva para a coleta, a ligação desses campos com o processo identitário torna esse processo mais complexo.

Os sistemas de informação em saúde têm funcionado como instrumentos para a produção de dados brutos destinados à construção de indicadores estatísticos sobre a população. Exemplos incluem o Sistema de Informações sobre Mortalidade (SIM), o Sistema de Informações sobre Nascidos Vivos (SINASC) e o Sistema de Informação de Agravos de Notificação (SINAN). Esses sistemas são os mais representativos e figuram entre os mais antigos no contexto do Sistema Único de Saúde (SUS)⁴⁻⁵.

Individualmente, esses sistemas permitem o mapeamento de aspectos como mortalidade, nascimento e doenças em um determinado contexto. Quando combinados, capturam informações abrangentes sobre a trajetória de vida, desde o nascimento, passando pelo acometimento de doenças até a morte. No escopo da Saúde Digital, os SIS podem participar das estratégias de interoperabilidade e modernização, como a prevista no Programa e-SUS Linha da Vida⁶. No âmbito do e-Saúde, alimentam os portais de transparência ativa⁷.

Assim como os SIS não atendem a todo o sistema de assistência, uma vez que foram concebidos para finalidades específicas de atenção à saúde⁸, as bases legais que delimitam a alimentação desses sistemas também podem isolar a coleta de algumas informações de diversidade, não garantindo a presença delas em todos os sistemas. Não há um arcabouço legal que padronize a coleta dessas informações; grande parte das formulações são decretos e portarias.

O registro de informações sobre raça/cor tornou-se obrigatório em todos os sistemas de informação em saúde do Brasil devido à Portaria nº 344/MS, de 1º de fevereiro de 2017, embora vigorasse como um atributo de reconhecimento individual desde a Portaria GM/MS nº 3.947, de 25 de novembro de 1998, que a colocava entre os atributos a serem adotados pelos sistemas de saúde

4. COELHO NETO, G. C. ; CHIORO, A. Afinal, quantos Sistemas de Informação em Saúde de base nacional existem no Brasil? *Cadernos de Saúde Pública*, v. 37, n. 7, p. e00182119, 2021. Disponível em: <https://www.scielo.br/j/csp/a/RzNmVjHqmLhPHZp-6gfcDC6H/?format=pdf&lang=pt>. Acesso em: 29 abr. 2024.

5. BRASIL. Ministério da Saúde. *A experiência brasileira em sistemas de informação em saúde*. Brasília: Editora do Ministério da Saúde, 2009. (Série B. Textos Básicos de Saúde, v. 1 - Produção e disseminação de informações sobre saúde no Brasil).

6. BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. Departamento de Articulação Estratégica de Vigilância em Saúde. *Guia de Vigilância em Saúde* [recurso eletrônico] / Ministério da Saúde, Secretaria de Vigilância em Saúde. Departamento de Articulação Estratégica de Vigilância em Saúde. - 5. ed. rev. e atual. Brasília: Ministério da Saúde, 2022. 1.126 p.

7. BRASIL. Ministério da Saúde. *Sistemas de informação da atenção à saúde: contextos históricos, avanços e perspectivas no SUS*. Brasília, DF: Cidade Gráfica e Editora LTDA, out. 2015.

8. BRASIL. Ministério da Saúde. *Sistemas de informação da atenção à saúde: contextos históricos, avanços e perspectivas no SUS*. Brasília, DF: Cidade Gráfica e Editora LTDA, out. 2015.

existentes à época⁹. Ressalta-se que, como participante indireta da obrigatoriedade de coleta definida pela Portaria 344/MS, a etnia se mescla com a coleta de raça/cor por estar entre as categorias definidas pelo Instituto Brasileiro de Geografia e Estatística (IBGE), padrão de classificação adotado. Nesse sentido, a marcação da etnia também pode ser vinculada à classificação das populações quilombolas, tratadas como grupos étnico-raciais.

A informação sobre orientação sexual e identidade de gênero é encontrada no Sistema de Informação de Agravos de Notificação (SINAN) desde 2014, especificamente e apenas quando há a notificação de violência, seja ela interpessoal ou autoprovocada¹⁰. Nota-se que essas informações estão relacionadas à legislação de registro de violência no Brasil, visando a defesa e garantia de direitos¹¹.

Embora existam políticas nacionais de saúde para a população Negra, Lésbicas, Gays, Bissexuais, Travestis e Transexuais (LGBT) e para os Povos Indígenas, além de legislações que favoreçam o acesso de migrantes à saúde e a própria Constituição Federal de 1988, que assegura o direito à saúde para todos em território brasileiro, os sistemas de saúde enfrentam limitações na captação das informações sobre a diversidade.

Parte-se da hipótese de que as bases legais que regem a coleta de informações sobre a diversidade advêm do campo que marca a trajetória social de determinada categoria e que esse marco legal, em algum momento, se conecta com a saúde. Tendo como objetivo principal reunir as normas jurídicas nacionais que influenciam direta e indiretamente a coleta de informações sobre diversidade na saúde, o artigo baseia-se em uma pesquisa documental feita em publicações técnicas disponibilizadas pelas agências oficiais nacionais. O material selecionado buscou responder à seguinte questão: quais são as normas nacionais que impactam ou impactaram a coleta de informações sobre diversidade nos sistemas de informação em saúde?

O trabalho começa apresentando uma breve visão sobre os Sistemas de Informação em Saúde e a Saúde Digital. Em seguida, aborda as informações de

9. BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. Departamento de Análise de Situação de Saúde. *Legislação Relativa aos Sistemas de Informações sobre Mortalidade (SIM) e sobre Nascidos Vivos (SINASC)*. Brasília: Ministério da Saúde, 2004.

10. OLIVEIRA, D.C. Representatividade da população LGBTQIA+ nas pesquisas epidemiológicas, no contexto da Política Nacional de Saúde Integral de Lésbicas, Gays, Bissexuais, Travestis e Transexuais: ampliar a produção de conhecimento no SUS para a justiça social. *Epidemiologia e Serviços de Saúde*, v. 31, n. 1, e2022020, 2022.

11. LEAL, C. H. S. ; SCALCO, M. L. A. ; NUNES, R. P. D. ; CONSORTII, E. R. ; KITAGAWA, B. Y. Vigilância de violências: considerações sobre as informações relativas às violências perpetradas contra a população LGBT no município de São Paulo. *Bis*, São Paulo, v. 2, n. 19, p. 55-61, dez. 2018. Disponível em: <https://docs.bvsalud.org/biblioref/2019/09/1016509/bis-v19n2-diversidade-55-61.pdf>. Acesso em: 19 abr. 2024.

diversidade e sua trajetória no campo da informação social. Por fim, apresenta um panorama das bases legais que regulam o uso dessas informações na saúde e como elas estão incorporadas nos sistemas de saúde. O artigo aborda a trajetória da coleta de informações sobre raça/cor/etnia e da população de Lésbicas, Gays, Bissexuais e Transexuais (LGBT).

1. Os Sistemas de Informação em Saúde e a Saúde Digital

Os registros eletrônicos de saúde são gerados como parte das transações normais do negócio estatal e contêm informações de indivíduos que acessam o serviço público, caracterizando tanto fatos individuais quanto coletivos. Utilizados como instrumentos da administração pública e criados para fins operacionais, esses dados, de abrangência nacional, passaram a ser utilizados para gerar informações públicas e estatísticas.

Esses registros, na forma como os conhecemos hoje, advêm da evolução do processo de sistematização dos serviços públicos do governo e das suas informações, marcado pelo desenvolvimento de ferramentas e métodos. Destacam-se nesse processo a incorporação da estatística como elemento do governo científico e a digitalização¹². O primeiro reforçou o apelo pela organização e sistematização da informação, condição necessária para prover estatísticas nacionais. O segundo, inserido no escopo das ações de racionalização administrativa ocorridas na década de 1990, enfatizou uma administração pública gerencial e fez uso da Tecnologia da Informação e Comunicação (TIC) como instrumento para o governo eletrônico. Essa iniciativa se fortaleceu diante da associação discursiva que aproxima a informação (e, conseqüentemente, as TICs) da governança e do desenvolvimento¹³⁻¹⁴. Na época, com o neoliberalismo como pano de fundo, era importante que os países em desenvolvimento tivessem uma “boa governança da gestão pública” a fim de assegurar benefícios financeiros internacionais¹⁵.

O potencial de gerar estatísticas e complementar o conhecimento produzido sobre a população a que esses registros se referem tem expandido

12. BRASIL. Ministério da Saúde. *A experiência brasileira em sistemas de informação em saúde*. Brasília: Editora do Ministério da Saúde, 2009. (Série B. Textos Básicos de Saúde, v. 1 - Produção e disseminação de informações sobre saúde no Brasil).

13. WORLD BANK. *Managing development: the governance dimension*. Washington, D.C.: World Bank Group, 1991. Disponível em: <http://documents.worldbank.org/curated/en/884111468134710535/Managing-development-the-governance-dimension>. Acesso em: 14 fev. 2024.

14. PANZARDI, R.; CALCOPIETRO, C.; IVANOVIC, E. F. *New-economy sector study: electronic government and governance - lessons from Argentina*. Working paper. Washington, DC: World Bank, jul. 2002. Disponível em: <https://documentos.bancomundial.org/es/publication/documents-reports/documentdetail/527061468769894044/new-economy-sector-study-electronic-government-and-governance-lessons-from-argentina>. Acesso em: 14 fev. 2024.

15. WORLD BANK. *Managing development: the governance dimension*. Washington, D.C.: World Bank Group, 1991. Disponível em: <http://documents.worldbank.org/curated/en/884111468134710535/Managing-development-the-governance-dimension>. Acesso em: 14 fev. 2024.

sua adesão entre pesquisadores, governos e agências de estatística¹⁶¹⁷¹⁸. Isso ocorre porque a coleta contínua dessas informações ao longo do tempo favorece análises longitudinais, possibilitando abordagens populacionais.

No que diz respeito aos registros administrativos de saúde, o Brasil tem investido, nos últimos anos, em ações de transparência ativa com o intuito de ampliar seu posicionamento na abertura de dados, estimulando a utilização e reutilização desses registros (desidentificados) como dados secundários para fins de investigação e políticas¹⁹. No ambiente nacional, repercute a percepção, trazida do Reino Unido, de que esses registros são um recurso inestimável para o bem público comum²⁰. Esse valor se amplia diante da possibilidade de interligação entre esses registros.

O escopo de monitoramento com vistas à produção de conhecimento relevante para a sociedade pode ser ampliado por ações como:

- a) Linkage entre bases de dados (*Data Linkage*). A aplicação dessa técnica estatística, que pode ser executada por métodos probabilístico e determinístico²¹, possibilita a vinculação de dados de distintas fontes a partir de registros comuns e se difunde como estratégia de vigilância²²⁻²³.
- b) Interoperabilidade. A capacidade de interligação e comunicação entre sistemas de informação de diferentes tecnologias. Essa estratégia incorpora-se à Política Nacional de Informação e Informática em Saúde (PNIIS)²⁴, de 2003, que advoga pela organização do Sistema Nacional de Informa-

16. SENRA, N. de C. A questão dos registros administrativos vis-à-vis a geração de estatísticas. *Revista Brasileira de Estudos de População*, [S. l.], v. 13, n. 2, p. 199–205, 1996. Disponível em: <https://rebep.org.br/revista/article/view/437>. Acesso em: 23 jul. 2024.

17. FERREIRA, F. P. M. Registros administrativos como fonte de dados estatísticos. *Informática Pública*, ano 10, n. 1, p. 81-93, 2008.

18. MELLO, Janine. Produção estatal de evidências e uso de registros administrativos em políticas públicas. In: KOGA, Natália Massaco (Org.) et al. *Políticas públicas e o uso de evidências no Brasil: conceitos, métodos, contextos e práticas*. Brasília: IPEA, 2022. p. 897-914.

19. BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde e Ambiente. Departamento de Análise Epidemiológica e Vigilância de Doenças não Transmissíveis. *Dados para Vigilância: perfis das bases de dados produzidas pela Vigilância em Saúde no Brasil*. Brasília: Ministério da Saúde, 2023. 127 p.: il.

20. ADMINISTRATIVE DATA RESEARCH UK. *Administrative data is an invaluable resource for public good*. Let's use it. Annual Report 2018–19. 2019.

21. COELI, Cláudia Medina. Ciência de dados populacionais. *Epidemiologia e serviços de saúde: revista do Sistema Único de Saúde do Brasil*, v. 31, n. 3, e2022119, 19 dez. 2022. doi:10.1590/S2237-96222022000300001.

22. BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. Departamento de Articulação Estratégica de Vigilância em Saúde. *Guia de Vigilância em Saúde* [recurso eletrônico] / Ministério da Saúde, Secretaria de Vigilância em Saúde. Departamento de Articulação Estratégica de Vigilância em Saúde. – 5. ed. rev. e atual. Brasília: Ministério da Saúde, 2022. 1.126 p.

23. BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. *Nota Técnica nº 34/2023: atualizações e recomendações para a vigilância de anomalias congênitas no Brasil*. Brasília, DF, 2023. Disponível em: <http://plataforma.saude.gov.br/anomalias-congenitas/nota-tecnica-34-2023.pdf>. Acesso em: 8 mar. 2024.

24. BRASIL. Ministério da Saúde. Secretaria Executiva. Departamento de Informática do SUS. *Política Nacional de Informação e Informática em Saúde: Proposta Versão 2.0* (Inclui deliberações da 12ª Conferência Nacional de Saúde). 2004. Disponível em: http://bvsmis.saude.gov.br/bvs/publicacoes/PoliticaInformacaoSaude29_03_2004.pdf. Acesso em: 1 ago. 2024.

ção em Saúde (SNIS) e sua adequação às diretrizes do Programa de Governo Eletrônico Brasileiro (e-Gov) e à estratégia do e-Saúde²⁵⁻²⁶.

Ambas as estratégias de integração envolvem ações de padronização da informação, com a criação de modelos de dados, e da tecnologia, com a definição de infraestrutura e padrões de conexão.

Um levantamento identificou que, entre 2010 e 2018, havia 54 sistemas de informação de saúde de abrangência nacional. Conforme o propósito de funcionamento, esses sistemas se organizam para fins de vigilância de eventos relevantes à saúde pública, controle e monitoramento de programas de saúde do Ministério da Saúde, cadastramento dos usuários da assistência (população, profissionais e serviços de saúde) e apoio à gestão eletrônica de políticas, processos e serviços. Os sistemas classificados nessa categoria apresentam características horizontais e visam à racionalização administrativa do SUS²⁷.

Os principais problemas identificados nesses sistemas estão principalmente ligados à sua fragmentação, reflexo da estrutura tripartite de administração da saúde, que envolve estados e municípios na gestão dos sistemas, e da especialização técnica, que cria um sistema para cada nova necessidade. Como consequência, os sistemas produzem a mesma informação, mas são orientados por métodos e regras de coleta distintos²⁸. Além disso, as mudanças nas versões dos sistemas para fins de modernização e melhoria podem levar à inconsistência das informações, devido à perda ou descontinuidade de dados²⁹. A coleta de informações também é uma questão, visto que poucos sistemas têm incorporado o registro eletrônico.

2. As informações de diversidade

A diversidade refere-se a categorias sociais utilizadas para descrever as diferenças entre as pessoas que compõem uma determinada população. Esses dados se concentram em características como raça/etnia, cidadania, status migratório,

25. BRASIL. Ministério da Saúde. *Portaria nº 589 de 20 de maio de 2015*. Institui a Política Nacional de Informação e Informática em Saúde (PNIIS). Diário Oficial da União: edição 96, seção 1, Brasília, DF, p. 72, 22 maio 2015.

26. BRASIL. Ministério da Saúde. *Portaria nº 2.073, de 31 de agosto de 2011*. Regulamenta o uso de padrões de interoperabilidade e informação em saúde para sistemas de informação em saúde no âmbito do Sistema Único de Saúde, nos níveis Municipal, Distrital, Estadual e Federal, e para os sistemas privados e do setor de saúde suplementar. Diário Oficial da União: seção 1, Brasília, DF, p.63, 1 set. 2011.

27. COELHO NETO, G. C. ; CHIORO, A. Afinal, quantos Sistemas de Informação em Saúde de base nacional existem no Brasil? *Cadernos de Saúde Pública*, v. 37, n. 7, p. e00182119, 2021. Disponível em: <https://www.scielo.br/j/csp/a/RzNmviHgm-LhPHZp6gfcdC6H/?format=pdf&lang=pt>. Acesso em: 29 abr. 2024. P.9.

28. BRASIL. Ministério da Saúde. *Sistemas de informação da atenção à saúde: contextos históricos, avanços e perspectivas no SUS*. Brasília, DF: Cidade Gráfica e Editora LTDA, out. 2015.

29. BRASIL. Ministério da Saúde. *Consolidação do Sistema de Informações sobre Nascidos Vivos*. Coordenação Geral de Informações e Análise Epidemiológica. 2011.

religião, gênero (incluindo identidade de gênero), idade, classe social, deficiência, orientação sexual, estado civil, entre outros. A relevância e o impacto de cada categoria variam de acordo com a sociedade, o tempo e o contexto³⁰. Esse tipo de informação tem o papel de evidenciar a diversidade como um aspecto positivo da sociedade, indo além da mera descrição da existência de diferenças³¹.

As informações sobre diversidade estão inseridas em um cenário de debate ampliado sobre: 1) o direito das minorias e o monitoramento do cumprimento das obrigações em matéria de direitos humanos; 2) a aplicação de legislação anti-discriminação; e 3) o acompanhamento dos progressos na consecução dos objetivos de desenvolvimento sustentável e igualdade social, entre outros³². Contudo, de forma mais contundente, trata-se de um debate sobre cidadania, centrado nas reflexões acerca da composição pluriétnica de uma nação^{33 34 35}.

No Brasil, as considerações sociais sobre a diversidade repousam sobre categorias como raça/cor; grupos étnico-raciais; povos e comunidades tradicionais, como quilombolas, povos indígenas, ciganos, comunidades de terreiro, seringueiros, pescadores artesanais, entre outros; Lésbicas, Gays, Bissexuais, Travestis e Transexuais (LGBT); e a população migrante, refugiada e apátrida^{36 37}.

No campo da saúde, esses grupos participam de forma direta ou transversal nas políticas nacionais, como a Política Nacional de Alimentação e Nutrição (1999), a Política Nacional de Redução da Morbimortalidade por Acidentes e Violências (2001), a Política Nacional de Atenção às Urgências, a Política Nacional de Atenção à Saúde dos Povos Indígenas (2002) e as Políticas Nacionais de Saúde Integral de Populações Específicas, como as da população negra (2009) e da população LGBT (2011)³⁸.

30. ROSENSTREICH, G. et al. *Diversity Data Collection: Exploratory Mapping & Reflection*. Una Europa, 2022. Disponível em: <https://una-europa.imgix.net/resources/Diversity-Data-Collection-Exploratory-Mapping-Reflection.pdf>. Acesso em: 14 fev. 2024.

31. BOTOKO CLAEYSEN, Catherine et al. *Diversity Data Collection: Exploratory Mapping & Reflection: Una Europa Diversity Council Action Group Data Collection Final Report 2022*. Una Europa, 2022. Disponível em: <https://paris1.hal.science/hal-03930967/>. Acesso em: 8 mar. 2024.

32. EC-EUROPEAN COMMISSION, Directorate-General for Justice and Consumers, FARKAS, L. *Analysis and comparative review of equality data collection practices in the European Union*. EC: Data collection in the field of ethnicity, Publications Office, 2017.

33. DE OLIVEIRA, Jane Souto. *Brasil mostra a tua cara: imagens da população brasileira nos censos demográficos de 1872 a 2000*. Rio de Janeiro: Escola Nacional de Ciências Estatísticas, 2003. 75 p. ISSN 1677-7093; n. 6.

34. COSTA, Fabiana Claudia Viana. *Designação e referência enunciativa do Censo demográfico 2000*. 2004. Dissertação (Mestrado em Linguística) – UNICAMP, Instituto de Estudos da Linguagem, Universidade Estadual de Campinas, Campinas, São Paulo, 2004.

35. LOVEMAN, M. A política de um cenário de dados transformado: estatísticas etnoraciais no Brasil em uma perspectiva comparativa regional. *Sociologias*, v. 23, n. 56, p. 110–153, jan. 2021.

36. ARRUTI, José Maurício. Etnicidade. In: SANSONE, L.; ALVES FURTADO, C. (org.). *Dicionário crítico das ciências sociais dos países de fala oficial portuguesa*. Salvador: EDUFBA, 2014. p. 199-2013.

37. MIGUEL, Nadya Maria Deps. *O Perfil do brasileiro construído pelo IBGE: uma memória discursiva dos Censos Demográficos de 1940 a 2010*. Tese (Programa de Pós-Graduação em Memória Social) – Universidade Federal do Estado do Rio de Janeiro, Rio de Janeiro, 2012.

38. BRASIL. Ministério da Saúde. Secretaria de Atenção à Saúde. *Nota Técnica nº 18/2014*. Revisão da Política Nacional de Promoção da Saúde. Brasília, 2014. Disponível em: <https://www.conass.org.br/biblioteca/wp-content/uploads/2014/01/NT-18-2014-Politica-de-Promo%CC%A7a%CC%83o-da-Sau%CC%81de.pdf>. Acesso em: 29 abr. 2024.

2.1 A trajetória da diversidade como informação social

A produção de informações sobre a diversidade no âmbito dos sistemas oficiais começou no final da década de 1990 com a inserção da categoria “cor ou raça”. Em 2002, adquiriu uma nova perspectiva com o apoio do Fundo de População das Nações Unidas (UNFPA), que promoveu o fortalecimento da capacidade nacional em assegurar direitos sociais com foco em gênero, raça e geração, em áreas como saúde reprodutiva, HIV/AIDS, prevenção da violência e igualdade de gênero³⁹. Para isso, previa-se a “capacitação para o uso dos registros administrativos e a melhoria dos sistemas existentes. Por melhoria entende-se a inclusão, em todos os registros voltados às pessoas, dos quesitos sexo, idade e raça”⁴⁰.

No cerne dessas iniciativas estava a criação de indicadores. A coleta de dados sobre diversidade geralmente utiliza indicadores, que são parâmetros mensuráveis que representam aspectos específicos de uma categoria de diversidade. Ao receberem significado, essas estatísticas são tratadas como indicadores de uma situação que será alvo de intervenção política. O objetivo é que a efetividade da política afete positivamente a realidade desses indicadores⁴¹.

Assim, à medida que o debate sobre o Estado de direito avança e políticas nacionais (estaduais ou municipais) são estruturadas, os registros administrativos precisam incorporar esses campos no escopo dos Sistemas de Informação (SIS), para fornecer subsídios aos levantamentos oficiais que utilizam o indivíduo como unidade de análise⁴². Contudo, ressalta-se que as informações necessárias para monitorar e avaliar as características da população brasileira são mediadas pelas especificidades do Sistema de Informação.

3. Metodologia

A análise documental, de caráter qualitativo, foi realizada a partir de consultas nos sítios eletrônicos oficiais do governo brasileiro. Foram priorizados documentos técnicos, regimentos e manuais. A consulta levantou informações sobre as políticas públicas e de direitos relacionadas à raça, etnia e à

39. FUNDO DE POPULAÇÃO DAS NAÇÕES UNIDAS. *Projetos e Programas Propostos: Assistência ao Governo do Brasil (DP/FPA/BRA/3)*. Fundo de População das Nações Unidas, 2001. Disponível em: https://brazil.unfpa.org/sites/default/files/pub-pdf/country_programme20022006_0.pdf. Acesso em: 29 abr. 2024.

40. OSÓRIO, Rafael Guerreiro. *O Sistema Classificatório de Cor e Raça do IBGE*. Brasília: Ipea, Ministério do Planejamento, Orçamento e Gestão, 2003. (Texto para discussão, 996). P. 37.

41. OSÓRIO, Rafael Guerreiro. *O Sistema Classificatório de Cor e Raça do IBGE*. Brasília: Ipea, Ministério do Planejamento, Orçamento e Gestão, 2003. (Texto para discussão, 996).

42. OSÓRIO, Rafael Guerreiro. *O Sistema Classificatório de Cor e Raça do IBGE*. Brasília: Ipea, Ministério do Planejamento, Orçamento e Gestão, 2003. (Texto para discussão, 996).

população de Lésbicas, Gays, Bissexuais, Travestis e Transexuais (LGBT). O levantamento dos decretos foi feito a partir das citações contidas nesses documentos. Já a avaliação das condições da informação social nos Sistemas de Informação em Saúde, para os propósitos deste artigo, priorizou apenas aqueles ligados à Atenção Básica: Sistema de Informações sobre Mortalidade (SIM), Sistema de Informações sobre Nascidos Vivos (SINASC), Sistema de Vigilância Alimentar e Nutricional (SISVAN), Sistema de Informações sobre Agravos de Notificação (SINAN) e o Sistema de Informações Ambulatoriais (SIA/SUS). Os casos foram avaliados segundo objetivo do sistema e a sua adequação à base legal das categorias de diversidade analisadas.

4. As bases legais e a incorporação da diversidade nos Sistemas em Saúde

As normas constitucionais que estabelecem a base de legitimidade para o desenvolvimento das políticas de saúde têm como ponto de partida o artigo 196 da Constituição Federal (1988), que assegura a saúde como um direito a ser garantido pelo Estado⁴³. Ressalta-se que a Constituição assegura outros direitos e garantias à diversidade, os quais, em termos gerais, podem ser agrupados nos eixos ligados à igualdade e não discriminação (artigos 3º, 5º, 14, 19, 215 e 242), aos direitos territoriais e culturais (artigos 216, 231 e 232) e aos direitos sociais (artigo 6º). No campo legislativo, a maior parte das normativas está no escopo dos Direitos Humanos e da Cidadania, além de serem incluídas na legislação que trata de crimes relacionados ao preconceito.

4.1 Raça/cor

O mapeamento realizado sobre as bases legais identificou um cenário normativo composto por duas leis, um decreto e três portarias. As portarias nº 3.947/GM/MS e nº 344/MS têm incidência direta na inserção da variável nos formulários de coleta do SUS. A Lei nº 12.288, considerada um marco legal fundamental na portaria nº 344/MS, embora aborde, entre outras questões, o direito à saúde, também dialoga com legislações que tratam de crimes relacionados ao preconceito, violência e intolerância. Esta lei e a portaria nº 992/GM/MS emergem como marcos para minimizar o quadro discriminatório tanto na esfera social quanto no âmbito do Sistema Único de Saúde (SUS). Abaixo está a relação dos marcos levantados:

43. BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidente da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 29 abr. 2024.

- Decreto nº 65.810, de 08 de dezembro de 1969: Convenção Internacional sobre a Eliminação de todas as Formas de Discriminação Racial.
- Portaria nº 3.947/GM/MS, de 25 de novembro de 1998: Aprova os atributos comuns a serem adotados, obrigatoriamente, por todos os sistemas e base de dados do Ministério da Saúde, a partir de 1º de janeiro de 1999.
- Portaria nº 992/GM/MS, de 13 de maio de 2009: Política Nacional de Saúde Integral da População Negra (PNSIPN).
- Lei nº 12.288, de 20 de julho de 2010: Estatuto da Igualdade Racial.
- Resolução nº 2/CIT, de 2 de setembro de 2014: II Plano Operativo (2013-2015) da PNSIPN no âmbito do Sistema Único de Saúde (SUS).
- Portaria nº 344/MS, de 01 de fevereiro de 2017: preenchimento obrigatório do quesito raça/cor nos formulários dos sistemas de informação em saúde.
- Lei nº 14.553 de 2023 que altera a Lei nº 12.288/2010: obrigatória a inclusão de campos para identificação étnico-racial em diversos documentos. A legislação abrange formulários de admissão e demissão no emprego, formulários de acidente de trabalho, instrumentos de registro do Sistema Nacional de Emprego (SINE) e documentos para inscrição no Regime Geral de Previdência Social. A inclusão também se aplica à Relação Anual de Informações Sociais (RAIS) e a questionários de pesquisas do IBGE.

Desde 1995, o SINASC utiliza o campo “RACACOR” para registro. No entanto, refletindo o impacto da Portaria nº 992/GM/MS/2009 e da Lei nº 12.288/2010, houve uma mudança na forma de notificação. A partir de 2011, além de coletar a informação sobre a raça/cor do recém-nascido, passou-se também a coletar a informação sobre a mãe⁴⁴. Essa mudança permitiu o mapeamento do acesso às políticas de saúde materno-infantil e foi uma estratégia para identificar discriminação racial. Até então, a ênfase do SINASC era a elaboração de estatísticas vitais^{45 46}.

44. BRASIL. Ministério da Saúde. *Consolidação do Sistema de Informações sobre Nascidos Vivos*. Coordenação Geral de Informações e Análise Epidemiológica. 2011.

45. BRASIL. Ministério da Saúde. Fundação Nacional de Saúde. *Manual de procedimentos do sistema de informações sobre nascidos vivos*. Brasília: Ministério da Saúde, 2001. 32 p.

46. BRASIL. Ministério da Saúde. *Consolidação do Sistema de Informações sobre Nascidos Vivos*. Coordenação Geral de Informações e Análise Epidemiológica. 2011.

No SIM e no SINASC, onde a introdução do preenchimento do quesito raça/cor é mais antiga, a completude da informação é maior⁴⁷. Parte dessa característica advém da matriz legal que amparou a criação dos sistemas. Ambos iniciaram a coleta no mesmo ano e são derivados das regras que regulam os registros públicos (Lei 6.015, de 31 de dezembro de 1973) e civis, especificamente as regras cartoriais, respectivamente⁴⁸.

4.2 Etnia

Desde o censo de 2000, o IBGE realiza o levantamento da raça, cor e etnia da população brasileira⁴⁹. Segundo os critérios definidos pelo instituto, a população pode ser classificada como branca, preta, amarela, parda ou indígena. Considera-se indígena aquele que se identifica como tal, seja por ligação com terras indígenas ou por vínculo com tradições⁵⁰ (Brasil, 2017). Assim, o conceito de “indígena” elaborado pelo IBGE está vinculado a grupos indígenas. Desde então, esse critério classificatório tem sido utilizado, especialmente a partir das portarias nº 3.947/GM/MS/1998 e nº 344/MS/2017.

Foi através do Decreto nº 6.040, de 7 de fevereiro de 2007, que foi instituída a Política Nacional de Desenvolvimento Sustentável dos Povos e Comunidades Tradicionais, ampliando a noção de etnia. A categoria de povos e comunidades tradicionais (PCTs) inclui as comunidades quilombolas, os povos indígenas, os ciganos, as comunidades de terreiro, os seringueiros, os pescadores artesanais, entre outros. Trata-se de um reconhecimento jurídico-formal que se insere no quadro de regulamentação fundiária⁵¹.

Os povos e comunidades tradicionais têm seu reconhecimento jurídico marcado por suas relações com o território. Desde a Constituição Federal de 1988 (CF/88), o Estado brasileiro trata os PCTs como organizações sociais que ocupam e utilizam territórios⁵².

47. COELHO, R. ; REMÉDIOS, J. ; NOBRE, V. ; MREJEN, M. O quesito raça/cor no DataSUS: evolução e determinantes da completude. *Nota Técnica n. 30*. IEPS: São Paulo, 2023.

48. BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. Departamento de Análise de Situação de Saúde. *Legislação Relativa aos Sistemas de Informações sobre Mortalidade (SIM) e sobre Nascidos Vivos (SINASC)*. Brasília: Ministério da Saúde, 2004.

49. BRASIL. Ministério da Saúde. *Guia de implementação do quesito Raça/Cor/Etnia*. Ministério da Saúde, Universidade de Brasília. Brasília: Ministério da Saúde, 2018. 38 p.: il.

50. BRASIL. Ministério do Desenvolvimento Social. *Trabalho social com famílias indígenas na proteção social básica*. Brasília, DF: MDS, Secretaria Nacional de Assistência Social, 2017.

51. BRASIL. Ministério da Cidadania. *Informativo PCT*. [Informativo]. Secretaria Nacional de Assistência Social, 2017. Disponível em: https://www.mds.gov.br/webarquivos/arquivo/assistencia_social/consulta_publica/Informativo%20PCT.pdf. Acesso em: 14 fev. 2024.

52. BRASIL. Ministério do Desenvolvimento Social. *Trabalho social com famílias indígenas na proteção social básica*. Brasília, DF: MDS, Secretaria Nacional de Assistência Social, 2017.

Neste sentido, o atendimento aos PCTs é caracterizado pela noção de coletivo, que vai além da noção de família ou indivíduo, e é regido pelos serviços de Atenção Primária à Saúde orientados por território, seja por Distritos Sanitários Especiais Indígenas (DSEI) ou por Comunidades Remanescentes de Quilombolas (CRQ)⁵³. A assistência de saúde abrange a atenção especializada, a atenção à saúde das mulheres e crianças, e a vigilância alimentar e nutricional, entre outros. Assim, há uma “vigilância socioassistencial com diagnóstico socioterritorial”⁵⁴.

Os parâmetros legais que orientam a coleta de dados dos PCTs, iniciada pelo censo, estão incorporados no quadro de ações do Ministério do Desenvolvimento Social e Combate à Fome (MDS), conforme o Decreto nº 6.040/2007^{55 56}. Assim, no âmbito da proteção social, as famílias indígenas e quilombolas devidamente registradas foram incluídas nos registros do Cadastro Único para Programas Sociais⁵⁷. A partir dessas considerações, as bases regulatórias da coleta de dados sobre etnia estão relacionadas a:

- Artigo 194 da Constituição Federal de 1988, seguridade social.
- Lei nº 8.742, de 7 de dezembro de 1993, Lei Orgânica de Assistência Social (LOAS)
- Lei nº 9.459, de 13 de maio de 1997, que acrescenta ao artigo 140 do Código Penal o inciso sobre a Injúria Racial.
- Lei nº 9.836, de 23 de setembro de 1999, sobre o Subsistema de Atenção à Saúde Indígena.
- Decreto nº 4887, de 20 de novembro de 2003, que trata as comunidades quilombolas como “grupos étnico-raciais.
- Decreto Legislativo nº 143, de 20 de junho de 2002, que aprova a Convenção 169 da Organização Internacional do Trabalho que trata sobre Povos Indígenas e Tribais.

53. BRASIL. Ministério do Desenvolvimento Social. *Trabalho social com famílias indígenas na proteção social básica*. Brasília, DF: MDS, Secretaria Nacional de Assistência Social, 2017.

54. BRASIL. Ministério da Cidadania. *Informativo PCT*. [Informativo]. Secretaria Nacional de Assistência Social, 2017. Disponível em: https://www.mds.gov.br/webarquivos/arquivo/assistencia_social/consulta_publica/Informativo%20PCT.pdf. Acesso em: 14 fev. 2024. P.15.

55. BRASIL. Ministério do Desenvolvimento Social. *Trabalho social com famílias indígenas na proteção social básica*. Brasília, DF: MDS, Secretaria Nacional de Assistência Social, 2017.

56. BRASIL. Ministério da Saúde. Secretaria de Atenção à Saúde. Departamento de Atenção Básica. Coordenação-Geral da Política de Alimentação e Nutrição. *Manual operacional para uso do Sistema de Vigilância Alimentar e Nutricional. SISVAN Versão 3.0. Normas e Manuais Técnicos*. Brasília: Ministério da Saúde, 2017.

57. BRASIL. Ministério da Cidadania. *Informativo PCT*. [Informativo]. Secretaria Nacional de Assistência Social, 2017. Disponível em: https://www.mds.gov.br/webarquivos/arquivo/assistencia_social/consulta_publica/Informativo%20PCT.pdf. Acesso em: 14 fev. 2024. P.15.

- Portaria nº 254/GM/MS, de 31 de janeiro de 2002, sobre a Política Nacional de Atenção à Saúde dos Povos Indígenas.
- Portaria nº 98, de 26 de novembro de 2007, que trata do Cadastro Geral de Comunidades Remanescentes de Quilombos
- Decreto nº 6.040, de 07 de fevereiro de 2007, que instituiu a Política Nacional de Desenvolvimento Sustentável de Povos e Comunidades Tradicionais.
- Decreto nº 6.261/2007 (revogado pelo Decreto nº 11.447, de 21 de março de 2023). Programa Aquilomba Brasil e o seu Comitê Gestor.
- Portaria nº 992/GM/MS, de 13 de maio de 2009: Política Nacional de Saúde Integral da População Negra (PNSIPN).
- Decreto nº 6.872, de 4 de junho de 2009, sobre o Plano Nacional de Promoção da Igualdade Racial (PLANAPIR), que no eixo 3, sobre Saúde, trata da ampliação do acesso a populações negras, indígenas e ciganas, e no escopo da saúde da família, às comunidades quilombolas.
- Decreto nº 10.088, de 05 de novembro de 2009 (e Decreto 5.051/2004), que acata o decreto legislativo da Convenção 169 da OIT e o princípio legal da autodeterminação étnica.
- Portaria nº 177, de 16 de junho de 2011, que define para alguns grupos populacionais o atendimento diferenciado para inclusão no Cadastro Único.
- Portaria nº 2.866, de 2 de dezembro de 2011, sobre a Política Nacional de Saúde Integral das Populações do Campo e da Floresta (PNSIPCF)
- Portaria GM/MS nº 3.396, de 11 de dezembro de 2020
- Decreto nº 12.128, de 1º de agosto de 2024, institui oficialmente o Plano Nacional de Políticas para Povos Ciganos.

O mapeamento realizado sobre as bases legais identificou um cenário normativo orientado ao reconhecimento de direitos, demarcação de territórios e gestão administrativa desses territórios. As ações de saúde são referenciadas pela Política Nacional de Saúde Integral das Populações do Campo e da Floresta (PNSIPCF) e pela Política Nacional de Saúde Integral da População Negra (PNSIPN). Essas políticas destacam as especificidades de saúde dessas populações, incluindo vulnerabilidades de acesso, violência e disputa territorial, questões de saúde mental e uso de psicotrópicos, acesso à alimentação e

doenças sexualmente transmissíveis, entre outras. A PNSIPCF, em particular, enfatiza aspectos de cidadania, segurança alimentar e nutricional, e desenvolvimento sustentável⁵⁸.

A avaliação de saúde desses grupos tende a ser caracterizada pelo espaço geográfico, por categorias de gênero, idade, raça/etnia e outros marcadores de populações específicas. Nos sistemas de saúde (SIS), a etnia pode ser coletada a partir de dois campos: raça/cor e povo e comunidade tradicional. Entre os sistemas ligados à Atenção Básica, o Sistema de Informações sobre Mortalidade (SIM), o Sistema de Informações sobre Nascidos Vivos (SINASC) e o Sistema de Informações sobre Agravos de Notificação (SINAN) utilizam o campo raça/cor para coletar informações sobre etnia. Em alguns casos, o campo logradouro, associado ao endereço (rua, avenida etc.), pode ser utilizado para registrar o nome da comunidade tradicional⁵⁹. Por sua conexão com o programa de vigilância nutricional e com as ações do Programa Bolsa Família, o Sistema de Vigilância Alimentar e Nutricional (SISVAN) dispõe do campo povo e comunidade tradicional⁶⁰.

Lésbicas, Gays, Bissexuais, Travestis e Transexuais (LGBT)

Os aspectos de saúde de lésbicas, gays, bissexuais, travestis e transexuais (LGBT) estão fortemente relacionados a questões de violência, ao processo de transexualização e ao enfrentamento do HIV/AIDS e das doenças sexualmente transmissíveis (DST). De fato, foi através do enfrentamento da epidemia de HIV/AIDS que as questões de saúde dessa população ganharam destaque no cenário brasileiro⁶¹. O quadro regulatório que rege a coleta de informações sobre esse grupo é relativamente recente, embora tenha sido precedido por debates no campo dos Direitos Humanos desde a década de 1980⁶², conforme se observa abaixo:

58. IEPS; UMANE; INSTITUTO VEREDAS. *Relatório Técnico nº1/2023. Saúde dos Povos Indígenas e Quilombolas*. Rio de Janeiro: IEPS, 2023.

59. BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. *Sistema de Informação de Agravos de Notificação. Ficha de Notificação*. Brasília: Ministério da Saúde, 2006.

60. BRASIL. Ministério da Saúde. Secretaria de Atenção à Saúde. Departamento de Atenção Básica. Coordenação-Geral da Política de Alimentação e Nutrição. *Manual operacional para uso do Sistema de Vigilância Alimentar e Nutricional. SISVAN Versão 3.0. Normas e Manuais Técnicos*. Brasília: Ministério da Saúde, 2017.

61. BRASIL. Ministério da Saúde. Secretaria de Gestão Estratégica e Participativa. Departamento de Apoio à Gestão Participativa. *Política Nacional de Saúde Integral de Lésbicas, Gays, Bissexuais, Travestis e Transexuais*. Ministério da Saúde, Secretaria de Gestão Estratégica e Participativa, Departamento de Apoio à Gestão Participativa. Brasília, DF: Ministério da Saúde, 1. ed., 2013.

62. BRASIL. Ministério da Saúde. Secretaria de Gestão Estratégica e Participativa. Departamento de Apoio à Gestão Participativa. *Política Nacional de Saúde Integral de Lésbicas, Gays, Bissexuais, Travestis e Transexuais*. Ministério da Saúde, Secretaria de Gestão Estratégica e Participativa, Departamento de Apoio à Gestão Participativa. Brasília, DF: Ministério da Saúde, 1. ed., 2013.

- Lei nº 7.716, de 5 de janeiro de 1989, crimes resultantes de preconceito.
- Portaria nº 2.227, de 14 de outubro de 2004, dispõe sobre a criação do Comitê Técnico para a formulação de proposta da política nacional de saúde da população de gays, lésbicas, transgêneros e bissexuais – GLTB.
- Portaria MS/GM nº 104, de 25 de janeiro de 2011, universaliza a notificação de violência doméstica, sexual e outras violências.
- Portaria nº 2.836, de 1º de dezembro de 2011, Política Nacional de Saúde Integral de Lésbicas, Gays, Bissexuais, Travestis e Transexuais (Política Nacional de Saúde Integral LGBT).
- Portaria MS/GM nº 1.271, de 06 de junho de 2014, insere na lista de doenças e agravos de notificação compulsória os casos de violência sexual e tentativa de suicídio.
- Portaria de Consolidação GM/MS nº 02, de 28 de setembro de 2017, que consolida Política Nacional de Saúde Integral LGBT dentre as políticas nacionais de saúde do Sistema Único de Saúde.
- Resolução CIT nº 26, de 28 de setembro de 2017, II plano operativo (2017-2019) da Política Nacional de Saúde Integral LGBT no âmbito do Sistema Único de Saúde.
- Projeto de Lei nº 1082, de 2023 (em tramitação), que propõe alterar a Lei nº 8.184, de 10 de maio de 1991, e coletar de forma obrigatória dados sobre a população LGBTQIA+ (lésbicas, gays, bissexuais, transexuais, queer, intersexuais, assexuais e outros) pelos censos e outros levantamentos periódicos da Fundação Instituto Brasileiro de Geografia e Estatística (IBGE).
- Portaria nº 762, de 7 de dezembro de 2023, institui a Rede Nacional de Evidências em Direitos Humanos, no âmbito do Ministério dos Direitos Humanos e da Cidadania.

A trajetória de coleta e incorporação das informações sobre a população LGBT nos Sistemas de Informação em Saúde (SIS) começa com o Sistema de Informação de Agravos de Notificação (SINAN), através do módulo de vigilância de violências, a partir de 2015⁶³. A estrutura do formulário desse módulo é capaz de registrar a orientação sexual (heterossexual, homossexual (gay/lésbica), bissexual), a identidade de gênero (travesti, mulher transexual, ho-

63. LEAL, C. H. S. ; SCALCO, M. L. A. ; NUNES, R. P. D. ; CONSORTII, E. R. ; KITAGAWA, B. Y. Vigilância de violências: considerações sobre as informações relativas às violências perpetradas contra a população LGBT no município de São Paulo. *Bis*, São Paulo, v. 2, n. 19, p. 55-61, dez. 2018. Disponível em: <https://docs.bvsalud.org/biblioref/2019/09/1016509/bis-v19n2-diversidade-55-61.pdf>. Acesso em: 19 abr. 2024.

mem transexual), bem como a motivação da violência (sexismo, homofobia/lesbofobia/bifobia/transfobia, racismo, intolerância religiosa, xenofobia, conflito geracional, situação de rua, deficiência)⁶⁴.

Os demais módulos do SINAN, incluindo aquele que monitora casos de HIV/AIDS, não possuem campos específicos para identidade de gênero e orientação sexual. Para esses casos, são utilizadas outras variáveis: no monitoramento do HIV/AIDS, por exemplo, a análise dos dados é feita com base no campo que captura o provável modo de transmissão sexual (homens que fazem sexo com homens (HSH) e mulheres que fazem sexo com mulheres (MSM))⁶⁵. Para os sistemas que não capturam essas informações, resta a variável sexo (masculino, feminino, ignorado).

Considerações finais

Essa breve análise das normas nacionais que regem a inclusão das categorias sociais que representam a diversidade nos sistemas de informação em saúde revela que a legislação pertinente foi construída e elaborada à medida que essas categorias obtinham reconhecimento social. No entanto, apesar de estarem asseguradas por programas de políticas públicas, a invisibilidade estatística ainda persiste para algumas dessas categorias.

A falta de infraestrutura e de gestão da informação, no sentido de criação de um padrão, tem se mostrado um limitador para a ampliação da inclusão de campos de informação capazes de representar essas categorias. Observa-se que os registros administrativos se constituem como uma fonte relevante de dados sobre a diversidade do país, além do censo.

Além disso, o reconhecimento dessas categorias, seja no contexto de doenças estigmatizantes ou de violência, como no caso da população LGBTQIA+, ou no contexto territorial, como para os povos e comunidades tradicionais (PCTs), influencia a forma como elas são incluídas nos sistemas de informação e quais sistemas serão considerados.

A trilha estratégica da Saúde Digital, assim como a de todos os negócios digitais governamentais, está sendo delineada por uma estrutura que avalia a maturidade institucional no uso dos dados. As considerações sobre como a

64. LEAL, C. H. S. ; SCALCO, M. L. A. ; NUNES, R. P. D. ; CONSORTII, E. R. ; KITAGAWA, B. Y. Vigilância de violências: considerações sobre as informações relativas às violências perpetradas contra a população LGBT no município de São Paulo. *Bis*, São Paulo, v. 2, n. 19, p. 55-61, dez. 2018. Disponível em: <https://docs.bvsalud.org/biblioref/2019/09/1016509/bis-v19n2-diversidade-55-61.pdf>. Acesso em: 19 abr. 2024. P.57.

65. CANAVESE, D. et al. Pela urgente e definitiva inclusão dos campos de identidade de gênero e orientação sexual nos sistemas de informação em saúde do SUS: o que podemos aprender com o surto de monkeypox?. *Ciência & Saúde Coletiva*, v. 27, n. 11, p. 4191-4194, nov. 2022.

população é incorporada nos levantamentos oficiais, embora sejam antigas, sempre estiveram na pauta da política de dados nacional adotada pelo governo. Isso ocorre porque os aspectos da população incluídos em um levantamento refletem uma época, seu contexto e os ideais dos constituintes da sociedade.

O que deve ser problematizado é o impacto da qualidade das informações que representam essas categorias nos usos futuros desses dados. Esta perspectiva enfatiza tanto o ciclo de vida dos dados quanto a noção de cauda longa dos dados. O ciclo de vida dos dados considera a evolução do acesso e compartilhamento, enquanto a cauda longa enfatiza a frequência de uso e consumo desses dados.

Se, de certa forma, as políticas sociais se tornam políticas de dados e informações, determinando como, quando e por que a coleta deve ocorrer, o desafio repousa em criar uma estratégia moderadora que se incorpore ao tratamento de dados, especialmente entre a coleta e o uso dessas informações. O descompasso entre a adequação do ente público para a captura, coleta e, conseqüentemente, o tratamento adequado dessas informações e o avanço da legislação de direitos pode ser compensado por estratégias de governança de dados.

Embora sejam coletadas informações individuais, a análise de dados sobre diversidade visa compreender um contexto coletivo. Além disso, a coleta e o uso de dados têm um impacto direto e de longo prazo nos direitos legais e sociais dessa população. Há uma necessidade de reconsiderar e reimaginar a estrutura dessa coleta, para abordar significativamente as preocupações relacionadas ao uso (e usufruto) desses dados e de outras tecnologias.

Nesse sentido, organismos internacionais defendem que o poder público adote modelos de governança de dados que sejam diferenciados por grupo social e suas especificidades. Tais modelos podem ser aprimorados para atender aos direitos dessas comunidades, utilizando estratégias normativas e princípios de dados voltados para a justiça social. Essa é uma área pouco debatida no Brasil, dada a experiência limitada do país na conformação de uma cultura de dados. No entanto, é considerada de extrema relevância, abordando, entre outros aspectos, a qualificação, a codificação e direcionando o uso desses dados. Essa estratégia também pode apoiar a lacuna (persistente) que relaciona a necessidade de ajuste do instrumento de coleta para captar informações relevantes e a capacidade de incorporação desse instrumento nos sistemas de informação, ao criar estratégias de tratamento e codificação de dados.

Referências

ADMINISTRATIVE DATA RESEARCH UK. *Administrative data is an invaluable resource for public good*. Let's use it. Annual Report 2018–19. 2019.

ARRUTI, José Maurício. Etnicidade. In: SANSONE, L.; ALVES FURTADO, C. (org.). *Dicionário crítico das ciências sociais dos países de fala oficial portuguesa*. Salvador: EDUFBA, 2014. p. 199-2013.

BALESTRA, C.; FLEISCHER, L. *Diversity statistics in the OECD: how do OECD countries collect data on ethnic, racial and indigenous identity?* OECD Statistics Working Papers, No. 2018/09, Paris: OECD Publishing, 2018. Disponível em: <https://doi.org/10.1787/89bae654-en>. Acesso em: 21 abr. 2023.

BOTOKO CLAEYSEN, Catherine et al. *Diversity Data Collection: Exploratory Mapping & Reflection: Una Europa Diversity Council Action Group Data Collection Final Report 2022*. Una Europa, 2022. Disponível em: <https://paris1.hal.science/hal-03930967/>. Acesso em: 8 mar. 2024.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidente da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 29 abr. 2024.

BRASIL. Ministério da Cidadania. *Informativo PCT*. [Informativo]. Secretaria Nacional de Assistência Social, 2017. Disponível em: https://www.mds.gov.br/webarquivos/arquivo/assistencia_social/consulta_publica/Informativo%20PCT.pdf. Acesso em: 14 fev. 2024.

BRASIL. Ministério da Cidadania. *Informativo PCT*. [Informativo]. Secretaria Nacional de Assistência Social, 2017. Disponível em: https://www.mds.gov.br/webarquivos/arquivo/assistencia_social/consulta_publica/Informativo%20PCT.pdf. Acesso em: 14 fev. 2024. P.15.

BRASIL. Ministério da Saúde. *A experiência brasileira em sistemas de informação em saúde*. Brasília: Editora do Ministério da Saúde, 2009. (Série B. Textos Básicos de Saúde, v. 1 – Produção e disseminação de informações sobre saúde no Brasil).

BRASIL. Ministério da Saúde. *Consolidação do Sistema de Informações sobre Nascidos Vivos*. Coordenação Geral de Informações e Análise Epidemiológica. 2011.

BRASIL. Ministério da Saúde. Fundação Nacional de Saúde. *Manual de procedimentos do sistema de informações sobre nascidos vivos*. Brasília: Ministério da Saúde, 2001. 32 p.

BRASIL. Ministério da Saúde. *Guia de implementação do quesito Raça/Cor/Etnia*. Ministério da Saúde, Universidade de Brasília. Brasília: Ministério da Saúde, 2018. 38 p.: il.

BRASIL. Ministério da Saúde. *Portaria nº 2.073, de 31 de agosto de 2011*. Regulamenta o uso de padrões de interoperabilidade e informação em saúde para sistemas de informação em saúde no âmbito do Sistema Único de Saúde, nos níveis Municipal, Distrital, Estadual e Federal, e para os sistemas privados e do setor de saúde suplementar. Diário Oficial da União: seção 1, Brasília, DF, p.63, 1 set. 2011.

BRASIL. Ministério da Saúde. *Portaria nº 589 de 20 de maio de 2015*. Institui a Política Nacional de Informação e Informática em Saúde (PNIIS). Diário Oficial da União: edição 96, seção 1, Brasília, DF, p. 72, 22 maio 2015.

BRASIL. Ministério da Saúde. Secretaria de Atenção à Saúde. Departamento de Atenção Básica. Coordenação-Geral da Política de Alimentação e Nutrição. *Manual operacional para uso do Sistema de Vigilância Alimentar e Nutricional. SISVAN Versão 3.0. Normas e Manuais Técnicos*. Brasília: Ministério da Saúde, 2017.

BRASIL. Ministério da Saúde. Secretaria de Atenção à Saúde. Departamento de Atenção Básica. Coordenação-Geral da Política de Alimentação e Nutrição. *Manual operacional para uso do Sistema de Vigilância Alimentar e Nutricional. SISVAN Versão 3.0. Normas e Manuais Técnicos*. Brasília: Ministério da Saúde, 2017.

BRASIL. Ministério da Saúde. Secretaria de Atenção à Saúde. *Nota Técnica nº 18/2014*. Revisão da Política Nacional de Promoção da Saúde. Brasília, 2014. Disponível em: <https://www.conass.org.br/biblioteca/wp-content/uploads/2014/01/NT-18-2014-Politica-de-Promo%CC%A7a%CC%83o-da-Sau%CC%81de.pdf>. Acesso em: 29 abr. 2024.

BRASIL. Ministério da Saúde. Secretaria de Gestão Estratégica e Participativa. Departamento de Apoio à Gestão Participativa. *Política Nacional de Saúde Integral de Lésbicas, Gays, Bissexuais, Travestis e Transexuais*. Ministério da Saúde, Secretaria de Gestão Estratégica e Participativa, Departamento de Apoio à Gestão Participativa. Brasília, DF: Ministério da Saúde, 1. ed., 2013.

BRASIL. Ministério da Saúde. Secretaria de Gestão Estratégica e Participativa. Departamento de Apoio à Gestão Participativa. *Política Nacional de Saúde Integral de Lésbicas, Gays, Bissexuais, Travestis e Transexuais*. Ministério da Saúde, Secretaria de Gestão Estratégica e Participativa, Departamento de Apoio à Gestão Participativa. Brasília, DF: Ministério da Saúde, 1. ed., 2013.

BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde e Ambiente. Departamento de Análise Epidemiológica e Vigilância de Doenças não Transmissíveis. *Dados para Vigilância: perfis das bases de dados produzidas pela Vigilância em Saúde no Brasil*. Brasília: Ministério da Saúde, 2023. 127 p.: il.

BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. Departamento de Articulação Estratégica de Vigilância em Saúde. *Guia de Vigilância em Saúde* [recurso eletrônico] / Ministério da Saúde, Secretaria de Vigilância em Saúde. Departamento de Articulação Estratégica de Vigilância em Saúde. – 5. ed. rev. e atual. Brasília: Ministério da Saúde, 2022. 1.126 p.

BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. Departamento de Análise de Situação de Saúde. *Legislação Relativa aos Sistemas de Informações sobre Mortalidade (SIM) e sobre Nascidos Vivos (SINASC)*. Brasília: Ministério da Saúde, 2004.

BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. *Nota Técnica nº 34/2023: atualizações e recomendações para a vigilância de anomalias congênitas no Brasil*. Brasília, DF, 2023. Disponível em: <http://plataforma.saude.gov.br/anomalias-congenitas/nota-tecnica-34-2023.pdf>. Acesso em: 8 mar. 2024.

BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. *Sistema de Informação de Agravos de Notificação. Ficha de Notificação*. Brasília: Ministério da Saúde, 2006.

BRASIL. Ministério da Saúde. Secretaria Executiva. Departamento de Informática do SUS. *Política Nacional de Informação e Informática em Saúde: Proposta Versão 2.0* (Inclui deliberações da 12ª Conferência Nacional de Saúde). 2004. Disponível em: http://bvsmms.saude.gov.br/bvs/publicacoes/PoliticalInformacaoSaude29_03_2004.pdf. Acesso em: 1 ago. 2024.

BRASIL. Ministério da Saúde. *Sistemas de informação da atenção à saúde: contextos históricos, avanços e perspectivas no SUS*. Brasília, DF: Cidade Gráfica e Editora LTDA, out. 2015.

BRASIL. Ministério do Desenvolvimento Social. *Trabalho social com famílias indígenas na proteção social básica*. Brasília, DF: MDS, Secretaria Nacional de Assistência Social, 2017.

CANAVESE, D. et al. Pela urgente e definitiva inclusão dos campos de identidade de gênero e orientação sexual nos sistemas de informação em saúde do SUS: o que podemos aprender com o surto de monkeypox?. *Ciência & Saúde Coletiva*, v. 27, n. 11, p. 4191–4194, nov. 2022.

COELHO NETO, G. C. ; CHIORO, A. Afinal, quantos Sistemas de Informação em Saúde de base nacional existem no Brasil? *Cadernos de Saúde Pública*, v. 37, n. 7, p. e00182119, 2021. Disponível em: <https://www.scielo.br/j/csp/a/RzNmVjHqmLhPHZp6gfcDC6H/?format=pdf&lang=pt>. Acesso em: 29 abr. 2024.

COELHO, R. ; REMÉDIOS, J. ; NOBRE, V. ; MREJEN, M. O quesito raça/cor no DataSUS: evolução e determinantes da completude. *Nota Técnica n. 30*. IEPS: São Paulo, 2023.

COELI, Cláudia Medina. Ciência de dados populacionais. *Epidemiologia e serviços de saúde: revista do Sistema Único de Saúde do Brasil*, v. 31, n. 3, e2022119, 19 dez. 2022. doi:10.1590/S2237-96222022000300001.

COSTA, Fabiana Claudia Viana. *Designação e referência enunciativa do Censo demográfico 2000. 2004*. Dissertação (Mestrado em Linguística)–UNICAMP, Instituto de Estudos da Linguagem, Universidade Estadual de Campinas, Campinas, São Paulo, 2004.

DE OLIVEIRA, Jane Souto. *Brasil mostra a tua cara: imagens da população brasileira nos censos demográficos de 1872 a 2000*. Rio de Janeiro: Escola Nacional de Ciências Estatísticas, 2003. 75 p. ISSN 1677-7093; n. 6.

EC-EUROPEAN COMMISSION, Directorate-General for Justice and Consumers, FARKAS, L. *Analysis and comparative review of equality data collection practices in the European Union*. EC: Data collection in the field of ethnicity, Publications Office, 2017.

FERREIRA, F. P. M. Registros administrativos como fonte de dados estatísticos. *Informática Pública*, ano 10, n. 1, p. 81-93, 2008.

FUNDO DE POPULAÇÃO DAS NAÇÕES UNIDAS. *Projetos e Programas Propostos: Assistência ao Governo do Brasil (DP/FPA/BRA/3)*. Fundo de População das Nações Unidas, 2001. Disponível em: https://brazil.unfpa.org/sites/default/files/pub-pdf/country_programme20022006_0.pdf. Acesso em: 29 abr. 2024.

IEPS; UMANE; INSTITUTO VEREDAS. *Relatório Técnico nº1/2023. Saúde dos Povos Indígenas e Quilombolas*. Rio de Janeiro: IEPS, 2023.

LEAL, C. H. S. ; SCALCO, M. L. A. ; NUNES, R. P. D. ; CONSORTII, E. R. ;

KITAGAWA, B. Y. Vigilância de violências: considerações sobre as informações relativas às violências perpetradas contra a população LGBT no município de São Paulo. *Bis*, São Paulo, v. 2, n. 19, p. 55-61, dez. 2018. Disponível em: <https://docs.bvsalud.org/biblioref/2019/09/1016509/bis-v19n-2-diversidade-55-61.pdf>. Acesso em: 19 abr. 2024.

LOVEMAN, M. A política de um cenário de dados transformado: estatísticas etnoraciais no Brasil em uma perspectiva comparativa regional. *Sociologias*, v. 23, n. 56, p. 110–153, jan. 2021.

MELLO, Janine. Produção estatal de evidências e uso de registros administrativos em políticas públicas. In: KOGA, Natália Massaco (Org.) et al. *Políticas públicas e o uso de evidências no Brasil: conceitos, métodos, contextos e práticas*. Brasília: IPEA, 2022. p. 897-914.

MIGUEL, Nadya Maria Deps. *O Perfil do brasileiro construído pelo IBGE: uma memória discursiva dos Censos Demográficos de 1940 a 2010*. Tese (Programa de Pós-Graduação em Memória Social) – Universidade Federal do Estado do Rio de Janeiro, Rio de Janeiro, 2012.

OLIVEIRA, D.C. Representatividade da população LGBTQIA+ nas pesquisas epidemiológicas, no contexto da Política Nacional de Saúde Integral de Lésbicas, Gays, Bissexuais, Travestis e Transsexuais: ampliar a produção de conhecimento no SUS para a justiça social. *Epidemiologia e Serviços de Saúde*, v. 31, n. 1, e2022020, 2022.

OSÓRIO, Rafael Guerreiro. *O Sistema Classificatório de Cor e Raça do IBGE*. Brasília: Ipea, Ministério do Planejamento, Orçamento e Gestão, 2003. (Texto para discussão, 996).

PANZARDI, R.; CALCOPIETRO, C.; IVANOVIC, E. F. *New-economy sector study: electronic government and governance – lessons from Argentina*. Working paper. Washington, DC: World Bank, jul. 2002. Disponível em: <https://documentos.bancomundial.org/es/publication/documents-reports/documentdetail/527061468769894044/new-economy-sector-study-electronic-government-and-governance-lessons-from-argentina>. Acesso em: 14 fev. 2024.

ROSENSTREICH, G. et al. *Diversity Data Collection: Exploratory Mapping & Reflection*. Una Europa, 2022. Disponível em: <https://una-europa.imgix.net/resources/Diversity-Data-Collection-Exploratory-Mapping-Reflection.pdf>. Acesso em: 14 fev. 2024.

SENRA, N. de C. A questão dos registros administrativos vis-à-vis a geração de estatísticas. *Revista Brasileira de Estudos de População*, [S. l.], v. 13, n. 2, p. 199–205, 1996. Disponível em: <https://rebep.org.br/revista/article/view/437>. Acesso em: 23 jul. 2024.

WORLD BANK. *Managing development: the governance dimension*. Washington, D.C.: World Bank Group, 1991. Disponível em: <http://documents.worldbank.org/curated/en/884111468134710535/Managing-development-the-governance-dimension>. Acesso em: 14 fev. 2024.



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 janeiro de 2025.