DIREITO DIGITAL

TEMÁTICAS URGENTES E NECESSÁRIAS

Cinthia Obladen de Almendra Freitas
Dânton Hilário Zanetti de Oliveira
Rafael Almeida Oliveira Reis
(Organizadores)

EDITORA ILUSTRAÇÃO

Cinthia Obladen de Almendra Freitas
Dânton Hilário Zanetti de Oliveira
Rafael Almeida Oliveira Reis
(Organizadores)

DIREITO DIGITAL

Temáticas Urgentes e Necessárias

Editora Ilustração
Santo Ângelo – Brasil
2026

Editor-chefe: Fábio César Junges
Imagem da capa: Freepik
Revisão: Os autores

CATALOGAÇÃO NA FONTE

D598 Direito digital [recurso eletrônico] : temáticas urgentes e necessárias / organizadores: Cinthia Obladen de Almendra Freitas, Dânton Hilário Zanetti de Oliveira, Rafael Almeida Oliveira Reis. - Santo Ângelo : Ilustração, 2026.
250 p.

ISBN 978-65-6135-204-8
DOI 10.46550/978-65-6135-204-8

1. Direito digital. 2. Tecnologia. 3. Inteligência artificial. I. Freitas, Cinthia Obladen de Almendra (org.). II. Oliveira, Dânton Hilário Zanetti de (org.). III. Reis, Rafael Almeida Oliveira (org.).

CDU: 34:004

Responsável pela catalogação: Fernanda Ribeiro Paz - CRB 10/ 1720

E-mail: eilustracao@gmail.com

www.editorailustracao.com.br

Conselho Editorial

EDITORA
ILUSTRAÇÃO

SUMÁRIO

APRESENTAÇÃO

O livro "direito DIGITAL: temáticas urgentes e necessárias" reúne artigos resultantes de pesquisas elaboradas por membros do Grupo de Estudos em Direito Digital (GEDDIG), ligado ao Programa de Pós-Graduação em Direito (PPGD) da Pontifícia Universidade Católica do Paraná (PUCPR) e por não membros, mas orientandos e orientandas e egressos e egressas do PPGD, em nível de Mestrado ou Doutorado, que foram ou estão sob a orientação da Prof.ª. Dr.ª. Cinthia Obladen de Almendra Freitas.

O GEDDIG foi formado dentro da área de concentração "Direito Socioambiental e Sustentabilidade" na linha de pesquisa "Estado, Sociedades, Povos e Meio Ambiente" e, assim, entendendo a ciência do Direito como organismo vivo e em mutação devido às novas tecnologias, o GEDDIG se dedica ao desenvolvimento de estudos e pesquisas ligados ao ramo do Direito Digital, ou seja, às intersecções entre Direito e Tecnologia em questões de relevância jurídica e social. Em sua proposta, o GEDDIG procura promover o diálogo contínuo e o intercâmbio científico entre acadêmicos interessados na discussão e aprofundamento dos temas de Direito Digital, a partir das seguintes iniciativas: (i) Reuniões de trabalho para estudos teóricos e aprofundamento dos temas de Direito Digital; (ii) Promover eventos acadêmicos (seminários, congressos, ciclos de palestras, núcleos de pesquisa, etc.); (iii) Produção de material acadêmico, científico, técnico e legislativo.

Iniciado em 2018, sob a perspectiva do estudo da Lei Geral de Proteção de Dados (LGPD) em processo de aprovação e depois aprovada, o GEDDIG vem acompanhando a evolução da aplicação da LGPD, portanto, trabalhando e discutindo sobre direitos fundamentais, dignidade da pessoa humana, proteção de dados pessoais, dados sensíveis, segurança da informação, riscos e Inteligência Artificial e, ainda, o projeto de alteração do Código Civil, em especial questões ligadas ao Direito Civil Digital.

Atualmente o GEDDIG é coordenado pela Prof,ª Dr.ª Cinthia Obladen de Almendra Freitas, tendo como coordenadores adjuntos o Prof. MSc. Dânton Hilário Zanetti de Oliveira e Prof. MSc. Rafael Almeida Oliveira Reis. O grupo é constituído por pesquisadores integrantes do PPGD da PUCPR ou outros, profissionais e estudantes em nível de especialização (*lato sensu*) ou graduação.

O livro é, para além dos resultados do GEDDIG, um convite aos interessados em adentrar novos temas advindos da interseção entre o Direito e a Tecnologia, especialmente para compreender reflexos das novas tecnologias no Direito Digital.

Cinthia Obladen de Almendra Freitas
Dânton Hilário Zanetti de Oliveira
Rafael Almeida Oliveira Reis
(Organizadores)

INTRODUÇÃO: O CIBERESPAÇO COMO UM ESPAÇO DE NÃO-COISAS

Cinthia Obladen de Almendra Freitas[1]

O Direito Digital é o ramo do Direito que se ocupa do estudo do conjunto de normas, aplicações, processos, relações jurídicas, doutrina e jurisprudência que surgem como consequência da utilização e desenvolvimento das novas tecnologias, especialmente das Tecnologias de Informação e Comunicação (TIC) e, mais recentemente, da Inteligência Artificial (IA).

Inicialmente deve-se ter por premissa que o Direito Digital transita em múltiplas sociedades, quais sejam: informacional, tecnológica, consumo, transparência, vigilância, controle e algoritmos. Essa diversidade de sociedades, considerando indivíduos, meio digital e aparatos tecnológicos subsistem tanto no mundo físico, mas especialmente no meio ambiente digital (CAVEDON et al., 2015). Assim, o Direito Digital precisa estar atento ao que acontece na sociedade contemporânea em termos de novas tecnologias e produz reflexos jurídicos, sociais, éticos e ambientais nas instituições jurídicas, de modo a estabelecer limites e normas para regular não somente o uso de aparatos tecnológicos, incluindo-se a Internet, mas aquilo que pode ser realizado tendo-se o meio ambiente digital como meio ou fim. A premissa é regular aquilo que afeta bens jurídicos e, também, as relações derivadas das ações realizadas por meio de não-coisas, bits (*binary digit*), zeros (0) e uns (1) (FREITAS, 2025) (HAN, 2022). Isto devido **à** sociedade de algoritmos que processa dados (*input*) em formato digital, ambos bits, confrontando a materialidade, pessoalidade, territorialidade, temporalidade e espacialidade da coisa física, material e tangível (FREITAS, 2025, p. 10). Portanto, cabe compreender que o advento da Internet, que revolucionou os meios de comunicação, estabeleceu o denominado ciberespaço, o qual se desenvolveu especialmente com a promessa de se constituir como um novo lugar para os indivíduos.

1 Professora Titular da PUCPR. Professora Permanente do Programa de Pós-Graduação em Direito (PPGD) da PUCPR. Doutora em Informática Aplicada. Membro Consultora da Comissão de Direito Digital e Proteção de Dados da OAB/PR. Membro Consultora do Instituto Nacional de Proteção de Dados (INPD). E-mail cinthia.freitas@pucpr.br

Na sociedade contemporânea, o cenário digital tem forte dependência da Internet, a qual constitui a rede mundial de computadores. Tal qual descrita por Laudon e Laudon (1999, p. 168) como sendo "a maior e mais rápida forma de implementação de uma autoestrada da informação", expressão mencionada em 1994 por Albert Arnold Gore, ou simplesmente Al Gore em uma palestra na Universidade de Los Angeles. Esta expressão carrega a importância da Internet para a informação e vice-versa. Entende-se também que a Internet tem papel fundamental na formação da sociedade informacional e todas as demais, especialmente na formação da sociedade de algoritmos, a exemplo das nove sociedades elencadas por Byung-Chul Han (2012): positividade, exposição, evidencia, pornográfica, aceleração, intimidade, informação, revelação, controle; caracterizando a sociedade da transparência. Pode-se mencionar ainda: sociedade de risco, sociedade da exposição, sociedade de vigilância e a sociedade de algoritmos.

Nos aspectos tecnológicos, a criação da ArpaNet em abril de 1969, ou seja, o núcleo central da Internet que foi desenvolvido pela *Advanced Research Projects Agency* (ARPA) do Departamento de Defesa dos Estados Unidos possibilitando o compartilhamento de dados e a troca de mensagens (correio eletrônico ou e-mail). Deve-se observar que a Internet surgiu durante a Guerra Fria, os Estados Unidos e a União Soviética disputavam a hegemonia política, econômica e militar no mundo. Assim, o objetivo inicial da ArpaNet era militar, tendo em vista que, caso os Estados Unidos fossem atacados e perdessem os meios convencionais de comunicação, as forças armadas norte-americanas poderiam manter a comunicação e a troca de informações.

Porém, nas décadas de 70 e 80, a Internet passou a ser utilizada para fins acadêmicos, isto é, para troca de ideias e mensagens entre professores e estudantes universitários. Somente na década de 90, com o desenvolvimento do serviço *World Wide Web* (daí surgiu o www que é utilizado para localizar sites) ou simplesmente web, pelo engenheiro inglês Tim Bernes-Lee, é que a Internet pode ampliar seus horizontes e de seus usuários. Neste contexto, o www foi o primeiro integrador de informações, permitindo que dados, informações e conteúdos pudessem ser acessados de qualquer lugar, por meio de uma forma simples e consistente. Em termos tecnológicos, o que possibilitou a Internet ser um diferencial, é a utilização do hipertexto, o qual constitui um padrão para apresentação das informações com base em uma linguagem denominada de HTML (*Hypertext Markup Language*). A base de transporte das informações na Internet é o protocolo TCP/IP (*Transmission Control Protocol/Internet Protocol*) (Comer, 1991). Assim,

no ambiente www diversas aplicações podem ser escritas no formato do protocolo de nível de aplicação do TCP/IP conhecido como http (*Hypertext Transfer Protocol*) (GARFINKEL; SPAFFORD, 1997).

O paradigma inicial da Internet era constituir-se em uma rede mundial de computadores trocando informações entre si, mas se tornou muito mais que isto. Deste modo, para auxiliar e facilitar a "navegação" foram desenvolvidos software denominados *browsers* ou navegadores. Observa-se que o verbo "navegar" está ligado à Internet devido ao fato do usuário poder passar de uma página web (*web page*) para outra por um simples *click* no *mouse* ou na tela, visto que cada palavra ou parte do texto pode estar ligada a outros textos, por isto, denomina-se de hipertexto ou *hyperlink*. Na verdade, o *hyperlink* não consiste somente no conceito de vínculos embutidos, para especificar textos dentro do mesmo arquivo ou computador, mas principalmente por conter *hyperlinks* para textos e arquivos localizados em outros computadores em diferentes localizações (LAUDON; LAUDON, 1999, p. 169).

Atualmente, pode-se constatar que qualquer tipo de informação pode ser acessada via Internet. Atingiu-se um estágio de desenvolvimento caracterizado pela capacidade de obter e compartilhar qualquer informação instantaneamente, ou seja, agregam-se os conceitos de velocidade, disponibilidade, acessibilidade, além de outros que estão fora do escopo do presente artigo, tais como: autenticidade, veracidade, confiabilidade e integridade (FREITAS, 2025, p. 145).

Todo este desenvolvimento estabeleceu um espaço ilimitado, propiciando a propagação de bens e serviços em uma escala global. Assim, *peopleware*, *software* e *hardware* encontram-se atrelados em um novo espaço, denominado ciberespaço, que engloba uma infraestrutura na qual trafegam não-coisas, bits – zeros e uns (FREITAS, 2025).

Para compreender a relação entre não-coisas e ciberespaço, necessita-se, inicialmente, apresentar os conceitos legal e técnico de ciberespaço. Mas antes é necessário, também, relembrar que o termo ciberespaço surgiu como Willian Gibson, em 1984, no livro de ficção científica *Neuromancer*, para designar um ambiente artificial no qual as relações sociais se desenvolveriam e onde trafegariam uma quantidade avassaladora de dados.

Juridicamente, o ciberespaço pode ser entendido como o: "ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação", a partir da definição encontrada na Estratégia

Nacional de Segurança do Ciberespaço 2019-2023, Resolução do Conselho de Ministros nº 92/19 (PORTUGAL, 2019). No Brasil, a Estratégia Nacional de Segurança Cibernética (E-Ciber), Decreto nº 10.222/2020, não apresenta definições, mas aplica o termo espaço cibernético (BRASIL, 2020).

Sob um olhar tecnológico, o ciberespaço é "constituído por comunicações eletrônicas de dados em um de três estados possíveis (ou por transmitir, ou em transmissão, ou já transmitidos) que fluem entre, e estão alicerçados em três camadas distintas (a física, a lógica e a cognitiva)", conforme Bravo (2021, p. 50). Interessante perceber as dimensões lógica e cognitiva do ciberespaço, de modo que Floridi (1999, p. 61-63) corrobora especialmente a dimensão cognitiva ao compreender a Internet de maneira técnica como a totalidade de três espaços diferentes: (i) físico ou infraestrutura; (ii) digital ou união de todas as memórias de todos os computadores da rede (*memory plataform*); (iii) semântico ou ciberespaço. Para Floridi (1999, p. 63-64) o ciberespaço constitui um espaço semântico ou conceitual sobre a totalidade de todos os documentos, serviços e recursos da Internet.

A partir do entendimento de Bravo (2021), pergunta-se: qual o objeto a ser transmitido? Aqui o ciberespaço se depara com não-coisas, visto que o objeto a ser transmitido são zeros (0) e uns (1), bits. Apesar de o ciberespaço depender de uma infraestrutura física como suporte e funcionamento para o trânsito de não-coisas, são as camadas lógica e cognitiva que trazem semântica à fluidez de não-coisas.

Freitas (2025, p. 5-15) detalha não-coisas, bem como a relação de não-coisas com o Direito, propondo uma travessia conceitual das coisas para não-coisas, reunindo fundamentos jurídicos, filosóficos e tecnológicos. Assim, a autora inicia suas reflexões sobre não-coisas com suporte na filosofia de Byung-Chul Han (2022) passando por diversos conceitos, a exemplo das cinco propriedades físicas que fundamentam o olhar jurídico das coisas considerando-se uma leitura a partir de aspectos tecnológicos do mundo digital, sendo tais propriedades: (i) materialidade, (ii) pessoalidade, (iii) territorialidade, (iv) temporalidade e (v) espacialidade. É aqui que o Direito das Coisas enfrenta um novo paradigma, visto que as coisas não são físicas, materiais e tangíveis no mundo digital. Como apontado pela autora, tem-se aqui um ponto de inflexão, uma necessidade de mudança radicalmente oposta, porém a teoria precisa ser complementar, visto não serem antagônicas, mas trechos diferentes de uma mesma trajetória

comum a ciência do Direito. Por isso, Freitas (2025, p. 5-15) também discute posse a partir do entendimento advindo do Direito das Coisas, mas o faz contrapondo os dois elementos essenciais da pose, ou seja, o poder físico sobre a coisa (*corpus*) e a intenção de ter a coisas como sua (*animus*) (BEVILAQUA, 2003, p. 20).

Observa-se assim a necessidade da existência da relação física de possuir a coisa, mas a materialidade já não existe quando se tem a coisa representada em meio digital, conforme Freitas (2025, p. 5-15). Isso significa que a coisa agora é composta por um conjunto de *bits* (*binary digit*), de zeros (0) e uns (1), combinados de modo a descrever a coisa para o mundo físico, analógico. O digital refere-se à representação por meio de valores discretos (0 e 1), portanto, uma representação matemática do descontinuo, mas quando corretamente formada tem-se a representação de um todo, de uma coisa.

Portanto, entende-se que o ciberespaço compreende o fluxo de não-coisas a partir de uma infraestrutura física, com semântica alicerçada em camadas lógica e cognitiva. Neste contexto, expande-se o conceito de ciberespaço agregando-se os seguintes elementos essenciais ao software, conforme Brooks Jr. (1986, p. 3): complexidade, conformidade, mutabilidade e invisibilidade. Há que se compreender que o ciberespaço depende de *software* para funcionar, a exemplo de protocolos, mecanismos de segurança, segurança da informação, entre outros.

Por todas estas propriedades e elementos essenciais é que não há delimitação física para este espaço cibernético, que está em todos os lugares e não tem um território ou espaço geográfico delimitado. No ciberespaço não há pessoalidade, cada usuário é um conjunto de bits, a partir de seus dados, ou seu endereço IP (*Internet Protocol*) de acesso, lembrando que não há individualidade, visto que a partir de um mesmo IP muitas pessoas tem acesso à Internet. Não há, também, temporalidade, visto que conforme Freitas (2025, p. 5-15), para não-coisas a passagem do tempo não ocorre a partir de uma sequência ordenada de eventos. No mundo digital e no ciberespaço, não há que se falar em linearidade do tempo, uma vez que no ciberespaço há que se carimbar (*timestamp*) com datas e horários aquilo que é realizado, transmitido por meio de *bits*, portanto, não-coisas.

Observou-se pelos estudos que as definições de ciberespaço estão sempre ligadas à infraestrutura, a rede de conexão e interconexão de computadores e aparatos digitais, mas Lévy (1999, p. 17) lembra que para além da infraestrutura, da camada física, há também "o universo oceânico

de informações que ela abriga, assim como seres humanos que navegam e alimentam este universo". Tem-se nesta definição trazida por Lévy que o ciberespaço é antes de tudo um espaço de e para comunicação, e não apenas comunicação entre indivíduos, mas também entre máquinas, algoritmos e fórmulas lógicas, bits, não-coisas. Neste sentido, foi o avanço das Tecnologia da Informação e da Comunicação (TICs) que possibilitou a criação deste espaço de interação, espaço este que se caracteriza por ser um ambiente "elástico e *online*, ou seja, não físico-territorial, que cada vez mais se expande e que possui tanta influência na sociedade que tem sido capaz de alterá-la e direcioná-la" (Freitas; Sousa, 2022, p. 878). E é este espaço que se tornou o espaço para a representação do ser humano, uma vez que assume-se, tal qual Floridi (1999, p. 65), que é no ciberespaço que o ser humano passa cada vez mais tempo como entidade virtual.

Questiona-se: diante de um ciberespaço de não-coisas, como tudo isto se reflete e afeta o Direito? Como afeta o Direito das Coisas? E, o Direito Digital? Acredita-se, como hipótese que pode vir a responder tais questões que será estabelecido um novo ramo no Direito, o Direito de Não-Coisas. Freitas (2025) não apresenta todas as respostas, ao contrário, deixa muitas perguntas por responder, mas cabe aos pesquisadores e juristas pensarem, principalmente, sobre os riscos relacionados ao Direito. Isto mesmo. Direito está atrelado a riscos, quais sejam: (i) a ausência de respostas por parte do Direito; (ii) a existência de respostas ruins ou inadequadas por parte do Direito; (iii) o não compreender a Inteligência Artificial (IA) como ciência e como seus sistemas estão e, ainda mais, afetarão a sociedade, o ser humano e o Direito Digital. E, finalmente, a constatação de entendimentos jurídicos e tecnológicos distintos entre si, porém para um mesmo elemento. Entende-se que cada vez mais Direito e Tecnologia precisam andar de mãos dadas para trilhar um caminho justo e ético voltado ao bem-estar e bem viver dos seres humanos.

Referências

BEVILAQUA, Clovis. Direito das coisas. Vol. I, Brasilia: Senado Federal, Conselho Editorial, 2003.

BRAVO, Rogério. **Segurança da informação, cibersegurança e cibercrime**: contributos para um alinhamento de conceitos. Lisboa, v. 12, 2021. Disponível em: https://www.academia.edu/40494857/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o_e_

ciberseguran%C3%A7a_aspetos_pr%C3%A1ticos_e_legisla%C3%A7%C3%A3o Acesso em: 27 set. 2025.

BRASIL. **Decreto nº 10.222, de 5 de fevereiro de 2020**. Estratégia Nacional de Segurança Cibernética. Brasília, DF: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm Acesso em: 27 set. 2025.

BROOKS JR, Frederick P. **No silver bullet**: essence and accident in software engineering. University of North Carolina, 1986. Disponivel em: http://worrydream.com/refs/Brooks-NoSilverBullet.pdf Acesso em: 27 set. 2025.

CAVEDON, Ricardo; FERREIRA, Heline Sivini; FREITAS, Cinthia Obladen de Almendra. O Meio Ambiente Digital sob a Ótica da Teoria da Sociedade de Risco: os avanços da informática em debate. **Revista Direito Ambiental e Sociedade**, v. 5, p. 194-223, 2015.

FLORIDI, Luciano. **Philosophy and Computing**: na introduction. London: Routledge, 1999.

FREITAS, Cinthia Obladen de Almendra Freitas. **Direito e Não-coisas**. Rio de Janeiro: Lumen Juris, 2025.

FREITAS, Cinthia Obladen de Almendra; SOUSA, Devilson da Rocha. O Contexto dos Direitos Humanos no Ciberespaço e o Papel das Empresas de Tecnologia a partir de uma Análise da Ação das Redes Sociais, **Revista Jurídica Luso-Brasileira (RJLB)**, vol. 8, n. 4, 2022.

GARFINKEL, Simson; SPAFFORD, Gene. **Web security & commerce**. O'Reilly & Associates, Inc., 1997.

HAN, Byung-Chul. **Não-coisas**: transformações no mundo em que vivemos. Trad. Ana Falcão Bastos. Lisboa: Relogio DAgua Editores, 2022.

HAN, Byung-Chul. **The transparency society**. Translated by Erik Butler. Stanford University Press, Stanford, California – USA, 2012.

LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de informação**. Rio de Janeiro: Livros Tecnicos e Cientificos S.A., 1999.

LÉVY, Pierre. **Cibercultura**. Rio de Janeiro: Editora 34, 1999.

PARISER, Eli. **O filtro invisível**: o que a internet está escondendo de você. (trad. Diego Alfaro). Rio de Janeiro: Zahar, 2012.

PORTUGAL. **Resolução do Conselho de Ministros (RCM) nº 92**, de 5 de junho de 2019. *Diário da República*, n. 108, série I, p. 2888-2895, 5 jun. 2019. Disponível em: https://dre.pt/dre/detalhe/resolucaoconselho-ministros/92-2019-122498962 Acesso em: 27 set. 2025.

Capítulo 1

O PARADOXO DA COMPLEXIDADE: O EXERCÍCIO DE DIREITOS INFORMACIONAIS NA SOCIEDADE INFORMACIONAL

Dânton Hilário Zanetti de Oliveira[1]

1 Introdução

A sociedade contemporânea vem experimentando, de modo cada vez mais intenso, o poder da informação. Na sociedade informacional, que encontra no capitalismo informacional uma de suas mais aparentes manifestações, a informação é, de fato, poder: poder de controle, de vigilância, bélico, econômico, tecnológico, científico e assim por diante.

Nessa sociedade, a informação assume um protagonismo ímpar, jamais antes experienciado pela humanidade, sendo considerada como um verdadeiro insumo essencial à cadeia de produção, incorporada desde a concepção de bens de consumo, à execução de serviços, mantendo igual relevância até mesmo após a conclusão de uma determinada relação de consumo, por exemplo.

A onipresença da informação na sociedade contemporânea se deve, em grande medida, à evolução das tecnologias da informação e comunicação (TICs)[2], que se faz tão importante quanto a própria eletricidade, como comparou Han (2018), ao afirmar que as mídias digitais fariam com que a informação estivesse "em meio a nós", deixando-nos "zonzos, surdos, cegos e mudos", o que caracterizaria uma verdadeira crise de cegueira e estupidez, embriagando-nos, como humanidade.

---

1 Mestre e Doutorando em Direito pela Pontifícia Universidade Católica do Paraná (PUCPR). Coordenador do Curso de Pós-graduação "Direito 4.0: Direito Digital, Proteção de Dados e Cibersegurança", da PUCPR. Professor do curso de graduação em Direito da FAE Centro Universitário. Advogado. E-mail danton.zanetti@pucpr.br.

2 Para Manuel Castells (2020, p. 87), as TICs representam um conjunto convergente de tecnologias em microeletrônica, computação (software e hardware), telecomunicações/ radiofusão e optoeletrônica.

Para o bem ou para o mal, tais tecnologias trazem consigo um perfeito paradoxo. Isto porque, de forma simultânea, abrem-nos o campo de visão, exponencializando a circulação da informação e nos deixam cegos, com uma sobrecarga de informação (*information overload*)[3] dificultando o acesso à informação.

A seu turno, o acesso à informação é um elemento chave para que, no seio da sociedade informacional, um indivíduo possa efetivamente se sentir inserido na sociedade e, assim, exercer uma miríade de direitos.

Dentre tais direitos, a fim de trazer recorte mais incisivo ao presente artigo e lhe permitir maior profundidade crítica, cabe destacar o direito à autodeterminação informativa, que, para os fins deste trabalho, será considerado um direito informacional por excelência. Sem que um indivíduo consiga acesso à informação, fatalmente, não conseguirá se autodeterminar frente às situações cotidianas, o que significa que não poderá exercer outros direitos fundamentais.

A falta de acesso à informação se deve, é claro, por múltiplos fatores, não sendo possível neste breve artigo abordar todos eles, embora seja possível, a partir desta premissa, indagar: em que medida a sociedade informacional impõe obstáculos ao exercício de direitos informacionais, especificamente à autodeterminação informacional?

Por meio do método dedutivo e da pesquisa fundada na revisão doutrinária, foi possível definir aquilo que se entende por sociedade informacional, demonstrar que a autodeterminação informacional é, reconhecidamente, um direito fundamental moderno e que, a despeito disto, existem diversos desafios a serem superados rumo à concretização do livre exercício de direitos informacionais.

Dentre os capítulos do presente artigo, o primeiro apresentará o conceito de sociedade informacional e contextualizará a relevância da informação e dos dados pessoais para o atual momento da civilização; o segundo tratará a respeito do reconhecimento da autodeterminação informacional como um direito fundamental e os reflexos disto para o surgimento e desenvolvimento do direito à proteção de dados pessoais; o terceiro capítulo visa demonstrar que a expressão "direitos informacionais" é polissêmica e multifacetada, o que, de um lado, permite abranger

3 Segundo Eduardo Magrani (2014, p. 114), "*information overload*" é um fenômeno que ocorre quando "a quantidade de informação captada pelo indivíduo excede sua capacidade de processá-las, gerando dificuldades de várias ordens como, por exemplo, na filtragem das informações, bem como na compreensão e tomada de decisões".

diversos direitos afetos à sociedade informacional, mas de outro, também complexifica e dificulta a garantia destes direitos.

Ao final, conclui-se que não apenas o reconhecimento jurídico, mas o efetivo respeito à autodeterminação informacional, a transparência, a prestação de contas e a responsabilização dos agentes de tratamento de dados pessoais se apresentam como medidas necessárias à abertura de um caminho possível para a redução da distância existente entre os fenômenos típicos da sociedade informacional e o exercício dos direitos informacionais.

2 Breves considerações acerca da sociedade informacional

O fenômeno da sociedade informacional foi ampla e profundamente estudado por Manuel Castells na célebre obra "A sociedade em rede"[4]. Nela, Castells demonstra o papel fundamental do desenvolvimento tecnológico ocorrido a partir da década de 1960 – especialmente no último quarto do século XX – para o alcance de um novo estágio econômico: a economia informacional (CASTELLS, 2020, p. 135).

Claramente dotada das características capitalistas, a economia informacional, ou o "capitalismo informacional" decorre da revolução tecnológica, sobretudo em relação às tecnologias da informação e comunicação (TICs), razão pela qual Castells parte de uma abordagem histórica do surgimento da Internet, passando a se debruçar sobre os reflexos de seu advento nos mais diversos campos da vida humana. Procurando elucidar sua concepção acerca da natureza informacional da sociedade moderna, Castells (2020, p. 88) a compara à sociedade industrial:

> A tecnologia da informação é para esta revolução o que as novas fontes de energia foram para as revoluções industriais sucessivas, do motor a vapor à eletricidade, aos combustíveis fósseis e até mesmo à energia nuclear. [...] O que caracteriza a atual revolução tecnológica não é a centralidade de conhecimentos e a informação mas a aplicação desses conhecimentos e dessa informação para a geração de conhecimentos e de dispositivos de processamento/comunicação da informação, em um ciclo de realimentação cumulativo entre a inovação e seu uso.

4 A fim de conferir maior objetividade e precisão metodológica ao presente artigo, adotar-se-á a teoria e definição de Manuel Castells acerca da "sociedade informacional", bem como de alguns outros autores com pensamentos convergentes, muito embora não se desconheça o fato de que diversos estudiosos, com linhas de pensamento particulares também endereçaram o tema, como, a título ilustrativo, fizeram (i) Fritz Machlup (1962), com a chamada "indústria baseada no conhecimento"; (ii) Marc Uri Porat (1977), com a chamada "economia da informação"; e (iii) Daniel Bell (1973), que apenas faz alusão a um novo paradigma social "pós-industrial" (CRUZ E SILVA, 2020, p. 31).

Verifica-se que a busca, a produção e o consumo da informação formam um ciclo que se repete sucessivamente sem cessar, uma vez que conhecimento gera mais conhecimento (que, por sua vez, gera ainda mais conhecimento) e, do ponto de vista tecnológico, este se torna uma ferramenta passível de ser aplicada e reaplicada mediante processos sequenciais de armazenamento, recuperação, processamento e transmissão da informação (BOFF; FORTES; FREITAS, 2018, p. 16).

Assim, se a informação é – figurativamente – a raiz, o caule e as folhas da sociedade contemporânea, servindo-lhe de insumo produtivo e, concomitantemente (e por mais paradoxal possa soar), bem de consumo, o *Big Data* assume uma posição chave no plano econômico e social, adentrando às mais diversas áreas da atividade humana. Portanto, não é meramente simbólica a homenagem de Cukier e Mayer-Schönberger (2013) a Manuel Castells, quando estes afirmaram que o *Big Data*[5] significa o cumprimento da promessa da chamada Sociedade Informacional, considerando que os dados assumem papel de protagonismo na sociedade contemporânea.

Uma interessante nuance entre os pontos de vista apresentados por Castells e Cukier e Mayer-Schönberger quanto à sociedade informacional é que, enquanto Castells atribui o desenvolvimento do informacionalismo[6] à revolução das TICs, Cukier e Mayer-Schönberger (2014, p. 72), embora não desprezem os avanços tecnológicos, acreditam que uma mudança social ainda mais profunda decorreria do fato de que atualmente há mais dados disponíveis, o que leva a uma melhor compreensão quanto ao próprio potencial dos dados e da possibilidade de seu aproveitamento em prol da extração de informações relevantes.

Essa crescente disponibilidade de dados para coleta e tratamento, por sua vez, seria consequência do fenômeno denominado *datafication* (ou "datificação", em português) que, segundo os autores, pode ser entendido como a transcrição do mundo real em dados quantitativa e qualitativamente,

---

5 O conceito de *Big Data,* embora dotado de certa imprecisão (CRAWFORD; SCHULTZ, 2014), conforme definição adotada pelo Grupo de Trabalho (ARTICLE 29 WORKING PARTY, 2013), *"Big data refers to the exponential growth both in the availability and in the automated use of information: it refers to gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed (hence the name: analytics100) using computer algorithms. Big data can be used to identify more general trends and correlations but it can also be processed in order to directly affect individuals.*

6 Segundo Castells (2020, p. 74), "o informacionalismo visa o desenvolvimento tecnológico, ou seja, a acumulação de conhecimentos e maiores níveis de complexidade do processamento da informação. [...] é a busca por conhecimentos e informação que caracteriza a função da produção tecnológica no informacionalismo".

de modo que este possa ser tabulado e analisado (CUKIER; MAYER-SCHÖNBERGER, 2014, p. 78).

Com efeito, a datificação é fenômeno decorrente do informacionalismo, uma das três principais características que definem a sociedade informacional, tal como concebida por Castells. Os outros dois caracteres consubstanciam aquilo que o referido autor denominou de sociedade em rede ("*the network Society*"), quais sejam, a globalização e o funcionamento em rede. A sociedade informacional, para Castells (2020, p. 135) é uma sociedade global, uma vez que a informação permite sua organização em escala global graças aos fluxos informacionais eficiente e aceleradamente impulsionados pelas TICs; é também uma sociedade em rede, porquanto as redes empresariais é que provocam os movimentos concorrenciais, que agora se desenvolvem a nível global.

A fim de exemplificar a organização em rede desta sociedade, Bruno Bioni (2019, p. 10) menciona uma famosa empresa do ramo de vestuário, mas que não produz suas mercadorias, dependendo de terceiros, em outros países (geralmente asiáticos e subdesenvolvidos); não possui lojas para comercialização de sua produção, distribuindo-as em estabelecimentos diversos mundo afora; não comercializa suas próprias mercadorias, dependendo de terceiros. Neste exemplo, fica claro o efeito em rede, evidenciando que a referida empresa gerencia suas operações apenas por meio do processamento de informações.

Outro efeito bastante evidente da sociedade informacional é a possibilidade de criação de novos modelos de negócio ofertados sob uma "aparente gratuitidade", custeados a partir de massiva coleta e posterior utilização de dados pessoais dos usuários (CASIMIRO, 2020, p. 105), conhecido como *"zero-price-advertisement business model"*. Nele, o consumidor não oferece contraprestação pecuniária pelos produtos ou serviços que consome, mas com o fornecimento de dados pessoais e com o recebimento de publicidade personalizada e direcionada de forma individualizada, com base em perfis comportamentais (BIONI, 2019, p. 49). É a receita decorrente da publicidade que garante a economicidade da operação.

É também importante ponderar que a geração e processamento exponenciais da informação não necessariamente trazem apenas efeitos positivos às relações modernas, haja vista que a revolução tecnológica e o informacionalismo fazem com que os atuais programas de computador e os

dispositivos contribuam para com a "inflação" da informação na sociedade (PARCHEN; FREITAS, 2016, p. 29).

Cada vez mais cobiçada e objeto de exploração, a informação torna-se um ativo econômico de grande valor, especialmente no que se refere a dados pessoais, ou seja, informações capazes de identificar ou tornar alguém identificável. Isto explica o já consagrado jargão "dados são o novo petróleo".[7]

Pode-se acrescentar, ainda, que a Sociedade de Informação se caracteriza por sua dinâmica e a constantes evolução e reinvenção, paradigma que se apresenta diante do rápido e ininterrupto desenvolvimento tecnológico, especialmente nas TICs (FREITAS; FERREIRA; CEVEDON, 2020, p. 9).

Assim, a revolução tecnológica e o advento da sociedade informacional alteram de forma indelével a relação entre economia, Estado e sociedade, que se reestruturam em torno da informação, um insumo essencial à economia produtiva capitalista, à formatação e concentração do poder Estatal e à configuração da cultura e vida em níveis individual e coletivo, com reflexos nos costumes, nas artes e nas próprias formas de relacionamento interpessoal. Todos esses campos passam a integrar o ciberespaço, interconectando-se em uma rede global.

3 A autodeterminação informacional como cerne dos direitos informacionais

O surgimento do direito à autodeterminação informacional tem origem em uma decisão do Tribunal Constitucional da Alemanha (*Bundesverfassungsricht*), na qual julgou-se inconstitucional a lei que previa o recenseamento da população e sua subsequente consolidação na doutrina.

Sob o persistente fantasma do nazismo, referida norma foi severamente criticada por diversos setores da sociedade civil, tanto pelo fato de submeter cada cidadão a responder 160 perguntas, quanto pelo posterior processamento informatizado das respectivas respostas e o confronto destas com os dados do registro civil, que inclusive poderia ensejar a retificação dos dados já existentes. A lei foi, então, declarada inconstitucional em

7 O jargão tem origem na manchete de capa da revista *The Economist*, de 06 de maio de 2017 "*The world's most valuable resource is no longer oil but data*", disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data; Acesso em: 27 set. 2025.

razão do reconhecimento ao direito de autodeterminação informacional da população alemã, que estaria sendo objeto de violação (DONEDA, 2019, p. 164-167).

Em síntese, entendeu a Corte alemã que a autodeterminação informacional resulta do poder de decisão sobre quais informações individuais alguém pode fornecer sobre si mesmo, bem como em que circunstâncias (MENDES, 2020, p. 228), ou seja, os limites em que os dados de um indivíduo podem efetivamente ser utilizados, pois seu maior objetivo é proporcionar controle sobre as próprias informações (DONEDA, 2020, p. 168-169).

A partir disto, constata-se que as finalidades atribuídas ao tratamento dos dados pessoais desempenham papel de grande relevância em um juízo de atendimento ao direito à autodeterminação informacional, seja para o tratamento direito, seja no que toca ao compartilhamento de dados pessoais, explicando Bioni *et. al.* (2020, p. 46) que

> O princípio material por detrás das normas de compartilhamento de dados consiste na diferenciação de acordo com a proximidade entre finalidade do levantamento e a nova finalidade perseguida com o compartilhamento. Aqui o princípio da vinculação finalística revela, mais uma vez, sua importância fundamental. O tratamento autorizado dos dados está restrito à finalidade que determinou seu levantamento. Toda mudança de finalidade representa uma nova intervenção nos direitos informacionais, e essa intervenção é tanto mais gravosa, quanto díspares forem a finalidade original e a finalidade que determina o compartilhamento. E, por conseguinte, as exigências a que deve estar submetido o compartilhamento serão tanto mais rigorosas quanto maior for a disparidade desses fins (BIONI, *et. al.,* 2020, p. 46).

Estas exigências devem ser encaradas sob a ótica do dever de transparência, necessária para conferir credibilidade nos atos de tratamento de dados pessoais e processamento da informação, haja vista que tais procedimentos devem estar abertos a serem desafiados pelos titulares envolvidos, razão pela qual "a qualidade, acessibilidade e compreensibilidade da informação são tão relevantes quanto ao seu nível de sensibilidade (VAINZOF, 2018, p. 56).

Para o jurista Hoffman-Riem (2021, p. 6), referida decisão pode ser considerada uma verdadeira *"landmark decision"*, haja vista que, além de reconhecer e definir o conceito e limites da autodeterminação informacional, serviu de alicerce para o desenvolvimento do direito à proteção de dados pessoais na Alemanha e no continente europeu como

um todo. Doneda (2020, p. 168) ainda acrescenta que a decisão também exerce grande influência sobre os países do sistema romano-germânico.

É curioso notar como a história se repete. Assim como na Alemanha, em 1983, o Brasil também teve – ainda que quase quarto décadas após – sua *landmark decision* acerca do reconhecimento da autodeterminação informacional e, de quebra, da proteção de dados pessoais como direitos fundamentais. Guardadas as devidas proporções, não se pode deixar de notar a semelhança do surgimento destes direitos fundamentais no ordenamento jurídico brasileiro, eis que também teve seu reconhecimento chancelado pela corte constitucional, o Supremo Tribunal Federal, quando do julgamento que declarou inconstitucional a Medida Provisória nº 954/2020. O objetivo da norma era autorizar o compartilhamento de informações e dados pessoais de cidadãos brasileiros para o Instituto Brasileiro de Geografia e Estatística (IBGE), órgão responsável pelo recenseamento da população (BRASIL, 2020).[8]

Embora não positivado expressamente na Constituição Federal, tanto a autodeterminação informacional quanto a proteção de dados pessoais merecem o *status* de direitos fundamentais, sendo que mesmo em outros países em que tais direitos foram reconhecidos com igual peso e natureza de forma autônoma, constata-se na experiência internacional uma paulatina incorporação destes direitos no texto constitucional (SARLET, 2021, p. 22).

Isto porque, a própria Constituição Federal permite a abertura do rol de direitos fundamentais previstos no artigo 5º, conforme disposição do parágrafo segundo desse mesmo dispositivo. Assim, é possível trabalhar uma interpretação constitucional sistemática, identificando na autodeterminação informacional elementos comuns em outros direitos fundamentais a ela relacionados, bem como sua identificação como um direito fundamental autônomo (FREITAS; FERREIRA, CEVEDON, 2020, p. 20).

Vale ponderar que a própria concepção de autodeterminação informacional não é absoluta e, como direito fundamental que é, também pode sofrer limitações, a depender de outros direitos. De outro lado, há casos em que a autodeterminação informacional deverá

8 Na paradigmática decisão, reconheceu-se que "A proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos, extraídos da garantia da inviolabilidade da intimidade e da vida privada (art. 5º, X), do princípio da dignidade da pessoa humana (art. 1º, III) e da garantia processual do habeas data (art. 5º, LXXII), previstos na Constituição Federal de 1988" (BRASIL, 2020).

ser compreendida em sua máxima extensão, como apontaram Eduardo Viana, Lucas Montenegro e Orlandino Gleizer (2020, p. 47) quando de seu parecer sobre consulta formulada a respeito de projeto de lei em trâmite para regular o uso de dados pessoais nas atividades de segurança pública e persecução penal no Brasil. Concluem os referidos juristas que a autodeterminação informacional: (i) é um direito fundamental que visa proteger o livre desenvolvimento da personalidade; (ii) como tal, impõe um "dever de abstenção geral do Estado em relação a todo e qualquer dado pessoal", evitando-se aos cidadãos uma sensação de constante vigilância e privilegiando o livre arbítrio e espontaneidade humanos; (iii) o Estado somente pode atuar em estrita observância à lei, ficando consequentemente impedido de operar atos de tratamento de dados pessoais sem prévia previsão legal, o que demanda o cumprimento das diretrizes quanto às reservas de lei e parlamentar e da proporcionalidade.

Nas palavras de Roberta Mauro Medina Maia (2019, p. 148), "Se dados pessoais são hoje bem jurídico", logo, é inequívoca a necessidade de tutelá-los, razão pela qual se fez necessário legislar sobre os aspectos extrapatrimoniais daquilo que hoje é tido como um verdadeiro ativo econômico, mas que – noutra faceta mais relevante – também exprime titularidade e, com isso, a necessidade de controle. Com efeito, precisou o legislador inclusive determinar a quem os dados pertencem, o que, empoderando o titular[9], dando-lhe controle, conferindo-lhe a prerrogativa de autodeterminar-se.

Partindo das lições de Castells, se a sociedade informacional encontra na informação sua principal força motriz, os direitos afetados pelo informacionalismo se agigantam em relevância, adentram ao centro do palco e recebem uma carga semântica nova, ressignificada. Assim como na sociedade industrial – objeto de frequente comparação de Castells – os direitos de propriedade (sobre os meios de produção, sobre a produção industrializada, sobre o salário recebido em contraprestação à mão de obra) se encontravam-se no centro das preocupações do Direito, na sociedade informacional a necessidade de controle sobre como o indivíduo se relaciona com suas próprias informações e os efeitos.

Nesse contexto é que se pode concluir que a autodeterminação informacional é a pedra angular dos direitos informacionais. Permitir que um indivíduo integre uma sociedade informacional sem lhe proporcionar

9 Nos termos do artigo 5º, da Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento".

a possibilidade de exercer controle quanto às suas próprias informações significa vulnerabilizá-lo e, consequentemente, inviabilizar o direito fundamental ao livre desenvolvimento de sua personalidade e, por que não dizer, de guiar os rumos de sua própria existência.

4 O desafio intrínseco ao exercício de direitos informacionais

Para os fins do presente trabalho, a expressão "direitos informacionais" deve ser compreendida em sentido amplo e como gênero, abrangendo todos os demais direitos que, como espécie, dependem ou decorrem do elo com a informação para o seu exercício ou manifestação.

Com base na lição de Ana Frazão (2019, p. 49), pode-se afirmar que os objetivos dos direitos informacionais transcendem o próprio individuo, na medida em que, para além da autonomia informativa e dignidade dos próprios titulares dos dados, alcançando até mesmo a higidez da própria democracia. Assim, partindo da premissa de que, no âmbito do Estado Democrático de Direito, o exercício efetivo das competências democráticas depende da ordem jurídica, a nível constitucional e legal, é necessário positivar institutos jurídicos capazes de garantir o desenvolvimento de toda a coletividade de indivíduos que integram a sociedade, assegurando o acesso à informação, seu entendimento esclarecido e, consequentemente, a autonomia cidadã (LANA; CORTIANO, 2020, p. 356).

Dentre o rol de direitos informacionais, a título meramente exemplificativo, partindo da Carta dos Direitos Fundamentais da União Europeia (2000), pode-se elencar os seguintes direitos: (i) proteção de dados pessoais (art. 8º)[10]; (ii) liberdade de expressão e de informação (art. 11º)[11]; (iii) a liberdade das artes e das ciências[12]; e (iv) informação e consulta dos trabalhadores nas empresas (art. 27º)[13]. Vale ressaltar que todos os direitos

10 "1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente."

11 "1. Todas as pessoas têm direito à liberdade de expressão. Este direito compreende a liberdade de opinião e a liberdade de receber e de transmitir informações ou ideias, sem que possa haver ingerência de quaisquer poderes públicos e sem consideração de fronteiras.
2. São respeitados a liberdade e o pluralismo dos meios de comunicação social."

12 "As artes e a investigação científica são livres. É respeitada a liberdade académica."

13 "Deve ser garantida aos níveis apropriados, aos trabalhadores ou aos seus representantes,

acima referidos encontram correspondência no ordenamento jurídico brasileiro, seja mediante previsão constitucional ou infraconstitucional, o que justifica o paralelo com a carta europeia.

Para Zygmunt Bauman (2001), sociólogo polonês reconhecido por identificar a liquidez como um elemento central na sociedade moderna, o acesso à informação – sobretudo em meio digital – passou a ser o direito humano "mais zelosamente defendido" na modernidade. Em complemento, Marcos Wachowicz (2016) afirma que sem a difusão da informação e acesso ao conhecimento, não há como promover o avanço tecnológico extraordinário alcançado pela sociedade informacional. Nas palavras de Boff, Fortes e Freitas (2018, p. 15), o acesso à informação, base para o exercício dos direitos informacionais, pode ser considerado "o grande desafio dos tempos atuais" e, em mesma esteira, Ascenção (2003) sentencia: "a informação é o elemento nuclear que está em jogo".

É nítida, pois, a relevância da informação. O maior desafio, na realidade, encontra-se no controle efetivo sobre a circulação da informação, sobretudo no tocante aos dados pessoais, ou seja, informações relacionadas a um determinado indivíduo, passíveis de identificá-lo ou torná-lo, de algum modo, identificável. Tal dificuldade pode ser explicada pela ótica da liquidez, apontada por Bauman, ou, conforme Ascenção (2012, p. 65), porque "A cultura que se amontoa em livros e papéis, que cada um possui mas são sempre insuficientes, pode ser substituída por uma cultura que se apoia em material digitalizado, de acesso fácil, ubíquo, instantâneo e barato". Logo, a liquidez, a ubiquidade, a instantaneidade, o baixo custo da produção e circulação da informação dificultam seu controle, especialmente em razão das TICs, que adjetivam a informação e viabilizam cada uma das características acima referidas.

Ao contrário do que possa parecer, ao afirmar a necessidade de controle da informação, não se está aqui advogando cegamente pela limitação do acesso à informação. Há casos em que o exercício dos direitos informacionais se efetiva por meio da liberdade de acesso à informação; noutros, por meio da restrição ao acesso, principalmente no contexto dos dados pessoais, em que o exercício do controle – ou melhor, autodeterminação – pelo titular implica verdadeira salvaguarda sobre a limitação quanto à coleta, uso, enfim, ao tratamento indevido dos dados pessoais.

---

a informação e consulta, em tempo útil, nos casos e nas condições previstos pelo direito comunitário e pelas legislações e práticas nacionais."

Esse regime dualista, por si só, já demonstra o paradoxo apontado, bem como a complexidade da questão envolvendo os direitos informacionais.

Mas, indo um pouco além, vale questionar por que em uma sociedade na qual a informação ostenta tamanho protagonismo – como esta que ficou conhecida justamente como a sociedade "informacional" – o acesso a informação seria um desafio? E mais: quais são os obstáculos entre o indivíduo e a informação?

Como ponto de partida para o enfrentamento da questão, pode-se mencionar um efeito negativo do informacionalismo, qual seja, o fenômeno chamado de *"information overload",* que se manifesta na capacidade de viabilização de um fluxo "quase inesgotável" de informação (MAGRANI, 2014, p. 114). Soma-se a isto a multiplicidade de formas de tratamento de dados e as inúmeras possibilidades de aplicação destes na identificação dos indivíduos que, não raras vezes, decorre de técnicas e processos tecnológicos opacos e pouco inteligíveis ao homem médio (LANA; CORTIANO, 2020, p. 357).

Questão de grande importância para o teórico Cass Sunstein (2007, p. 302) é a exclusão digital e a falta de acesso ao conhecimento sobre novas tecnologias que se tornam praticamente essenciais ao desenvolvimento de ações cotidianas. Ao tratar deste ponto em específico, Ivar Hartmann (2013, p. 88-89) destaca que se o acesso à Internet (e, consequentemente à informação) é reconhecido como um direito fundamental, também há que se garantir informação a respeito de como acessar (ou buscar) acesso à informação, trazendo à tona a ideia de *"information literacy training"*). Inclusive, segundo o autor, a ausência desse "treinamento" representaria a violação de direitos sociais informacionais.

A referida opacidade no tratamento de dados pessoais é bastante sensível e demanda atenção tanto daqueles que arquitetam e desenvolvem novas tecnologias movidas a dados, quanto dos operadores do Direito, responsáveis por arquitetar o ambiente normativo-regulatório endereçando problemas ligados à privacidade, proteção de dados pessoais e, enfim, à garantia da autodeterminação informacional e exercício de direitos informacionais.

Neste sentido, Ana Frazão (2019, p. 38-39) alerta para a dificuldade de acesso a medidas de *accountability,* ou seja, de mecanismos de auditoria e controle, especialmente no tocante ao emprego de tecnologias baseadas em algoritmos e no *Big Data,* apontando como medidas necessárias à

mitigação de riscos processos voltados à aferição da qualidade dos dados e de seu processamento. O controle da qualidade dos dados estaria relacionado aos atributos da veracidade, exatidão precisão, acurácia e pertinência quanto às finalidades do tratamento, enquanto o controle da qualidade do processamento dos dados trataria mais especificamente da idoneidade da tecnologia empregada nos atos de tratamento de dados.

Para Thiago Luís Santos Sombra (2019, p. 209), o termo *"accountability"* vai além, partindo-se "(d)o pressuposto de que uma ordem político-democrática se consolida e se legitima mediante a responsabilização de uns perante outros, tendo em vista uma relação balizada pelo exercício de manifestações de poder".

Assim, tanto a possibilidade de exigir a prestação de contas quanto aos atos de tratamento de dados pessoais realizados, quanto a de permitir a responsabilização do agente de tratamento envolvidos dependem de transparência. Nesse contexto, a transparência qual se refere à possibilidade de compreensão da interface de comunicação adotada (ou disponibilizada) por um determinado agente de tratamento, bem como dos parâmetros utilizados para a obtenção da informação resultante do processamento de dados (HOFFMANN-RIEM, 2021, p. 87).

Ocorre que, ante ao desenvolvimento acelerado de novas tecnologias e formas de fluxos informacionais, sobretudo aqueles ocorridos em meio digital, a tutela jurídica dos direitos informacionais ainda vem sendo amadurecida nos ordenamentos jurídicos a nível internacional, procurando o Brasil, aos poucos, acompanhar as novas ondas geracionais de leis (inclusive em matéria de privacidade e proteção de dados pessoais). Nesse sentido, constata Gustavo Tepedino (2009, p. 17) que tal avanço tecnológico altera de forma radical a própria técnica legislativa, cada vez mais composta por cláusulas abertas, deveres gerais de conduta e normas de caráter principiológico. Isto faz da norma ambiente mais permeável, permitindo ao intérprete adaptar a aplicação de regras às particularidades do caso concreto.

Em relação à permeabilidade normativa, vale ressaltar que embora a origem do conceito de autodeterminação informacional remonte à década de 1980, percebe-se que o mesmo ainda se encontra em franca evolução, necessitando inclusive da ação do tempo para uma melhor acomodação às tecnologias hoje existentes, às suas finalidades e forma de sua utilização, bem como ao contexto normativo atualmente vigente.

Nesse sentido, Lawrence Lessig (1996, p. 41) faz interessante análise a respeito de Constituições concebidas no passado, em épocas em que a tecnologia existente era "imperfeita", afirmando que

> Nesse mundo, a liberdade reinava, não tanto porque a lei positiva a criava; mas porque as tecnologias imperfeitas se submetiam à justiça. Quando as tecnologias daquele mundo mudam, nós nos confrontamos com uma escolha. Nós podemos permitir que a ideia de eficiência tecnológica impere nesse novo espaço digital fazendo com que as liberdades protegidas pela Constituição se esvaziem; ou nós podemos recriar as esferas de liberdade para superar àquelas pensadas em um contexto de imperfeição tecnológica.

Seguindo a mesma linha de Lessig, o Supremo Tribunal Federal na emblemática decisão em que restaram reconhecidos os direitos à autodeterminação informacional e à proteção de dados pessoais, o Ministro Gilmar Mendes, em seu voto, faz o importante registro de que "nunca foi estranha à jurisdição constitucional a ideia de que os parâmetros de proteção dos direitos fundamentais devem ser permanente abertos à evolução tecnológica" (BRASIL, 2020, p. 12).

Observe-se que o jurista italiano Stefano Rodotà (2008, p. 41) foi cirúrgico ao identificar um dos principais fatores que complexificam a possibilidade de exercício de direitos informacionais, ao explicar que essa "nova angústia nasce da consciência da forte defasagem entre a rapidez do progresso técnico-científico e a lentidão com que amadurece a capacidade de controle dos processos sociais que acompanham tal progresso". Portanto, ainda que se pensem instrumentos normativos para assegurar a autodeterminação informacional e o exercício de direitos informacionais, por vezes tal tarefa parecerá inócua, tendo em vista a diferença da velocidade na qual evoluem as TICs, quando comparadas aos instrumentos jurídico-institucionais.

É por isto que Rodotà (2008, p. 41) alerta para a notória dificuldade em se regular uma realidade em ritmo de contínua e acelerada transformação. Tal conclusão é corroborada por Hoffmann-Riem (2021, p. 7-8), que aponta que o advento de inovações – especialmente aquelas de natureza disruptiva – coloca em xeque a efetividade dos instrumentos jurídicos tradicionais, provocando reflexão acerca da medida em que seriam necessários novos institutos ou modelos de governança.

Assim, constata-se que as TICs contribuíram decisivamente para com as características que definem a sociedade informacional – informacionalismo, globalização e funcionamento em rede – bem como

para o surgimento de um novo ambiente que desafia a noção de tempo e espaço.

O território digital sem fronteiras criado por meio dessas tecnologias, denominado ciberespaço, torna praticamente livre a produção e circulação da informação, do conhecimento, de os bens intelectuais etc., razão pela qual Marcos Wachowicz (2016), também alerta para a complexidade do exercício dos direitos informacionais em decorrência da inexistência de um direito positivo interno positivo capaz de solucionar problemas de forma eficiente ante ao efeito transfronteiriço das relações sociais modernas, que invariavelmente encontrarão limites na própria possibilidade de atuação soberana do Estado e sua incapacidade em regulamentar o ciberespaço.

São estes, portanto, alguns dos grandes problemas a serem superados no âmbito da sociedade informacional, pois ao mesmo tempo em que desafiam a livre circulação da informação, essencial para a concretização de uma série de direitos informacionais ligados ao acesso à informação, também podem fragilizar a autodeterminação informacional dos indivíduos, sobretudo no que concerne à proteção dos dados pessoais dos respectivos titulares.

5 Conclusão

É conhecida a dificuldade do Direito em regular adequadamente as relações sociais desenvolvidas no âmbito de uma sociedade que encontra na rápida evolução da tecnologia e no crescimento exponencial da circulação de informações o seu *status quo* atual.

Por isto, uma vez apresentados os principais elementos que caracterizam a etapa civilizatória atual, que vem sendo denominada de sociedade informacional, e a importância da informação e das tecnologias que viabilizam sua circulação para o desenvolvimento das relações humanas, demonstrou-se o papel da autodeterminação informacional como direito que dá suporte a diversas outras garantias individuais exercidas ou manifestadas graças ao elo com a informação.

Nada obstante, um repensar crítico quanto à estrutura institucional e sobretudo normativa já existentes, bem como a busca por uma aproximação colaborativa entre diferentes nações e blocos econômicos, de modo a buscar uma compreensão coletivista do fenômeno do informacionalismo e suas consequências, aparentam ser medidas salutares e cada vez mais necessárias.

Da privacidade até a manifestação pública do pensamento individual, é o controle – e, mais, a medida do controle – sobre a circulação da informação que ditará o grau de proteção ou de permissibilidade do exercício de direitos informacionais.

Essa dualidade é que pode ser entendida como o aludido paradoxo ao exercício de direitos informacionais em plena sociedade informacional, haja vista que, quanto mais avançam as TICs, maiores são as possibilidades de circulação da informação. Por outro lado, quanto mais informações circulam, mais difícil é o controle destas.

A autodeterminação informacional, portanto, ao mesmo tempo em que se vê ameaçada, é, também, a medida de salvaguarda que servirá de antídoto aos males que a afligem.

Referências

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 03/2013 on purpose limitation.** 2013. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf Acesso em: 27 set. 2025.

ASCENSÃO, José de Oliveira. **Propriedade Intelectual e Internet**. Texto apresentado na Conferência II Cibernética, Florianópolis, 14.11.2003. p. 25. Disponível em: https://www.fd.ulisboa.pt/wp-content/uploads/2014/12/Ascensao-Jose-PROPRIEDADE-INTELECTUAL-E-INTERNET.pdf Acesso em: 27 set. 2025.

ASCENSÃO, José de Oliveira. **Questões Críticas do Direito da Internet**. *In* WACHOWICZ, Marcos; PRONER, Carol (org.). Inclusão tecnológica e Direito à Cultura: movimentos rumo à sociedade democrática do conhecimento (p. 39-68). Florianópolis: Fundação Boiteux, 2012.

BAUMAN, Zygmunt. **Modernidade líquida.** Rio de Janeiro: Zahar, 2001.

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

BIONI, Bruno; *et. al.* **Proteção de dados no campo penal e de segurança pública: nota técnica sobre o Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal**. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2020.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade: do direito às novas tecnologias na sociedade da informação.** Rio de Janeiro: Lumen Juris, 2018.

CASIMIRO, Sofia de Vasconcelos. **Novas guerras em novos campos de batalha: o RGPD europeu e as gigantes tecnológicas norte-americanas.** *In* WACHOWICZ, Marcos (org.). Proteção de dados pessoais em perspectiva: LGPD e RGPD na ótica do direito comparado (p. 104-125). Curitiba: Gedai, UFPR, 2020.

CASTELLS, Manuel. **A sociedade em rede.** 21ª ed. São Paulo: Paz e Terra, 2020.

CRAWFORD, Kate; SCHULTZ, Jason. **Big data and Due Process: toward a Framework to Redress Predictive Privacy Harms.** Boston College Law Review, v. 55, n.1, 2014.

CRUZ E SILVA, Rodrigo Otávio. **Sociedade informacional, direitos autorais e acesso: o problema das licenças compulsórias de obras literárias esgotadas no Brasil.** 2020. 319 f. Tese. Doutorado em Direito. Curitiba-PR, Universidade Federal do Paraná, 2020.

CUKIER, Kenneth; MAYER-SCHÖNBERGER. **Big Data: a revolution that will transform how we live, work and think.** Mariner Books: Boston, 2014.

CUKIER, Kenneth; MAYER-SCHÖNBERGER. **The Rise of Big Data. How It's Changing the Way We Think About the World.** Foreign Affairs, Vol. 92, n. 3, 2013.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados.** 2ª ed. São Paulo: Thomson Reuters, 2019.

FRAZÃO, Ana. **Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados.** *In* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro (p. 23-52). São Paulo: Thomson Reuters Brasil, 2019.

FREITAS, Cinthia Obladen de Almendra; FERREIRA, Heline Sivini; CEVEDON, Ricardo. **A bolha informacional e os riscos dos mecanismos de busca na personalização do usuário de internet: reflexões sobre o direito à autodeterminação informacional.** Revista

Brasileira de Direito, Passo Fundo, vol. 16, n. 3, p. 1-24, Setembro-Dezembro, 2020.

HAN, Byung-Chul. **No enxame: perspectivas do digital.** Trad. Lucas Machado. Petrópolis: Vozes, 2018.

HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital: Transformação digital; desafios para o direito.** Trad. Italo Fuhrmann. Rio de Janeiro: Forense, 2021.

LANA, Alice de Perdigão; CORTIANO, Marcelle. **Direito à autodeterminação informativa e o exercício democrático: reflexões sobre as experiências alemã e brasileira.** *In* WACHOWICZ, Marcos (org.). Proteção de dados pessoais em perspectiva: LGPD e RGPD na ótica do direito comparado (p. 355-385). Curitiba: Gedai, UFPR, 2020.

LESSIG, Lawrence. **Reading The Constitution in Cyberspace**. Emory Law Review, wv. 45, p. 869-910, 1996.

MAGRANI, Eduardo. **Democracia conectada: a internet como ferramenta de engajamento político-democrático.** Curitiba: Juruá, 2014.

MENDES, Laura Schertel. **Autodeterminação informacional: origem e desenvolvimento conceitual na jurisprudência da Corte Constitucional alemã.** *In* CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel (coord.). Lei Geral de Proteção de Dados (Lei nº 13.709/2018): a caminho da efetividade: contribuições para a implementação da LGPD (p. 211-241). São Paulo: Thomson Reuters, 2020.

SARLET, Ingo Wolfgang. **Fundamentos Constitucionais: O Direito fundamental à proteção de dados.** *In.* DONEDA, Danilo *et. al.* Tratado de proteção de dados pessoais. Rio de Janeiro: Forense (p. 21-60), 2021.

SUNSTEIN, Cass. **Republic.com 2.0**. Princeton University Press, 2007.

THE ECONOMIST. **The world's most valuable resource is no longer oil but data".** Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data Acesso em: 27 set. 2025.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia (2000/C 364/01).** Jornal Oficial das Comunidades Europeias, 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_

pt.pdf Acesso em: 27 set. 2025.

VAINZOF, Rony. **Dados pessoais, tratamento e princípios.** *In* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: RT, 2018.

VIANA, Eduardo; MONTENEGRO, Lucas; GLEIZER, Orlandino. **A esfera protegida dos dados pessoais e as intervenções informacionais do Estado.** Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2020/12/NOTA-T%C3%89CNICA-PROTE%C3%87%C3%83O-DE-DADOS-NO-CAMPO-PENAL-E-DE-SEGURAN%C3%87A-P%C3%9ABLICA-VF-31.11.2020.pdf Acesso em: 27 set. 2025.

WACHOWICZ, Marcos. **O "novo" direito autoral na sociedade informacional.** *In*. LEITE, José Rubens Morato; WOLKMER, Antonio Carlos. (Org.). Os "novos" Direitos no Brasil, 3ª ed. São José dos Campos: Saraiva Jur, 2016.

Capítulo 2

TECNOLOGIAS DE RECONHECIMENTO FACIAL E SEGURANÇA PÚBLICA: AS DUAS FASES DO MOVIMENTO BRASILEIROS DE REGULAÇÃO

Diogo Dal Magro[1]
Cinthia Obladen de Almendra Freitas[2]

1 Introdução

As tecnologias de reconhecimento facial têm sido elencadas como potentes ferramentas na área da Segurança Pública. Todavia, movimentos sociais e acadêmicos recentes têm levantado questionamentos éticos, sociais, políticos, jurídicos e também democráticos sobre os usos estatais dessas tecnologias em ambientes públicos urbanos. Consequência desses debates foi o banimento dessas tecnologias levados a cabo por cidades e estados dos Estados Unidos da América, e mais recentemente, a restrição do uso de tecnologias de reconhecimento facial para monitoramento, na União Europeia.

O presente estudo, no entanto, para além de refletir apenas os impactos diretos e isolados da aplicação de tais tecnologia, propõe realizar uma análise de quais caminhos percorridos pelo Brasil para regulação de tecnologias de reconhecimento facial. Por certo, trata-se de um território delicado. Essas tecnologias são empregadas para aprimorar a Segurança Pública, mas há debates em que o uso indiscriminado pode comprometer direitos e liberdades fundamentais. Também os riscos de monitoramento em massa sem a adequada regulamentação, podendo erodir a privacidade individual e restringir a liberdade de expressão. Nesse contexto, a problemática recai sobre a participação política, na medida em que os

1

2 Professora Titular da PUCPR. Professora Permanente do Programa de Pós-Graduação em Direito (PPGD) da PUCPR. Doutora em Informática Aplicada. Membro consultora da Comissão de Direito Digital e Proteção de Dados da OAB/PR. Membro Consultora do Instituto Nacional de Proteção de Dados (INPD). E-mail cinthia.freitas@pucpr.br

processos democráticos podem ser afetados caso os cidadãos se sintam vigiados e restringidos em suas ações públicas.

Nesse contexto, o problema de pesquisa se resume na seguinte indagação: Como as tecnologias de reconhecimento facial vem sendo reguladas pelo Brasil? A hipótese de pesquisa reside na assertiva de que o Brasil, antes de adotar uma estratégia regulatória genuinamente nacional, tem sido afetado pelos movimentos, primeiro, de banimento de aplicações de tecnologias de reconhecimento facial ocorrido nos Estados Unidos da América e, segundo, pelo movimento europeu de regulação de tecnologias de reconhecimento facial, inseridas no contexto da regulação da Inteligência Artificial.

O objetivo geral é analisar como as propostas legislativas brasileiras, de âmbito municipal, estadual e federal, sofrem influências de movimentos como os de banimento de tecnologias de reconhecimento facial no Estados Unidos da América e do processo da União Europeia de regulação de tecnologias de reconhecimento facial inseridas no contexto de regulação da Inteligência Artificial. Assim, inicia-se apresentando as justificativas da sociedade civil pró-banimento da aplicação de tecnologias de reconhecimento facial em algumas cidades dos Estados Unidos da América, para, na sequência, apresentar o modelo adotado pela União Europeia no contexto do Regulamento Europeu Inteligência Artificial. Por fim, se analisa as propostas legislativas brasileiras, influenciadas pelos setores acadêmico e social brasileiro, sobre a aplicação de tecnologias de reconhecimento facial. Consequentemente, o trabalho analisa como as propostas sofreram alterações, decorrentes das influências dos movimentos americano e europeu.

O método de abordagem utilizado para desenvolvimento da pesquisa foi o hipotético-dedutivo, sendo os procedimentos e as técnicas a pesquisa bibliográfica e documental. Parte-se da premissa de que tecnologias de reconhecimento facial aplicadas pela Segurança Pública brasileira foram objeto de propostas legislativas a partir de 2020, sendo que, nesse período, houve uma mudança no processo de normatização, decorrente de influências dos movimentos de regulação dessas tecnologias no contexto norte-americano e europeu. O foco do estudo encontra-se no cenário brasileiro, portanto, é apontado como essas influências modificaram o caminho brasileiro de regulação dessas tecnologias, sendo possível observar o fenômeno em duas fases distintas.

2 Reflexões a partir de casos de banimentos da aplicação de tecnologias de reconhecimento facial nos Estados Unidos da América

A Cidade e Condado de San Francisco, no estado da California, entabulou o movimento de banimento da aplicação de tecnologias de reconhecimento facial nos Estados Unidos da América. Em 31 de maio de 2019, o *Board of Supervisors promulgou a Ordinance n° 103-19*, introduzindo *o Chapter 19B: Acquisition of Surveillance Technology*, ao *Administrative Code*. Ainda, em 20 de dezembro de 2019, a *Ordinance n° 286-19* foi promulgada, alterando e incluindo, além de outros itens, outras exceções ao banimento do reconhecimento facial, permitindo a aquisição e a retenção da tecnologia sob determinadas circunstâncias (SAN FRANCISCO, 2019).

O processo de discussão e aprovação da legislação que culminou no banimento do reconhecimento facial contou com a participação de instituições, associações e organizações sociais, além de cidadãos, que encaminharam correspondências aos Supervisores, apresentando seu apoio ou oposição ao então projeto de legislação, com as respectivas razões. A *Coalition on Homelessness – San Francisco* também manifestou seu apoio ao então projeto, postulando que que, mesmo que a tecnologia seja "precisa" e não tenha como alvo direto as pessoas de cor, a própria natureza da tecnologia tende a se concentrar nas comunidades mais pobres e desprivilegiadas da cidade, dada a atual estrutura social e econômica da sociedade americana. Trouxe, para isso, o exemplo dos residentes de abrigos, que desde 2004 foram obrigados a submeter a imagens biométricas de seu rosto para se qualificarem para leitos de abrigos de 90 dias. Essa prática imediatamente levou muitos moradores indocumentados a ficarem com medo do uso dessa tecnologia para encontrá-los e deportá-los, e os abrigos viram uma diminuição no uso de indivíduos indocumentados (COALITION ON HOMELESSNESS, 2019).

A *Color Of Change*, ao apoiar o projeto legislativo, postulou que os vieses de dados e algorítmicos em aplicações envolvendo técnicas de reconhecimento facial, uma forma comumente mal utilizada de tecnologia de vigilância, apresenta riscos à sua implantação. O Rekognition, software de reconhecimento facial da Amazon, por exemplo, combinou falsamente um número desproporcionalmente alto de membros negros do Congresso Americano com fotos de pessoas presas. No entanto, mesmo que o

viés fosse de alguma forma eliminado dos algoritmos e bases de dados, afirmou que sua implantação ainda prejudicaria a Segurança Pública e as comunidades negras, levando ao perfilamento (*profiling*) (COLOR OF CHANCE, 2019).

Uma coalizão de vinte e cinco organizações de direito civil assinaram conjuntamente uma carta de apoio ao projeto de legislação. Além das razões concernentes às tecnologias de vigilância de um modo geral, consta um tópico concernente à como a legislação protegeria a população de San Francisco da vigilância facial enviesada. Nesse sentido, a carta afirma que a aplicação dessa tecnologia por agências governamentais representa uma ameaça à Segurança Pública e ao bem-estar das pessoas em San Francisco, independentemente da precisão alcançada pelos algoritmos (ACLU OF NORTHERN CALIFORNIA et al, 2019, p. 4).

A carta aponta que a vigilância facial também alimentará a vigilância governamental invasiva e discriminatória. Isso porque, segundo o documento, as pessoas devem ser livres para viver suas vidas diárias sem que o governo saiba se elas visitam um bar ou uma clínica de aborto, marcham em um comício político ou participam de um serviço religioso. No entanto, com o toque de um botão, a cidade pode adicionar vigilância facial a câmeras de CFTV (Circuito Fechado de Televisão) públicas, luzes de rua inteligentes equipadas com sensores ou até câmeras corporais usadas por policiais, criando uma rede de vigilância em toda a cidade que pode rastrear e reconhecer os moradores enquanto eles se movem pela cidade. (ACLU OF NORTHERN CALIFORNIA et al, 2019, p. 5).

Por fim, a carta aponta que a vigilância facial não tornaria a comunidade de San Francisco mais segura e poderia causar danos graves. Isso porque, esfriaria o engajamento civil e sujeitaria os moradores e visitantes a monitoramento contínuo e contatos potencialmente violentos com a aplicação da lei, se produzidos resultados errôneos. Independentemente da precisão, os sistemas construídos para vigilância facial amplificariam e exacerbariam preconceitos históricos e já existentes prejudicando imigrantes, minorias religiosas, ativistas e pessoas de cor. Assim, uma identificação – precisa ou não – poderia custar a liberdade ou mesmo a vida das pessoas, motivo pelo qual San Francisco deveria se recusar a seguir esse caminho (ACLU OF NORTHERN CALIFORNIA et al, 2019, p. 5).

Já a Cidade de Somerville, no estado de Massachusetts, foi a segunda cidade a banir a aplicação de tecnologias de reconhecimento facial, por meio da *Ordinance n° 2019-16*, aprovada em 27 de junho de 2019, pelo

City Council. A referida legislação adicionou ao *Chapter 9 - Offenses and Miscellaneous Provisions do Code of Ordinances*, uma emenda ao *Article III. - Offenses Against the Person*, introduzindo a subseção 25 (SOMERVILLE, 2019).

Em Somerville, também houve participação social e popular no processo legislativo de aprovação do banimento da aplicação voltada à vigilância facial. A *American Civil Liberties Union* (ACLU), por meio de seu Conselheiro de Políticas de Tecnologia e Liberdades Civis de Massachusetts, enviou um testemunho em apoio à proibição da vigilância facial, em 09 de maio de 2019. De acordo com o documento, são (03) três as principais áreas de preocupação em relação a essas tecnologias: (i) uso não regulamentado da tecnologia; (ii) seus perigos intrínsecos; e (iii) direitos civis e liberdades civis (FALCON, 2019, p. 1).

Com relação ao uso não regulamentado da tecnologia, o texto remete que a ausência – até então – de regulamentação faz com que a disseminação dessa tecnologia ocorra no escuro, sem debate público ou supervisão democrática. As agências governamentais adotavam-na, apesar da ausência de regulamentações de privacidade, de imprecisão da tecnologia e de ameaças que ela representa para sociedades livres e abertas (FALCON, 2019, p. 1).

Já no que concerne aos direitos e liberdade civis, o documento refere que a vigilância facial é uma ameaça a esses, em especial, como a tecnologia de reconhecimento facial afeta os direitos e liberdades da Primeira Emenda da Constituição Americana. Isso porque, conforme o texto da carta, se o governo puder rastrear todos que vão a um local de culto, um comício político ou procuram atendimento médico reprodutivo ou de uso de substâncias, haveria perda da liberdade de expressão (falar livremente), impossibilitando criticar livremente o governo e exercer o direito de liberdade de crença e de consciência. Além disso, cita o exemplo da China, afirmando que o governo autoritário utiliza vigilância facial para realizar controle social – *social score* (FALCON, 2019, p. 1-2).

A Cidade de Berkeley, no estado da California, foi a quarta cidade a banir a aplicação de técnicas de reconhecimento facial no país. O *Municipal Code of Ordinances* já contava, desde 2018, com o *Chapter 2.99 – Acquisition and Use of Surveillance Technology*, sendo que, em 29 de outubro de 2019, o *City Council* aprovou a *Ordinance 7676-NS*, introduzindo no item *2.99.020 – Definitions* o conceito de reconhecimento facial, além

de acrescentar no item *2.99.030 – City Council Approval Requirement* as provisões de banimento do reconhecimento facial (BERKELEY, 2018).

Em 10 de outubro de 2019, 14 (quatorze) organizações/instituições assinaram conjuntamente uma carta de suporte ao então projeto de legislação que visava banir a aplicação de técnicas de reconhecimento facial nos EUA. O documento menciona a divulgação de um relatório sobre tecnologia de vigilância, em 25 de junho de 2019, por David Kaye, então Relator Especial para a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão da ONU, o qual pede uma moratória mundial no que se refere ao uso de tecnologias de vigilância, como é o caso do reconhecimento facial. Segundo o relator, as tecnologias de vigilância podem significar uma interferência aos Direitos Humanos, como o direito à privacidade, liberdade de expressão, associação e reunião, crença religiosa, não discriminação e participação pública e, contudo, essas tecnologias não estão sujeitas a nenhum controle global ou nacional efetivo (SECURE JUSTICE et al, 2019, p. 2).

A carta também menciona que a vigilância pode impor um *status quo* autoritário, impedindo uma mudança social positiva, citando exemplos de que jovens explorando a sexualidade podem não se sentir à vontade para visitarem um bar gay pela primeira vez ou muçulmanos podem ficar receosos ao frequentar mesquitas. Assim, a vigilância pelo reconhecimento facial pode dificultar a formação de relacionamentos inter-raciais e do mesmo sexo ou ajudar pessoas a fugir da escravidão e outras formas de perseguição (SECURE JUSTICE et al, 2019, p. 4).

O documento conclui que a saúde da democracia depende da capacidade de, ocasionalmente, rejeitar a tecnologia de reconhecimento facial, por ser demais radical para ser utilizada na comunidade americana. Isso porque, a população já está perdendo a capacidade de se mover e de associar livremente, devido ao histórico de localização poder ser rastreado por leitores de placas de veículos ou por torres de telefonia móvel. Assim, o reconhecimento facial seria mais uma tecnologia colocada a esse dispor (SECURE JUSTICE et al, 2019 p. 4).

A Cidade de Brookline, no estado de Massachusetts, foi a quinta cidade a aprovar uma legislação banindo o uso de sistemas baseados em reconhecimento facial. Em 11 de dezembro de 2019, a cidade aprovou a introdução do *Article 8.39 – Ban on Town Use of Face Surveillance, ao General By-Laws of the Town of Brookline* (BROOKLINE, 2019). A proposta legislativa para banimento do uso de sistemas baseados em

reconhecimento facial em Brookline foi submetida por Amy Hummel, membro do Advisory Committee. O documento conta com uma descrição das razões da proposta legislativa, sendo o primeiro tópico sobre a tecnologia de reconhecimento facial como uma afronta a uma sociedade livre. Nesse sentido, o efeito da tecnologia é o de forçar pessoas a carregarem um crachá de identificação, de modo que pessoas livres não precisam e não devem fazê-lo, principalmente sendo permanente, imutável e biométrico. Desse modo, a tecnologia facilita o rastreamento de movimentos em ambientes públicos, hábitos e associações de cada indivíduo, na medida em que pessoas que desejam buscar tratamento para transtorno por uso de substâncias ilícitas, visitar reuniões de alcoólicos anônimos, procurar atendimento de saúde reprodutiva, visitar amigos e familiares, ou então participar de protestos políticos, não podem deixar seus rostos em casa, não havendo dissociação entre a pessoa e a identidade. Ainda, dados coletados para fins de reconhecimento facial podem ser facilmente armazenados, compartilhados e agregados para mapear diferentes atividades, ligações, padrões e preferências dos indivíduos, sendo que tais capacidades são uma maldição em uma sociedade livre (TOWN OF BROOKLINE, 2019).

O segundo ponto aborda a falibilidade do software em classificar desproporcionalmente mulheres e pessoas de cor, e que essas imprecisões colocam em condição de desigualdade alguns indivíduos e grupos em maior risco de identificação como "falsos positivos", o que é prejudicial e pode até ser traumático. O problema é exacerbado pelos preconceitos raciais e outros preconceitos já estarem embutidos em bancos de dados existentes, como é o caso de bancos de dados de aprisionados, os quais podem conter imagens capturadas após a prisão, podendo incluir os rostos de indivíduos que podem ser totalmente inocentes. Ainda, quando há falsos positivos, o trauma e o estigma que afetam as vítimas do erro continuam mesmo após os erros serem oficialmente corrigidos (TOWN OF BROOKLINE, 2019).

O terceiro tópico aponta como a legislação e as políticas são inexistentes ou totalmente inadequadas em determinadas situações. Assim como outras tecnologias novas e emergentes, o uso de software de reconhecimento facial está rapidamente se tornando onipresente nos setores público e privado, antes mesmo da maioria das comunidades poder responder com uma legislação apropriada. Também a monetização e a facilidade de aquisição de tecnologia de vigilância, incluindo as tecnologias de reconhecimento facial, tornam a disseminação do uso não regulamentado não apenas certa, mas rápida. A infraestrutura de vigilância, criada inteiramente fora de qualquer supervisão ou estrutura regulatória é

ruim o suficiente em si mesma. Por sua vez, permitir o reconhecimento facial não regulamentado apenas agravaria esse problema, incentivando a proliferação de um estado de vigilância, baseado na suspeita e desconfiança de todas as pessoas (TOWN OF BROOKLINE, 2019).

Ao aprovar uma lei semelhante em nível local, o quinto tópico conclui arrazoando que há a possibilidade de se juntar às cidades vizinhas que reconhecem os perigos que o uso da tecnologia de reconhecimento facial apresenta para uma sociedade livre, além de demonstrar apoio às propostas federais. Não seria necessário, portanto, aguardar pela distopia digital, na medida em que seria possível agir no presente para proteger e preservar as liberdades para a próxima geração de moradores de Brookline (TOWN OF BROOKLINE, 2019).

O Condado de King (King County), no estado de Washington, foi a vigésima primeira legislação "municipal" a banir o uso do reconhecimento facial. Em 01 de junho de 2021, o King County Council aprovou a *Ordinance 19296*, adicionando ao *Title 2 – Administration,* do *King County Code,* o capítulo *2.67 - Facial Recognition Technology Use* (KING COUNTY, 2021).

Com relação aos comentários presentes no processo legislativo, a *OneAmerica (With Justice for All – Formerly Hate Free Zone)*, organização a enviar correspondência, tem como missão promover os princípios fundamentais da democracia e justiça. Ainda, a OneAmerica é a maior organização de defesa de imigrantes e refugiados no estado de Washington, sendo que, desde 2001, fortalece comunidades de imigrantes e refugiados para promover a democracia e a justiça usando as ferramentas de defesa de políticas, liderança de base e organização comunitária (ONEAMERICA, 2021).

O documento aponta que tecnologias de reconhecimento facial invadem a privacidade, dando poder sem precedentes ao governo. Com relação à imprecisão, assinala que estudos demostram que as tecnologias de reconhecimento facial resultam em falsos positivos, principalmente para pessoas da África Ocidental e Oriental, Ásia Oriental e em mulheres e crianças, o que denota preocupação, dado que mais da metade de todos os imigrantes nos Estados Unidos são mulheres, 27% são asiáticos e 10% são africanos (ONEAMERICA, 2021).

Independentemente da precisão, registra que o reconhecimento facial também permite o racismo sistêmico e a injustiça, vez que agências governamentais podem usar o reconhecimento facial para rastrear

movimentos de indivíduos e associações sem o seu conhecimento ou consentimento, desencorajando a liberdade de expressão e de associação, minando a liberdade de imprensa e ameaçando o livre exercício da religião. Isso tudo poderia afetar a participação de indivíduos indocumentados no ativismo público por medo de que as informações sejam compartilhadas entre as agências de aplicação da lei e as autoridades de imigração. Por fim, ressalta que o uso de reconhecimento facial em sistemas de imigração pode ter impactos severos em comunidades marginalizadas, incluindo auto-peticionários da *Violent Against Women Act* (VAWA) e requerentes e destinatários de vistos T (Vítima de Atividade Criminosa) e U (Vítima de Tráfico Humano) (ONEAMERICA, 2021).

A Cidade de Baltimore, no estado de Maryland, foi a vigésima segunda cidade a aprovar legislação restringindo o uso do reconhecimento facial, ao implementar uma moratória no uso das tecnologias. Em 14 de junho de 2021, o *City Council* aprovou a *Ordinance 21-038*, que fez duas alterações no *City Code*: primeiro, adicionou a *Section 41-4 ao Subtitle 41 Prohibited Contracts, no Article 5 - Finance, Property, and Procurement*; segundo, adicionou o *Subtitle 18. Surveillance ao Article 19 - Police Ordinances* (BALTIMORE, 2021).

No que concerne aos comentários públicos favoráveis ao processo legislativo, destaca-se o documento que é um testemunho de Charles E. Sydnor III, Senador do *Senate of Maryland*, representando o Distrito 44. O testemunho dá conta de que tecnologias de reconhecimento facial desenvolveram-se tão rapidamente que os formuladores de políticas foram deixados para trás enquanto tentavam entender a tecnologia, suas ramificações e usos pelos governos e população. Por isso, trabalhar posteriormente para tentar equilibrar os direitos constitucionais e Segurança Pública é um desafio, mas que pode e deve ser feito. O documento conclui afirmando que não é desejável que direitos sejam prejudicados porque não houve tempo para entender verdadeiramente as consequências do uso dessa tecnologia, discuti-la publicamente e chegar a uma decisão com base nos ideais e princípios democráticos do país (THE SENATE OF MARYLAND, 2021).

Esse processo de equilibrar os direitos fundamentais e face da Segurança Pública foi estruturado, na União Europeia, a partir da regulação da Inteligência Artificial. Se, no contexto dos Estados Unidos da América, conforme aqui apresentado, a regulação, inclusive com processos de banimentos, restrições e moratórias às aplicações de tecnologias de

reconhecimento facial utilizadas na Segurança Pública ocorreu de modo pontual, em cidades e estados conduzindo processos autônomos de regulação, a União Europeia, de modo diverso, estruturou a regulamentação de tecnologias de reconhecimento facial a partir de uma normativa para o bloco. Nesse sentido, são apresentados alguns pontos do modelo europeu de regulação dessas tecnologias, para compreender as diferenças desse processo.

3 O movimento europeu de regulação e restrição de aplicações de tecnologias de reconhecimento facial

Embora na União Europeia os movimentos da sociedade civil e organizações em defesa dos Direitos Humanos também debateram aspectos críticos de tecnologias de reconhecimento facial desde o mesmo período que os movimentos americanos, o processo de regulamentação foi estabelecido posteriormente. Proposto pela Comissão Europeia em abril de 2021 e aprovado pelo Parlamento Europeu e pelo Conselho em dezembro de 2023, o Regulamento Europeu Inteligência Artificial (Regulamento IA – *AI Act*) iniciou o processo de entrada em vigor apenas em 2024, de forma parcial (UNIÃO EUROPEIA, 2024).

Importante esclarecer que o Regulamento Europeu Inteligência Artificial entrou em vigor oficialmente em 1º de agosto de 2024, estabelecendo o primeiro marco regulatório abrangente sobre Inteligência Artificial no mundo. No entanto, a aplicação de suas regras ocorre de forma gradual, já que, em 2 de fevereiro de 2025, passaram a valer as proibições contra usos de Inteligência Artificial considerados de risco inaceitável (como sistemas de "*social scoring*" e manipulação subliminar) e também as obrigações de letramento (literacia/alfabetização) em Inteligência Artificial para provedores e usuários. Em seguida, em 2 de agosto de 2025, entraram em vigor as regras específicas para modelos de uso geral (*General-Purpose AI - GPAI*), que incluem sistemas de Inteligência Artificial de grande escala, como modelos fundacionais (UNIÃO EUROPEIA, 2024).

A partir de 2 de agosto de 2026, o Regulamento passa a ser aplicável de maneira mais ampla, impondo as suas principais obrigações, sobretudo para sistemas classificados como de alto risco, que devem cumprir requisitos rigorosos de segurança, transparência e supervisão humana. Já os sistemas de alto risco que estão integrados a produtos regulados (como dispositivos médicos ou automotivos) têm prazo estendido até 2 de agosto de 2027 para

adequação. Dessa forma, a entrada em vigor do Regulamento Europeu Inteligência Artificial é marcada por uma implementação escalonada, permitindo tempo para adaptação dos diferentes atores e setores impactados (UNIÃO EUROPEIA, 2024).

Conforme o próprio Regulamento, o objetivo da adoção da normativa da União Europeia tem com objetivo a adoção de uma Inteligência Artificial (IA) que seja centrada no ser humano e seja confiável, para, ao mesmo tempo, assegurar a proteção da saúde, da segurança, dos direitos fundamentais contidos na Carta dos Direitos Fundamentais da União Europeia, em especial a democracia, o Estado de direito e a proteção do ambiente, a proteção contra os efeitos nocivos dos sistemas de Inteligência Artificial, além de apoiar a inovação (UNIÃO EUROPEIA, 2024). Dito de outro modo, a normativa visa equilibrar os usos da Inteligência Artificial com a observância dos direitos fundamentais, em especial, os princípios da democracia e do Estado de direito, fortes pilares da União Europeia pós Segunda Guerra Mundial.

Ainda nos considerandos (o de número (14)), o Regulamento afirma que o conceito de "dados biométricos" deve ser interpretado conforme o conceito já existente, na acepção do "artigo 4.º, ponto 14, do Regulamento (UE) 2016/679, do artigo 3.º, ponto 18, do Regulamento (UE) 2018/1725 e do artigo 3.º, ponto 13, da Diretiva (UE) 2016/680." (UNIÃO EUROPEIA, 2024). Isso porque, "os dados biométricos podem permitir a autenticação, identificação ou categorização de pessoas singulares e o reconhecimento de emoções de pessoas singulares." (UNIÃO EUROPEIA, 2024).

É preciso explicar melhor esse ponto. Esse trecho do Regulamento informa que não há a criação de uma definição própria de dados biométricos, mas sim a adoção e a harmonização do conceito já existente em outras normativas da União Europeia, a saber: o *General Data Protection Regulation – GDPR* (Regulamento 2016/679); o Regulamento 2018/1725 (que dispões sobre a proteção de dados pessoais nas instituições da União Europeia) e a Diretiva 2016/680 (que dispõe sobre a proteção de dados pessoais no âmbito penal/policial). Assim, qualquer interpretação ou aplicação do conceito, no âmbito do Regulamento Europeu Inteligência Artificial, deve seguir o que já está consolidado nesses diplomas (UNIÃO EUROPEIA, 2024).

Na prática, significa que informações resultantes de aferições físicas, fisiológicas ou comportamentais que permitam identificar uma

pessoa de forma única (como impressões digitais, reconhecimento por meio da face, reconhecimento de íris, de voz, de padrões de digitação, etc.) são tratadas como dados biométricos, ou seja, com proteção reforçada. O Regulamento ainda vai além e esclarece que dados biométricos não servem apenas para autenticação ou identificação, mas também podem ser usados para categorização (por exemplo, segmentar pessoas por idade, sexo ou características físicas) e até para reconhecimento de emoções, o que amplia o leque de situações em que regras mais restritivas e de maior responsabilidade são previstas pelo Regulamento para serem aplicadas (UNIÃO EUROPEIA, 2024).

Outro considerando (o de número (15)) diferencia as aplicações de identificação biométrica daquelas de verificação biométrica (autenticação), o que acarreta implicações práticas importantes, na medida em que o Regulamento disciplina de modo diverso cada um dos casos (UNIÃO EUROPEIA, 2024).

Na identificação biométrica, o sistema cruza os dados coletados de uma pessoa (por exemplo, sua face captada por uma câmera) com um banco de dados de referência que contém informações de várias outras pessoas, a fim de determinar "quem é" o indivíduo. Essa prática, segundo o Regulamento, usualmente é feita sem o conhecimento ou consentimento prévio do sujeito, o que pode gerar riscos significativos de vigilância em massa e de violação de direitos fundamentais, razão pela qual o Regulamento a classifica como de alto risco ou até como uso proibido em determinados contextos (conforme se explica a seguir) (UNIÃO EUROPEIA, 2024).

Já na verificação biométrica (incluindo a autenticação), a lógica é distinta: os dados biométricos são utilizados apenas para confirmar se a pessoa é, de fato, quem afirma ser, mediante comparação com uma informação previamente fornecida pelo próprio titular. Trata-se de um uso limitado e controlado, geralmente voltado para segurança de dispositivos, serviços ou acessos restritos, como ocorre no desbloqueio de celulares por impressão digital ou no reconhecimento facial para acessar uma conta bancária ou realizar o acesso a um prédio. Por se tratar de uma aplicação direcionada e menos intrusiva, o Regulamento não a submete às mesmas restrições severas da identificação biométrica, embora siga exigindo conformidade com regras de proteção de dados pessoais (UNIÃO EUROPEIA, 2024).

Em outro considerando (o de número (18)), o Regulamento elabora um conceito específico para os chamados sistemas de reconhecimento de emoções, ou seja, sistemas de Inteligência Artificial que tentam

inferir estados emocionais ou intenções de uma pessoa a partir de seus dados biométricos. Esses dados podem envolver expressões faciais ou características vocais ou gestuais, e o regulamento lista exemplos claros de emoções que entram nesse campo, como felicidade, tristeza, raiva, vergonha ou entusiasmo. A ênfase recai no caráter interpretativo da tecnologia, ou seja, não é apenas registrar uma expressão (como um sorriso), mas sim atribuir a essa expressão um estado emocional (como concluir que alguém está feliz) (UNIÃO EUROPEIA, 2024).

Ainda com relação aos sistemas de reconhecimento de emoções, o Regulamento estabelece exceções importantes. Estados físicos, como dor ou fadiga, não se enquadram no conceito de reconhecimento de emoções, o que permite que tecnologias voltadas à segurança no transporte, que detectam cansaço de motoristas ou pilotos, não entram nessa categoria. Da mesma forma, a mera captação de expressões ou gestos visíveis, sem que se faça uma inferência emocional, também está de fora das proibições. Portanto, o Regulamento concentra sua disciplina em usos considerados sensíveis, nos quais há controvérsias em termos de precisão técnica e riscos para a privacidade e autonomia individual (UNIÃO EUROPEIA, 2024).

Outros considerandos ainda: (43) proíbe sistemas de Inteligência Artificial que criem bases de dados de reconhecimento facial a partir da coleta aleatória de imagens da internet ou de câmeras de CCTV, por representarem risco de vigilância em massa e graves violações à privacidade; e (54) classifica como de alto risco os sistemas de identificação biométrica à distância, bem como usos de categorização biométrica e de reconhecimento de emoções (quando não proibidos), pelo potencial de vieses e discriminação, mas exclui dessa categoria a verificação biométrica para autenticação e os sistemas voltados exclusivamente à cibersegurança e proteção de dados (UNIÃO EUROPEIA, 2024).

O regulamento adota uma estratégia central de classificação de sistemas de Inteligência Artificial baseada em níveis de risco, o que, a partir disso, determina as obrigações e restrições aplicáveis em cada caso. A classificação é dividida em 04 (quatro) riscos: (i) risco inaceitável, sendo sistemas de Inteligência Artificial cuja utilização é considerada incompatível com os direitos fundamentais e, por isso, são proibidos; (ii) alto risco, que envolvem aplicações que podem impactar de forma significativa a segurança, a saúde ou os direitos fundamentais, sendo permitidos, mas sujeitos a regras rígidas, como testes de qualidade de dados, documentação técnica, supervisão humana, avaliação de conformidade e registro em

banco europeu; (iii) risco limitado, incluindo sistemas que interagem diretamente com pessoas e que, para evitar engano, devem cumprir obrigações de transparência; e por fim, de (iv) risco mínimo ou inexistente, compreendidas como aplicações consideradas de uso cotidiano e sem impactos relevantes para direitos fundamentais ou segurança, sendo que esses sistemas não estão sujeitos a obrigações específicas pelo regulamento, ficando a adesão a códigos de conduta como algo voluntário (UNIÃO EUROPEIA, 2024).

Entre as aplicações consideradas de risco inaceitável, previstas no Artigo 5º do Regulamento, e, portanto, tidas como práticas proibidas, está a "utilização de sistemas de identificação biométrica à distância em "tempo real" em espaços acessíveis ao público para efeitos de aplicação da lei" (UNIÃO EUROPEIA, 2024). No entanto, o Regulamento estabelece as devidas exceções a essa proibição, de modo que sistemas de identificação biométrica, entre os quais estão contidas as tecnologias de reconhecimento facial, podem ser usados para: (i) "busca seletiva de vítimas específicas de rapto, tráfico de seres humanos ou exploração sexual de seres humanos, bem como a busca por pessoas desaparecidas"; e (ii) "prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas singulares ou de uma ameaça real e atual ou real e previsível de um ataque terrorista" (UNIÃO EUROPEIA, 2024).

Ainda, a terceira exceção à proibição, autoriza o uso dessas tecnologias para (iii) "a localização ou identificação de uma pessoa suspeita de ter cometido uma infração penal, para efeitos da realização de uma investigação criminal, ou instauração de ação penal ou execução de uma sanção penal" (UNIÃO EUROPEIA, 2024). No entanto, para que seja autorizada a utilização dessas tecnologias nesse caso, a pessoa suspeita obrigatoriamente precisa haver cometido uma "das infrações referidas no anexo II e puníveis no Estado-Membro em causa com pena ou medida de segurança privativa de liberdade de duração máxima não inferior a quatro anos" (UNIÃO EUROPEIA, 2024).

As infrações referidas nesse artigo e presente no Anexo II do Regulamento são de natureza grave, nas quais incluem-se terrorismo, homicídio, tráfico de seres humanos, órgãos, armas e materiais nucleares, exploração sexual e pornografia infantil, e crimes que são abrangidos pela jurisdição do Tribunal Penal Internacional, criado pelo Estatuto de Roma (UNIÃO EUROPEIA, 2024).

Note-se, que o processo normativo de regulação que alcança as tecnologias de reconhecimento facial na União Europeia é muito diverso do ocorrido no âmbito dos Estados Unidos da América. O processo regulatório da União Europeia é estruturado e baseado em risco, envolvendo um marco legal abrangente e vinculante que define categorias de risco, obrigações detalhadas e proibições específicas. A União Europeia adota uma abordagem preventiva, priorizando a proteção de direitos fundamentais, a transparência, a não discriminação e a segurança, impondo requisitos rigorosos para sistemas de alto risco ou proibindo usos inaceitáveis.

Nos Estados Unidos da América, pelo contrário, há uma ausência de lei federal abrangente equivalente, de modo que a regulação é fragmentada e setorial, variando conforme o estado, a cidade ou a aplicação. Disso resulta em uma abordagem reativa e descentralizada, onde tecnologias de reconhecimento facial operam sem requisitos uniformes de avaliação de riscos, supervisão humana ou limites claros sobre coleta e uso de dados biométricos, enquanto em outros casos, houve a proibição radical dessas tecnologias.

Desse modo, esses elementos são importantes para que, a partir disso, se passe a compreender como o percurso que o Brasil tem realizado no que concerne à regulação do uso de tecnologias de reconhecimento facial em ambientes públicos se situa na análise intersecionada aqui proposta. Dito em outro modo, considerando esses elementos, qual o caminho que o Brasil tem indicado adotar na regulamentação de tecnologias de reconhecimento facial?

4 A conjuntura regulatória brasileira sobre tecnologias de reconhecimento facial

No contexto nacional, a primeira fase de surgimento de regulação de tecnologias de reconhecimento facial foi influenciada pelo movimento americano, principalmente, visando o banimento dessas tecnologias. De modo semelhante ao ocorrido nos Estados Unidos da América, esse movimento de restringir e banir tecnologias de reconhecimento facial na Segurança Pública brasileira foi descentralizado, tendo sido protagonizado por estados e, principalmente, municípios.

A primeira legislação nacional exclusiva sobre tecnologias de reconhecimento facial foi a Lei n° 6.712, aprovada no Distrito Federal, em 10 de novembro de 2020 (DISTRITO FEDERAL, 2020). A lei do

Distrito Federal traz pontos que merecem comento. Ao dispor sobre o uso de tecnologias de reconhecimento facial na Segurança Pública do Distrito Federal, a legislação criou o conceito de vigilância contínua, entendida, em resumo, como o rastreamento de um indivíduo identificado durante um período superior a 72 (setenta e duas) horas. Na prática, não há nenhuma proibição de uso de técnicas baseadas em reconhecimento facial, sendo somente restringido o tempo de monitoramento do indivíduo, vez que se restringe apenas a vigilância contínua.

A vedação da vigilância contínua levanta uma série de questionamentos sobre o alcance prático dessa proibição. A legislação não estabelece nenhuma medida apta a apurar por quanto tempo perdura o rastreamento, de modo que, pelo que está exposto, não há mecanismos hábeis para que uma pessoa possa se valer a fim de demonstrar eventual transposição desse limite. Por isso, a previsão se torna sem efeito, irrisória, dado que, sem mecanismos tecnológicos capazes de fazer cumprir com o prazo estabelecido e produzir a respectiva prova, a legislação se torna mera política de boas práticas.

Outro ponto é com relação às informações coletadas por tecnologias de reconhecimento facial, consideradas dados pessoais sensíveis e que, portanto, pela referida lei, deve ser respeitada a Lei Federal nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD). Aqui há um imbróglio. A própria LGPD, no seu artigo 4°, inciso III, alínea a, prevê sua não aplicação para o tratamento de dados pessoais realizado para fins exclusivos de Segurança Pública, o que é o caso. Ainda, o §1º do artigo 4° da LGPD também traz previsão de que, em se tratando de Segurança Pública, "o tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei" (BRASIL, 2018).

A não edição, até o momento, de legislação específica pelo Congresso Nacional, implica em lacuna da proteção de dados pessoais tratados com a finalidade de Segurança Pública. Em que pese, portanto, o diploma legal do Distrito Federal conter mandado de observância à LGPD, essa disposição é contrária à própria LGPD. Partindo-se do princípio da hierarquia entre leis federal e estadual (pirâmide normativa), a lei do Distrito Federal – que a editou na competência de ente estadual – não pode violar disposição de lei federal. No campo de existência, validade e eficácia, a lei distrital,

embora cumpra com a premissa de existência, não cumpre com a validade, dado que é contrária a preceitos de lei superior, e, portanto, nesse ponto em comento não pode ser aplicada.

A lei distrital também estabelece um período de 05 (cinco) anos para armazenamento de dados coletados por para fins de aplicação em sistemas de reconhecimento facial, devendo haver a eliminação das informações passado o prazo. No entanto, não resta claro sobre quais informações esse prazo se aplica, se às imagens coletadas, se às imagens que geraram reconhecimento, se aos dados de identificação e as imagens dos reconhecimentos ou outras informações.

Já em 2021, duas propostas legislativas foram apresentadas no Município do Rio de Janeiro e no Estado do Rio de Janeiro, respectivamente. O Projeto de Lei n° 824/2021 foi apresentado em 05 de outubro de 2021, na Câmara Municipal do Rio de Janeiro (CÂMARA MUNICIPAL DO RIO DE JANEIRO, 2021), enquanto o Projeto n° 5440/2021 foi apresentado em 08 de dezembro de 2021, na Assembleia Legislativa do Estado do Rio de Janeiro (ALERJ, 2021). Ambos os projetos possuem texto similar, dispondo sobre a restrição no uso de tecnologias de reconhecimento facial pelo Poder Público.

Os projetos, além de similares, foram elaborados com contribuições dos mesmos pesquisadores, motivo pelo qual ambas as justificativas também são precipuamente semelhantes. A justificativa afirma que diversos locais públicos da cidade possuem tecnologias de detecção de rostos, de temperatura, além de aplicativos de cadastro para visitação, como demonstração de que a cidade utiliza novas tecnologias na área da Segurança Pública (CÂMARA MUNICIPAL DO RIO DE JANEIRO, 2021).

A justificativa também se pauta no movimento de banimentos dessas tecnologias nos Estados Unidos da América e na Europa, retratado anteriormente. Também, destaca o posicionamento da sociedade civil, especialmente uma carta aberta capitaneada pela *Access Now*, em parceria com a *Amnesty International, European Digital Rights* (EDRi), *Human Rights Watch, Internet Freedom Foundation* (IFF) e o Instituto Brasileiro de Defesa do Consumidor (IDEC), se posicionando pelo banimento de tecnologias de vigilância biométricas em espaços públicos (ACESS NOW et al, 2021).

Impulsionado pelo movimento americano, até 30 de junho de 2022, municípios (Florianópolis, Porto Alegre, Vitória, Salvador, Belo

Horizonte, Contagem, Curitiba, Niterói, São Gonçalo, Campinas e São Paulo) e estados (Minas Gerais, Bahia, Ceará e São Paulo) brasileiros possuíam projetos de lei protocolados nas Câmaras de Vereadores para restringir a utilização de tecnologias de reconhecimento facial pelo poder público municipal. A iniciativa #SaiDaMinhaCara, articulada pelas organizações Coding Rights, MediaLab/UFRJ, Rede Lavits, Instituto Brasileiro de Defesa do Consumidor (IDEC) e Centro de Estudos de Segurança e Cidadania (CESeC), mobilizou mais de 50 (cinquenta) parlamentares nas esferas federal, estadual e municipal, a apresentarem projetos de lei banindo o uso de reconhecimento facial (DAL MAGRO, 2022).

O cenário brasileiro começou, entretanto, começou a mudar. Se, até então, as iniciativas eram municipais e estaduais, ou seja, descentralizadas e isoladas, a partir de 2022, é preciso registrar que o tema do uso e regulação de tecnologias de reconhecimento facial entrou em pauta nas atividades da CJSUBIA – Comissão de Juristas responsável por subsidiar elaboração de substitutivo sobre inteligência artificial no Brasil, criada pelo Ato do Presidente do Senado Federal, nº 4, de 2022, de 17 de fevereiro de 2022 (SENADO FEDERAL, 2022).

Nos debates da comissão, destaca-se pronunciamento de André Lucas Fernandes, representando o Instituto de Pesquisa em Direito e Tecnologia do Recife, durante a 3ª Sessão Ordinária, ocorrida em 29 de abril de 2022 (CJSUBIA, 2022). O painelista pontuou que a graduação dos riscos decorrentes do emprego da Inteligência Artificial envolve, necessariamente, uma análise dos bens jurídicos tutelados. Nesse sentido, há bens jurídicos que já são protegidos em maior grau do que outros, levando à duas medidas possíveis: (i) uma análise setorial para compreender a necessidade de construção das diretrizes que devem estar na legislação e daquelas que podem aguardar regulamentação futura e (ii) "seleção de onde não queremos ir, como nos casos de reconhecimento facial para segurança pública." (CJSUBIA, 2022).

Como se observa, o contexto regulatório brasileiro sobre tecnologias de reconhecimento facial inaugurou um novo capítulo em 2022, o que é considerado, nessa pesquisa, como a segunda fase. Embora a lei do Distrito Federal e os projetos de lei municipais e estaduais já estivessem presentes em Câmaras de Vereadores e Assembleias Legislativas, o tema passou a se fazer presente na agenda do Congresso Nacional, efetivamente, somente a partir de 2022. E é por isso que, em nível federal, o Brasil discute atualmente

Projeto de Lei n.º 2338/2023 (atualmente na Câmara dos Deputados, depois de já ter a tramitação encerrada no Senado), que visa dispor obre "o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana" (BRASIL, 2023).

O texto do Projeto de Lei, inspirado no Regulamento aprovado pela União Europeia, apresenta diversos pontos de convergência que se assemelham à previsão do Regulamento Europeu com o objetivo de estabelecer uma legislação de aplicação ampla e geral aos diversos tipos de sistemas de IA desenvolvidos e em utilização. Assim, o projeto brasileiro também aborda previsão para regulação de tecnologias de reconhecimento facial, mas de modo diverso.

Em seu Artigo 13, estão previstas as hipóteses consideradas de risco excessivo, e que, portanto, estão vedadas, incluindo-se o desenvolvimento, a implementação e o uso de sistemas de Inteligência Artificial "IV – em sistemas de identificação biométrica à distância, em tempo real e em espaços acessíveis ao público" (BRASIL, 2023). As exceções, no entanto, podem ser vistas como mais restritivas do que aquelas contidas no Regulamento Europeu, na medida em que se pode utilizar tecnologias de identificação biométrica para:

> a) instrução de inquérito ou processo criminal, mediante autorização judicial prévia e motivada, quando houver indícios razoáveis da autoria ou participação em infração penal, a prova não puder ser feita por outros meios disponíveis e o fato investigado não constituir infração penal de menor potencial ofensivo;
>
> b) busca de vítimas de crimes e de pessoas desaparecidas, ou em circunstâncias que envolvam ameaça grave e iminente à vida ou à integridade física de pessoas naturais;
>
> c) flagrante delito de crimes punidos com pena privativa de liberdade superior a 2 (dois) anos, com imediata comunicação à autoridade judicial;
>
> d) recaptura de réus evadidos e cumprimento de mandados de prisão e de medidas restritivas ordenadas pelo Poder Judiciário.
>
> § 1º Os desenvolvedores de sistemas de IA devem adotar medidas para coibir o uso de seus sistemas para as hipóteses descritas no caput deste artigo.
>
> § 2º O uso de sistemas a que se refere o inciso IV deste artigo deverá ser proporcional e estritamente necessário ao atendimento do interesse público, observados o devido processo legal e o controle judicial, bem como os princípios e direitos previstos nesta Lei e, no que couber, na

> Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), especialmente a garantia contra a discriminação e a necessidade de revisão da inferência algorítmica pelo agente público responsável. (BRASIL, 2023)

O que se observa é: as propostas municiais e estaduais da primeira fase, influenciadas pelo movimento americano de banimento de tecnologias de reconhecimento facial, tinham como objetivo o banimento e a restrição de tecnologias de reconhecimento facial pelo poder público municipal e estadual, ou seja, buscavam, de forma descentralizada, local e independente, estabelecer medidas isoladas de restrição quase total ao uso dessas tecnologias; a segunda fase, marcada pela discussão atual no Congresso Nacional, portanto, a nível federal, e influenciada pelo movimento normativo europeu, adota uma postura estruturada, com ênfase no equilíbrio entre a manutenção da Segurança Pública, sopesada pela garantia dos direitos fundamentais, em especial, de proteção de dados pessoais, privacidade, liberdade e não discriminação.

5 Conclusão

A extensa vereda apresentada aqui assegura algumas conclusões, ainda que breves e parciais, sobre o caminho percorrido pelo Brasil, até aqui, no objetivo de normatizar o uso de aplicações de tecnologias de reconhecimento facial na Segurança Pública brasileira. Diante da análise feita, é possível observar que a evolução das propostas legislativas sobre reconhecimento facial no Brasil revela uma mudança significativa de abordagem.

A primeira fase, marcada por iniciativas municipais e estaduais, inspiradas no movimento norte-americano de banimento, caracterizou-se pela adoção de medidas fragmentadas e restritivas, que buscavam proibir quase integralmente a utilização dessas tecnologias pelo poder público. Essa postura refletia uma reação preventiva e local diante dos riscos sociais e jurídicos já identificados no debate internacional. No entanto, o enfraquecimento do movimento e os embates político-jurídicos, limitou a adoção dessa abordagem.

Na segunda fase, o cenário ganha maior complexidade e maturidade normativa. O deslocamento da discussão para o âmbito federal, por meio do Congresso Nacional, indica a busca por uma regulação mais abrangente e estruturada, alinhada às diretrizes internacionais, especialmente as europeias. Diferentemente da primeira fase, em que prevalecia o viés de

contenção, a nova etapa aponta para um esforço de compatibilização entre o uso legítimo do reconhecimento facial e a salvaguarda dos direitos fundamentais.

Esse movimento demonstra que o Brasil não caminha para uma solução simplista de proibição ou liberalização irrestrita, mas sim para a construção de um marco regulatório que reconhece, de um lado, as potencialidades, e de outro, os riscos inerentes a essas tecnologias. Tecnologias de reconhecimento facial, quando desenvolvidas e utilizado sob parâmetros claros de transparência, proporcionalidade, necessidade e supervisão adequada, pode desempenhar um papel relevante em matéria de Segurança Pública, sem, contudo, comprometer garantias constitucionais.

Assim, a trajetória legislativa nacional reflete uma transição: de uma resistência inicial, marcada pelo banimento e pela tentativa de bloqueio total, para um modelo normativo que procura estabelecer um equilíbrio entre inovação tecnológica e proteção de direitos. Essa evolução demonstra não apenas a influência dos referenciais internacionais, mas também a necessidade de o Brasil construir soluções normativas próprias, que dialoguem com seu contexto democrático, jurídico e social, garantindo que o avanço tecnológico se dê em consonância com os valores fundamentais do Estado de Direito.

Por fim, não se descuida que a aqui chamada segunda fase também carece de aperfeiçoamento. É necessário adotar uma abordagem multidisciplinar, onde governos, especialistas em tecnologia, acadêmicos e a sociedade civil devem colaborar para criar regulamentações transparentes e éticas. A pesquisa contínua sobre a precisão e os impactos sociais dessas tecnologias também é essencial, o que deve refletir na possibilidade de rápida e eficiente adequação normativa.

Referências

ACESS NOW *et al*. **Carta aberta para banimento global de usos de reconhecimento facial e outros reconhecimentos biométricos remotos que permitam vigilância em massa, discriminatória e enviesada.** [s.l.], 07 jul. 2021. Disponível em: https://www.accessnow.org/ban-biometric-surveillance/ Acesso em: 27 set. 2025.

ACLU OF NORTHERN CALIFORNIA *et al*. San Francisco, 09 abr. 2019. Disponível em: https://sfgov.legistar.com/LegislationDetail.aspx?ID=3953862&GUID=926469C0-A7BA-47D3-BB32-

05C2C6D8EB2B Acesso em: 27 set. 2025.

ALERJ (Assembleia Legislativa do Estado do Rio de Janeiro). **Lei nº 6.528, de 11 de setembro de 2013.** Regulamenta o artigo 23 da Constituição do Estado. Rio de Janeiro, RJ: Assembleia Legislativa do Estado do Rio de Janeiro, 2013. Disponível em: http://alerjln1.alerj.rj.gov.br/contlei3846e60a583257be5005ec84a?OpenDocument Acesso em: 27 set. 2025.

BALTIMORE. **Baltimore City Code.** Baltimore, MD, 14 jun. 2021. Disponível em: https://legislativereference.baltimorecity.gov/city-codes Acesso em: 27 set. 2025.

BERKELEY. **Municipal Code.** Title 2, Administration. Chapter 2.99 - Acquisition and Use of Surveillance Technology. Berkeley, CA, 2018. Disponível em: https://berkeley.municipal.codes/BMC/2.99 Acesso em: 27 set. 2025.

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 27 set. 2025.

BRASIL. **Projeto de Lei nº 2.338, de 2023 (S-F).** Dispõe sobre o uso da Inteligência Artificial. Autor: Senador Rodrigo Pacheco (PSD-MG). Apresentado em 03 mai. 2023. Situação: aguardando parecer da Comissão Especial destinada a proferir parecer ao PL nº 2338/2023, do Senado Federal. Brasília: Senado Federal / Câmara dos Deputados. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2487262 Acesso em: 27 set. 2025.

CÂMARA MUNICIPAL DO RIO DE JANEIRO. **Projeto de Lei n° 824/2021.** Dispõe sobre a Proibição do Uso de Tecnologias de Reconhecimento Facial pelo Poder Público Municipal. Autoria: Vereador Reimont Luiz Otoni Santa Bárbara. Rio de Janeiro, RJ: Câmara Municipal do Rio de Janeiro, 05 de outubro de 2021 Disponível em: http://aplicnt.camara.rj.gov.br/APL/Legislativos/scpro2124.nsf/10325872700723005?OpenDocument&CollapseView Acesso em: 27 set. 2025.

CJSUBIA – Comissão de Juristas responsável por subsidiar elaboração de substitutivo sobre inteligência artificial no Brasil. Senado Federal. Secretaria-Geral da Mesa. **Ata da 3ª reunião, ordinária, da Comissão de Juristas responsável por subsidiar elaboração de substitutivo sobre inteligência artificial no Brasil da 4ª Sessão Legislativa Ordinária**

da 56ª legislatura, realizada em 29 de abril de 2022, sexta-feira, no Senado Federal, anexo ii, ala Senador Alexandre Costa, plenário nº 7. Brasília, DF: Senado Federal. Disponível em: https://legis.senado.leg.br/comissoes/comissao?codcol=2504 Acesso em: 27 set. 2025.

COALITION ON HOMELESSNESS. San Francisco, 20 mar. 2019. Disponível em: https://sfgov.legistar.com/LegislationDetail.aspx?ID=3953862&GUID=926469C0-A7BA-47D3-BB32-05C2C6D8EB2B Acesso em: 27 set. 2025.

COLOR OF CHANGE. San Francisco, 27 mar. 2019. Disponível em: https://sfgov.legistar.com/LegislationDetail.aspx?ID=3953862&GUID=926469C0-A7BA-47D3-BB32-05C2C6D8EB2B Acesso em: 27 set. 2025.

DAL MAGRO, Diogo. **Riscos Jurídicos de Tecnologias de Reconhecimento Facial na Segurança Pública para a democracia brasileira.** 2022. 192 f. Dissertação (Mestrado) - Curso de Programa de Pós-Graduação Stricto Sensu em Direito, Faculdade Meridional, Passo Fundo, 2022.

DISTRITO FEDERAL. **Lei n° 6.712, de 10 de novembro de 2020.** Dispõe sobre o uso de tecnologia de reconhecimento facial – TRF na segurança pública e dá outras providências. Brasília: Câmara Legislativa. Disponível em: https://legislacao.cl.df.gov.br/Legislacao/consultaTextoLeiParaNormaJuridicaNJUR-560365!buscarTextoLeiParaNormaJuridicaNJUR.action Acesso em: 27 set. 2025.

FALCON, Emiliano. **ACLU Testimony in Support of Face Surveillance Ban.** [s.l.], 09 maio 2019. Disponível em: http://somervillecityma.iqm2.com/Citizens/Detail_Meeting.aspx?ID=2941 Acesso em: 27 set. 2025.

KING COUNTY. **King County Code.** Title 2 – Administration. 2.67 - Facial Recognition Technology Use. King County, WA, 01 jul. 2021. Disponível em: https://kingcounty.gov/council/legislation/kc_code/05_Title_2.aspx Acesso em: 27 set. 2025.

ONEAMERICA. **May 3, 2021.** Seattle, WA, 03 maio 2021. Disponível em: https://mkcclegisearch.kingcounty.gov/LegislationDetail.aspx?ID=4793336&GUID=260D1D8E-6553-4583-B75B-92FB4C5886C8&Options=Advanced&Search=&FullText=1 Acesso em: 27 set. 2025.

SECURE JUSTICE *et al*. **Re: Consent Agenda Item 24, Facial Recognition Technology.** [s.l.], 10 out. 2019. Disponível em: https://

records.cityofberkeley.info/PublicAccess/paFiles/cqFiles/index.html Acesso em: 27 set. 2025.

SENADO FEDERAL. **Ato do Presidente do Senado Federal nº 4, de 2022.** Institui Comissão de Juristas responsável por subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei nºs 5.051, de 2019, 21, de 2020, e 872, de 2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil. Autoria: Senador Rodrigo Pacheco. Brasília, DF: Senado Federal. Disponível em: https://legis.senado.leg.br/comissoes/comissao?codcol=2504 Acesso em: 27 set. 2025.

SOMERVILLE. **Code of Ordinances.** Chapter 9 - Offenses and Miscellaneous Provisions. Article III. - Offenses Against the Person. Sec. 9-25. - Banning the usage of facial recognition surveillance technology. Somerville, MA, 2019. Disponível em: https://library.municode.com/ma/somerville/codes/code_of_ordinances?nodeId=PTIICOOR_CH9OFMIPR_ARTIIIOFAGPE_DIV1GE_S9-25BAUSFARESUTE Acesso em: 27 set. 2025.

THE SENATE OF MARYLAND. **Testimony in Support of Council Bill 21-001, as amended.** Annapolis, MD, 06 jun. 2021. Disponível em: https://legislativereference.baltimorecity.gov/city-codes Acesso em: 27 set. 2025.

TOWN OF BROOKLINE. **Reports OF Select Board and Advisory Committee on the Articles in the Warrant for the Special Town Meeting to be held in the High School Auditorium Tuesday, November 19, 2019 at 7:00 P.M.** Town of Brookline, MA, 2019. Disponível em: https://www.brooklinema.gov/DocumentCenter/View/20751/Combined-Reports-November-2019-Brookline-Special-Town-Meeting-with-Supplements Acesso em: 27 set. 2025.

UNIÃO EUROPEIA. **Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024.** Estabelece regras harmonizadas em matéria de inteligência artificial e altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Lei da Inteligência Artificial). Jornal Oficial da União Europeia, L 2024/1689, 12 jul. 2024. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/ptg Acesso em: 27 set. 2025.

Capítulo 3

QUANDO O CÓDIGO VIRA LEI E A LEI VIRA CÓDIGO: O PARADIGMA DO CÓDIGO-LEI-FONTE NA ERA DA INTELIGÊNCIA ARTIFICIAL

Fabiana Faraco Cebrian[1]

1 Introdução

A sociedade contemporânea testemunha uma simbiose cada vez mais profunda entre o direito e a tecnologia, marcada por uma transformação que transcende a mera digitalização de processos para alcançar uma reconfiguração ontológica da própria experiência normativa.

A digitalização massiva de interações sociais, econômicas e políticas, impulsionada pela onipresença da internet, pela proliferação de dispositivos conectados e pela ascensão da Inteligência Artificial (IA), deslocou o eixo de poder e regulação de formas que o pensamento jurídico tradicional apenas começa a compreender e assimilar. Se antes a norma jurídica, o código-lei, constituía a principal ferramenta de ordenação social, que estabelece por meio da linguagem natural os parâmetros de conduta e os limites da liberdade, hoje ela divide o palco regulatório com uma força igualmente eficiente, porém muito mais veloz e pervasiva, o código-fonte, a instrução computacional que define a arquitetura tecnológica e as possibilidades concretas de ação na infosfera.

Este artigo investiga a crescente convergência entre esses dois códigos, um processo que redefine a natureza da regulação social e que levanta desafios para a teoria e a prática jurídicas, especialmente com o advento da IA generativa. Esta última, com a capacidade de produzir conteúdo, desde textos jurídicos até códigos de programação, introduz uma nova dimensão na relação entre direito e tecnologia, onde a própria criação normativa pode ser mediada por algoritmos.

1 Mestre em Direito pela PUCPR. Mestre em engenharia pelo IME/RJ. Graduada em engenheira pela Unesp e em Direito pela PUCPR. Especialista em governança de IA e proteção de dados. Email fabiana.cebrian@anpd.gov.br

Neste contexto, observa-se na sociedade contemporânea a infosfera, um conceito que abarca tanto o ambiente físico quanto o digital no qual a existência e as manifestações do ser humano são continuamente influenciadas e moldadas por um complexo conjunto de algoritmos, bem como por fatores culturais, políticos, sociais e tecnológicos. Paralelamente, os seres humanos também moldam a infosfera por meio de suas ações, decisões e criações. Isso demonstra a natureza interativa da relação entre os seres humanos e o ambiente informacional.

O presente artigo adota o método de pesquisa hipotético-dedutivo e parte da hipótese central de que a automação crescente do direito não representa uma mera digitalização de processos, mas uma reconfiguração ontológica da experiência normativa que exige um novo paradigma teórico, o código-lei-fonte, capaz de articular a eficiência tecnológica com as garantias fundamentais do Estado de Direito. A metodologia compreende uma revisão bibliográfica da literatura jurídica, filosófica e tecnológica, com foco nos trabalhos de Floridi e Lessig, um exame crítico das experiências de automação jurídica e, por fim, uma síntese propositiva do conceito de código-lei-fonte.

Diante do exposto, a pergunta de pesquisa que este artigo procura responder é: Como a convergência entre o código-lei e o código-fonte, mediada pela Inteligência Artificial, transforma a natureza da regulação social e exige um novo paradigma teórico para a governança na infosfera?

Para responder a esta questão, o artigo explora a imersão na infosfera, a teoria do código é lei, os desafios da IA Generativa e as oportunidades e riscos da automação jurídica que culminam na proposição do código-lei-fonte como um conceito-chave para a compreensão e orientação desta nova realidade regulatória. A pesquisa contribui para o campo do Direito e tecnologia ao demonstrar que o desenvolvimento de um código-lei-fonte, uma norma que seja ao mesmo tempo compreensível aos seres humanos e operacional por máquinas, pode ser essencial para enfrentar os desafios impostos pela era digital.

2 A relação entre o código-lei e o código-fonte na infosfera: uma análise jurídico-tecnológica-social

A sociedade contemporânea atravessa uma profunda transformação paradigmática na forma como indivíduos, o Estado e as instituições se inter-relacionam, marcada por uma transição contínua do espaço físico

para o ambiente digital. Este movimento, impulsionado por contínuos avanços tecnológicos, posiciona a humanidade em uma crescente imersão que promove o surgimento de um novo espaço ontológico que Floridi denominou como infosfera, também chamada de *information sphere* (FLORIDI, 2014, p. 40-43). Este conceito reflete a atmosfera digital que envolve o mundo físico e permeia a sociedade contemporânea, de modo a criar um ambiente densamente informatizado que modela a maneira pela qual a realidade é experimentada, as interações são estabelecidas e como a compreensão do mundo é construída (FLORIDI, 2010, p. 18).

A infosfera é uma esfera informacional composta por todas as entidades informacionais, sejam elas físicas ou artificiais, e engloba suas propriedades, seus processos, interações e relações. Logo, não se restringe apenas ao ambiente digital, mas também incorpora o mundo real e analógico e suas interações. Nela, as entidades e agentes são todos igualmente informacionais, ou seja, seres humanos, dados, processos, dispositivos tecnológicos, são compostos e interpretados como informação. Deste modo, passa a ser obscura a distinção entre ser humano e objetos, uma vez que todas as atividades podem ser interpretadas como uma leitura e gravação. Assim, os seres humanos e as máquinas são agentes informacionais de maneira equivalente (FLORIDI, 2014, p. 40-41).

Nesse contexto, os algoritmos assumem um papel central como elementos intrínsecos e definidores da existência humana. Eles não apenas facilitam as atividades diárias, mas alteram a percepção da realidade e a forma de viver em sociedade e permitem a massificação de um modo de vida cada vez mais híbrido, no qual o digital e o físico se entrelaçam de maneira intrincada e inseparável. O modo de vida híbrido da sociedade contemporânea pode ser ilustrado pelo conceito de *onlife*, proposto por Floridi (FLORIDI, 2014, p. 43). No cenário *onlife*, a vida *online* e *offline* se fundem de tal forma que se tornam indistintas e resultam em uma existência informacional que reflete a realidade contemporânea, permeada por informações e algoritmos. O ambiente passa a ser simultaneamente *online* e *offline*, e os seres humanos começam a passar a maior parte do tempo *onlife*. Portanto, estão simultaneamente conectadas ao mundo digital e ao mundo físico e a distinção entre *online* e *offline* torna-se cada vez mais inseparável.

Desta forma, a onipresença de dispositivos conectados e o acesso facilitado à internet não apenas reconfiguram a vida cotidiana, mas também impõem desafios inéditos ao universo jurídico, que se vê

compelido a reinterpretar e adaptar seus dogmas a um cenário de fronteiras fluidas e interações desterritorializadas. Este ambiente leva a necessidade de se compreender a complexa e dinâmica interação entre o código-lei e o código-fonte. Observa-se que para operacionalizar o modo de vida *onlife* na infosfera, são necessários algoritmos, responsáveis pela intermediação tecnológica entre o ambiente online e offline, sendo que o código-fonte é a base para execução de algoritmos. Ou seja, é por meio do código-fonte que os algoritmos computacionais são implementados, sendo este a representação textual de um programa, escrito em linguagem de programação específica, com uma sintaxe definida (RUSSEL; NORVIG, 2013). O código-fonte refere-se à programação e determina o funcionamento de um sistema e as ações possíveis dentro dele, independentemente de ser escrito ou não por programadores.

A infosfera não é um mero espaço virtual, mas uma camada indissociável da existência humana, onde as fronteiras entre o online e o offline se dissolvem. Nesse ambiente, a sociedade se torna fluida e multifacetada. Essa plasticidade identitária e territorial da sociedade, ao mesmo tempo que expande as possibilidades de ser, estar e permanecer, tensiona os conceitos jurídicos clássicos como capacidade, responsabilidade e titularidade de direitos, exigindo uma nova hermenêutica para a proteção da pessoa humana em sua integralidade digital.

O termo código-lei refere-se às normas jurídicas, escritas em linguagem natural e tradicionalmente posta pelo Estado. Nesse ponto, as normas jurídicas, que incluem outras formas de produção normativa, não apenas as leis, enfrentam as dificuldades iniciais em acompanhar as rápidas transformações sociais provocadas pela evolução tecnológica, implicando em uma nova dimensão de interação entre a sociedade e a tecnologia na infosfera. Observa-se que uma das diferenças fundamentais entre o código-lei e o código-fonte é a forma como são codificados. O primeiro em linguagem natural escrita, o segundo em linguagem de programação, respectivamente. Assim, a regulação do comportamento na infosfera transcende a mera aplicação de normas estatais, ou seja, o código-lei, e encontra no próprio design da tecnologia e no seu código-fonte uma de suas mais potentes manifestações.

Conforme Lessig, o código informático, a arquitetura de software e protocolos que governam o ambiente digital atua como uma poderosa força regulatória, moldando comportamentos e definindo os limites da liberdade no ciberespaço, muitas vezes de forma mais eficaz que a própria

legislação (LESSIG, 2006). Em sua teoria do código é lei, é possível observar que o código-fonte funciona como uma forma de lei. Este ponto demonstra a demonstra a complexidade relacionada com a governança contemporânea, principalmente em uma sociedade algorítmica. Se o código é lei, de modo a regular o comportamento humano de maneira tão eficaz quanto as normas tradicionais, portanto, existem dois códigos, o código-lei visível, escrito em linguagem natural e sujeito a processos democráticos e o código-fonte invisível, com características técnicas, escrito em linguagem de programação, capaz de codificar valores e estabelecer prioridades de maneira não explícita ou transparente aos seres humanos e sociedade algorítmica (LESSIG, 1999, p. 136-137). Ou seja, uma regulação visível e uma regulação invisível. Essa arquitetura invisível, mas onipresente, pré-define o que é possível ou impossível fazer no ambiente digital, influenciando desde a liberdade de expressão até a proteção de dados pessoais.

Neste sentido, observa-se uma crescente migração do exercício de direitos e obrigações do espaço físico e analógico para o espaço digital, conforme destacado por Lessig em sua teoria do código é lei (LESSIG, 2000, p. 1-5). Os seres humanos estão cada vez mais sem a possibilidade de escolher em qual espaço, físico ou digital, deseja utilizar ou permanecer. Na contemporaneidade, uma vasta gama de atividades cotidianas envolve a criação de um login, acompanhado pela necessidade de fornecer dados pessoais, para permitir o acesso a serviços e informações.

Nesse horizonte, a eficácia regulatória do código decorre de mecanismos que operam by design: defaults, permissões e proibições incorporadas em protocolos, sistemas de autenticação, listas de controle de acesso e camadas de interoperabilidade. De acordo com Lessig, esses artefatos, combinados a incentivos de mercado e expectativas sociais, configuram as quatro modalidades que agem como forças que regulamentam o comportamento das pessoas, tanto no mundo físico quanto no digital, sendo eles (LESSIG, 2006, p. 122):

- A lei: Regulamenta por meio de sanções legais aplicadas pelo governo, como multas, penas de prisão ou outras punições impostas ex post facto para quem viola a legislação.
- As normas sociais: Exercem constrangimento por meio de aprovação ou desaprovação e estigma social. O comportamento é moldado pela pressão da comunidade e pela cultura vigente.

- O mercado: Regula o comportamento por meio do preço, da oferta e da demanda. O custo financeiro de um produto ou serviço influencia a conduta do indivíduo, e faz com que certas ações e produtos sejam mais ou menos viáveis.
- A arquitetura ou código: Refere-se às características tecnológicas do mundo que limitam ou permitem certas ações. No mundo digital, o código ou a arquitetura do software é a modalidade mais importante, pois determina o que é tecnicamente possível ou impossível para os usuários. A arquitetura desempenha no digital o papel mais imediato e onipresente de modelagem de condutas.

Essas quatro modalidades não atuam de forma isolada, mas interagem umas com as outras, podendo se apoiar ou competir entre si. Assim, quando um serviço exige identidade verificada para participar, quando um protocolo dificulta a portabilidade de dados, ou quando um algoritmo prioriza certos conteúdos, o resultado é uma regulação material que antecede a interpretação jurídica e, muitas vezes, a torna redundante.

Deste ponto, surge a urgência de um constitucionalismo do código, se a arquitetura é um espaço de exercício de poder, ela deve incorporar garantias procedimentais e substantivas, como transparência auditável, possibilidade de contestação, justificativas acessíveis, governança de versões e accountability sobre mudanças de parâmetros críticos. Em termos institucionais, isso implica redesenhar a relação entre direito e tecnologia para que a lei recupere capacidade de modular o código, como por exemplo com o registro de decisões algorítmicas e seu impacto *ex ante*, sem perder de vista que o ser humano que opera a engenharia continuará a ser o primeiro campo onde liberdades e restrições são efetivamente decididas. Portanto, reconhecer que código é lei não é capitular ao tecnodeterminismo, mas exigir que o espaço técnico seja também um espaço de juridicidade e de controle democrático.

A emergência da infosfera e de suas formas de regulação intrínsecas não ocorre no vácuo, mas no seio de profundas transformações sociais que dão origem a novas configurações coletivas. A tecnologia atua como um catalisador para o surgimento de múltiplas sociedades, cada uma com suas lógicas e desafios específicos. Uma das mais influentes conceituações é a de Sociedade de Risco, desenvolvida pelo sociólogo Ulrich Beck (BECK, 1998, p. 64). Originalmente pensada para a modernidade tardia industrial, sua teoria adquire uma nova reflexão na era digital. Beck argumenta que a

sociedade contemporânea é caracterizada pela produção de riscos que são consequências das próprias ações e decisões humanas, riscos estes que são globais, imprevisíveis e muitas vezes invisíveis (CAVEDON; FERREIRA; FREITAS, 2015). Nesse contexto, Cavedon, Ferreira e Freitas analisaram o meio ambiente digital e as possíveis consequências decorrentes da interação do ser humano com esse ambiente sob a perspectiva da Teoria da Sociedade de Risco (CAVEDON; FERREIRA; FREITAS, 2015, p. 205).

Os riscos, impulsionados pelos constantes avanços da ciência, da tecnologia e da indústria, assumem novas características, isto é, deixaram de ser calculáveis e seus efeitos passaram a ser imprevisíveis. Esses riscos abstratos apresentam um potencial que ultrapassa as fronteiras físicas e temporais. A informática, com sua crescente penetração, exemplifica essas novas modalidades de risco. Logo, trata-se de uma sociedade caracterizada pela incerteza e imprevisibilidade, isto permite a sua correlação com a tecnologia e com os riscos por ela produzidos, diante de suas numerosas questões e interconexão tecnológica com a sociedade contemporânea.

Portanto, ao aplicar essa lente ao meio ambiente digital, percebe-se que a informática e a interconexão global, ao mesmo tempo que geram inúmeros benefícios, produzem novas modalidades de risco cujos efeitos ultrapassam fronteiras físicas e temporais, como ciberataques, desinformação em massa e vulnerabilidades sistêmicas de privacidade (CAVEDON; FERREIRA; FREITAS, 2015, p. 194-223). A gestão desses riscos abstratos e de potencial catastrófico torna-se um dos principais desafios para o Direito e para a governança na sociedade digital.

Dentro do panorama das múltiplas sociedades, a sociedade informacional, conforme definida por Castells, ocupa um lugar de destaque. Castells propõe uma distinção importante entre sociedade da informação, termo que poderia se aplicar a qualquer época histórica onde a informação foi relevante, e sociedade informacional, que descreve uma forma específica de organização social na qual a geração, o processamento e a transmissão de informação se tornam as fontes primordiais de produtividade e poder (CASTELLS, 2020, p. 83-85). Esta nova estrutura social é caracterizada pela sua lógica de rede, onde as conexões flexíveis e globais entre indivíduos, organizações e instituições, potencializadas pelas TICs, transcendem as fronteiras geográficas e culturais. A rede não é apenas uma ferramenta, mas a própria morfologia da sociedade, reconfigurando todos os aspectos da vida, da economia à cultura, e estabelecendo um novo

paradigma tecnológico que redefine as relações de produção e poder em escala planetária.

A mesma infraestrutura tecnológica que sustenta o fluxo de informações na sociedade informacional pavimenta o caminho para o que Rodotà e outros teóricos descreveram como a sociedade de vigilância. A capacidade de coletar, armazenar e analisar volumes massivos de dados pessoais em tempo real transforma a tecnologia em um potente instrumento de monitoramento e controle social. Rodotà argumenta que a privacidade individual se encontra sob crescente ameaça, não apenas pela vigilância constante, mas também pela concentração do controle sobre esses dados nas mãos de poucas entidades, sejam elas estatais ou corporativas (RODOTÀ, 2008, p. 26-28). Nesta sociedade, a privacidade transcende a dimensão puramente individual para adquirir um caráter coletivo, pois a análise de dados agregados pode impactar e influenciar grupos inteiros, levantando questões profundas sobre poder e discriminação. Complementarmente, Roger Clarke cunhou o termo *dataveillance* para descrever essa vigilância sistemática e automatizada por meio da coleta e análise de dados, propondo uma análise crítica sobre a legitimidade, necessidade e transparência de tais práticas (CLARKE, 1988, p. 499). A tensão entre os benefícios da análise de dados e a proteção do direito fundamental à privacidade torna-se, assim, um dos dilemas centrais da governança na sociedade de vigilância.

A evolução das sociedades de risco, informacional e de vigilância converge para uma nova configuração social: a sociedade algorítmica. Este conceito, explorado por autores como Schuilenburg e Peeters, descreve uma realidade na qual algoritmos computacionais exercem uma influência cada vez mais determinante na estruturação da vida social e na tomada de decisões em esferas críticas (SCHUILENBURG; PEETERS, 2021). Os algoritmos definidos sequências finitas de instruções bem definidas que transformam entrada em saídas desejadas (CORMEN et al., 2012, p. 3), deixaram de ser meras ferramentas de otimização para se tornarem agentes constitutivos da própria estrutura social. Eles não apenas automatizam processos, mas passam a governar a sociedade de novas maneiras, mediando o acesso à informação, moldando oportunidades e predizendo condutas. Nesse processo, os seres humanos são frequentemente reduzidos a conjuntos de dados e perfis comportamentais, operados por lógicas computacionais que podem ser opacas e contestáveis (SCHUILENBURG; PEETERS, 2021, p. 9).

A ascensão da sociedade algorítmica acarreta profundos desafios jurídicos e regulatórios. A crescente dependência de algoritmos em áreas como finanças, justiça criminal, saúde e emprego levantam questões sobre direitos fundamentais. A privacidade é desafiada pela perfilamento (*profiling*) e pela predição de comportamentos, a igualdade é ameaçada por vieses discriminatórios embutidos nos próprios algoritmos e a liberdade de expressão é moldada por sistemas de recomendação e moderação de conteúdo.

Diante da crescente complexidade que envolve diferentes sociedades, infosfera e modo de vida *onlife*, emergem propostas inovadoras que buscam aproximar o código-lei do código-fonte. Uma das mais notáveis é a abordagem conhecida como Rule as Code (RaC), ou Regra como Código, A premissa do RaC é a transcrição de regras e regulamentos, como leis e políticas públicas, em uma lógica computacional (código), de modo que possam ser interpretados e até mesmo executados diretamente por sistemas informáticos (WADDINGTON, 2020, p. 180). Outra proposta é denominada *Computational Law* (Direito Computável), que explora como as normas jurídicas podem ser modeladas computacionalmente para melhorar sua clareza, consistência e aplicação (GENESERETH, 2016). Ambos os conceitos serão explorados no item 3.

A relação entre o código-lei e o código-fonte não deve ser vista como uma substituição, mas sim de necessária coexistência, tradução e equilíbrio. A evolução da norma jurídica na infosfera exige uma adequação à sociedade digitalizada, mas essa adequação não pode prescindir dos princípios e garantias fundamentais que estruturam o Estado de Direito. Trata-se de buscar uma sinergia onde a tecnologia possa servir à aplicação mais eficaz da lei, ao mesmo tempo que a lei estabelece os limites éticos e jurídicos para o desenvolvimento e uso da tecnologia.

3 O código-lei-fonte: a convergência entre direito e computação na sociedade algorítmica

A imersão da sociedade na dinâmica algorítmica e a consolidação de um modo de vida *onlife*, na qual as fronteiras entre o físico e o digital se dissolvem, estabelecem o cenário para transformações do pensamento jurídico contemporâneo. Neste contexto, a eficácia e a aplicabilidade da norma jurídica tradicional, ou código-lei, são desafiadas pela velocidade e complexidade da infosfera.

A sociedade contemporânea está imersa em uma cultura algorítmica, um conceito cunhado por Lévy para descrever um novo paradigma de pensamento e ação em um mundo crescentemente orientado por algoritmos (LÉVY, 2011). Esta cultura não se restringe ao avanço tecnológico, ela implica uma mudança de mentalidade que valoriza o pensamento algorítmico como ferramenta para navegar e estruturar a realidade.

É nesse contexto que é possível analisar a transformação da norma jurídica, código-lei, em regras técnicas e automatizadas, código-fonte, um processo impulsionado pela onipresença da tecnologia, materializada nas visões da computação ubíqua de Weiser e do *everyware* de Greenfield. Logo, a invisibilidade e a integração da computação no cotidiano estão redefinindo as formas de regulação social, deslocando o poder normativo do Estado para as arquiteturas de software que governam a infosfera.

A jornada para essa transformação pode-se iniciar com a visão de Weiser sobre a computação ubíqua. Weiser previu uma era em que a tecnologia se tornaria mais eficaz à medida que desaparecesse da consciência do usuário, integrando-se de forma tão natural ao ambiente a ponto de se tornar uma tecnologia calma (WEISER, 1993, p. 75). Em vez de interagirmos com um computador como um objeto distinto, a computação estaria difusa em nosso entorno, embutida em objetos e espaços. Essa visão se concretiza hoje na proliferação de dispositivos móveis, sensores inteligentes e, de forma mais ampla, na Internet das Coisas (IoT), na qual objetos cotidianos se conectam e trocam dados, criando um ambiente responsivo e informacional (ASHTON, 2009, p. 97-114). A tecnologia, portanto, deixa de ser um instrumento para se tornar o próprio ambiente, um ecossistema digital que permeia o espaço físico.

Ao expandir a visão de Weiser, Greenfield propõe o conceito de *everyware*, uma fusão de everywhere (todos os lugares) e hardware, para descrever uma realidade onde qualquer objeto, desde roupas e edifícios até espaços públicos, pode se tornar uma interface computacional (GREENFIELD, 2006, p. 9). A teoria de Greenfield não se concentra apenas no aspecto tecnológico, mas investiga profundamente as implicações sociais e culturais dessa integração. No mundo do *everyware*, a interação humana não é mais com dispositivos isolados, mas com uma rede densa e interconectada de sistemas que operam, muitas vezes, sem a nossa consciência direta. Isso altera fundamentalmente nossa percepção de espaço, tempo e interação social, borrando as fronteiras entre o público e o privado, o físico e o virtual.

Esses fenômenos de computação ubíqua e *everyware* são a manifestação prática do que Schwab denominou Quarta Revolução Industrial, caracterizada por um impacto sistêmico, escala abrangente e um ritmo de mudança exponencial que redefine a própria condição humana (SCHWAB, 2016, p. 13). Contudo, enquanto Schwab foca nos aspectos industriais e econômicos, Floridi oferece uma perspectiva filosófica complementar com sua noção de Quarta Revolução informacional. Para Floridi, a revolução atual reside na redefinição de nossa identidade e autocompreensão. Com o advento das TICs, a sociedade foi deslocada de sua posição privilegiada como os únicos agentes processadores de informação e passa a coexistir em um ecossistema mais amplo de agentes informacionais que inclui tanto seres humanos quanto entidades artificiais (FLORIDI, 2014, p. 93-94). É uma mudança ontológica que permite repensar o que significa ser humano em uma realidade cada vez mais informacional.

A consequência direta dessas mudanças é o poder desproporcional que o código-fonte adquire na infosfera. A regulação se torna invisível para o usuário comum, que interage com interfaces digitais sem ter consciência das regras codificadas que governam seu comportamento. O controle sobre essa arquitetura regulatória está concentrado nas mãos de poucas entidades privadas, que detêm uma capacidade quase ilimitada de definir as regras do jogo dentro de suas plataformas e que moldam desde a visibilidade de conteúdo até as interações sociais permitidas. A falta de transparência sobre como os algoritmos funcionam e como o código-lei é transcrito agrava essa assimetria de poder, dificulta a contestação e o exame público (FREITAS, 2021, p. 223).

A trajetória da cultura algorítmica à computação ubíqua e à experiência *onlife* revela uma trajetória de crescente integração entre tecnologia e vida cotidiana que cria as condições ideais para a transformação do código-lei em código-fonte. Este percurso demonstra que o código-fonte se consolidou como uma força regulatória primária na infosfera que opera com uma eficiência e uma invisibilidade que desafiam os mecanismos tradicionais de governança jurídica e democrática. A capacidade de embutir normas diretamente na infraestrutura digital representa uma mudança paradigmática na forma como o poder é exercido e o comportamento social é moldado.

Como apontado, a inserção da sociedade no ambiente digital é dependente de algoritmos. Conforme aponta Kitchin, a palavra algoritmo

é polissêmica e pode ser interpretada de maneiras distintas por engenheiros, cientistas sociais e pelo público em geral, o que pode levar a uma abstração mistificadora (KITCHIN, 2017, p. 16). Para superar essa barreira, é fundamental entender o algoritmo não apenas como uma série de passos técnicos, mas como um artefato cultural e social que participa ativamente da formalização das experiências humanas na sociedade movida a dados. Este processo de conversão da vida em dados é a base para a Descoberta de Conhecimento (KD - *Knowledge Discovery*), um campo que, segundo Fayyad et al., utiliza algoritmos para extrair padrões e gerar conhecimento útil a partir de grandes volumes de dados brutos (FAYYAD; PIATETSKY-SHAPIRO; SMYTH, 1996, p. 37-54). Ao processar nosso comportamento online, preferências e interações, os algoritmos não são meros operadores neutros, eles desempenham um papel ativo na formação de realidades sociais, econômicas e políticas, como destaca Kitchin, consolidam a estrutura da sociedade algorítmica.

A relação intrínseca e, por vezes, conflituosa entre o universo jurídico e o computacional pode ser sistematizada para melhor compreensão. Schrepel propõe uma taxonomia que ilumina as diferentes formas como direito e código se observam e interagem na sociedade contemporânea (SCHREPEL, 2023, p. 8). A primeira perspectiva é a de que a Lei é Código, uma visão que remonta a teóricos como Miguel Reale, que concebia o direito como uma espécie de software social, um conjunto de tipificações e regras que orientam o comportamento em sociedade, análogo ao modo como o código-fonte direciona o hardware (REALE, 2004, p. 186). Nesta visão, o direito, em sua linguagem natural, seria a própria programação da vida social.

Em contraposição, surge a perspectiva de que o Código é Lei, teoria desenvolvida por Lessig. Aqui, a arquitetura do ciberespaço, o código-fonte, funciona como uma forma de lei, que pode regular o comportamento de maneira muitas vezes mais eficaz que a norma estatal, pois define as próprias possibilidades de ação no ambiente digital (LESSIG, 1999, p. 3-8). Por fim, a terceira observação é a de que o Direito precisa do Código. Esta visão pragmática reconhece que a lei, por si só, pode ser insuficiente para regular a complexidade da infosfera. A combinação entre a norma jurídica e o código-fonte poderia, então, superar as limitações de detecção e aplicação da lei no ambiente digital e aproveitar o poder regulatório da tecnologia para alcançar os objetivos do direito de forma mais eficiente (SCHREPEL, 2023, p. 8).

A partir dessa taxonomia, derivam-se diferentes métodos de aplicação que aprofundam a interação entre os dois domínios. O Código da Lei refere-se à busca por maior sistematização e clareza na própria norma jurídica, que, mesmo em linguagem natural, se beneficia de uma estrutura lógica e organizada para garantir sua eficácia. Por outro lado, a Lei do Código descreve a realidade em que o código-fonte de plataformas e sistemas já incorpora regras formais e pode atuar como a principal fonte de regulamentação em determinados contextos digitais, embora isso levante sérios problemas de opacidade e responsabilização (SCHREPEL, 2023, p. 10).

A *distinção mais determinante, contudo, reside entre os conceitos de Código como Lei (Code* as Law) e Lei como Código (*Law as Code*), este último também conhecido como *Computational Law*. A ideia de Código como Lei não significa que o código substitui a lei, mas que ele pode ser usado como uma extensão ou ferramenta para aplicar e maximizar a eficácia da norma jurídica. O código-fonte, embora formalmente tenha pouco poder regulatório próprio, pode ser projetado para garantir a conformidade com as obrigações legais. Por exemplo, um veículo autônomo cujo GPS impede que o limite de velocidade legal seja ultrapassado ilustra essa abordagem. O código não é a lei de trânsito, mas ele a executa compulsoriamente.

Essa perspectiva se alinha à teoria de Lessig, que identifica quatro forças reguladoras do comportamento: a lei, as normas sociais, o mercado e a arquitetura (o código). Lessig demonstrou que o código não é apenas um objeto passivo de regulação, mas um regulador ativo e poderoso (LESSIG, 2000, p. 89-90). A arquitetura do ciberespaço, definida pelo seu código, restringe e possibilita ações e funciona como uma *lex informatica*, um conjunto de regras que é imposto pela própria tecnologia.

A abordagem da Lei como Código, ou *Computable Law*, representa um passo adiante na fusão entre a ciência jurídica e a informática. Conforme definido por Genesereth, o objetivo é representar a lei em formatos lógicos e computacionalmente tratáveis, como regras condicionais, que permitam a análise, verificação e, em última instância, a aplicação automatizada por sistemas de computador (GENESERETH, 2021). A meta não é substituir o raciocínio jurídico, mas aumentá-lo, de modo a utilizar a capacidade computacional para tornar a lei mais clara, consistente, previsível e acessível. Ao modelar a legislação em linguagem formal, busca-se identificar ambiguidades, inconsistências e lacunas que podem passar despercebidas na linguagem natural.

Uma implementação prática e cada vez mais explorada dessa ideia é o *Rule as Code* (RaC). A ideia tem sido objeto de estudo por organizações como a Organização para a Cooperação e Desenvolvimento Econômico (OCDE). A premissa do RaC é a transcrição de regras e regulamentos, como as de um regulamento tributário, de um programa de benefício social ou de uma licença ambiental, em uma lógica computacional (código), de modo que possam ser interpretados e até mesmo executados diretamente por sistemas informáticos (WADDINGTON, 2020, p. 180). O potencial dessa abordagem reside na promessa de aumentar a eficiência, a transparência e a acessibilidade do sistema jurídico e permitir, por exemplo, a automação da verificação de conformidade ou a prestação de serviços governamentais de forma mais ágil e precisa. Um sistema de imposto de renda que calcula automaticamente a obrigação do contribuinte com base nas regras codificadas é um exemplo clássico. Contudo, os desafios são igualmente grandes. A textura aberta do direito, a presença de princípios e conceitos que exigem interpretação valorativa, é notoriamente difícil de traduzir para a lógica binária do código. O risco de simplificação excessiva, que ignora as nuances e exceções do mundo real, é constante. Portanto, exige uma governança robusta e mecanismos de contestação. Questões de governança, responsabilidade por erros no código e a necessidade de garantir a contestabilidade das decisões automatizadas são preocupações centrais (MOHUN; ROBERTS, 2020, p. 5-7).

Desta forma, a síntese dessas abordagens aponta para a emergência de um conceito híbrido, de modo a emergir o conceito de código-lei-fonte. Esta não é uma mera tradução literal da norma jurídica para uma linguagem de programação, mas sim a criação de um sistema simbiótico onde o código-fonte e o código-lei coexistem e se complementam. O código-lei-fonte permitiria que a norma, redigida em linguagem natural, fosse utilizada em conjunto com modelos computacionais que representam e aplicam suas regras. Por exemplo, a lógica de uma audiência de conciliação, com suas condições e resultados, pode ser expressa em uma estrutura de programação, isso demonstra como regras processuais podem ser mapeadas em código.

O desenvolvimento do código-lei-fonte, contudo, deve ser guiado por princípios. Como alertam Barraclough et al., o objetivo não é criar uma cópia exata da lei em código, mas sim modelos codificados de uma representação do que a lei determina (BARRACLOUGH; FRASER; BARNES, 2021, p. 3). Isso implica reconhecer que um único modelo pode se apoiar em múltiplos documentos legais e que a natureza computacional

não altera a importância e a primazia da norma jurídica. A transparência e a prestação de contas são fundamentais, o código-lei-fonte deve ser submetido a processos democráticos de revisão e controle para garantir a salvaguarda dos direitos e liberdades individuais. A autonomia humana e a soberania do direito, enquanto expressão da vontade social em linguagem natural, devem ser preservadas, forma a posicionar o código-lei-fonte como um instrumento secundário, ainda que a serviço da norma jurídica.

A análise desde a sociedade algorítmica até a proposição de um código-lei-fonte revela um caminho de inevitável e crescente convergência entre o direito e a ciência da computação. A análise da taxonomia de Schrepel e a distinção entre Código como Lei e Lei como Código demonstram que a interação entre esses dois mundos não é apenas uma possibilidade teórica, mas uma realidade em construção. A exploração de abordagens como *Rule as Code* e *Computable Law* evidencia um esforço consciente para aproveitar o potencial da tecnologia a fim de aprimorar a eficácia, a transparência e a acessibilidade do sistema jurídico e enfrentar os desafios impostos pela complexidade da infosfera.

Reafirma-se, portanto, que o desenvolvimento de um código-lei-fonte não deve ser visto como uma rendição do direito à lógica da máquina, mas como uma evolução na qual o direito aprende a falar a língua da tecnologia para melhor cumprir sua missão social. A chave para o sucesso reside em manter a primazia da norma jurídica e garantir que a automação da regra não signifique a abdicação do valor, da justiça e da capacidade de interpretação que caracterizam o fenômeno jurídico.

O desafio contemporâneo é, portanto, o de promover um equilíbrio entre esses dois códigos. É preciso construir pontes entre o mundo do Direito e o da ciência da computação, para que a governança algorítmica seja não apenas eficiente, mas também justa, transparente e alinhada aos valores de uma sociedade democrática. Em última análise, deve-se assegurar que, mesmo na era da computação ubíqua, a tecnologia permaneça a serviço da humanidade, e não o contrário.

Ao olhar para o presente e também para o futuro, a Inteligência Artificial (IA) surge como o próximo catalisador dessa integração. Com sua capacidade de processar linguagem natural e desenvolver modelos adaptativos, a IA oferece a possibilidade de criar formas ainda mais sofisticadas e dinâmicas de codificar o código-lei. Isso aponta para a necessidade de uma governança proativa, que não apenas reaja às inovações, mas que participe ativamente de seu desenho e que assegure que o futuro

da regulação na sociedade digital seja não apenas mais eficiente, mas fundamentalmente mais justo e humano.

Em resposta a esses desafios, o ordenamento jurídico brasileiro tem desenvolvido marcos regulatórios importantes, como o Marco Civil da Internet (Lei nº 12.965/2014) (BRASIL, 2014), que estabelece princípios para o uso da rede, e a Lei Geral de Proteção de Dados Pessoais (LGPD, Lei nº 13.709/2018) (BRASIL, 2018), que visa proteger os dados dos cidadãos e garantir sua autodeterminação informativa. Adicionalmente, o debate em torno da regulamentação da Inteligência Artificial, exemplificado pelo Projeto de Lei nº 2.338/2023 (BRASIL, 2023), sinaliza a preocupação do legislador em estabelecer um arcabouço ético e jurídico para o desenvolvimento e uso dessas tecnologias.

4 Código-lei e código-fonte na era da inteligência artificial: entre regulação algorítmica e produção normativa automatizada

Os algoritmos na atualidade transcendem o papel de meros operadores e desempenham um papel ativo na formação de realidades sociais, econômicas e políticas dentro da sociedade algorítmica. Essa é uma relevante mudança de perspectiva, pois destaca os impactos sociais e culturais dos algoritmos, em vez de apenas seus aspectos tecnológicos.

Dentro deste contexto, o potencial transformador das tecnologias é uma constante na história humana, desde a invenção da roda até a complexa arquitetura da Inteligência Artificial (IA) contemporânea. Cada inovação tecnológica introduz novos paradigmas que moldam o desenvolvimento social, cultural e econômico. Hoje, a IA permeia o cotidiano de forma ubíqua e, muitas vezes, imperceptível, presente em chat de conversa, aplicativos de recomendação, sistemas de navegação e assistentes virtuais.

A interação humano-máquina vive uma quebra de paradigma, não são mais os humanos que precisam aprender a linguagem das máquinas, mas as máquinas que aprenderam a se comunicar em linguagem natural. Este ponto, aumenta a complexidade e a confiança depositada nesses sistemas. Nesse contexto, Floridi adverte sobre a necessidade de uma compreensão nuançada dos impactos da IA, para evitar tanto a subutilização por medo de seus riscos quanto o mau uso ou a superutilização acrítica (FLORIDI et al., 2018, p. 690-691). Um dos desafios mais prementes é a opacidade. O funcionamento interno de modelos de IA avançados, como as Redes Adversárias Generativas (GANs) e os grandes modelos de linguagem (a

exemplo do GPT), é ininteligível para a maioria dos usuários e, em muitos casos, até mesmo para seus desenvolvedores. Desta forma, cria-se o que se convencionou chamar de problema da caixa-preta (FLORIDI et al., 2018, p. 700). Essa falta de transparência dificulta a responsabilização, a contestação de decisões automatizadas e a construção de uma confiança pública sólida na tecnologia.

A opacidade dos sistemas de IA agrava um de seus problemas mais insidiosos, a capacidade de perpetuar e amplificar vieses e preconceitos existentes na sociedade. Como bem aponta Doneda, a qualidade dos resultados de um sistema de IA tem correlação direta com a qualidade dos dados com os quais ele é treinado, se os dados históricos estão repletos de preconceitos, o algoritmo os reproduzirá de forma automatizada e em larga escala (DONEDA et al., 2018, p. 5). Modelos complexos como as GANs (GOODFELLOW et al., 2014, p. 1-9), que aprendem a gerar novos dados e imitam a distribuição dos dados de entrada, são particularmente suscetíveis a esse problema. O desbalanceamento nos dados de treinamento, seja entre classes distintas, como a sub-representação de certas etnias, ou dentro de uma mesma classe, como a escassez de imagens de mulheres em profissões de liderança, leva à geração de resultados que não apenas refletem, mas reforçam estereótipos e desigualdades estruturais (CEBRIAN; FREITAS, 2023).

Essa problemática é aprofundada pela crítica de Emily Bender et al aos grandes modelos de linguagem, que eles metaforicamente denominam papagaios estocásticos (BENDER et al., 2021, p. 611). O argumento central é que, apesar de serem treinados com vastas quantidades de texto extraído da internet, esses modelos não garantem diversidade de perspectivas. Ao contrário, a raspagem massiva de dados tende a super-representar pontos de vista hegemônicos, de usuários mais jovens e de países desenvolvidos, enquanto marginaliza outras vozes (BENDER et al., 2021, p. 613). Dessa forma, os modelos aprendem e propagam padrões de linguagem abusiva, preconceitos e visões de mundo limitadas, que estavam presentes nos dados originais. A sofisticação com que geram textos coerentes esconde o fato de que estão, em essência, recombinando padrões estatísticos sem qualquer compreensão real do conteúdo, o que os torna veículos para a disseminação de desinformação e visões de mundo enviesadas (BENDER et al., 2021, p. 614).

A capacidade de modelos generativos, como as GANs, de gerar dados sintéticos, como conteúdos, imagens, textos, sons que imitam

a realidade, mas que nunca existiram, introduz outra camada de complexidade. A crescente dificuldade em distinguir o conteúdo real do sintético levanta profundas questões sociais e epistemológicas. O risco iminente é a criação de uma infosfera majoritariamente sintética, na qual a informação autêntica se torna cada vez mais rara, diluída em um oceano de conteúdo gerado por máquinas. Esse cenário ameaça erodir a confiança nas fontes de informação e na própria percepção da realidade.

Essa proliferação de dados sintéticos, combinada com a opacidade dos algoritmos, pode representar uma ameaça direta à autonomia humana. Como alerta Doneda, é imperativo avaliar os efeitos dessas tecnologias sobre a autonomia humana para preservar os direitos fundamentais (DONEDA et al., 2018, p. 3). A exposição contínua a um ambiente informacional curado por algoritmos pode limitar o acesso a perspectivas diversas e minar a capacidade crítica do indivíduo, tornando-o mais suscetível à manipulação externa e assim pode comprometer a autodeterminação que é a base de uma sociedade democrática.

A ameaça à autonomia é agravada pela ilusão de compreensão semântica que os modelos de linguagem projetam. Conforme esclarece Floridi, esses sistemas, embora extremamente sofisticados na geração de textos contextualmente relevantes, operam em um nível puramente sintático. Eles são capazes de identificar e replicar padrões estatísticos em sequências de palavras, mas não possuem consciência textual ou a capacidade de compreender o significado, a veracidade ou as implicações do conteúdo que geram (FLORIDI, 2014, p. 137-138). A propensão humana a atribuir significado e intencionalidade a esses textos sintéticos cria um paradoxo: consideramos como informação significativa aquilo que, na definição de Floridi, é apenas conteúdo semântico sem uma confirmação definitiva de sua veracidade ou falsidade (FLORIDI, 2010, p. 42).

Um dos riscos a longo prazo é o do ciclo contínuo de treinamento, onde dados sintéticos gerados por uma IA são coletados e utilizados para treinar a próxima geração de modelos. Esse processo, por vezes chamado de colapso do modelo, pode levar a uma amplificação exponencial de vieses e a uma degradação progressiva da qualidade e da diversidade da informação. O sistema passa a aprender de suas próprias criações, que são reflexos imperfeitos e enviesados da realidade, de forma a entrar em um ciclo de feedback que o distancia cada vez mais do mundo real. A consequência final é a poluição da infosfera com conteúdo de baixa

qualidade e a erosão da confiança pública, não apenas na IA, mas em todo o ecossistema informacional.

A transposição desses desafios para o domínio jurídico revela uma complexidade ainda maior. As iniciativas de uso de IA Generativa no Poder Judiciário e no processo legislativo, embora promissoras em termos de eficiência, levantam questões fundamentais sobre a natureza do direito. Nesse sentido, a Teoria Tridimensional do Direito de Reale oferece um arcabouço teórico indispensável. Reale postula que o fenômeno jurídico é uma unidade indissociável de três dimensões: fato, o acontecimento social, valor, a significação atribuída ao fato, e a norma, a regra que disciplina o fato à luz do valor (REALE, 2002, p. 539). A aplicação da IA no direito, se focada apenas na dimensão da norma, resulta em uma simplificação que pode desconsiderar a complexidade dos fatos sociais e a pluralidade de valores que o direito visa proteger. Portanto, a adoção de tecnologias de IA no campo jurídico exige uma abordagem que respeite essa interdependência e garanta que a eficiência algorítmica não se sobreponha à justiça e à equidade.

Essa interdependência entre as dimensões do direito torna-se particularmente relevante ao considerar a teoria de Lessig sobre a dualidade regulatória na sociedade algorítmica. De acordo com Lessig, o código é lei, demonstra a complexidade relacionada com a governança contemporânea, principalmente em uma sociedade algorítmica. Se o código é lei, de modo a regular o comportamento humano de maneira tão eficaz quanto as normas tradicionais, portanto, existem dois códigos o código-lei visível e o código-fonte invisível, com características técnicas, escrito em linguagem de programação, capaz de codificar valores e estabelecer prioridades de maneira não explícita ou transparente aos seres humanos e sociedade algorítmica (LESSIG, 1999, p. 136-137). Ou seja, uma regulação visível e uma regulação invisível.

A dualidade dos códigos implica que o código-fonte em sistemas de IA não são apenas um conjunto de instruções técnicas, mas um sistema que apresenta características distintas em virtude de sua capacidade de modelar o fato social, de influenciar decisões e regular o comportamento assim como as normas jurídicas tradicionais, ou seja, o código-lei. Os debates sobre a regulamentação da IA reconhecem a complexidade dessa realidade. A proposta de regulamento, tanto no Brasil quanto o regulamento na União Europeia, ao introduzirem ambientes de teste regulatório ou *sandbox,* permite que os sistemas de IA sejam testados dentro de parâmetros

controlados para assegurar a conformidade com os regulamentos existentes. Portanto, o *Sandbox* é um campo de testes que pode verificar se os aspectos regulatórios foram adequadamente implementados ao sistema.

Ou seja, uma parte do processo de conformidade de um sistema de IA envolve transformar a regulação visível em código-fonte, com a finalidade de que os sistemas operem de acordo com os requisitos regulatórios, mitigar riscos imprevisíveis e promover uma forma de controle. Por exemplo, PL 2338/2023 (BRASIL, 2023) ao dispor que a não discriminação é um fundamento, princípio e direito, o código-fonte do sistema de IA deve ser projetado e modelado para evitar o uso de variáveis que resultem em decisões discriminatórias. Logo, o regulamento deixa de ser apenas considerado como uma norma escrita, mas passa a ser integrado diretamente ao processo de desenvolvimento e treinamento de sistemas de IA. Assim, os sistemas podem automaticamente seguir os critérios definidos pelas regulamentações.

Logo, o processo de verificação de conformidade com os regulamentos envolve a transformação da regulação visível (código-lei) em uma forma de regulação invisível, uma vez que a lei será materializada no código-fonte dos sistemas de IA testados. Assim, haveria uma regulação visível que se tornaria invisível pelo código-fonte. Mesmo que os regulamentos envolvam processos democráticos e sejam explícitos em relação aos seus comandos, de maneira neutra e objetiva, a subjetividade dos sistemas de IA podem criar novas formas de regulamentação que não sejam imediatamente evidentes para os seres humanos ou usuários de tais sistemas.

Uma das transformações mais significativas emerge da capacidade crescente da inteligência artificial de gerar código de programação de forma autônoma. Esta revolução, materializada em ferramentas como GitHub Copilot, ChatGPT Code Interpreter e outros sistemas de programação assistida por IA, representa uma mudança fundamental: pela primeira vez na história, não são apenas os humanos que produzem o código computacional.

A OCDE, em seu relatório sobre governança com IA, reconhece que esta capacidade de automação da programação representa tanto uma oportunidade quanto um desafio para a governança pública (OECD, 2024). Por um lado, permite a implementação mais rápida e consistente de políticas públicas através de sistemas automatizados; por outro, introduz novos riscos relacionados à transparência,

Esta transformação é particularmente relevante no contexto do Regulamento de IA da União Europeia (AI Act), que entrou em vigor em 2024 (UNIÃO EUROPEIA, 2024). O regulamento estabelece requisitos específicos para sistemas de IA de alto risco que incluem obrigações de transparência, explicabilidade e auditabilidade. Quando a própria IA é utilizada para gerar o código que implementa as obrigações, surge um paradoxo regulatório: como garantir a transparência de sistemas criados por processos que são, eles próprios, opacos?

A resposta a este paradoxo pode residir no desenvolvimento de metodologias de IA explicável aplicadas à geração de código. Floridi, em sua obra sobre ética da IA, argumenta que a explicabilidade não deve ser vista apenas como um requisito técnico, mas como um imperativo ético fundamental para preservar a agência humana em sociedades cada vez mais automatizadas (FLORIDI et al., 2018, p. 697). No contexto da programação assistida por IA, isso significa desenvolver sistemas capazes não apenas de gerar código funcional, mas de explicar as decisões de design e implementação que orientaram sua criação.

Paralelamente à revolução na programação, observa-se uma tendência emergente de utilização da inteligência artificial no próprio processo de elaboração normativa. Esta aplicação, ainda em seus estágios iniciais, representa uma extensão lógica da capacidade da IA de processar grandes volumes de texto e identificar padrões complexos em documentos jurídicos.

Experiências pioneiras demonstram o potencial da IA para auxiliar na redação de leis, identificação de inconsistências normativas e análise de impacto regulatório. Os Emirados Árabes Unidos tornaram-se o primeiro país a anunciar o uso de IA para revisar e ajustar legislação existente, bem como para escrever leis inteiramente novas, com expectativa de tornar o processo 70% mais rápido (ERIKSSON, 2025). Estes sistemas podem processar vastos corpora de legislação existente, jurisprudência e doutrina para sugerir redações mais precisas, identificar potenciais conflitos normativos e até mesmo prever os efeitos sociais e econômicos de propostas legislativas.

A OCDE, por meio de seus Princípios de IA, enfatizam a importância de uma IA centrada no ser humano e que respeite os valores democráticos (OECD, 2019). No contexto da elaboração normativa, isso significa que a IA deve funcionar como ferramenta de apoio aos legisladores, não como substituta do processo democrático de criação de leis. A legitimidade

democrática da norma jurídica deriva não apenas de seu conteúdo, mas do processo participativo e deliberativo através do qual é criada.

Contudo, o uso de IA na elaboração normativa levanta questões complexas sobre autoria, responsabilidade e legitimidade democrática. Quando um algoritmo sugere uma redação específica que é posteriormente adotada pelo legislador, quem é o verdadeiro autor da norma? Como garantir que vieses algorítmicos não influenciem indevidamente o conteúdo das leis? Como preservar o caráter deliberativo e participativo do processo legislativo em um contexto de automação crescente?

Estas questões tornam-se ainda mais complexas quando é considerado que os próprios sistemas de IA utilizados na elaboração normativa são, eles mesmos, produtos de código gerado por outros sistemas de IA. Emerge assim uma cadeia recursiva de automação: IA que gera o código para sistemas de IA que auxiliam na criação de normas que regulamentam o uso de IA. Esta recursividade não é meramente técnica, mas ontológica, que permite questionar as próprias categorias tradicionais de agência, autoria e responsabilidade no direito.

Apesar dos desafios e riscos identificados, é fundamental reconhecer que a integração da inteligência artificial nos processos jurídicos e normativos também oferece oportunidades significativas para o aprimoramento da justiça e da eficiência do sistema legal. Uma análise equilibrada deve considerar não apenas os perigos, mas também o potencial transformador positivo dessas tecnologias.

Em primeiro lugar, a IA pode contribuir significativamente para a democratização do acesso à justiça. Sistemas de IA podem tornar serviços jurídicos mais acessíveis a populações de baixa renda por meio de sistemas de triagem automatizada de casos e ferramentas de autoatendimento para questões legais simples. Pesquisas sobre o uso de IA no setor público, destaca que a automação inteligente no avanço dos serviços de e-governo com o objetivo de minimizar o tempo de processamento, reduzir custos e melhorar a satisfação dos cidadãos, permite que recursos sejam direcionados para casos mais complexos que requerem expertise especializada (AL-MUSHAYT, 2019, p. 146821-146834).

Segundo, a IA oferece possibilidades para a melhoria da consistência e previsibilidade do sistema jurídico. Algoritmos podem identificar inconsistências na aplicação de normas, detectar padrões de discriminação em decisões judiciais e promover maior uniformidade na interpretação legal. Floridi argumenta que, quando adequadamente implementada, a IA

pode funcionar como um espelho ético de modo que possa contribuir para uma maior equidade no sistema de justiça (FLORIDI et al., 2018, p. 700).

Terceiro, a capacidade da IA de processar e analisar grandes volumes de dados jurídicos pode facilitar a identificação de lacunas normativas e a antecipação de problemas regulatórios. Sistemas de IA podem analisar tendências sociais, econômicas e tecnológicas para sugerir áreas que necessitam de nova regulamentação ou atualização de normas existentes. Esta capacidade preditiva pode tornar o sistema jurídico mais responsivo e adaptável às mudanças sociais.

Quarto, a automação de tarefas rotineiras com o uso da IA pode liberar profissionais do direito para atividades de maior valor agregado, como aconselhamento estratégico, mediação de conflitos complexos e desenvolvimento de políticas públicas inovadoras.

Os desafios impostos pela disseminação da Inteligência Artificial são profundos e multifacetados e toca em questões centrais de justiça, equidade e autonomia. A opacidade dos sistemas, a amplificação de vieses, a proliferação de dados sintéticos e a ameaça à autonomia individual exigem uma resposta regulatória e ética robusta. Como defende Floridi, a IA deve ser projetada para diminuir a desigualdade e promover o empoderamento social, com respeito à autonomia humana (FLORIDI et al., 2018, p. 701). Para isso, a explicabilidade e a transparência não são opcionais, mas sim pilares essenciais para a construção da confiança pública. O objetivo não deve ser, como adverte Floridi, o de adaptar a sociedade a uma IA fraca e reprodutiva, mas sim o de desenvolver uma IA forte e produtiva que sirva para fortalecer os valores e as estruturas de uma sociedade justa e democrática (FLORIDI et al., 2018, p. 143).

5 Considerações finais

O artigo partiu da imersão na infosfera de Floridi e culminou na análise da dualidade regulatória de Lessig e revela que a convergência entre o código-lei e o código-fonte não é uma mera possibilidade futura, mas uma realidade em plena construção. A ascensão da Inteligência Artificial Generativa acelera e complexifica este processo, ao mesmo tempo que introduz uma recursividade inédita: a IA que gera o código para sistemas de IA que, por sua vez, auxiliam na criação de normas que regulamentam a própria IA.

Este ciclo desafia as categorias tradicionais de autoria, responsabilidade e legitimidade democrática e exige um novo paradigma teórico para sua compreensão e governança. A hipótese central do trabalho, de que a automação crescente do direito representa uma reconfiguração ontológica da experiência normativa, foi corroborada. O conceito de código-lei-fonte emerge, portanto, não como uma simples tradução da norma jurídica para a linguagem de máquina, mas como uma síntese teórica que busca articular a eficiência algorítmica com as garantias fundamentais do Estado de Direito. Trata-se de reconhecer que o código-fonte, ao regular o comportamento na infosfera, opera como uma forma de lei, mas que esta lei invisível deve permanecer subordinada à primazia axiológica do código-lei, este sim fruto de um processo democrático e deliberativo.

As experiências pioneiras em jurisdições como os Emirados Árabes Unidos e os debates em torno do *AI Act* da União Europeia demonstram que a automação normativa é uma via de mão dupla. Se por um lado oferece oportunidades para aprimorar a eficiência, a consistência e o acesso à justiça, por outro, acarreta riscos de opacidade, discriminação e erosão da autonomia humana. A resposta a este dilema não reside na rejeição da tecnologia, mas na sua criteriosa incorporação, guiada por princípios éticos sólidos como a explicabilidade, a transparência e o design centrado no ser humano, como defendido pela OCDE e por pensadores como Floridi.

A Teoria Tridimensional do Direito de Miguel Reale mostrou-se um arcabouço teórico indispensável, ao nos lembrar que a norma jurídica é uma unidade indissociável de fato, valor e norma. A aplicação da IA no direito, se focada apenas na dimensão da norma, arrisca-se a uma simplificação. O desafio, portanto, é o de desenvolver sistemas de IA capazes de compreender, ou ao menos respeitar, a complexidade dos fatos sociais e a pluralidade de valores que o direito visa proteger.

Conclui-se, assim, que a compreensão aprofundada e crítica da dinâmica entre Direito e tecnologia tornou-se uma condição de possibilidade para a proteção efetiva dos direitos fundamentais na era digital. O papel do jurista é transformado e exige um conhecimento interdisciplinar que permita dialogar com a ciência da computação, a sociologia e a ética. O desafio é, em suma, o de assegurar que, na infosfera, o código-fonte permaneça sujeito ao primado do código-lei, e que ambos sirvam ao propósito maior de promover a dignidade da pessoa humana. O conceito de código-lei-fonte, como proposto neste artigo, oferece um primeiro passo na construção de um referencial teórico para esta tarefa.

Referências

AL-MUSHAYT, Omar Saeed. Automating E-Government Services with Artificial Intelligence. **IEEE Access**, v. 7, p. 146821-146834, 2019.

ASHTON, Kevin. That 'Internet of Things' Thing. **RFiD Journal**. p. 97-114. 2009.

BECK, Ulrich. **La sociedad del riesgo**: hacia una nueva modernidad. Trad. de Jorge Navarro, Daniel Jiménez, Maria Rosa Borrás. Barcelona: Paidós, 1998. 294 p.

BARRACLOUGH, Tom; FRASER, Hamish; BARNES, Curtis. **Legislation as Code for New Zealand**: Opportunities, risks, and recommendations. 2021. 168 p.

BENDER, Emily M. et. al. On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? Proceedings of FAccT: Fairness, Accountability, and Transparency, p. 610-623, mar. 2021.

BRASIL. **Lei 12.965/2014**. Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 27 set. 2025.

BRASIL. **Lei 13.709/2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm Acesso em: 27 set. 2025.

BRASIL. Projeto de Lei 2.338/2023. Dispõe sobre o uso da Inteligência Artificial.

CASTELLS, Manuel. **A sociedade em rede**. 21ª ed. São Paulo: Paz e Terra, 2020. 629p.

CAVEDON, Ricardo; FERREIRA, Helini Sivini; FREITAS, Cinthia Obladen de Almendra. O meio ambiente digital sob a ótica da Teoria da Sociedade de Risco: os avanços da informática em debate. **Revista Direito Ambiental e Sociedade**, v. 5, p. 194-223, 2015.

CLARKE, Roger. Information technology and dataveillance. **Communications of the ACM**, v. 31, n. 5, p. 498-512, 1988.

CEBRIAN, Fabiana Faraco; FREITAS, Cinthia Obladen de Almendra. Aplicação da ética by design em redes adversárias generativas na proteção da autonomia humana. in: VEIGA, F. S.; BACELAR, J. A. F.; OLIVEIRA, F. A. L. **Direitos fundamentais e sustentabilidade ambiental**, Porto/Belém: Instituto Iberoamericano de Estudos Jurídicos e

Universidade da Amazônia, 2023.

CORMEN, Thomas H. et al. **Algoritmos**: Teoria e Prática. 3. ed. Rio de Janeiro: Elsevier, 2012. 944p.

DONEDA, Danilo Maganhoto. et al. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. **Revista Pensar**, Fortaleza, v. 23, n. 4, p. 1-17, out./dez. 2018.

ERIKSSON, Viktor. Here's the country that will be the first to use AI do write laws. **Computerworld**, 22. abr. 2025. Disponível em: https://www.computerworld.com/article/3967266/heres-the-country-that-will-be-the-first-to-use-ai-to-write-laws.html Acesso em: 27 set. 2025.

FAYYAD, Usama, PIATETSKY-SHAPIRO, Gregory, SMYTH, Padhraic. From Data Mining to Knowledge Discovery: An Overview. In: Advances in Knowledge Discovery and Data Mining. **American Association for Artificial Intelligence**. v. 17, n. 3, 1996. p. 37–54.

FLORIDI, Luciano. **Information:** A Very Short Introduction. Oxford: Oxford University Press, 2010. 130 p.

FLORIDI, Luciano. **The 4th Revolution**: How the Infosphere is Reshaping Human Reality. New York: Oxford University Press, 2014.

FLORIDI, Luciano; et al. **AI4People**: An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. Minds and Machines, n. 28, p. 689-707, nov. 2018.

FREITAS, Cinthia Obladen de Almendra. A obscuridade dos algoritmos e a revisão da tomada de decisão automatizada diante de segredos comerciais e industriais. In: **Sociedade Informacional e Propriedade Intelectual**. Org. Wachowicz, Marcos.; Cortiano, Marcelle. Curitiba: Gedai Publicações/UFPR, 2021.

GENESERETH, Michael. **Computational Law**: The Cop in the Backseat. Stanford Codex Blog, 2016. Disponível em: https://law.stanford.edu/2016/01/13/michael-genesereths-computational-law-the-cop-in-the-backseat Acesso em: 27 set. 2025.

GENESERETH, Michael. What is Computational Law? Complaw Corner, Codex: **The Stanford Center for Legal Informatics**, mar., 2021.

GOODFELLOW, Ian. et al. **Generative Adversarial Networks**. Advances in Neural Information Processing Systems (NIPS 2014), v. 27,

p. 1-9, 2014.

GREENFIELD, Adam. **Everyware**: the dawning age of ubiquitous computing. AIGA: New Riders, 2006.

KITCHIN, Rob. Thinking critically about and researching algorithms. **Information, Communication & Society**, v. 20, n.01, p. 14-29, 2017.

LESSIG, Lawrence. **Code, and other laws of cyberspace**. New York: Basic Books, 1999.

LESSIG, Lawrence. Code is Law: On Liberty in Cyberspace. **Harvard Magazine**, p. 1-5, jan./fev. 2000.

LESSIG, Lawrence. **Code**: Version 2.0. New York: Basic Books, 2006.

LÉVY, Pierre. **O que é virtual**. São Paulo: Editora 34, 2011.

OECD. **AI Principles**. Paris: OECD Publishing, 2019. Disponível em: https://oecd.ai/en/ai-principles Acesso em: 27 set. 2025.

OECD. **Governing with Artificial Intelligence**. Paris: OECD Publishing, n. 20, 2024.

MOHUN, James; ROBERTS, Alex. Cracking the Code: Rulemaking for humans and machines. **OECD** (Organization for Economic Co-operation and Development) - **Working Papers on Public Governance**, n. 42, 2020.

REALE, Miguel. **Filosofia do direito**. 20. ed. São Paulo: Editora Saraiva, 2002.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RUSSEL, Stuart Jonathan; NORVIG, Peter. **Inteligência Artificial**. 3 ed., Rio de Janeiro: Elsevier, 2013.

SCHUILENBURG, Marc; PEETERS, Rick. **The Algorithmic Society Technology, Power, and Knowledge**. New York: Routledge, 2021.

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

UNIÃO EUROPEIA. **Regulamento (UE) 2024/1689** do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial (Regulamento IA). Jornal Oficial da União Europeia, L 1689, 12 jul. 2024.

WADDINGTON, Matthew. **Rule as code**. Law in Context, v. 37, n. 01, p. 179-186, 2020.

WEISER, Mark. Some Computer Science Issues in Ubiquitous Computing. **Communications of the ACM**, v. 36, n. 07. p. 75 - 84, jul. 1993.

Capítulo 4

A *WEB* ESTÁ MORTA? *BOTS* NAS REDES E PERIGOS PARA OS CONSUMIDORES

Heloísa Daniela Nora[1]

1 Introdução

Nas últimas décadas, o avanço tecnológico e o crescimento das redes sociais transformaram a forma como as pessoas se conectam e interagem. Esse novo ambiente dinâmico também trouxe desafios significativos para a proteção dos consumidores, especialmente com a disseminação de *bots* – programas automatizados que interagem de maneira autônoma com usuários *online*.

Especificamente, o Artigo 6º do Código de Defesa do Consumidor (CDC) assegura direitos fundamentais, como a proteção contra publicidade enganosa ou abusiva, e a garantia de informações corretas e completas sobre produtos e serviços. No entanto, a atuação desses robôs, muitas vezes de forma velada e manipuladora, ameaça esses direitos ao veicular conteúdos que nem sempre refletem a realidade, impactando diretamente o comportamento dos consumidores.

Além dos desafios trazidos pela atuação desses robôs, a sociedade contemporânea enfrenta o fenômeno da *Infocracia*, conceito discutido pelo filósofo Byung-Chul Han. Esse termo descreve uma era marcada pela superabundância de informações, em que o excesso de dados leva à manipulação sutil e ao controle das percepções individuais. Na *Infocracia*, a comunicação perde seu caráter autêntico, e os indivíduos são constantemente expostos a conteúdos que visam influenciar seu comportamento, muitas vezes de forma imperceptível. Nas redes sociais, essa realidade é intensificada pela ação dos *bots*, que amplificam o fluxo de informações automatizadas e promovem uma comunicação superficial, direcionada por algoritmos que priorizam o engajamento ao invés da veracidade.

1 Bacharel em Direito pela PUCPR, advogada, mestre em Direito pela PUCPR. Email heloisadnora@gmail.com

Essa dinâmica conecta-se à chamada "Teoria da *Internet* Morta", que sugere que boa parte do conteúdo disponível *online* é gerado não por pessoas reais, mas por robôs programados para simular interações humanas. Segundo essa teoria, a *internet* estaria saturada de conteúdos automatizados: o que diminui a autenticidade das interações e cria uma esfera digital artificial e manipuladora. No contexto de consumo, essa saturação de informações automatizadas torna-se uma ferramenta poderosa para influenciar o comportamento dos usuários, colocando em risco o direito à informação correta e completa, garantido pelo Código de Defesa do Consumidor.

Diante desse cenário, por meio de metodologia hipotético-dedutiva com revisão e levantamento bibliográfico, analisa-se a utilização dos *bots* a fim de responder à seguinte pergunta: os *bots* maliciosos influenciam e prejudicam os consumidores nas redes sociais? A hipótese desenvolvida foi a de que as redes sociais e o aumento na utilização de *bots* é prejudicial para os consumidores. O objetivo geral da pesquisa é demonstrar que o uso de *bots* nas redes pode comprometer o direito dos consumidores à informação clara e verdadeira, promovendo práticas enganosas e manipuladoras que afetam negativamente suas decisões de compra.

2 Na encruzilhada da internet

Nos últimos anos, testemunhamos uma metamorfose contínua da paisagem digital, onde novas tecnologias emergem sem que a sociedade tenha tempo suficiente para adaptar-se. Essa evolução revela uma interseção entre tecnologia, cultura e sociedade, desafiando nossa compreensão convencional da *Internet* como um meio dinâmico e em constante evolução.

No ambiente digital contemporâneo, as redes sociais emergem como poderosas plataformas de comunicação e interação, desempenhando um papel central na formação de opiniões e comportamentos dos consumidores. No entanto, juntamente aos benefícios proporcionados por essas plataformas, surgem também desafios significativos, especialmente no que diz respeito à influência e manipulação por meio de agentes automatizados, conhecidos como *bots* – robôs programados para interagir de forma autônoma, que podem disseminar informações, promover produtos e até mesmo distorcer percepções, tudo de maneira invisível para os usuários (ITSRio, *on-line*).

À luz do Código de Defesa do Consumidor brasileiro, surge a necessidade de analisar como a presença desses robôs nas redes sociais pode impactar esses direitos. O CDC estabelece que toda informação ou comunicação publicitária deve ser clara, precisa e verdadeira, proibindo práticas enganosas que possam induzir o consumidor ao erro (BRASIL, 1990).

Antes de aprofundar o assunto, entretanto, é essencial compreender a posição do consumidor perante a legislação brasileira. Foi com a Constituição Federal de 1988 que o direito do consumidor foi reconhecido como um direito fundamental, previsto no art. 5º, XXXII, que dispõe que: "o Estado promoverá, na forma da lei, a defesa do consumidor" (BRASIL, 1988). Foi apenas em setembro de 1990, que ocorreu a promulgação da lei que instituiu o CDC. Segundo Nunes (2017, p. 15), essa legislação chegou tardiamente no Brasil, uma vez que a proteção ao consumidor já era uma realidade em outros países, como nos Estados Unidos, onde o processo de defesa do consumidor começou com a Lei Sherman, em 1890 – quase um século antes da criação do CDC.

Além disso, a Constituição Federal de 1988, em seu Ato das Disposições Constitucionais Transitórias (ADCT), art. 48[2], determinava que o Congresso Nacional deveria elaborar um código de defesa do consumidor em até 120 dias após a promulgação da Constituição, o que não foi cumprido no prazo estipulado. Esse atraso, conforme apontado por Nunes (2017), evidencia uma defasagem histórica na legislação brasileira em relação à proteção dos direitos do consumidor. Apesar do atraso em sua promulgação, o CDC possui uma base sólida, o que permite uma definição clara das relações de consumo, com base nos elementos objetivos e subjetivos estabelecidos pela doutrina.

Para que se configure uma relação de consumo, é necessário entender que existem elementos objetivos e subjetivos (GRINOVER et al., 2022). Enquanto os elementos objetivos englobam o produto e/ou serviço, os subjetivos tratam do consumidor e fornecedor – sem a presença de um desses elementos, a relação jurídica não é de consumo e deverá ser tratada a partir do direito civil.

Entendidos os atores dessa relação, é interessante analisar seus elementos subjetivos: o consumidor e o fornecedor (GRINOVER et al., 2022). O consumidor, aqui em sentido estrito, encontra sua definição no

2 Texto do art. 48: "O Congresso Nacional, dentro de cento e vinte dias da promulgação da Constituição, elaborará código de defesa do consumidor.".

art. 2º do CDC (BRASIL, 1990): "Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final.". Não apenas o art. 2º dispõe sobre o consumidor, é possível observar no parágrafo único do mesmo artigo que dispõe (BRASIL, 1990): "Equipara-se a consumidor a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo". Também há de mencionar os arts. 17 e 29, igualmente do CDC, que trazem a definição de consumidores equiparados, com a seguinte redação, sucessivamente (BRASIL, 1990): "Para os efeitos desta Seção, equiparam-se aos consumidores todas as vítimas do evento" e "Para os fins deste Capítulo e do seguinte, equiparam-se aos consumidores todas as pessoas determináveis ou não, expostas às práticas nele previstas.". Dentre as características desses consumidores, está a vulnerabilidade, que consta na CF art. 5º, XXXII (BRASIL, 1988). Conforme o art. 4º do CDC, a vulnerabilidade não é apenas característica e sim um princípio que deve ser protegido (GRINOVER, *et al*. 2022).

Quanto ao fornecedor, conforme o art. 3º do CDC, este é compreendido como qualquer pessoa física ou jurídica, de natureza pública ou privada, nacional ou estrangeira, além de entes despersonalizados, que desempenhem atividades relacionadas à produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos, bem como a prestação de serviços. Para Araújo Junior e Giancoli (2024), o fornecedor deve atuar de forma habitual, exercendo uma atividade econômica organizada e contínua, seja empresarial ou não, com o objetivo de fornecer produtos ou serviços no mercado de consumo de maneira independente.

Os elementos objetivos da relação de consumo, por sua vez, são o produto e o serviço. O produto é definido no art. 3º, §1º do CDC, como qualquer bem, seja móvel ou imóvel, material ou imaterial. De acordo com Araújo Junior e Giancoli (2024, p. 31), os produtos são bens econômicos introduzidos pelo fornecedor no mercado de consumo, resultantes de um processo de produção em larga escala, que envolve a transformação econômica.

O serviço, conforme o art. 3º, §2º do CDC, refere-se a qualquer atividade ofertada no mercado de consumo, mediante remuneração, incluindo serviços bancários, financeiros, de crédito e securitários, com exceção das relações de caráter trabalhista. Para que a prestação de serviço se enquadre no âmbito do CDC, ela deve ser contínua, constituindo uma atividade regular e organizada, e não uma transação isolada. Além disso, é

necessário que o serviço seja prestado mediante pagamento, caracterizando uma relação econômica que justifica a aplicação das normas protetivas ao consumidor (ARAÚJO JUNIOR; GIANCOLI, 2024, p. 31).

Embora o sistema de proteção ao consumidor seja uma conquista relativamente recente, ele se baseia em uma sólida estrutura constitucional, complementada por dispositivos materiais que geram impactos positivos na sociedade. Conforme destacado por Efing e Resende (2015, p. 144), os direitos básicos do consumidor, listados no art. 6º do CDC, refletem uma preocupação social do legislador, que, com o devido respaldo constitucional, conseguiu estabelecer uma legislação de ampla proteção. No entanto, é no art. 4º do CDC que se encontram os princípios que fundamentam a Política Nacional das Relações de Consumo, cujo objetivo é atender às necessidades dos consumidores, promover o respeito à sua dignidade, saúde e segurança, além de proteger seus interesses econômicos e melhorar sua qualidade de vida. Esses princípios são construídos com base em dois pilares centrais, a vulnerabilidade, vista anteriormente, e a informação, conforme ressaltam Efing e Resende (2024, p. 131).

O primeiro princípio estabelecido no art. 4º é o reconhecimento da vulnerabilidade do consumidor no mercado de consumo. Esse reconhecimento é essencial, pois parte da premissa de que o consumidor, em geral, encontra-se em desvantagem frente aos fornecedores, necessitando, portanto, de especial proteção. Em seguida, o princípio da ação governamental busca garantir que o Estado atue diretamente para proteger o consumidor, seja por meio de iniciativas próprias, do incentivo à criação de associações representativas ou pela garantia de produtos e serviços com padrões adequados de qualidade, segurança e durabilidade.

A harmonização de interesses entre os participantes das relações de consumo é outro princípio fundamental, pois visa compatibilizar a proteção do consumidor com o desenvolvimento econômico e tecnológico, sempre com base na boa-fé e no equilíbrio entre as partes. A educação e a informação de consumidores e fornecedores também são destacadas, com vistas à melhoria contínua do mercado de consumo. Dessa forma, promove-se o conhecimento dos direitos e deveres de ambos, contribuindo para um ambiente de consumo mais justo e transparente (GRINOVER et al., 2022).

O incentivo ao controle de qualidade e à criação de mecanismos eficientes para a solução de conflitos é um princípio que reforça a responsabilidade dos fornecedores em garantir a segurança e a qualidade

dos produtos e serviços ofertados. Paralelamente, o princípio da repressão de abusos visa combater práticas prejudiciais aos consumidores, como a concorrência desleal e o uso indevido de marcas e invenções, que podem causar danos ao mercado.

A racionalização e a melhoria dos serviços públicos também são prioridades estabelecidas no art. 4º, demonstrando a importância de aperfeiçoar a prestação desses serviços à sociedade. Com a inclusão recente pela Lei nº 14.181/2021, dois novos princípios foram incorporados: a educação financeira e ambiental dos consumidores, visando prepará-los para uma conduta de consumo mais consciente e sustentável, e a prevenção e tratamento do superendividamento, com o intuito de evitar a exclusão social daqueles que enfrentam dificuldades financeiras.

Assim, o conjunto desses princípios não apenas orienta a proteção ao consumidor, mas também estabelece diretrizes para a atuação do Estado e dos fornecedores, promovendo a transparência e a harmonia nas relações de consumo. A estrutura jurídica proporcionada pelo CDC, aliada a esses princípios, visa criar um mercado de consumo equilibrado, onde os direitos dos consumidores são respeitados e as práticas abusivas são reprimidas, garantindo uma melhor qualidade de vida e maior segurança para as partes presentes nessa relação.

Após verificar os princípios e direitos estabelecidos pelo CDC, observa-se que se trata de uma estrutura robusta para a proteção dos consumidores em várias dimensões. Especificamente, o Artigo 6º, inciso IV do CDC assegura direitos básicos, como a proteção contra publicidade enganosa ou abusiva, e a garantia de informações corretas e completas sobre os produtos e serviços ofertados. No entanto, a atuação de *bots* nas redes sociais pode comprometer diretamente esses direitos ao propagar conteúdos que não refletem a realidade, ou que foram concebidos para manipular o comportamento dos consumidores, sem que eles percebam a interferência. Para isso, com auxílio da obra de Byung-Chul Han, será traçado um paralelo entre a *Infocracia* e os consumidores, para que seja possível chegar a problemática do presente trabalho.

3 O consumidor e a infocracia

Ao refletir sobre as transformações da sociedade, Byung-Chul Han (2022), filósofo conhecido por suas análises sobre a sociedade digital, ressalta como a cultura contemporânea é marcada pela pressão constante

para produzir, consumir e comunicar incessantemente. Nesse contexto, insere-se a Teoria da *Internet* Morta, apontando para uma virtualidade saturada por conteúdo repetitivo e algoritmos que promovem uma positividade artificial. Antes de adentrar a Teoria mencionada, entretanto, é importante considerar o papel das redes sociais na configuração dessa realidade digital. Inicialmente concebidas como plataformas para conectar pessoas e compartilhar experiências, as redes sociais assumiram novas formas à medida que se tornaram partes essenciais do cotidiano. No entanto, o que se percebe é que muitas vezes ao invés de promoverem uma comunicação autêntica e significativa, elas se transformam em ferramentas de consumo, impulsionadas por algoritmos que privilegiam o engajamento imediato em detrimento da profundidade e autenticidade.

Nesse cenário, a utilização de robôs automatizados em redes sociais amplifica esse controle invisível, pois esses agentes são programados para promover produtos, ideias ou informações com um único objetivo: maximizar o engajamento e, por conseguinte, o consumo. O resultado é uma paisagem digital saturada por algoritmos, distorcendo a realidade e induzindo comportamentos de consumo que muitas vezes não correspondem às necessidades reais dos consumidores.

As redes sociais tornaram-se espaços onde a atenção é uma mercadoria disputada, moldando não apenas as interações *online*, mas também as percepções do mundo. A incessante busca por compartilhamentos e validação pelos usuários, muitas vezes impulsionadas por pagamentos oferecidos pelas plataformas, criam um ciclo de produção e consumo que se alinham com a visão de Han (2022), como se verá a seguir.

No início do capítulo que segue o nome da obra, *Infocracia*, Han (2022, p. 25) traz a seguinte colocação:

> Ficamos atordoados pela embriaguez de comunicação e informação. O tsunami de informação desencadeia forças destrutivas. Abrange também, nesse meio-tempo, âmbitos políticos e leva a fraturas e disrupções mássicas no processo democrático. A democracia degenera em infocracia.

A sociedade atual pode ser descrita pela embriaguez causada pelo volume esmagador de comunicação e informação – que gera um estado de sobrecarga. A fórmula trazida pelo autor para a submissão do regime de informação é a seguinte: "comunicamo-nos até morrer." (HAN, 2022, p. 34). Em outras palavras, vive-se em uma época em que a comunicação constante e a sobrecarga informacional se tornaram tão dominantes que a

sociedade se encapsula em um ambiente onde a comunicação incessante é incentivada (até mesmo, exigida), levando os usuários a sentirem uma obrigação a se conectar e estar disponíveis. A comunicação incessante pode, paradoxalmente, levar a uma falta de comunicação genuína e significativa, ainda mais quando essa comunicação sequer é realizada com seres humanos.

A fórmula trazida por Han pode ser entendida como uma metáfora potente para descrever o fenômeno em que os indivíduos se veem compelidos a estar permanentemente conectados. A sociedade está imersa em um ciclo de comunicação incessante, onde o silêncio e o distanciamento são quase impossíveis, resultando em uma pressão constante para produzir conteúdo, interagir e *consumir*. Isso cria um ambiente onde a sobrecarga informacional não apenas dificulta a compreensão e análise crítica dos dados recebidos, mas também dilui a qualidade das interações humanas.

A crítica de Han aos *followers* (seguidores) nas redes sociais reflete essa lógica (HAN, 2022, p. 48). Ele compara os seguidores a súditos, subordinados aos influenciadores digitais que ditam tendências, comportamentos e, cada vez mais, padrões de consumo. Esses influenciadores exercem um poder simbólico nas mídias, transformando seus seguidores em *zumbis de consumo* – consumidores passivos que seguem ordens implícitas, movidos não por vontade própria, mas por forças invisíveis como algoritmos e *marketing* digital. Nesse cenário, a comunicação perde seu sentido original de troca autêntica e se transforma em uma mídia de massa, onde indivíduos são manipulados para consumir e reproduzir padrões.

Essa comunicação sem comunidade, como Han descreve, destrói a essência do que deveria ser o diálogo humano. A noção de comunidade implica uma troca recíproca e significativa, algo que as redes sociais, na busca incessante por engajamento, diluíram. O autor sugere que essa dinâmica ameaça a própria democracia, ao transformar os cidadãos em consumidores e seguidores passivos, incapazes de exercer um pensamento crítico ou agir de maneira independente. Nesse novo regime, o poder não está mais na ação política consciente, mas na capacidade de manipular a comunicação e o consumo por meio da tecnologia e dos algoritmos.

A utilização de *bots* nas redes sociais intensifica ainda mais essa distorção. Esses agentes automatizados, muitas vezes programados para replicar padrões de interação humana, adicionam uma camada de artificialidade à já fragilizada comunicação *online*. Esses robôs podem

disseminar conteúdos, influenciar opiniões e, sobretudo, induzir comportamentos de consumo de maneira imperceptível para o usuário. Para o consumidor, os perigos são evidentes: as informações propagadas por *bots* podem ser enganosas, manipuladas e programadas para maximizar engajamento sem qualquer preocupação com a veracidade ou o impacto das mensagens, violando diretamente o que está previsto no art. 6º, inciso IV do CDC (BRASIL, 1990).

Nesse sentido, a ideia de Han sobre o fim da democracia através dessa comunicação superficial encontra eco na crítica ao uso indiscriminado de *bots*; afinal, em vez de facilitar um ambiente de escolhas conscientes e informadas, a automação das interações favorece a criação de um espaço de manipulação, onde o consumidor é constantemente bombardeado com conteúdos que podem não ser genuínos ou transparentes.

Essa reflexão se conecta diretamente com a Teoria da *Internet* Morta, que propõe que uma parcela significativa do conteúdo gerado *online* não é mais produto de interações humanas genuínas, mas sim fruto de algoritmos e robôs automatizados. Isso cria uma virtualidade saturada por interações repetitivas e inautênticas, um ambiente em que a comunicação não promove mais a troca de ideias, mas apenas a reprodução de comportamentos induzidos.

Portanto, os perigos dos *bots* para os consumidores são profundos: ao manipularem informações e comportamentos, eles distorcem as relações de consumo, comprometendo direitos fundamentais garantidos pelo CDC, como a transparência e a veracidade das informações. Além disso, essa proliferação de *bots* alimenta a criação de um ambiente de comunicação artificial, onde os consumidores são levados a tomar decisões sem estarem plenamente conscientes dos fatores que as influenciam, reforçando a crítica de Byung-Chul Han sobre o estado de comunicação na sociedade atual.

Da mesma forma, Manuel Castells (1999), em sua análise da Revolução da Tecnologia da Informação, observa que a produtividade e a competitividade no novo capitalismo informacional derivam diretamente da capacidade de inovação e da flexibilidade. Castells afirma que essa revolução não só gerou uma nova economia, como também transformou as relações de poder em um cenário global interconectado (CASTELLS, 1999). Sua ideia de uma sociedade em rede, organizada em torno de uma cultura da *virtualidade real*, ilustra como as redes de informação permeiam todos os aspectos da vida contemporânea, difundindo-se em uma escala global.

Portanto, ao olhar para essa transformação sob a ótica de Castells, percebe-se que o novo capitalismo informacional e a sociedade em rede não apenas moldam a economia global, mas também influenciam as formas como as informações são consumidas e distribuídas. No entanto, à medida que essas redes se tornam mais complexas e integradas, o controle das informações por algoritmos e *bots* coloca novos desafios à autonomia dos indivíduos e à veracidade dos conteúdos. Esses elementos serão explorados ao analisar a Teoria da *Internet* Morta, que aponta para um cenário digital saturado por interações artificiais, onde grande parte da comunicação não é mais realizada por seres humanos, mas por robôs.

3 A teoria da internet morta

A Teoria da Internet Morta (do inglês, *Dead Internet Theory*) trazia a possibilidade de que a *Internet* conhecida hoje pelos usuários, poderia eventualmente tornar-se um espaço virtual carente de atividade humana e interações. A especulação surgiu da combinação de alguns fatores, como por exemplo, o fato de a maioria do conteúdo consumido *online* ser criado por robôs (PLACIDO, 2024). O ano para o final da *Internet*, para os criadores dela, seria 2016. Por mais que a data já tenha passado, as mudanças no cenário atual trazem realidade para esse cenário, até então, fantasioso.

Antes que o assunto seja aprofundado, é necessário trazer uma breve diferenciação. Apesar da utilização das palavras *Internet* e *web* como sinônimos, existem diferenças entre ambos os conceitos. Enquanto a *Internet*[3] se relaciona com a parte de infraestrutura da rede, a *web* pode ser vista como a camada de aplicações em que o usuário de fato interage com os conteúdos disponíveis (LAUDON; LAUDON, 2007). Dessa forma, a teoria deveria ser chamada de "Teoria da *Web* Morta", afinal, é na *web* que a distribuição de conteúdos está sendo afetada.

Por mais que tenha suas raízes em teorias que parecem distantes da realidade, a Teoria pode ser observada em interações no dia a dia, com o aumento constante de conteúdos sintéticos gerados por robôs. A *web* conhecida pelos usuários pode não estar completamente morta, mas não é possível negar sua transformação ao longo do tempo, mudança esta incrementada pela introdução das tecnologias de Inteligência Artificial

3 Segundo Laudon e Laudon (2007, p. 410) a internet é a rede global que usa padrões universais para conectar milhões de redes diferentes.

(IA). De acordo com o *Bad Bot Report*, realizado pela Imperva em 2024, 49,6% de todo o tráfego da internet revelou-se ser de *bots* isto é, quase metade de toda a movimentação na *web* é realizada por robôs. Em 2023 a *NewsGuard*, através de seu centro de rastreamento de Inteligência Artificial, identificou 49 sites de notícias gerados inteiramente ou em sua maior parte por Inteligência Artificial – os sites funcionam com pouca, ou nenhuma, atividade e supervisão humana e publicam artigos inteiramente escritos por robôs. Parece-nos que se vive um conto de Edgar Allan Poe (1844), onde não se pode acreditar no que se ouve, e apenas uma parte do que você vê[4].

Há oito anos, a teoria da *Internet* Morta era vista como uma tese conspiratória, mas o crescimento do conteúdo criado por *bots* transforma a forma como se navega na *web*. Diante desse cenário, é necessário analisar o impacto dos *bots* maliciosos para compreender os desafios que essa evolução impõe ao consumidor, como a manipulação da informação, a violação de privacidade e a criação de ambientes digitais enganosos.

3.1 *Bots* maliciosos e os perigos para o consumidor

Antes de adentrar no problema dos *bots* maliciosos é interessante compreender a diferença entre um *bot* "bom" e um *bot* "malicioso". Como já discutido, no contexto da internet, um *bot* é uma aplicação de *software*[5] que executa tarefas automatizadas (NORDVPN, 2023). Essas tarefas podem variar de ações simples, como preencher um formulário, a funções mais complexas, como extrair dados de um site.

Os *bots* maliciosos, por sua vez, são aplicações de *software* que realizam tarefas automatizadas com intenções prejudiciais: esses robôs podem extrair dados de *sites* sem permissão para reutilizá-los, obtendo vantagem competitiva (KASPERSKY, *online*). Muitas vezes, são usados para *scalping*, que envolve adquirir itens de disponibilidade limitada e revendê-los a um preço mais alto. *Bots* maliciosos também podem ser utilizados para criar ataques de DDoS[6] direcionados a aplicativos; além de realizar atividades criminosas, como fraude e roubo (BRANDÃO, 2023).

4 Do original: "*Believe nothing you hear, and only one-half that you see*." (POE, 1844, p. 4)

5 Um *software* se define como: "[...] instruções detalhadas e pré-programadas que controlam e coordenam o trabalho dos componentes de *hardware* em um sistema de informação" (LAUDON; LAUDON, 2007, p. 419).

6 É uma tentativa de tornar um sistema, serviço ou rede indisponível para seus usuários, sobrecarregando-o com uma grande quantidade de tráfego malicioso. Esse tráfego geralmente

Entretanto, nem todos os *bots* encontrados na *internet* são maliciosos. Também existem *bots* bons que desempenham funções importantes como, por exemplo, indexar sites para motores de busca ou monitorar o desempenho dos próprios sites. *Googlebot* e *Bingbot* são exemplos de rastreadores de mecanismos de busca que ajudam a criar e manter um índice pesquisável de páginas da *web* (KASPERSKY, *online*). Ao indexar páginas, esses *bots* ajudam as pessoas a encontrar os conjuntos mais relevantes de sites que correspondem às suas consultas. Esses *bots* são essenciais para negócios *online*, permitindo que clientes em potencial encontrem e acessem facilmente seus sites, produtos e serviços (IMPERVA, 2024).

Um exemplo prático de *bot* malicioso prejudicando consumidores através de propaganda enganosa pode ser observado em um exemplo hipotético de campanhas fraudulentas de produtos de emagrecimento nas redes sociais: imagine que um *bot* foi programado para promover um suplemento dietético de efeitos rápidos, supostamente "natural" e "comprovado cientificamente".

Para criar uma falsa credibilidade, esse agente automatizado inunda a página do produto com centenas de avaliações positivas e comentários de "usuários" (na realidade, perfis falsos), destacando perdas de peso rápidas e promessas de resultados sem nenhum esforço. Esses *bots* também replicam esses comentários em grupos de discussão, *hashtags* populares e até enviam mensagens diretas para potenciais consumidores. Dessa forma, ao buscar por informações sobre o suplemento, o consumidor se depara com uma avalanche de avaliações positivas e declarações de sucesso, ficando mais propenso a adquirir o produto acreditando em seus benefícios.

No entanto, ao consumir o produto, o consumidor descobre que ele é ineficaz e, pior, pode causar reações adversas. Esse caso é uma violação direta do artigo 6º do CDC, que garante o direito do consumidor à informação correta e proteção contra propagandas enganosas (BRASIL, 1990). A atuação dos *bots* maliciosos nesse cenário demonstra a vulnerabilidade do consumidor, que confiou nas avaliações como fonte de credibilidade, sem saber que estava sendo induzido por um esquema automatizado de falsificação de opiniões.

Ao propagar publicidade enganosa, esses *bots* violam diretamente o direito dos consumidores a informações claras, verdadeiras e precisas. A capacidade desses robôs de operar em grande escala, simulando interações

vem de várias fontes diferentes (distribuídas), daí o termo *distributed*.

humanas em plataformas de redes sociais, *sites* de avaliação e até mesmo em sistemas de mensagens, aumenta sua eficácia em distorcer a percepção dos consumidores. Assim, eles não só comprometem o direito à informação, mas também exploram a vulnerabilidade, pois o consumidor, sem uma base de dados confiável e transparente, tem suas chances de fazer escolhas informadas severamente prejudicadas.

4 A *internet* está morta?

No cenário em evolução das mídias sociais, o que se observa é uma transformação marcada pelo desenvolvimento rápido das tecnologias. A rede, antes aclamada como um pilar da interação humana e conectividade, se torna cada vez mais artificial. Essa tendência requer um exame crítico, especialmente à luz de suas implicações para o bem-estar social e a integridade da comunicação digital. Essa transição levanta preocupações sobre a diminuição da essência de conexões autenticas na esfera digital, moldando cada vez mais as percepções e comportamentos dos usuários, direcionando a narrativa digital para seus objetivos determinados algoritmicamente.

O problema se agrava porque muitos podem ter dificuldade para discernir o que é real e o que é falso[7], e, nesse sentido, a ideia de Han (2022) sobre o fim da democracia por meio da comunicação superficial se reflete na crítica ao uso indiscriminado de *bots*: em vez de promover um ambiente de escolhas conscientes e informadas, a automação das interações favorece um espaço de manipulação, onde o consumidor é continuamente bombardeado com conteúdos que podem não ser genuínos ou transparentes.

A solução pode residir em uma integração equilibrada e ética. Os consumidores e fornecedores devem estar cientes desses desenvolvimentos. Não é um apelo para evitar o progresso tecnológico, mas para orientá-lo de maneira que respeite e promova os valores humanos e a saúde societal. Priorizar a alfabetização digital, desenvolver ferramentas para detecção de *bots*, com por exemplo, o PegaBot[8] e estabelecer padrões éticos para o uso dessas ferramentas são passos críticos na preservação da integridade dos

7 Aqui, interpretando o "real" como criado por humanos e o "falso" como criado por robôs.

8 É um projeto do Instituto do Tecnologia e Sociedade do Rio de Janeiro (ITS Rio) e do Instituto Equidade & Tecnologia, com apoio e financiamento da União Europeia. Na plataforma, o usuário pode verificar a atividade de uma conta de rede social para saber a probabilidade do perfil ser *bot* (ITSRIO, *online*).

ambientes *online*. Isso implica que, à medida que atravessamos o cenário digital em rápida evolução, o imperativo de uma abordagem centrada no ser humano em interações digitais torna-se cada vez mais evidente.

Embora a integração de *bots* nas mídias sociais introduza novas vias de engajamento e eficiência, ela não deve eclipsar a necessidade fundamental de conexão humana autêntica. Como parte de uma sociedade cada vez mais digital, há uma responsabilidade coletiva de garantir que o avanço tecnológico aprimore, em vez de prejudicar, a experiência humana no domínio digital. A *Internet* e as mídias sociais foram desenvolvidas para facilitar o acesso a boas informações e manter as pessoas conectadas umas às outras; assim, é essencial que esses propósitos sejam preservados. Nesse sentido, escreve Capra (2002, p. 26):

> A cultura que criamos e sustentamos com nossas redes de comunicações determina não só nossos valores, crenças e regras de conduta, mas até mesmo a nossa percepção da realidade.

Dessa forma, percebe-se que a vulnerabilidade do consumidor no ambiente digital é amplificada pela atuação de *bots* maliciosos, que operam de forma invisível e manipuladora, distorcendo informações, influenciando decisões de compra e comprometendo o direito à informação clara e verdadeira, garantido pelo CDC. A presença dessas ferramentas automatizadas evidencia a assimetria de poder e a fragilidade do consumidor frente às complexidades do ambiente *online*, colocando em risco seus direitos fundamentais.

No entanto, afirmar que a internet está completamente "morta", dominada apenas por *bots* e interações automatizadas, pode ser uma visão extrema. A vitalidade da *internet* depende de como é utilizada e de como os usuários são educados para navegar de maneira crítica e informada. A educação digital é, portanto, fundamental para que os consumidores sejam capazes de discernir informações falsas e práticas enganosas, fortalecendo a transparência e a autenticidade nas interações *online*. Ao capacitar os usuários a identificar *bots* maliciosos, promove-se um ambiente digital mais seguro e participativo, onde a *internet* pode continuar a ser um espaço de conexão e troca genuína.

Portanto, a *internet* ainda não está morta, mas sua sobrevivência depende diretamente da combinação de uma educação digital que empodere os consumidores a exercerem seus direitos de forma consciente e protegida.

5 Considerações finais

Diante dos diversos aspectos analisados no artigo sobre a influência dos *bots* maliciosos nas redes sociais e seus impactos no consumidor, pode-se concluir que o ambiente digital contemporâneo apresenta desafios à proteção dos direitos dos consumidores. A atuação desses agentes automatizados com capacidade de disseminar informações enganosas e manipular decisões de compra, evidencia um cenário de vulnerabilidade que compromete princípios fundamentais do CDC, especialmente os direitos à informação verídica e à proteção contra práticas abusivas.

Sob a perspectiva teórica de Byung-Chul Han e Manuel Castells, observa-se que a saturação de interações artificiais – ou a "Teoria da *Internet* Morta" – transforma o ambiente digital em um espaço onde a comunicação genuína e as interações humanas autênticas tornam-se escassas. O consumidor, nesse contexto, é exposto a um fluxo incessante de informações muitas vezes manipuladas por algoritmos e *bots* programados para maximizar o engajamento, distorcendo a realidade e fragilizando a autonomia nas decisões de compra.

Para enfrentar esses desafios, é crucial desenvolver nos consumidores a habilidade de discernir informações verídicas de conteúdos manipulados. A transparência nas interações digitais e o fortalecimento das práticas éticas no uso de *bots* representam um passo importante para preservar a integridade das relações de consumo, permitindo que o ambiente digital continue sendo um espaço de troca genuína, e humana.

Referências

ARAUJO JUNIOR, Marco Antonio; GIANCOLI, Brunno. **Curso de direito do consumidor**. 6. ed. São Paulo: SaraivaJur, 2024.

BRANDÃO. Marcelo. **Bots estão dominando o tráfego das Teles – e isso pode ser perigoso.** Consumidor Moderno, 2023. Disponível em: https://consumidormoderno.com.br/bots-trafego-teles/ Acesso em 11 de nov. de 2024.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República,. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituiçao.htm Acesso em: 27 set. 2025.

BRASIL. Lei Nº 8.078, de 11 de setembro de 1990. **Dispõe sobre a proteção do consumidor e dá outras providências**. Brasília, DF: Diário Oficial da União, 1990.

CASTELLS, Manuel. 1999. **A sociedade em rede**. São Paulo: Paz e Terra, 1999.

EFING, Antônio Carlos; RESENDE, Augusto César Leite de. **Educação para o consumo consciente: um dever do Estado**. Revista de Direito Administrativo, Rio de Janeiro, n. 259, p. 197-224, 12 ago. 2015.

FRITJOF, Capra. **As conexões ocultas: Ciência para uma vida sustentável**. Editora Cultrix, São Paulo: 2022.

GRINOVER, Ada Pellegrini *et al.* **Código brasileiro de defesa do consumidor**: comentado pelos autores do Anteprojeto do CDC e da Lei do Superendividamento. 13. Rio de Janeiro: Forense, 2022. 1 recurso online. ISBN 9786559645527.

HAN, Byung-Chul. **Infocracia: digitalização e a crise da democracia**. Tradução de Gabriel S. Philipson. Petrópolis, RJ: Vozes, 2022.

IMPERVA. **Bad Bot Report**. 2024. Disponível em: https://www.imperva.com/resources/resource-library/reports/2024-bad-bot-report/ Acesso em: 27 set. 2025.

ITSRio. **PegaBot: Descubra se aquele perfil de rede social é bot**. Plataforma em fase de testes. Disponível em: https://itsrio.org/pt/projetos/pegabot/ Acesso em: 27 set. 2025.

KASPERKY. **Bots – significado e definição**. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-are-bots# Acesso em: 27 set. 2025.

LAUDON, Kenneth C.; LAUDON, Jane P. **Sistemas de Informação Gerenciais**. Tradução de Thelma Guimarães. 7. ed. São Paulo: Pearson Prentice Hall, 2007.

NEWSGUARD. **Rise of the Newsbots: AI-Generated News Websites Proliferating Online.** 2023. Disponível em: https://www.newsguardtech.com/special-reports/newsbots-ai-generated-news-websites-proliferating/ Acesso em: 27 set. 2025.

NORDVPN. **O que são bots, tipos de bots e os perigos que eles trazem**. 2023. Disponível em: https://nordvpn.com/pt-br/blog/bot-o-que-e/ Acesso em: 27 set. 2025.

NUNES, Luiz Antonio Rizzatto. Consumidor. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: **Direitos Difusos e Coletivos**. Nelson Nery Jr., Georges Abboud, André Luiz Freire (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/320/edicao-1/consumidor Acesso em: 27 set. 2025.

PLACIDO, Dani Di. **The Dead Internet Theory, Explained**. Forbes, 2024. Disponível em: https://www.forbes.com/sites/danidiplacido/2024/01/16/the-dead-internet-theory-explained/?sh=50c6b60557c2 Acesso em: 27 set. 2025.

POE, Edgar Allan. **The System of Dr. Tarr and Prof. Fether**. 1844. Disponível em: https://pinkmonkey.com/dl/library1/tarr.pdf Acesso em: 27 set. 2025.

Capítulo 5

REDES DE INDIGNAÇÃO DE (DES) ESPERANÇA

Heloísa Daniela Nora[1]
Willian Ryutaro Kobe[2]

1 Introdução

O conceito de ciberespaço, inicialmente cunhado por William Gibson na década de 1980, descreve um ambiente imersivo onde a mente humana pode acessar e manipular dados através de interfaces neurais. Essa visão futurista estabeleceu uma fundação significativa para a compreensão da interação entre homem e máquina, influenciando o imaginário popular sobre a tecnologia e o futuro digital.

Complementando a visão de Gibson, Pierre Lévy, filósofo francês conhecido por suas contribuições ao estudo das tecnologias digitais, ampliou o conceito de ciberespaço como um vasto terreno de interação humana. Contudo, a cibercultura também traz desafios significativos para a democracia – a interconexão global de computadores e redes levanta questões sobre como os movimentos sociais que emergem nesse ambiente podem impactar a ordem democrática no mundo físico, ou o mundo "real".

Neste contexto, o trabalho pretende estudar os movimentos sociais que se impulsionam pelas redes, trazendo questionamentos sobre sua regulação. Como metodologia de pesquisa, adotou-se o método dedutivo e bibliográfico, formulando-se hipótese como ponto de partida desta pesquisa, bem como pela revisão e análise crítica da literatura existente acerca da temática. Diante deste cenário, observou-se o presente problema de pesquisa: regular as redes sociais é a resposta?

Como hipótese, formulou-se que: nos tempos atuais, a *Internet* é mais que um mero meio de comunicação. Logo, buscando confirmar a

1 Bacharel em Direito pela PUCPR, advogada, mestre em Direito pela PUCPR. Email heloisadnora@gmail.com

2 Bacharel em Direito pela PUCPR, advogado licenciado, mestre em Direito pela PUCPR. Email william.taro@gmail.com

hipótese e orientar o trabalho, estabeleceu-se como objetivos: analisar os conceitos de cibercultura, ciberdemocracia, democracia e os movimentos sociais impulsionados pelas redes.

Este artigo explora essas dinâmicas investigando como a cibercultura pode tanto fomentar a participação democrática quanto ser usada para minar as bases da ordem democrática. A partir das ideias de pensadores como Gibson, Lévy e Castells, busca-se compreender as contradições e implicações da interação entre ciberespaço, sociedade e democracia, especialmente no contexto de eventos significativos que ilustram essas tensões. Como principal conclusão, constatou-se que a análise das dinâmicas entre tecnologia e sociedade é vital para maximizar os benefícios da cibercultura, promovendo um futuro digital democrático e seguro.

2 O não-espaço da mente e a cibercultura

No panorama contemporâneo, a interseção entre tecnologia e sociedade é cada vez mais evidente e impactante. A emergência da cibercultura como um campo de estudo reflete não apenas a proliferação das tecnologias digitais, mas também a forma como essas tecnologias moldam e são moldadas pelas práticas culturais e sociais. A sociedade é marcada pela utilização de recursos tecnológicos e evoluções alavancadas nesse meio, sobretudo aos espaços conectados à rede mundial de computadores.

O termo *ciberespaço* foi empregado pela primeira vez por William Gibson (1984), em sua obra escrita na década de 1980 – onde aproxima a relação entre o homem e a máquina, instaurando um modelo futurista em uma época preponderantemente analógica: "O ciberespaço [...]. Linhas de luz alinhadas que abrangem o universo não-espaço da mente; nebulosas e constelações infindáveis de dados" (GIBSON, 1984, p. 25). Gibson descreve o ciberespaço como um ambiente imersivo, onde a mente humana pode acessar e manipular dados através de interfaces neurais, navegando por uma paisagem digital tridimensional. O termo cunhado por Gibson se tornou emblemático e influenciou profundamente o imaginário popular sobre tecnologia e o futuro digital, além disso, sua representação como um espaço vasto e misterioso, repleto de oportunidades e perigos, ecoando nas discussões contemporâneas sobre a *Internet* e a sociedade digital.

Essa interconexão global de computadores e redes é entendida por Gibson como um não-espaço. Então é interessante indagar se os movimentos sociais que se reverberam nesse local poderiam impactar tanto

a rede de forma a trazer perigo para a democracia no mundo físico. Seriam as linhas de luzes, aqui interpretadas como fluxos de dados e informações que transitam nesse não-espaço da mente, um lugar onde as ideias transcendem essas limitações? A imensidão e complexidade desse ciberespaço, igualadas a nebulosas e constelações, são possíveis de se regular?

A visão quase fantasiosa de William Gibson sobre o ciberespaço como um ambiente imersivo e tridimensional, onde a mente humana pode navegar e manipular dados, estabeleceu uma fundação significativa para a forma como se concebe a interação entre homem e máquina. Essa perspectiva futurista, não só influenciou o imaginário popular sobre o futuro digital, mas também suscitou debates sobre as potencialidades e os riscos desse novo domínio. Foi inserido nesse contexto que Pierre Lévy (1956), filósofo francês conhecido por suas contribuições ao estudo das tecnologias digitais amplia o conceito de ciberespaço – as linhas de luz alinhadas que abrangem o universo não-espaço da mente, interpretando-o como um vasto terreno de interação humana que deve ser acessível a todos ali inseridos. Lévy destaca a importância de democratizar o acesso às tecnologias para a construção de uma *tecnodemocracia*, onde a participação ativa de todos os indivíduos pode promover uma sociedade mais inclusiva e colaborativa. Assim, a visão de Gibson e Lévy converge na ideia de que o ciberespaço, além de um campo de possibilidades tecnológicas, é também um espaço de transformação social profunda e inclusiva.

Para o francês, reconhecido por sua postura otimista em relação à cibercultura e ciberdemocracia, é na esfera da virtualidade que a contemporaneidade produz o conhecimento, definindo a cibercultura como: "o conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço." (LÉVY, 1999, p. 17).

Lévy (1999, p. 185) enxerga no ciberespaço não apenas a *Internet*, mas um vasto terreno onde a humanidade se manifesta e interage em todas as suas dimensões. Um espaço que requisita uma comunicação interativa e comunitária, que possibilita a abertura para a criação de um formato de inteligência que se torna coletiva. Para ele, democratizar o acesso às tecnologias é essencial para concretizar uma *tecnodemocracia*, na qual todos possam participar ativamente do desenvolvimento e uso dessas ferramentas, contrariando a predominância das multinacionais e grandes corporações. Nesse sentido, o francês não apenas vislumbra o ciberespaço como uma revolução, mas como um espaço onde a sociedade pode alcançar novos

patamares de inclusão, participação e colaboração, construindo assim um futuro mais democrático e igualitário.

Ao decorrer de sua obra, mais especificamente no capítulo que atine às proposições, Lévy (1999, p. 185-199) assevera que os impactos da era digital na esfera democrática são profundos, destacando múltiplas facetas que configuram a ciberdemocracia, a qual se centra no conceito de inteligência coletiva, pelo qual Lévy argumenta que a cibercultura capacita grupos a colaborar e compartilhar conhecimento de maneiras inovadoras, transcendendo barreiras físicas e geográficas tradicionais. A concepção da *Internet* como um espaço público imaterial é outro aspecto essencial em sua abordagem, onde o autor vislumbra nesta plataforma digital um ambiente propício para debates democráticos e interações participativas, onde indivíduos podem contribuir de maneira equitativa para a formação de opiniões coletivas.

Além disso, o autor enfatiza vigorosamente a democratização do conhecimento viabilizada pela cibercultura, sendo que esta nova era digital oferece oportunidades sem precedentes para reduzir disparidades informacionais entre diferentes estratos sociais, ampliando assim o acesso universal à informação e ao saber, promovendo a participação política e engajamento cívico que emergem como outras dimensões cruciais exploradas por Lévy, na medida em que a cibercultura facilita formas inclusivas de participação nas decisões democráticas, antes restritas por limitações físicas e estruturais, fomentando uma esfera pública mais dinâmica e acessível.

Por fim, Pierre (1999, p. 185-199) examina como a cibercultura fomenta novas modalidades de expressão política e organização social, catalisando movimentos sociais e ativismo online que transcendem fronteiras físicas e desafiam hierarquias estabelecidas, muito parecido com o que se observará no próximo tópico, quando apresentado o trabalho de Manuel Castells.

Assim, através de suas ideias visionárias e profundamente reflexivas Lévy oferece um panorama abrangente e provocativo sobre o papel transformador da cibercultura na contemporaneidade, convidando à reflexão sobre os caminhos futuros da democracia digital. Contudo, embora o filósofo francês adote uma perspectiva otimista quanto ao potencial democratizador da tecnologia digital, não deixa de reconhecer os desafios e dilemas associados, como questões de poder e controle que permeiam esses

avanços, ressaltando a necessidade de um exame crítico contínuo sobre as repercussões sociais e políticas da ciberdemocracia.

De fato, a influência nas questões políticas é significativa, pois o ciberespaço facilita formas inclusivas de participação nas decisões democráticas, antes restritas por limitações físicas e estruturais. A cibercultura capacita grupos a colaborar e compartilhar conhecimento de maneiras inovadoras, promovendo a participação política e o engajamento cívico. No entanto, o mesmo ambiente que promove a democracia pode também ser usado para atentados contra a ordem democrática, assim, embora haja um potencial democratizador, é necessário um exame crítico contínuo das repercussões sociais e políticas da ciberdemocracia.

Logo, pela análise das ideias de Lévy, observa-se que cibercultura pode fortalecer a democracia por meio da promoção da participação social, no entanto, a realidade percebida nos tempos atuais indica que o mesmo ambiente que poderia incentivar a participação em prol da democracia, pode, como observado pelo incidente do dia 08 de janeiro de 2023, instrumentalizar atentados contra a ordem democrática. No próximo tópico, serão exploradas as dinâmicas e implicações dessas contradições, buscando compreender como a cibercultura pode tanto fomentar a participação democrática quanto ser usada para minar as bases da ordem democrática.

3 A democracia e o não-espaço

Insere-se nesse contexto de uma sociedade conectada por fios invisíveis de conexão institutos que existem há tempos e se consolidam em nossa sociedade. O lugar (ou, talvez, não-lugar) onde as ideias e informações transcendem as limitações físicas ainda demandam conexões e bases para seu funcionamento. A democracia, palavra que carrega o significado de ser o "poder do povo", é um conceito fundamentado na noção de uma comunidade política em que todas as pessoas possuem o direito de participar dos processos políticos e de debater políticas de igual para igual, alimentados pela liberdade de expressão e dignidade humana. Na democracia ateniense nunca deve ter se imaginado que instrumentos democráticos estariam sendo debatidos em aparelhos movimentados por correntes elétricas, transistores, linhas de código e protocolos que os conectam a redes de interação contínua. Mas, antes de

discutir a ciberdemocracia nas redes sociais, é interessante observar como a democracia em si pode ser pensada no contexto brasileiro.

No voto de Rosa Weber (BRASIL, 2023, p. 13), ao discutir a democracia, parte-se de uma noção de uma democracia consensual que categoriza o instituto enquanto processo de conflitos que comporta formas ampliadas de respostas e de contestabilidade. Nesse modelo, entretanto, as eleições não esgotam os procedimentos de solução de desacordos, tampouco encerram os arranjos participativos da sociedade e da veiculação de suas preferencias heterogêneas.

No cenário da democracia constitucional (BRASIL, 2023), estruturada pelo ideal de compartilhamento de poder e responsabilidade entre diversas instituições e regras, entre os Poderes da República e a heterogeneidade do tecido social, a participação, a representação e o controle de constitucionalidade assumem a condição de elementos cardinais dos processos decisórios. Nesse perfil da democracia constitucional enquadra-se o estado democrático de direito brasileiro consagrado com a Constituição Federal de 1988. O que significa afirmar o compromisso constitucional como razão para o agir de todos os atos estatais, e mesmo os particulares. A vigência das normas nas democracias constitucionais deve observância ao parâmetro de controle constitucional.

Nesse sentido, Arend Lijphart (2000, p. 7) distingue entre democracia majoritária e democracia consensual com base em suas características institucionais e nos princípios que orientam suas práticas políticas:

> El contraste entre mayoritarismo y consenso aparece en la definición más básica y literal de democracia, a saber, gobiemo del pueblo o, en el caso de la democracia representativa, gobiemo de los representantes del pueblo. La famosa estipulación del presidente Abraham Lincoln va más allá y afirma que el gobiemo es no sólo del pueblo sino también para el pueblo o, lo que es lo mismo, el gobiemo actúa de acuerdo con las preferencias del pueblo.[3]

Na democracia majoritária, a característica principal é a regra da maioria, onde decisões políticas são tomadas com base no apoio da maioria simples dos representantes eleitos. Esse modelo tende a concentrar o poder

3 Tradução livre: O contraste entre majoritarismo e consenso aparece na definição mais básica e literal de democracia, a saber, governo do povo ou, no caso da democracia representativa, governo dos representantes do povo. A famosa estipulação do presidente Abraham Lincoln vai além e afirma que o governo é não só do povo, mas também para o povo, ou seja, o governo age de acordo com as preferências do povo.

em um único partido ou grupo, facilitando uma governança mais ágil, mas potencialmente excluindo minorias da tomada de decisões. As democracias majoritárias geralmente apresentam sistemas eleitorais majoritários ou de pluralidade, como o sistema de voto distrital uninominal, que favorecem a formação de governos com maiorias sólidas e estáveis. Além disso, a democracia majoritária frequentemente exibe um executivo dominante em relação ao legislativo, um sistema bipartidário, um sistema unitário e centralizado de governo, e uma constituição flexível que pode ser alterada com maior facilidade, ainda segundo Lijphart (2000, p. 8):

> Ésta es la esencia del modelo mayoritario de democracia. La respuesta mayoritaria es simple y directa y desprende un gran atractivo, puesto que es obvio que el gobiemo de la mayoría y de acuerdo con los deseos de la mayoría se acerca más al ideal democrático de 'gobiemo del y para el pueblo' que el gobiemo por y de acuerdo con una minoría.[4]

Em contraste, a democracia consensual é caracterizada por uma ampla inclusão e compartilhamento de poder entre diversos grupos políticos, sociais e étnicos. Este modelo busca uma governança mais inclusiva e representativa, promovendo a estabilidade política em sociedades heterogêneas. As democracias consensuais utilizam sistemas eleitorais proporcionais, que asseguram uma representação mais equitativa das minorias e incentivam a formação de coalizões multipartidárias. Lijphart (2000) destaca que nas democracias consensuais, o poder executivo e legislativo tendem a ser equilibrados, há uma tendência ao multipartidarismo, e um sistema de governo descentralizado e federalista é comum. Além disso, as constituições nas democracias consensuais são frequentemente rígidas, requerendo maiorias qualificadas para serem alteradas, o que proporciona uma proteção adicional contra mudanças impulsivas e assegura a estabilidade das regras do jogo político.

Lijphart (2000) argumenta que, embora as democracias majoritárias possam ser mais eficientes na tomada de decisões, as democracias consensuais são mais eficazes em promover a coesão social e a estabilidade em sociedades pluralistas. As democracias consensuais, ao promoverem a inclusão e a participação de uma maior diversidade de grupos, tendem a ser mais estáveis e a proporcionar uma governança mais equitativa e duradoura. Essa distinção entre os dois modelos de democracia

4 Tradução livre: Esta é a essência do modelo majoritário de democracia. A resposta majoritária é simples e direta e possui um grande apelo, pois é óbvio que o governo da maioria e de acordo com os desejos da maioria se aproxima mais do ideal democrático de "governo do e para o povo" do que o governo por e de acordo com uma minoria.

é fundamental para entender como diferentes sistemas políticos podem ser desenhados para melhor atender às necessidades específicas de diferentes sociedades. Levando em consideração o voto de Rosa Weber (BRASIL, 2023), o modelo de democracia que mais se assemelha ao contexto brasileiro é o da democracia consensual, afinal, é um modelo que enfatiza a inclusão, a participação e o controle de constitucionalidade, destacando a importância da participação, representação e a contestabilidade contínua dos processos decisórios, indo além das eleições como único mecanismo de solução de desacordos.

Entretanto, a introdução da ciberdemocracia proposta por Pierre Lévy (1999) nesse panorama apresentado até então, adiciona uma nova dimensão à análise de Lijphart (2000) sobre democracia majoritária e consensual. Lévy propõe que a ciberdemocracia, facilitada pelo avanço das tecnologias digitais e da *Internet*, pode transformar a forma como a democracia é praticada, promovendo uma participação mais direta e constante dos cidadãos nos processos políticos. A ciberdemocracia, como visto no primeiro tópico do trabalho, possui o potencial de aumentar a transparência, a comunicação e a colaboração entre governantes e governados, ampliando as oportunidades para a deliberação pública e a tomada de decisões compartilhada.

Integrando as ideias de Lijphart e Lévy, pode-se argumentar que a ciberdemocracia tem o potencial de mitigar algumas das limitações tanto da democracia majoritária quanto da consensual. Por exemplo, em um sistema majoritário, onde a exclusão de minorias pode ser um problema, a ciberdemocracia pode facilitar mecanismos de participação que garantam que vozes diversas sejam ouvidas e consideradas. Em sistemas consensuais, onde a negociação e o compromisso são fundamentais, as plataformas digitais podem aprimorar a comunicação e a coordenação entre diferentes grupos, tornando o processo de construção de consenso mais eficiente e inclusivo.

Arend Lijphart, em suas teorias sobre democracia majoritária e consensual, e Pierre Lévy, com sua proposta de ciberdemocracia, fornecem uma base para entender como as redes digitais podem potencializar a governança democrática. Nesse sentido, Manuel Castells (2013) oferece uma análise crítica sobre o impacto das redes sociais e das tecnologias de comunicação na formação de novos movimentos sociais, que emergem como respostas às crises de legitimidade e representação das democracias liberais. A partir deste ponto é que se examinam como as redes sociais

impulsionam a democracia e fomentam novos movimentos, explorando as ideias de Castells e sua relevância para a prática democrática na era digital.

4 Movimentos sociais na rede

Os movimentos sociais, para Castells (2013), surgem do sentimento compartilhado de injustiça, desigualdade e opressão, facilitado pela capacidade das tecnologias de rede de criar um sujeito coletivo global. Antes da era digital os movimentos sociais dependiam de líderes formais, tornando-se vulneráveis à repressão através da detenção daquele que os liderava. As redes sociais, no entanto, permitem que esses movimentos se auto-organizem, automobilizem e autoliderem, transformando a rede no sujeito coletivo de mobilização e liderança. Exemplos notáveis incluem o Movimento Primavera Árabe e o *Occupy Wall Street*, que se beneficiaram significativamente da mobilização e coordenação via redes sociais.

O Movimento Primavera Árabe (ELIAS, 2023) foi uma série de protestos, levantes e revoluções que ocorreram principalmente no Oriente Médio e no Norte da África, a partir de dezembro de 2010. Esse movimento foi impulsionado por uma combinação de fatores sociais, econômicos e políticos, incluindo corrupção, falta de liberdade política, desemprego, desigualdade social e violação de direitos humanos. Essa insatisfação generalizada com regimes autoritários e a busca por maior justiça social e política foram os fatores principais que desencadearam os movimentos.

O ponto de partida ocorreu na Tunísia, em dezembro de 2010, quando Mohamed Bouazizi, um jovem comerciante de 25 anos, ateou fogo ao próprio corpo como forma de protesto às atitudes de autoridades locais (GARDNER, 2011). Esse ato desesperado desencadeou uma onda de protestos massivos que levou à queda do presidente Zine El Abidine Ben Ali, que estava no poder há mais de duas décadas, em janeiro de 2011. A partir da Tunísia, os protestos rapidamente se espalharam para outros países da região, incluindo Egito, Líbia, Síria, Iémen e Bahrein, cada um com suas especificidades e desfechos.

As redes sociais desempenharam um papel crucial na organização, mobilização e disseminação de informações durante a Primavera Árabe, segundo Castells (2013, p. 11): "Os movimentos espalharam-se por contágio num mundo ligado pela internet sem fio e caracterizado pela difusão rápida, viral, de imagens e ideias.". Plataformas como *Facebook, Twitter, YouTube* e outros se tornaram ferramentas essenciais para ativistas

e cidadãos comuns que buscavam promover mudanças e desafiar regimes autoritários (CASTELLS, 2013, p. 11):

> Movimentos sociais conectados em rede espalharam-se primeiro no mundo árabe e foram confrontados com violência assassina pelas ditaduras locais. Vivenciaram destinos diversos, incluindo vitorias, concessões, massacres repetidos e guerras civis.

Nos Estados Unidos, o movimento *Occupy Wall Street* (OWS) (OCCUPY WALL STREET, 2019), foi igualmente conectado em redes no ciberespaço e no espaço urbano. Em resumo, foi um protesto social que começou em setembro de 2011, em Nova York. Inspirado pelos movimentos da Primavera Árabe, o OWS visava chamar a atenção para as desigualdades econômicas e sociais, a corrupção política e a influência desproporcional das grandes corporações nos processos democráticos. O slogan *We are the 99%*[5] tornou-se o lema do movimento, destacando a disparidade entre a vasta maioria da população e o 1% mais rico.

O *Occupy* não tinha uma liderança centralizada ou uma lista de demandas formais: era um movimento que funcionava como uma plataforma para diferentes grupos e indivíduos expressarem suas preocupações e propostas. No entanto, alguns dos principais temas incluíam a desigualdade econômica, com críticas à crescente disparidade entre ricos e pobres e a exigência de uma distribuição mais justa da riqueza. As redes sociais desempenharam um papel crucial na organização e disseminação de informações, como bem descrito por Castells (2013, p.12):

> Nos Estados Unidos, o movimento *Ocuppy Wall Street,* tão espontâneo quanto os outros e igualmente conectado em redes no ciberespaço e no espaço urbano, tornou-se o evento do ano e afetou a maior parte do país, a ponto de a revista Time atribuir ao "Manifestante" o título de personalidade do ano. E o lema dos 99%, cujo bem-estar fora sacrificado em benefício do 1% que controla 23% das riquezas do país, tornou-se tema regular na vida política americana.

A globalização e a informacionalização, impulsionadas por redes de tecnologia, melhoram a capacidade produtiva, a criatividade cultural e o potencial de comunicação, mas também têm privado sociedades de direitos políticos e privilégios. Castells (2013) destaca que a aceleração do tempo histórico e a abstração do poder nas redes de computadores desintegraram os mecanismos tradicionais de controle social e representação política e isso resulta em uma crise de legitimidade, onde os cidadãos percebem que os atores do sistema político não os representam mais. A desconexão

5 Com tradução literal para: *nós somos os 99%.*

entre o que os cidadãos pensam e querem e as ações daqueles que elegemos alimenta essa crise, exacerbando o sentimento de impotência e alienação.

Castells (2013) também introduz o conceito de *espaço da autonomia*, onde a interação entre o espaço dos fluxos na *internet* e o espaço dos lugares ocupados cria um ambiente híbrido para a ação coletiva. Esse espaço permite que os movimentos sejam simultaneamente locais e globais, conectando-se com o mundo inteiro e aprendendo de outras experiências de mobilização. A horizontalidade das redes favorece a cooperação e a solidariedade, reduzindo a necessidade de liderança formal e fomentando uma desconfiança profunda em relação à delegação de poder.

Em sua obra "Ruptura: a crise da democracia liberal", Castells (2018) traz um conceito interessante sobre a construção do "eu" na era digital, enfatizando como as redes sociais e as tecnologias de comunicação moldam a identidade individual e coletiva. O autor argumenta que a emergência dessas tecnologias transforma até a construção da identidade; as redes sociais permitem a construção de identidades múltiplas e dinâmicas que facilitam a expressão pessoal e a autonomia digital. Esse fenômeno reflete em mudanças significativas em relação as formas tradicionais de construção de identidade, formando um novo "eu" contemporâneo. Talvez esse "eu" receba conteúdos direcionados e nunca veja o outro lado da moeda. Talvez esse "eu" não consiga distinguir informações falsas de verdadeiras na rede (CASTELLS, 2018).

A análise de Manuel Castells sobre o "eu" na era digital revela uma transformação profunda na maneira como as identidades são formadas e vividas – as redes e esse não-espaço criam oportunidades para a autoexpressão e a construção de identidades múltiplas e dinâmicas. O espaço da autonomia que emerge dessas interações digitais permite que os indivíduos exerçam maior controle sobre suas identidades e encontrem comunidades de apoio e validação. Esta evolução tem implicações significativas para a democracia e os novos movimentos sociais, pois a construção do "eu" está intrinsecamente ligada à capacidade de participação e mobilização coletiva.

Entretanto, não apenas movimentos em prol da democracia se desenvolvem nesse novo ambiente facilitado pelas redes sociais. Os ataques do dia 08 de janeiro foram amplamente influenciados pelas redes, que serviram como uma plataforma para a mobilização e organização das manifestações. A rápida conexão entre os apoiadores do ex-presidente Jair Bolsonaro (PL) feitas pelas redes permitiu que as "convocações" para o ato transcendessem barreiras geográficas e físicas, além de serem

usadas para transmitir ao vivo os eventos, criando um ciclo contínuo de retroalimentação entre as ações físicas e as reações online (SCHREIBER, 2024).

As redes sociais desempenharam um papel crucial na mobilização e mudança social ao permitir a comunicação instantânea e a coordenação de ações coletivas. Castells (2013) observa que a mudança social é essencialmente motivada emocionalmente, e que as redes sociais facilitam a superação do medo e o compartilhamento de indignação. A raiva e a identificação de responsáveis catalisam a mobilização, enquanto o entusiasmo e a solidariedade, reforçados pela comunicação em rede, transformam indivíduos em um ator coletivo consciente. Após os ataques realizados em território brasileiro, surgem novamente os debates sobre regulação desses ambientes digitais.

4 Reflexões sobre redes sociais e sua regulação

A regulação das redes é um assunto muito debatido no contexto de uma sociedade envolvida em uma cibercultura. Isso devido à medida que o uso da Internet expande – permitindo a liberdade dos usuários ao publicar conteúdos e comunicar-se a todo momento por meio de diversos recursos inseridos nesse não-espaço. Entretanto, como visto no tópico anterior, os fins dessas comunicações nem sempre trazem ações sem consequências. Uma das preocupações centrais desses debates é a responsabilidade das plataformas por conteúdos publicados por seu usuário (caso houvesse dano a um terceiro envolvido). Essa é uma discussão que se apresenta na área da responsabilidade civil; e é desse movimento que surgem questões que seguem o objetivo principal desse trabalho: seria a regulação das redes a resposta?

Como bem explorado por Teffé (2024) em seu artigo, as plataformas digitais já foram vistas como intermediadoras neutras de conteúdo, servindo como uma plataforma, com pouco ou nada de gerência sobre o conteúdo gerado por seus usuários. Mas, com o aumento do volume de conteúdo nocivo nas redes, o que se percebe é um movimento de mudança na percepção do papel das redes. Nos Estados Unidos, as decisões da Suprema Corte perpassam o tema ao analisar se provedores de aplicações podem se enquadrar como uma rede de apoio na realização de atentados terroristas, por exibirem conteúdos relacionados ao grupo Estado Islâmico (ISIS)[6].

6 A Suprema Corte dos Estados Unidos decidiu por unanimidade que as plataformas de redes

Em um dos casos, *Twitter vs. Taamneh*, a família de Nawras Alassaf (vítima fatal de um ataque terrorista) tentou responsabilizar o *Twitter, Facebook* e *Google* por disseminar informações e "encorajar" o ataque. O outro, *Gonzalez vs. Google*, a família de Nohemi Gonzalez acusou o Google como responsável pelo ataque terrorista perpetrado pelo ISIS em Paris (2015) por promover vídeos do grupo no *YouTube*. Ambas as alegações foram rejeitadas pela decisão unanime proferida pela Suprema Corte.

O ministro responsável pela decisão, Clarence Thomas, fundamenta sua decisão escrevendo: "A mera criação desses algoritmos não constitui culpabilidade, mais do que ocorreria com uma companhia telefônica, cujos serviços são usados por um traficante que usa seu celular para vender drogas" (MELO, 2023), ainda: "No fundo, as alegações nesses casos se apoiam menos em má conduta afirmativa e mais em uma suposta falha em impedir o ISIS de usar essas plataformas." (MELO, 2023). Interessante observar que as redes sociais, nessa decisão, são vistas como mero instrumentos de comunicação. Entretanto, não há como negar que podem ser mais que isso: o conceito de uma ciberdemocracia desenvolvida nas redes, de movimentos articulados em suas vastas conexões descartam essa possibilidade. Não seria responsabilidade das plataformas, então, criar alguma forma de moderação?

Visto isso, interessante observar os movimentos que ocorreram na Europa com a entrada em vigência da Lei de Serviços Digitais[7] (DAS) em 2022, que estabeleceu um quadro de responsabilização para as plataformas atuantes na Uniao Europeia, exigindo que elas atuem de forma ativa no combate de conteúdos ilegais e na proteção de direitos fundamentais (EUROPEAN COMMISSION, 2024). O DAS tem mecanismos que permitem que os usuários sinalizem conteúdo ilegal e chamam as plataformas a cooperarem com sinalizadores que identifiquem e removam esse conteúdo (TEFFÉ; SOUZA, 2024, p. 25-37).

No Brasil, a lei que estabelece os princípios, garantias, direito e deveres do uso da *Internet* é o Marco Civil da Internet (Lei 12.965 de 2014). Entretanto, após seus 10 anos em vigor, os ambientes *online* se alteram e provocam repercussões que sequer se imaginaria na época. Um dos artigos desta legislação que recebe muita atenção é o artigo 19, da seção

sociais não podem ser responsabilizadas civilmente por postagens de seus usuários. Ver: https://www.conjur.com.br/2023-mai-19/suprema-corte-eua-redes-nao-sao-responsaveis-posts/ Acesso em 23 de maio de 2025.

7 *Digital Services Act*, em inglês.

sobre "Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros" que conta com a seguinte redação:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

Referido artigo é tema de discussão no Recurso Extraordinário 1.037.396 pelo Supremo Tribunal Federal (MARTINS, 2024). Como discutido anteriormente, o Marco Civil da Internet regula sobre uma *Internet* que não existe mais. Afinal, na época em que a lei foi promulgada o que o legislador buscava era garantir o impedimento à censura e o direito à liberdade de expressão. Essa proteção ao provedor tem como fruto uma realidade de outros países, aplicadas na década de 1990 e no início dos anos 2000 – época em que a *Internet* ainda dava seus primeiros passos (MARTINS, 2024). Logo, resta assinalar que existe uma lacuna legislativa que regule um ciberespaço com redes que não são mais meros meios de comunicação.

Ainda sobre o assunto Teffé (2024) discute a necessidade de que desenvolver uma estratégia eficaz de moderação de conteúdo é essencial para enfrentar discursos extremistas, de ódio e violentos. No entanto, responsabilizar as plataformas de forma desproporcional pelo conteúdo gerado por terceiros pode resultar em censura excessiva, prejudicando a liberdade de expressão e a diversidade de opiniões – sendo assim, a moderação deve ser equilibrada e transparente, protegendo as liberdades constitucionais enquanto previne danos, com discussões públicas e envolvendo múltiplos setores.

Existem argumentos que levantam que a autorregulação pode ser uma solução promissora, apoiando a auto-organização de agentes privados conforme suas especialidades e dinâmicas de mercado juntamente ao estabelecimento de parâmetros gerais de interesse público importantes para o Estado democrático. Esta abordagem visa evitar a concentração excessiva de poder nas plataformas, garantindo um ambiente digital mais equilibrado. Adicionalmente, sugere-se que as plataformas criem órgãos de supervisão para assegurar transparência e proporcionalidade nas decisões de moderação. Também é pertinente considerar mais exceções ao artigo 19

do MCI, baseadas em direitos já estabelecidos, para responder às demandas atuais. Sobre esse assunto, escreve Scalcon (2024):

> Seria relevante desenvolver, pois, instrumentos de autorregulação que possibilitem limitar o alcance, a propagação e o compartilhamento de conteúdo suspeito. Os algoritmos poderiam identificar conteúdos suspeitos e, ato contínuo, moderar a sua propagação. Esta singela ideia pode se prestar a mitigar, em algum grau, parcela dos dilemas decorrentes da imbricação entre liberdades constitucionais, direito penal e regulação de redes sociais.

Os ataques do dia 08 de janeiro apenas reforçam a pressão por uma maior regulação do meio digital, afinal, as redes sociais foram utilizadas tanto para instigar quanto para articular os atos extremistas, além de transmitir as ações em tempo real. O debate sobre regulação, moderação de conteúdos e responsabilidade civil das plataformas digitais é complexo e deve levar em conta todo o sistema de regulação digital já existente e em discussão, incluindo proteção de dados pessoais, inteligência artificial e neutralidade da rede. As legislações devem evoluir para proteger direitos fundamentais, promover a inovação e garantir um ambiente *online* seguro. Este desafio é compartilhado por todos os países e blocos regionais, que devem continuar a debater suas normas considerando o desenvolvimento tecnológico e as mudanças sociais, políticas e culturais.

5 Considerações finais

A cibercultura, ao proporcionar novas formas de interação e participação, tem o potencial de fortalecer a democracia ao promover a inclusão social e o engajamento cívico. Através das redes sociais, indivíduos podem se organizar, compartilhar informações e mobilizar-se para causas comuns, ultrapassando barreiras geográficas e temporais. No entanto, a mesma infraestrutura que facilita a participação democrática também pode ser utilizada para fins que ameaçam a ordem democrática, como observado nos eventos de 08 de janeiro de 2023. Este paradoxo evidencia a necessidade de uma compreensão crítica e equilibrada do impacto das tecnologias digitais na sociedade.

A questão da regulação das plataformas digitais emerge como um tema central nesse contexto. A responsabilidade das empresas de tecnologia pelo conteúdo gerado por seus usuários é um ponto de debate, especialmente diante de incidentes onde a disseminação de informações nocivas resulta em danos reais. A busca por um equilíbrio entre a liberdade de expressão e

a prevenção de abusos é essencial para garantir que a cibercultura contribua positivamente para a sociedade sem restringir a inovação tecnológica.

As abordagens adotadas em diferentes regiões, como a Lei de Serviços Digitais (DAS) na Europa, oferecem modelos para a criação de um ambiente digital mais seguro e responsável, essas iniciativas visam estabelecer padrões de conduta e mecanismos de controle que protejam os direitos fundamentais dos usuários e assegurem a integridade das redes sociais. No Brasil, a discussão sobre a atualização do Marco Civil da Internet é crucial para acompanhar as mudanças rápidas e significativas no uso das tecnologias digitais.

Por fim, o que se percebe é que a cibercultura apresenta tanto oportunidades quanto desafios para a democracia. A potencialização da participação cívica e a inclusão social são contrabalançadas pela necessidade de regulação e responsabilidade no ambiente digital. A análise contínua e crítica das dinâmicas entre tecnologia e sociedade é vital para maximizar os benefícios da cibercultura enquanto se mitiga seus riscos, promovendo um futuro digital mais justo e democrático.

Referências

BRASIL, Supremo Tribunal Federal. *Arguição de Descumprimento de Preceito Fundamental – ADPF 442*. Relator: Min. Rosa Weber.

CASTELLS, Manuel. *Redes de Indignação e Esperança*. Movimentos sociais na era da Internet. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

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

ELIAS, Alice. *Primavera Árabe: os movimentos lutaram por justiça, democracia, direitos humanos, dignidade e liberdade dos abusos policiais*. Os movimentos lutaram por justiça, democracia, direitos humanos, dignidade e liberdade dos abusos policiais. 2023. Disponível em: https://www.fflch.usp.br/50927#:~:text=A%20Primavera%20Árabe%20foi%20uma,de%20desemprego%2C%20corrupção%20e%20pobreza Acesso em: 27 set. 2025.

EUROPEAN COMMISSION. *The Digital Services Act*. Homepage. Disponível em: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en Acesso

em: 27 set. 2025.

GARDNER, Frank. *O homem que 'acendeu' a fagulha da Primavera Árabe*. 2011. BBC News. Disponível em: https://www.bbc.com/portuguese/noticias/2011/12/111217_bouazizi_primavera_arabe_bg Acesso em: 27 set. 2025.

GIBSON, William. *Neuromancer*. São Paulo: Aleph, 1984.

LÉVY, Pierre. *Cibercultura.* São Paulo: Ed. 34, 1999.

LIJPHART, Arend. *Modelos de democracia: Formas de Gobierno y resultados em treinta y seis países*. Tradução de Carme Castellnou. 1 ed, Editorial Ariel S.A: Barcelona, 2000.

MARTINS, Thiago Souza. *Elon Musk, STF e a (in)constitucionalidade do art. 19 do MCI: independente de julgamento no supremo, existem lacunas a serem preenchidas na legislação brasileira. Independente de julgamento no Supremo, existem lacunas a serem preenchidas na legislação brasileira.* 2024. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/elon-musk-stf-e-a-inconstitucionalidade-do-art-19-do-mci-15042024 Acesso em: 27 set. 2025.

MELO, João Ozorio de. *Para Suprema Corte dos EUA, redes não são responsáveis por posts de usuários.* 2023. ConJur. Disponível em: https://www.conjur.com.br/2023-mai-19/suprema-corte-eua-redes-nao-sao-responsaveis-posts/ Acesso em: 27 set. 2025.

SCALCON, Raquel. *Os desafios da identificação de conteúdo criminoso em redes sociais: exame do crime de "incitação", em qualquer das suas modalidades, possui enorme complexidade no contexto das redes.* Exame do crime de 'incitação', em qualquer das suas modalidades, possui enorme complexidade no contexto das redes. 2024. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/os-desafios-da-identificacao-de-conteudo-criminoso-em-redes-sociais-05062024 Acesso em: 27 set. 2025.

SCHREIBER, Mariana. *8 de janeiro: as perguntas sem respostas um ano após ataques*. 2024. BBC News. Disponível em: https://www.bbc.com/portuguese/articles/c06y1vekdgeo Acesso em: 27 set. 2025.

TEFFÉ, Chiara de. *Moderação de conteúdo e responsabilidade civil em plataformas digitais: um olhar atual*. 2024. ITSRio. Disponível em: https://itsrio.org/pt/publicacoes/moderacao-de-conteudo-e-responsabilidade-civil-em-plataformas-digitais-um-olhar-atual-2/ Acesso em: 27 set. 2025.

TEFFÉ, Chiara Spadaccini de; SOUZA, Carlos Affonso. Moderação de conteúdo e responsabilidade civil em plataformas digitais: um olhar sobre as experiências brasileira, estadunidense e europeia. In: Joyceane Bezerra de Menezes, Fernanda Nunes Barbosa. (Org.). A prioridade da pessoa humana no Direito Civil-Constitucional: estudos em homenagem a Maria Celina Bodin de Moraes. 1.ed. Foco, 2024, p. 25-37.

Capítulo 6

A EXPANSÃO DE UMA SOCIEDADE TECNOLÓGICA DE RISCO A PARTIR DA PANDEMIA DE COVID-19

Marina Schmidlin Sponholz[1]
Heline Sivini Ferreira[2]
Cinthia Obladen de Almendra Freitas[3]

1 Introdução

As novas tecnologias passaram a exercer um protagonismo na sociedade contemporânea, de forma que não há mais como se viver desconectado delas. A utilidade e a potencialidade que essas tecnologias trouxeram transformaram o cotidiano, o *ser* e a própria existência da humanidade. Mas com o surgimento da sociedade tecnológica, decorrente da evolução das Tecnologias de Informação e Comunicação (TICs) e de uma maior, mais natural e espontânea interação dos indivíduos com elas, também surgiram novos riscos de tal forma que a sociedade de risco tradicionalmente concebida se viu transformada. Os riscos passaram a ser de cada vez mais difícil percepção, visto que foram invisibilizados pelas diversas promessas de maravilhas que as tecnologias iriam proporcionar.

Ocorre que, a partir de 2020, com a ocorrência da pandemia de COVID-19, esse cenário de risco tecnológico viu-se ainda mais obscurecido

1 Mestre em Direito pelo Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná (PUCPR). Advogada. Membro relatora da Comissão de Direito Digital e Proteção de Dados da OAB/PR. L.L.M em Direito Empresarial pela Fundação Getúlio Vargas FGV-Rio. Bacharela em Direito pelo Centro Universitário Curitiba. Associada do Instituto Brasileiro de Direito de Família (IBDFAM). Membro do Instituto dos Advogados do Paraná. Email marinasponholz@gmail.com

2 Doutora e Mestre em Direito pela Universidade Federal de Santa Catarina. Professora Adjunta no Curso de Graduação e no Programa de Pós-Graduação em Direito (PPGD) da PUCPR. Professora Colaboradora no curso de Pós-Graduação da Universidade Federal de Santa Catarina. Email heline.ferreira@pucpr.br

3 Professora Titular da PUCPR. Professora Permanente do Programa de Pós-Graduação em Direito (PPGD) da PUCPR. Doutora em Informática Aplicada. Membro consultora da Comissão de Direito Digital e Proteção de Dados da OAB/PR. Membro Consultora do Instituto Nacional de Proteção de Dados (INPD). Email cinthia.freitas@pucpr.br

diante da necessidade que a sociedade desenvolveu em relação às tecnologias. A crise sanitária e suas medidas restritivas fizeram com que a humanidade aderisse às novas tecnologias e migrasse para o digital com urgência, na tentativa de viabilizar parte da normalidade da vida, enfrentando os desafios que foram surgindo à medida que o isolamento social se estendia. No entanto, sem que a humanidade percebesse, a aceleração da transformação digital propiciada pela emergência do coronavírus fez surgir novas ameaças relacionadas às tecnologias, porque a sua disseminação ocorreu em uma velocidade desenfreada e sem o devido preparo da sociedade. A urgência fez com que a migração para o digital não seguisse um planejamento e consequentemente que os problemas que já existiam fossem exacerbados.

Assim, em face da crescente importância das novas tecnologias na sociedade contemporânea, o objetivo geral desta pesquisa é refletir sobre como a pandemia de COVID-19 promoveu a evolução da sociedade tecnológica para a sociedade tecnológica de risco, expandindo-a aceleradamente. Como objetivos específicos, tem-se: (i) estudar a teoria da sociedade de risco global no contexto de uma sociedade movida pelas tecnologias, em especial pelas TICs; (ii) examinar como a emergência do coronavírus impulsionou a aceleração da transformação digital e, por fim; (iii) analisar como, ao promover a aceleração da transformação digital, a pandemia de COVID-19 expandiu uma sociedade tecnológica de risco.

Visando o desenvolvimento da pesquisa dentro dos objetivos propostos, adotou-se o método de pesquisa hipotético-dedutivo e utilizou-se da pesquisa bibliográfica e documental. Partiu-se da hipótese de que a aceleração da transformação digital causada pela emergência sanitária do coronavírus trouxe novas ameaças e intensificou outras que já existiam, expandindo e consolidando uma sociedade tecnológica de risco que já vinha, de uma forma mais lenta, se estruturando.

O artigo foi desenvolvido em três tópicos. No primeiro deles, buscou-se apresentar como o advento das novas tecnologias, em especial das TICs, alçou a sociedade de risco concebida por Ulrich Beck a um outro patamar, fazendo surgir uma sociedade tecnológica de risco. No segundo, analisa-se como a pandemia de COVID-19 promoveu uma aceleração da transformação digital que vinha se desenvolvendo na sociedade ao longo de vários anos e, com isso, mudanças outrora paulatinas foram repentinamente antecipadas. Por fim, no terceiro e último capítulo, examina-se como a aceleração da transformação digital impulsionada pela pandemia de COVID-19 trouxe consigo várias ameaças à humanidade -

graves, imperceptíveis, sem limitação de tempo e de espaço e que possuem em sua origem a ação humana como causa.

2 Tecnologias, revolução digital e sociedade de risco

A passagem de uma modernidade sólida para uma nova fase, que é "leve", "líquida", "fluida" e mais dinâmica, impactou profundamente a vida humana em todos os seus aspectos (Bauman, 2021). O estágio líquido da modernidade afetou a própria condição humana, criando um cenário de instabilidade e insegurança que faz surgir novas ameaças a partir do enfraquecimento do coletivo e do incentivo ao transitório (Bauman, 2021, p. 23-24).

Diante de riscos novos, muitas vezes imperceptíveis e com um potencial de destruição previamente desconhecido, numa fase de evolução da sociedade a que Beck (2010, p. 23-28) denomina de modernidade avançada, a produção social de riqueza passa a ser acompanhada pela produção social do risco. Com isso, os problemas relacionados à produção, definição e distribuição das ameaças fabricadas acabam se sobrepondo aos tradicionais problemas de escassez, fazendo com que a sociedade, até então inserida em uma lógica de distribuição de riquezas, veja-se diante da necessidade de distribuir também riscos (Beck, 2010, p. 23-28).

Esta mudança se insere no contexto da chamada sociedade de risco, uma fase de evolução da sociedade marcada pelo surgimento de ameaças globais, ou seja, capazes de afetar a humanidade como um todo, ainda que resguardadas as questões relacionadas às vulnerabilidades. Está-se diante de riscos com causas modernas, produto do maquinário do progresso e, ainda, agravados pela noção subdesenvolvida de desenvolvimento, focada essencialmente no crescimento econômico. São riscos que se projetam globalmente, seguindo a ideia de "efeito bumerangue" e ameaçando a vida do planeta em todas as formas (Beck, 2010, p. 23-28).

Com o advento da sociedade de risco, percebe-se que as ameaças, também presentes na sociedade industrial, sofreram modificações qualitativas – os riscos passaram de concretos a abstratos. Nessa perspectiva, atravessam fronteiras, evidenciando que não existe um cenário de segurança dentro da lógica de superexploração do mundo (Beck, 2002, p. 75-77). Assim, a segunda modernidade depara-se com ameaças globais, transfronteiriças e transtemporais que, embora desencadeadas por ações

antrópicas (Ferreira, 2016), revelam-se como imprevisíveis e incontroláveis (Cavedon; Ferreira; Freitas, 2015, p. 200).

Neste estágio da modernidade, e pela própria natureza das ameaças fabricadas, os riscos possuem um potencial de destruição ainda desconhecido, sabendo-se apenas que são compartilhados por diferentes povos de distintas nações, mesmo que em diferentes níveis (Ferreira, 2016, p. 122). Essa perda da capacidade de previsão e controle, que caracterizou a sociedade industrial, evidencia que no mundo globalizado a figura do Estado se mostra insuficiente para lidar com os novos contextos de risco (Bauman; Bordoni, 2016). Como consequência, percebe-se a falência dos padrões de segurança instituídos e consolidados na primeira modernidade, uma vez que as "[...] relações de definição simplistas já não constituem instrumentos válidos para determinar, regular, avaliar e controlar os riscos" (Ferreira, 2016, p. 130).

Nesse modelo de organização social que se forja em torno do risco, as novas tecnologias e a velocidade com que as inovações ocorrem, exercem grande influência, sobretudo quando se fala em ausência de previsão e controle (Beck, 2002, p. 95-96). Assim, em que pese a necessária e contínua expansão da tecnologia, não se pode negar que esse processo está associado a uma transformação significativa de ambientes e espaços no contexto da modernidade (Ferreira, 2016, p. 130). A sociedade de risco alia-se à sociedade tecnológica e, em uma expressão também global, surgem tecnologias ubíquas e pervasivas, ou seja, de fácil difusão, presentes em toda parte e a todo momento (Floridi, 2015, p. 43).

E quando os indivíduos conferem a essas tecnologias um papel de protagonismo em suas vidas, aceitam que a tecnologia assuma certo comando sobre determinados aspectos de sua existência, em um contexto permeado por riscos abstratos. Pode-se então afirmar que ao se estabelecer essa relação de interdependência entre seres humanos e novas tecnologias, a exemplo das Tecnologias da Informação e Comunicação (TICs), modificam-se espaços e ambientes, que, agora, se tornam mais propícios à difusão de ameaças qualitativamente diferenciadas (Beck, 2002; 2010).

Considerando a fase que Schwab (2016, p. 16) denomina de Quarta Revolução Industrial, em razão da expansão das próprias tecnologias e da ocorrência de uma Revolução Digital, os riscos expressam-se de forma diferente, são cada vez mais líquidos e difíceis de determinar. Seguindo a mesma lógica capitalista que justifica a criação do risco pela obtenção do lucro, como se mencionou acima, as novas ameaças vão se imiscuindo no

modo de vida moderno como uma necessidade premente, impactando, inclusive, o "ser" humano e sua autonomia (Morin; Kern, 2003, p. 65-67).

Percebe-se, portanto, que a Revolução Digital imprime na sociedade de risco uma nova faceta – para além da preocupação com as mudanças climáticas, com a geração de energia nuclear e com a biossegurança dos organismos transgênicos, por exemplo. E como representação das incertezas que permeiam a segunda modernidade, as novas tecnologias se mostram intrusivas e abrangentes, mais sofisticadas e potentes, seduzindo e ao mesmo tempo isolando (Morin; Kern, 2003, p. 65-67).

A ubiquidade e a pervasividade que caracterizam essas novas tecnologias provocaram grandes transformações sociais: de forma discreta e praticamente imperceptível tecnologias como os algoritmos passaram a controlar as pessoas e a direcionar como elas devem viver (Zuboff, 2020, p. 277); comunidades foram substituídas por coletivos digitais que se constituem como agrupamentos de indivíduos singularmente isolados (Han, 2017, p. 113-114); democracias sucumbem ao surgimento de um panóptico digital delineado pelas tecnologias (Han, 2017, p. 106-109); e a desigualdade social aumenta.

Se em algum momento os riscos foram percebidos como uma oportunidade para as novas tecnologias, dentro do que Castells (2015, p. 110-112; 115) considera uma nova economia baseada no investimento em tecnologia da informação e no crescimento da produtividade, impulsionada constantemente por inovações de alto risco; o tempo evidenciou que o próprio uso dessas tecnologias e o ingresso dos indivíduos no mundo digital também representam riscos. Assim como ocorre na sociedade de risco, o encanto da aceleração, da praticidade e do mundo novo criado pelas TICs tem também o seu lado perverso e obscuro.

Assim, conforme surgiram novas tecnologias, também surgiram novos riscos, imperceptíveis e globais, sem limitação de tempo e de espaço (Ferreira, 2016, p. 123-128). É nesse contexto que a sociedade tecnológica de risco avança, sempre entrelaçada a riscos qualitativamente diferenciados (Cavedon; Ferreira; Freitas, 2015, p. 197). E muito embora essa expansão esteja associada a ameaças, sabe-se que a emergência do paradigma *Everyware* é inevitável (Greenfield, 2006, p. 89) - cada vez mais a sociedade se verá interagindo com tecnologias ubíquas, disruptivas e pervasivas. E isto terá um impacto significativo na esfera da vida privada.

3 Aceleração da transformação digital impulsionada pela pandemia de Covid-19

No início de 2020, a aceleração que vinha impactando vários setores da vida dos indivíduos (Morin; Kern, 2003, p. 95) se viu substituída por uma paralisia completa e atônita provocada pelo surgimento da COVID-19. A humanidade, que vinha se estruturando com o propósito de apenas acelerar o progresso (Capella, 1998, p. 24-25) e aumentar o bem-estar, viu-se então obrigada a focar em sua própria sobrevivência.

A globalização intensificada aumentou as zonas de vulnerabilidade social e também os riscos sanitários. A conexão das partes da Terra e seus centros econômicos se tornou tão íntima que limitar a disseminação de determinada patogenia se tornou um desafio (Dörre, 2020, p. XXXIII). E não foi diferente no caso da pandemia de COVID-19, já surgida em um contexto de *policrise* (Morin; Kern, 2003, p. 94), ou seja, de diferentes crises que se entrelaçam e se sobrepõem.

Um dos grandes impactos da pandemia de COVID-19 foi a aceleração de uma transformação digital que, embora já viesse ocorrendo, não estava sendo atentamente observada (IBM, 2020, p. 01-02). Com a necessidade de isolamento social e de continuação das rotinas e negócios, houve uma maior difusão do modelo de interação social limitado, controlado e reduzido a tecnologias digitais que não compreendem a complexidade da sociedade e a importância da construção de ligações, e não apenas de pontes (Pariser, 2012, p. 20-21). No momento de crise, o que importava era que as pessoas estivessem conectadas entre si. Em um segundo plano, ficaram os valores e a qualidade dessa conexão social.

A emergência sanitária causada pelo COVID-19 conduziu o uso das tecnologias a um outro patamar, evidenciando seu potencial não apenas no auxílio ao confronto da doença, mas, sobretudo, de manter as pessoas conectadas (United Nations, 2020b, p. 02). As transformações que eram projetadas para um tempo futuro tiveram que ser aceleradas, e a conectividade passou a ser vista como uma necessidade crítica (United Nations, 2020b, p. 06). A Internet, que já se propagava como uma ferramenta de muita utilidade, passou a ser também vista como um instrumento de reforço da segurança sanitária. De igual maneira, as tecnologias permitiram que as relações passassem a ser compreendidas, e cada vez mais vividas, num espaço não material, sem limitações geográficas,

e as fronteiras - que já não eram mais barreiras desde que se iniciou a globalização - foram definitivamente rompidas.

A conexão digital passou a ser exigida numa intensidade jamais vista. Repentinamente, de forma não apenas acelerada mas também intensa, a humanidade se deparou com significativas transformações. Se com o advento das TICs já era difícil levar uma vida sem a integração tecnológica, após a pandemia não foi mais possível se conceber viver de uma forma *offline*.

O paradigma *Everyware* (Greenfield, 2006), segundo o qual todas as informações tornam-se acessíveis de qualquer lugar, em qualquer momento e que demonstra que as novas tecnologias estão cada vez mais pervasivas e ubíquas, ficou ainda mais evidente, pois os avanços tecnológicos já vinham ocorrendo, foram propulsados a outro patamar. Pessoas e negócios foram forçados a aderirem às mais diversas tecnologias, em especial de informação e comunicação para que pudessem se manter ativos. A tecnologia se apresentou como a solução para conciliar o distanciamento social e a preservação sanitária, com o atendimento das necessidades de sobrevivência da humanidade e de funcionamento dos negócios, pois foi ela que possibilitou que o mundo não parasse.

Houve um impulsionamento da digitalização das transações financeiras (Lima; Francisco, 2021, p. 23-24) e também uma profunda transformação nas relações de trabalho e no setor de ensino (Dörre, 2020, p. XXXIV) em ritmo e proporção jamais antes vistos. O estímulo que ocorreu ao desenvolvimento da tecnologia da informação, a substituição parcial do ser humano como ser social e as restrições forçadas de atividades cotidianas tradicionais contribuíram para a migração não apenas para o digital, mas também para o virtual, na busca da imitação da funcionalidade física na interação entre as pessoas (Kostenko, 2022, p. 03).

A propulsão da adoção de novas tecnologias se apresentou – ao menos de início - como um grande favor vindo da pandemia de COVID-19, como se ela tivesse proporcionado uma evolução que era prevista para ocorrer em décadas, apenas em um biênio, e o fato dela ter ocorrido em meio a Quarta Revolução Industrial (Schwab, 2016), propiciou que as tecnologias encontrassem o terreno fértil da necessidade e da demanda social. Se o mundo já vinha enfrentando uma revolução na qual as tecnologias e a inovação difundiam-se muito mais rápido e amplamente (Schwab, 2016, p. 17), com o surgimento de uma demanda global por soluções que possibilitassem que os indivíduos continuassem suas vidas

mesmo em meio ao cenário caótico pandêmico, criou-se o cenário perfeito para a aceleração da transformação digital e para o protagonismo das tecnologias - em especial das TICs.

Vive-se a Era da Informação (Castells, 2022) e, por esta razão, dentre as diversas tecnologias que surgem as TICs são as ferramentas tecnológicas sem as quais não se pode conceber a sociedade. Considerando a importância e o valor das informações nos tempos hodiernos, a pandemia de COVID-19 evidenciou que tais tecnologias precisam ser vistas com a devida importância que elas têm, como verdadeiras forças ambientais que ao provocarem grandes transformações, impactam radicalmente a vida humana e sua existência (Floridi, 2015).

Se o advento da sociedade tecnológica fez com que mudasse a autoconcepção dos indivíduos, seu modo de socializar, sua concepção da realidade e suas interações com a realidade (Floridi, 2015, p. 02), o advento da pandemia de COVID-19 consolidou tais transformações e favoreceu não apenas a disseminação, mas também a aceitação social das TICs, tanto pelos indivíduos como por empresas. Com as restrições impostas pela pandemia, principalmente por conta do isolamento social e do fechamento de fronteiras, não havia como as interações sociais (reuniões, aulas, trabalho, etc.) ocorressem de forma presencial, então a humanidade não teve outra opção que não a de se render ao uso de tecnologias para conseguir continuar suas atividades.

O fato de a pandemia trazer um olhar positivo sobre as tecnologias contribuiu em muito para que se acelerasse a transformação digital. O uso de tecnologias como, por exemplo, as de geolocalização para realizar o controle de disseminação do vírus trouxe maior efetividade às medidas restritivas que estavam sendo impostas e fez com que as ferramentas tecnológicas fossem vistas como instrumentos auxiliares à promoção da saúde pública (Bulzico, 2022, p. 77-78). Redes sociais mediadas por computadores, que já vinham se apresentando como o "novo padrão de sociabilidade" (Castells, 2015, p. 135), acabaram se consolidando como a nova forma de estruturação das relações sociais. Negócios que aos poucos aumentavam a sua interação com as tecnologias, vislumbraram novas oportunidades e passaram a enxergar a aceleração de sua transformação digital como um investimento (IBM, 2020, p. 01-03).

Sempre se soube que o mundo estava passando por uma transformação digital, mas de acordo com relatório da IBM, foi com a pandemia de COVID-19 que se criou um senso de urgência em torno

desta transformação. Ela alterou a forma como as organizações em todo o mundo operam ao acelerar o processo de transformação digital de diversas empresas e possibilitar que diversas iniciativas de inovação que encontravam resistência fossem finalmente implementadas, pois as reações induzidas por ela acabaram mostrando que os executivos podiam confiar mais no que a tecnologia pode fazer (IBM, 2020, p. 02-03).

Antes da pandemia, muitas organizações aparentemente desconfiavam de sua capacidade tecnológica, mas após a sua ocorrência, perceberam o potencial das novas tecnologias e vislumbram a aceleração da transformação digital como uma estratégia de negócio (IBM, 2020, p. 03). Assim, a pandemia evidenciou a importância das tecnologias tanto sob o viés da sobrevivência como também sob a ótica do mercado enquanto um investimento estratégico.

Ao mesmo tempo em que o coronavírus trouxe uma enorme ressignificação para o modo de viver da humanidade, o cenário de indecisão fez com que as prioridades dos negócios mudassem (IBM, 2020, p. 01). A aceleração da transformação digital passou a ser vista como uma oportunidade de as empresas reforçarem a sua competitividade, fortalecerem sua força de trabalho, aprimorarem o relacionamento com os clientes e angariarem parcerias (IBM, 2020, p 01). Portanto, a "transformação digital nunca foi apenas sobre a tecnologia" (IBM, 2020, p. 02), ela depende que existam condições para que ela ocorra, como incentivos, um cenário favorável e interesse social. E foi isso que ocorreu durante a emergência sanitária de COVID-19.

Neste sentido, a 34ª Edição de Pesquisa Anual de Uso de TI nas Empresas realizada em 2023 pelo Centro de Tecnologia de Informação Aplicada da Escola de Administração de Empresas de São Paulo da Fundação Getúlio Vargas constatou que a Pandemia da COVID-19 promoveu uma antecipação da transformação digital de 1 a 4 anos dentro de mais de 10.000 empresas pesquisadas (Meirelles, 2023, p. 05; 151). Ou seja, o que era previsto para ser realizado dentro de anos, acabou sendo feito dentro de meses (Meirelles, 2023, p. 53) e há uma contribuição da pandemia para esta aceleração.

Inclusive, em razão do crescimento do trabalho e da educação à distância que foram incentivados pelo isolamento social durante o período pandêmico, há uma tendência de que o número de dispositivos digitais (computador, notebook, tablet e smartphone) em uso no Brasil – que atualmente são 447 milhões (Meirelles, 2023, p. 91) - continue

aumentando. Isto porque, segundo Fernando S. Meirelles, a pandemia transformou de forma permanente o uso da tecnologia de informação, a qual passou a ser vista como complementar à capacidade humana, ou seja, há mais do que nunca uma busca de integrar e potencializar as capacidades humanas com as digitais (Meirelles, 2023, p. 151-152).

A pandemia de COVID-19 quebrou grande parte da resistência que existia com relação às tecnologias. A necessidade de adoção de tecnologias fez com que a transição para o digital fosse mais agradecida do que questionada. Os indivíduos precisavam fazer compras, usar o banco, trabalhar, estudar e levar a sua vida o mais próximo possível do que estavam acostumados e as tecnologias foram o instrumento que tornou isso o possível. Se com o advento das TICs se pode afirmar que houve uma evolução para uma *onlife* (Floridi, 2015), com a pandemia de COVID-19 esta vida *online* foi ainda mais aperfeiçoada e aprofundada.

Ao evidenciar que a sociedade depende das tecnologias, em especial as de informação e comunicação, para o seu funcionamento a pandemia serviu como propulsora da aceleração da transformação digital. A COVID-19 "foi um alerta de que o inesperado e o improvável é mais tangível e plausível do que se previa anteriormente" (IBM, 2020, p. 08, tradução nossa)[4] e que aquilo que foi para muitos uma desgraça, para outros foi uma oportunidade. Por esta razão, muitos consideram que a pandemia favoreceu o progresso e ofereceu uma oportunidade para se construir melhores negócios e um mundo melhor ao propiciar a aceleração da transformação digital (IBM, 2020, p. 08).

E de fato a pandemia de coronavírus impulsionou diversas tecnologias, em especial de informação e comunicação, de uma tal forma que promoveu uma aceleração na transformação digital da sociedade impactando pessoas e negócios. Ocorre que, se já era complexo "ser" humano em uma era hiperconectada (Floridi, 2015, p. 09), com a pandemia o desafio se tornou ainda maior: além da própria existência humana ser transformada, ela passou a ser condicionada pelo nível de familiaridade dos indivíduos com as tecnologias. As tecnologias passaram a ser imprescindíveis para qualquer um que deseje efetivamente viver.

4 Texto original: "The pandemic was a wake-up call that the unexpected and the unlikely are more tangible and plausible than anyone previously anticipated."

4 A aceleração da transformação digital provocada pela pandemia de Covid-19 e a expansão de uma sociedade tecnológica de risco

O surgimento de pandemias no decorrer da história e em especial no decorrer do último século, evidencia a proporção global que as mais diversas ameaças do mundo vêm adquirindo. Diferenciando-se dos surtos, epidemias e endemias, as pandemias são declaradas quando uma doença se torna uma ameaça global, ou seja, quando ocorre em diversos países ou continentes (Instituto Butantan, 2020) e por esta razão elas representam de modo muito explícito como o mundo e todos os seus integrantes estão interconectados tanto para o bem como para o mal.

Pandemias são um desafio típico do Antropoceno (United Nations, 2020a, p. 03-04), pois demonstram como a falsa sensação de indestrutividade e superioridade da humanidade culminou numa maior vulnerabilidade da existência humana. Elas evidenciam como comportamentos humanos ao provocarem diversas transformações sociais, econômicas e políticas também são cada vez mais responsáveis pelos diversos riscos e perigos que a humanidade enfrenta.

A partir de 2020, com a ocorrência da pandemia de COVID-19 havia a esperança de que a iminência da morte rodeando a todos traria uma maior lucidez, espírito coletivo e solidariedade. No entanto, o afastamento da percepção do coletivo como um todo que já vinha ocorrendo desde o surgimento de uma sociedade de controle e transparência aumentou (Han, 2017, p. 113-114) e agravou-se a separação entre humanos e a separação da humanidade da natureza (United Nations, 2020a, p. 03-04).

O ser humano, crente de sua superioridade e de sua possibilidade de controle de tudo e de todos, ao ser confrontado pela sociedade de risco, percebe que não tem – se é que algum dia teve - controle sobre as ameaças que o rodeiam. Quanto mais a humanidade quer ter controle mais ela o perde (Beck, 2012, p. 23-24). Neste sentido, o período pandêmico evidenciou que instrumentos como a ciência e a tecnologia que supostamente deveriam estar à serviço da humanidade são desenvolvidos cada vez mais em benefício do mercado e de sua lógica de lucro (Greenfield, 2006, p. 211) sem pensar no bem dos indivíduos.

A pandemia impulsionou o espaço digital de uma forma recorde e evidenciou que as tecnologias são uma realidade que possibilita que as pessoas interajam das mais diversas formas entre si, mas que também têm

uma face ruim, pois se não forem usadas com cautela podem fazer mal à humanidade (Pérez, 2021, p. 89-92). A pandemia de COVID-19 mostrou que assim como as tecnologias digitais têm o potencial de propiciar mudanças positivas, elas também podem agravar problemas já existentes (United Nations, 2020b, p. 03).

Quando a Internet surgiu esperava-se que ela inevitavelmente revolucionaria e redemocratizaria o mundo, pois "nivelaria a sociedade, desbancaria as elites e traria uma espécie de utopia global libertadora". No entanto, ela não proporcionou a "conectividade cívica" que se esperava, pelo contrário, possibilitou que as pessoas construíssem suas bolhas e se isolassem umas das outras, que é o contrário do que a democracia exige (Pariser, 2012, p. 10-11). A revolução digital proporcionou o surgimento de um enxame digital, ou seja, de um aglomerado de indivíduos singularizados que não possuem uma alma que os une entre si (Han, 2018, p. 27).

E se o mundo digital já vinha mudando (Pariser, 2012, p. 11), tornando os indivíduos mais afastados uns dos outros e manipuláveis (Pariser, 2012, p. 14-15), a partir da pandemia de COVID-19, obrigando ao isolamento social e forçando o uso de tecnologias para a interação social, os custos pessoais e sociais que já estavam sendo verificados (Pariser, 2012, p. 18) se tornaram ainda maiores. Afinal, quanto maior o protagonismo e a participação das tecnologias na vida dos sujeitos, mais poderosas e ameaçadoras elas se tornam sobre a humanidade, pois "quando a tecnologia passa a nos mostrar o mundo, acaba por se colocar entre nós e a realidade, como a lente de uma câmera", podendo deformar a percepção que se tem sobre ele (Pariser, 2012, p. 18).

Assim, a imersão forçada da humanidade nas tecnologias condicionou a sua própria existência: as pessoas somente podiam existir plenamente, ou seja, exercer plenamente a sua personalidade por meio do uso de tecnologias, pois seu trabalho, sua interação social e até mesmo a sua sobrevivência passaram a depender direta ou indiretamente de tecnologias. As compras, consultas médicas, reuniões, aulas, operações bancárias e financeiras e as mais variadas ações da vida cotidiana passaram a depender de uma interação com as tecnologias e aqueles que não se adequassem a este novo estilo de vida estariam fatalmente privados do exercício da sua personalidade e de uma existência digna do que aqueles fossem nativos digitais ou ao menos imigrantes digitais (Prensky, 2001).[5]

5 Segundo Marc Prensky (2001, p. 01-03), o mundo não voltará a ser como era antes e quem for esperto aceitará esta realidade e buscará se adequar. Mas aqueles que não nasceram neste mundo digital, considerados imigrantes, mesmo tentando, jamais terão a mesma familiaridade

Ao se verificar os riscos surgidos com o advento de uma sociedade tecnológica, se constata que a humanidade se tornou vítima da própria torpeza e ganância: a revolução digital levou a sociedade a uma nova crise de poder e soberania sustentada pela ordem capitalista (Han, 2018, p. 26; 31-33). E com a aceleração da transformação digital provocada pela pandemia de COVID-19, se verifica que além de tais riscos serem potencializados, também surgiram novos. Houve a expansão da sociedade tecnológica de risco de diversas formas e há uma responsabilidade da humanidade por isso, afinal grande parte dos problemas enfrentados na atualidade decorrem dos sistemas financeiros e econômicos que são geridos por ela e que se pautam no crescimento econômico a qualquer custo (Settele; Díaz; Brondizio, 2020).

Em que pese na modernidade avançada os riscos sejam universais, existem alguns que acabam sendo distribuídos de um modo específico para determinadas camadas sociais e acabam por reforçar o esquema de classes (Beck, 2010, p. 41-43) e é justamente isto que se verifica no caso da aceleração da transformação digital provocada pela pandemia de COVID-19. Afinal, em que pese a crise gerada pela emergência sanitária do coronavírus seja resultante da convergência de várias outras crises, dentre as quais a social, ambiental, política e econômica (Medina, 2021, p. 30), se verifica que "os gigantes da tecnologia como Amazon, Google e Facebook são os que mais lucram" neste contexto de "capitalismo digital" (Maciel; Mattos, 2020, p. 684).

A pandemia consolidou, desta forma, a economia da informação, que é uma economia que "reúne a informática e sua tecnologia na geração de valor", que é capitalista (em que pese se difira do capitalismo clássico), que se trata de um modelo que possui falhas e riscos, que se expande de forma desigual e que "afeta a tudo e a todos, mas é inclusiva e exclusiva ao mesmo tempo" (Castells, 2022, p. 210-211).

Problemas de exclusão digital, já existiam na sociedade em razão da extrema desigualdade social que assola o mundo, mas com a aceleração da transformação digital eles foram potencializados, ou seja, tiveram o risco de serem aumentados bem como adquiriram um potencial lesivo ainda maior. Com a ocorrência da pandemia de COVID-19 quem não soube lidar bem com as tecnologias tinha muito mais chances de acabar excluído dos negócios, do mercado de trabalho, da sociedade e privado do exercício pleno de sua personalidade enquanto ser humano, afinal as "Atividades

com as novas tecnologias que aqueles que são considerados nativos da nova era.

econômicas, sociais, políticas, e culturais essenciais por todo o planeta estão sendo estruturadas pela Internet e em torno dela, como por outras redes de computadores" e por esta razão, estar excluídos das redes baseadas na Internet "é sofrer uma das formas mais danosas de exclusão em nossa economia e em nossa cultura" (Castells, 2015, p. 09).

Estar fora da sociedade da informação, ou seja, não integrar a rede sustentada pelas tecnologias, em especial de informação e comunicação, possui uma penalidade cada vez maior (Castells, 2022, p. 124) que equivale a uma sentença de morte, pois significa não fazer parte de praticamente todos os processos e relações sociais, já que atualmente as tecnologias passaram a fazer parte deles (Souza, 2021, p. 211-212). E a aceleração da transformação digital, aumentou mais ainda os riscos de isto acontecer, pois trouxe o risco de aumento da exclusão digital, o qual inclusive posteriormente acabou se vendo concretizado.

Esta preocupação se viu retratada inclusive numa correspondência enviada pelo Secretário Geral das Nações Unidas António Guterres ao evento de tecnologia Web Summit, em dezembro de 2020:

> A pandemia de Covid-19 acelerou nossa dependência de tecnologias digitais e destacou os benefícios da conectividade para salvar vidas. À medida que as sociedades trancaram e isolaram as pessoas, o acesso à Internet e os avanços digitais mantiveram as pessoas conectadas e as sociedades funcionando.
>
> Mas a pandemia também está destacando e exacerbando desigualdades de todos os tipos, incluindo a exclusão digital. Aqueles sem acesso à tecnologia digital – quase metade do mundo – não têm oportunidades de estudar, se comunicar, negociar, trabalhar e participar de muito do que agora é a vida normal para a metade mais rica do mundo. (Guterres, 2020, s.p., tradução nossa)[6]

Se um processo de migração para o digital que estava sendo percorrido ao longo de vários anos já estava reproduzindo desigualdades[7], quando ele foi acelerado pela pandemia de COVID-19 surgiu o risco de tal

6 Texto original: "The Covid-19 pandemic has accelerated our dependence on digital technologies and highlighted the life-saving benefits of connectivity. As societies have locked down and sent people into isolation, internet access and digital advances have kept people connected and societies running.
But the pandemic is also highlighting and exacerbating inequalities of all kinds, including the digital divide. Those without access to digital technology – almost half the world – are denied opportunities to study, communicate, trade, work and participate in much of what is now normal life for the richer half of the world."

7 Sobre a consolidação das desigualdades sociais pela divisão digital, vide Castells, 2015, p. 252 e seguintes.

situação se agravar ainda mais. "As divisões digitais refletem e ampliam as desigualdades sociais, culturais e econômicas existentes" (United Nations, 2020b, p. 10), por isso houve um aumento do risco de que determinadas regiões do planeta fossem deixadas para trás nesta transformação digital.

As economias mais desenvolvidas se preocupam com si próprias, em conseguirem acelerar a sua própria transformação digital, mas outros países que não possuem a mesma renda, habilidades, infraestrutura e condições não conseguem aproveitar tal situação para se desenvolverem (Schwab, 2016, p. 52) ou acabam fazendo uma transição deficiente e perigosa para o digital. Então, se a própria revolução digital aumentou a desigualdade entre os países (Schwab, 2016, p. 53), porque nem todos tinham as mesmas condições, ao acelerar tal transformação a pandemia permitiu que a divisão digital entre os países ricos e pobres fosse ainda mais severa (Dörre, 2020, p. XXXIV-XXXV), afinal "A geografia das redes é uma geografia tanto de inclusão quanto de exclusão, dependendo do valor atribuído por interesses socialmente dominantes" (Castells, 2015, p. 242).

Mas os riscos e consequências negativas[8] que surgem não são apenas para os mais pobres ou digitalmente excluídos, pois de acordo com o secretário-geral da ONU, para aqueles que têm acesso às tecnologias digitais, o aumento da conectividade proporcionado pela pandemia aumentou a sua vulnerabilidade a danos e abusos. Um exemplo citado por António Guterres é o aumento desproporcional do assédio online de mulheres e meninas e de exploração sexual infantil online durante o período de restrições impostas pela COVID-19 (Guterres, 2020).

Com o aumento da adesão ao mundo digital, a tendência foi de que os criminosos fossem atrás de onde as suas vítimas estão, então assim como houve um aumento do número de pessoas que migraram para o digital, também houve um aumento do cometimento de crimes no meio ambiente virtual. Segundo monitoramento da Agência Nacional de Proteção de Dados Pessoais (Agência Nacional De Proteção De Dados Pessoais, 2021) houve um aumento de aproximadamente 300% na criminalidade cibernética em razão da intensificação do uso da Internet durante o período de isolamento social decorrente de COVID-19 (Agência Câmara De Notícias, 2021).

Por esta razão, de acordo com a Federação Brasileira de Bancos (FEBRABAN), "Com a pandemia do novo coronavírus, criminosos estão aproveitando o maior tempo *online* das pessoas e o aumento das transações

8 Entenda-se aqui consequências negativas como a concretização dos riscos, ou seja, como uma ameaça que acabou se vendo concretizada.

digitais devido ao isolamento social para aplicar golpes financeiros". Levantamentos feitos em 2020, mostram um crescimento nas tentativas de fraudes financeiras contra brasileiros durante o período de isolamento social (de 80% nas tentativas de ataques de *phishing*, de 70% na fraude do falso funcionário e de 65% no golpe do motoboy) e o diretor da Comissão Executiva de Prevenção a Fraudes da FEBRABAN, Adriano Volpini adverte que isto se deve ao fato de que por não conhecerem tão bem o mundo digital e suas ameaças as pessoas acabam não adotando o mesmo comportamento de segurança que têm no mundo físico (Federação Brasileira De Bancos, 2020).

Ao mesmo tempo, as condições nas quais a migração para o digital ocorreu durante o período pandêmico, trouxe riscos relativos à segurança cibernética, porque não ocorreu de forma tecnicamente segura em muitos casos. "A maioria das empresas foi forçada a ativar rapidamente os recursos de colaboração remota devido ao COVID-19, mas seu ecossistema geral de TI não estava pronto para isso" (Chaloupka, 2022, s. p., tradução nossa)[9]. Muitas empresas e pessoas físicas não tiveram tempo hábil e nem os recursos financeiros necessários para fazer essa transição para o digital de forma segura, rápida e eficiente. A realidade da maioria é muito diferente das grandes corporações que têm capital, mão de obra e infraestrutura para acelerar a sua transformação digital e mesmo assim sofreram com ataques cibernéticos durante a crise de COVID-19.

Houve também um aumento dos riscos relativos à privacidade e segurança da informação (Agência Nacional De Proteção De Dados Pessoais, 2021), pois quanto maior a interação dos indivíduos com as tecnologias e maior for a sua exposição fomentada pela sociedade da informação, mais vulneráveis os sujeitos se tornam e mais a sua privacidade se encontra ameaçada. Se no capitalismo de vigilância enfrentado atualmente, a privacidade se tornou "o preço a se pagar por abundantes prêmios de informação, conexão e outros bens digitais quando, onde e como fossem desejados" (Zuboff, 2020, p. 72), com a pandemia de COVID-19, trazendo a necessidade de uso das tecnologias, o risco à privacidade foi levado a outro nível, pois as pessoas estavam mais preocupadas em resolver os seus problemas imediatos e não estavam atentas para a forma como seus dados estavam sendo tratados no uso destas tecnologias e nem se a sua privacidade estava sendo respeitada.

9 Texto original: "Most companies were forced to quickly enable remote collaboration capabilities due to COVID-19, but their overall IT ecosystem was not ready for it.".

Além disto, a própria pandemia intensificou a coleta, o processamento e a circulação de dados pessoais decorrente da pandemia de COVID-19, trazendo vários riscos à privacidade e proteção de dados dos indivíduos (Wimmer, 2021). O uso da tecnologia de geolocalização, já mencionada neste artigo, é um dos exemplos de como os dados dos sujeitos passaram a estar mais ameaçados, afinal na tentativa de controle da doença, os indivíduos passaram a ser controlados por meio dos seus próprios dados (Bulzico, 2022, p. 79-85). A situação se torna ainda mais grave quando se sabe que em razão da situação de emergência muitos destes dados foram coletados sem a autorização de seus titulares (Bulzico, 2022, p. 78) e têm sido utilizados de forma abusiva, gerando riscos individuais e coletivos (Machado; Mendes, 2020).

Da mesma forma, o trabalho acabou refém de uma "dominação tecnológica inédita na história do capitalismo", pois as tecnologias contribuem para a dominação e reprodução de desigualdades por grandes empresas, favorecendo o contexto contemporâneo "marcado pela ausência de salários fixos e pelo aprofundamento da precariedade e da indignidade do trabalho em escala global" (Maciel; Mattos, 2020, p. 683). As tecnologias já vinham se apresentando como um instrumento de poder, controle e de dominação de tal forma que "o conhecimento tecnológico se torna a principal força produtiva atual", mas durante a crise sanitária causada pelo coronavírus este papel se viu concretizado (Maciel; Mattos, 2020, p. 683-684).

Ainda, a aceleração da transformação digital proporcionada pela pandemia de COVID-19 agravou a dificuldade de formação de comunidades. Se com a revolução digital, os indivíduos passaram a se aglomerar apenas com interesses específicos e sem uma formação firme (Han, 2018, p. 30), tal crise do coletivo se agravou ainda mais, pois os coletivos passaram a ser ainda mais efêmeros, se desfazendo mais rápido ainda do que se formaram sem a formação de "nós" genuínos. Com a migração forçada para o digital, surgiram mais homens digitais, ou seja, mais indivíduos isolados e singularizados pelas tecnologias e o social deu lugar à solidão (Han, 2018, p. 28-29; 33). Mesmo conectadas pelas tecnologias, as pessoas nunca estiveram tão distantes entre si com relação à valores e propósitos, pois "A mídia digital cria mais distância do real do que as mídias analógicas" (Han, 2018, p. 56). Na busca pela sobrevivência, cada um pensa em si e há uma "erosão da solidariedade" que já estava precária na contemporaneidade (Dörre, 2020, p. XXXII).

Portanto, a aceleração da transformação digital propiciada pela pandemia de COVID-19 expandiu o cenário de múltiplas crises (Morin; Kern, 2003, p. 94) vivenciado na modernidade, desencadeando o surgimento de novos riscos e o agravamento de outros que já existiam, expandindo a sociedade tecnológica de risco que vinha se desenvolvendo desde o avanço das novas tecnologias. Evidenciou-se o capitalismo de risco que se vive nos tempos hodiernos e os novos problemas da humanidade, abrindo uma oportunidade de reflexão sobre as transformações que a sociedade deseja fazer (Dörre, 2020, p. VII) caso deseje optar pela prevenção ao invés de viver rodeada por riscos cada vez maiores.

5 Considerações finais

O artigo analisou que a partir do surgimento das novas tecnologias, também surgiram com elas novos riscos, cada vez mais invisíveis e globais, sem limitação de tempo e de espaço, e que por isso se pode afirmar que com o avanço tecnológico ocorreu também uma evolução da sociedade de risco. Então, em que pese a tecnologia junto com a ciência seja essencial para evolução da sociedade e possua vários benefícios, ela também traz consigo vários riscos complexos, desconhecidos, imprevisíveis e incontroláveis.

Além disto, analisou-se como a pandemia do coronavírus impulsionou a interação social com diversas tecnologias, em especial de informação e comunicação, de uma tal forma que promoveu uma aceleração na transformação digital da sociedade, propiciando que aquilo que era previsto para ocorrer em anos, ocorresse em meses por uma questão de emergência. Demonstrou-se como o uso de tecnologias passou a estar atrelado com uma questão de sobrevivência e com isso houve uma aceleração da migração da população para o digital.

Ao fim, concluiu-se que a aceleração da transformação digital provocada pela pandemia de COVID-19 não foi um processo apenas benéfico, pois trouxe consigo diversos novos riscos, agravou outros que já existiam, expandiu a sociedade tecnológica de risco e a consolidou. Para tal foram apresentados diversos problemas que surgiram com a aceleração digital e como eles evidenciam o aumento das ameaças às quais a sociedade passou a estar exposta.

Desta forma, estabeleceu-se a relação entre a pandemia de COVID-19, que ao proporcionar uma aceleração da transformação digital, e a criação de novos riscos e o agravamento de outros já existentes,

e com isso entende-se que esses elementos promoveram uma expansão da sociedade tecnológica de risco que vinha se consolidando desde que as novas tecnologias passaram a ter um papel tão importante social, econômica, política e culturalmente. Além disto, demonstrou que a humanidade continua sendo responsável pelos riscos cabendo a ela reconhecer a sua responsabilidade pelo caos instaurado e mudar de postura, pois caso contrário ela terá traçado um destino trágico para si própria, criando novos riscos cada vez mais graves e ameaçadores à contemporaneidade e às gerações futuras.

Referências

AGÊNCIA CÂMARA DE NOTÍCIAS. **Deputada e especialistas sugerem educação contra vazamento de dados na internet.** 02 dezembro 2021. Disponível em: https://www.camara.leg.br/noticias/834497-deputada-e-especialistas-sugerem-educacao-contra-vazamento-de-dados-na-internet/#:~:text=Desde%20o%20in%C3%ADcio%20da%20pandemia,Prote%C3%A7%C3%A3o%20de%20Dados%20(ANPD) Acesso em: 27 set. 2025.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS. **ANPD participa de Seminário que discute o combate aos crimes cibernéticos**. 02 dezembro 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-participa-de-seminario-que-discute-o-combate-aos-crimes-ciberneticos Acesso em: 27 set. 2025.

BAUMAN, Zygmunt. **Modernidade Líquida**. Rio de Janeiro: Zahar, 2021.

BAUMAN, Zygmunt; BORDONI, Carlo. **Estado de Crise**. Rio de Janeiro: Zahar, 2016.

BECK, Ulrich. **La sociedad del riesgo global**. Espanha: Siglo Veintiuno, 2002.

BECK, Ulrich. **Sociedade de Risco***:* rumo a uma outra modernidade. Tradução: Sebastião Nascimento. São Paulo: Editora 34, 2010.

BECK, Ulrich. A reinvenção da política: rumo a uma teoria da modernidade reflexiva. In: GIDDENS, Anthony; LASH, Scott; BECK, Ulrich. **Modernização reflexiva**: política, tradição e estética na ordem social moderna. Tradução: Magda Lopes. São Paulo: UNESP, 2012. p. 11-87.

BULZICO, Bianca Amorim. O Uso da Geolocalização em Tempos de COVID-19 e a Consequente Ameaça aos Direitos Individuais na Manipulação de Dados Pessoais pelo Poder Público. In: FREITAS, Cinthia Obladen de Almendra; OLIVEIRA, Dânton Hilário Zanetti de (org.). **Sociedade informacional e a lei geral de proteção de dados pessoais**: diálogos contemporâneos entre direito e tecnologia. Rio de Janeiro: Lumen Juris, 2022. p. 77-96.

CAPELLA, Juan Ramón. **Os cidadãos servos**. Porto Alegre: Sergio Antonio Fabris, 1998.

CASTELLS, Manuel. **A Galáxia Internet**: reflexões sobre a internet, os negócios e a sociedade. Tradução: Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2015.

CASTELLS, Manuel. **A sociedade em rede** – A era da informação: economia, sociedade e cultura. Tradução: Roneide Venancio Majer. 24. ed. Rio de Janeiro: Paz e Terra, 2022.

CAVEDON, Ricardo; FERREIRA, Heline Sivini; FREITAS, Cinthia Obladen de Almendra. O meio ambiente digital sob a ótica da Teoria da Sociedade de Risco: os avanços da informática em debate. **Revista Direito Ambiental e sociedade**, v. 5, n. 1, p. 194-223, 2015.

CHALOUPKA, Bedrich. Cybersecurity lessons from the hybrid workplace surge: New risks and how to counter them. **HEWLETT-PACKARD ENTERPRISE**, 16 jun. 2022. Disponível em: https://community.hpe.com/t5/the-cloud-experience-everywhere/cybersecurity-lessons-from-the-hybrid-workplace-surge-new-risks/ba-p/7168596 Acesso em: 22 jul. 2025.

DÖRRE, Klaus. Capitalismo de risco. Landnahme, crise bifurcada, pandemia: chance para uma revolução sustentável? **Revista Sociedade e Estado**, v. 35, n. 3, p. VII- LII, set./dez. 2020.

FEDERAÇÃO BRASILEIRA DE BANCOS. **Conheça as tentativas de golpes financeiros mais comuns na pandemia e saiba como evitá-los**. 21 setembro 2020. Disponível em: https://portal.febraban.org.br/noticia/3522/pt-br/ Acesso em: 27 set. 2025.

FERREIRA, Heline Sivini. A dimensão ambiental da teoria da sociedade de risco. In: FERREIRA, Heline Sivini; FREITAS, Cinthia Obladen de Almendra (orgs.). **Direito Socioambiental e Sustentabilidade**: Estados, Sociedades e Meio Ambiente. Curitiba: Letra da Lei, 2016. p. 108-158.

FLORIDI, Luciano (ed.). **The Onlife Manifesto**: Being Human in a

Hyperconnected Era. Springer Open, 2015.

GREENFIELD, Adam. **Everyware**: The dawning age of ubiquitous computing. Berkeley-CA: AIGA, 2006.

GUTERRES, António. **Secretary-General's message to Web Summit**. United Nations. Lisbon, 04 dec. 2020. Disponível em: https://www.un.org/sg/en/content/sg/statement/2020-12-04/secretary-generals-message-web-summit Acesso em: 27 set. 2025.

HAN, Byung-Chul. **No enxame**: perspectivas do digital. Tradução: Lucas Machado. Petrópolis, RJ: Vozes, 2018.

HAN, Byung-Chul. **Sociedade da Transparência**. Tradução: Enio Paulo Giachini. Petrópolis, RJ: Vozes, 2017.

IBM. **COVID-19 and the future of business**. Setembro 2020. Disponível em: https://www.ibm.com/downloads/cas/1APBEJWB Acesso em: 27 set. 2025.

INSTITUTO BUTANTAN. **Entenda o que é uma pandemia e as diferenças entre surto, epidemia e endemia**. 2020. Disponível em: https://butantan.gov.br/covid/butantan-tira-duvida/tira-duvida-noticias/entenda-o-que-e-uma-pandemia-e-as-diferencas-entre-surto-epidemia-e-endemia Acesso em: 27 set. 2025.

KOSTENKO, O. V. Electronic Jurisdiction, Metaverse, Artificial Intelligence, Digital Personality, Digital Avatar, Neural Networks: Theory, Practice, Perspective. **World Science**, 1 (73), jan. 2022, p. 01-13.

LIMA, Herbert; FRANCISCO, Eduardo De Rezende. REVOLUÇÃO NOS MEIOS DE PAGAMENTO DIGITAIS. *GV EXECUTIVO*, v. 20, n. 1, jan./mar. 2021, p. 23-25.

MACHADO, Diego Carvalho; MENDES, Laura Schertel. Tecnologias de perfilamento e dados agregados de geolocalização no combate à COVID-19 no Brasil: uma análise dos riscos individuais e coletivos à luz da LGPD. **Revista Direitos Fundamentais & Justiça**, Belo Horizonte, a. 14, número especial, p. 105-148, nov. 2020. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/1020/998 Acesso em: 27 set. 2025.

MACIEL, Fabrício; MATTOS, Patrícia. Como pensar o capitalismo contemporâneo? Considerações preliminares. **Revista Sociedade e Estado**, v. 35, n. 3, p. 673- 694, set./dez. 2020.

MEDINA, Alice Maria Corrêa. Nem cá, nem lá – Para onde a pandemia de COVID-19 pode levar, já que perto/longe é nenhum lugar? **Revista Letras Raras**. Campina Grande, v. 10, n. 4, p. 30-41, dez. 2021.

MEIRELLES, Fernando de Souza**. Relatório da Pesquisa Anual do Uso de Tecnologia de Informação nas Empresas**. 34 ed. São Paulo: Centro de Tecnologia de Informação Aplicada da Escola de Administração de Empresas de São Paulo da Fundação Getúlio Vargas (FGVcia), abril 2023. Disponível em: https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/pesti-fgvcia-2023_0.pdf Acesso em: 27 set. 2025.

MORIN, Edgar; KERN, Anne Brigitte. **Terra-Pátria**. Porto Alegre: Sulina, 2003.

PARISER, Eli. **O filtro invisível**: o que a internet está escondendo de você. Tradução: Diego Alfaro. Rio de Janeiro: Zahar, 2012.

PÉREZ, Mara Gómez. Cautivos en la red. El impacto del metaverso en el derecho de acceso a la información y la protección de datos personales. **IUS ET SCIENTIA**, v. 7, n. 2, p. 88-95, 2021.

PRENSKY, Marc. Digital natives, digital immigrants. On the Horizon, **MCB University Press**, v. 9, n. 5, p. 01-06, 2001.

SCHWAB, Klaus. **A Quarta Revolução Industrial**. Tradução: Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SETTELE, Josef; DÍAZ, Sandra; BRONDIZIO, Eduardo. COVID-19 stimulus measures must save lives, protect livelihoods, and safeguard nature to reduce the risk of future pandemics. **Intergovernmental Science-Policy Platform on Biodiversity and Ecosystem Services (IPBES)**, Bonn, Germany, 27 apr. 2020. Disponível em: https://www.ipbes.net/covid19stimulus Acesso em: 27 set. 2025.

SOUZA, Jéssica Jane de. Indicadores, dataísmo e opacidade: Reflexões acerca de um controle sem alma. **Revista Jurídica do Instituto dos Advogados do Paraná**. Curitiba: NCA Comunicação e Editora., n. 45, p. 197-229, maio 2021.

UNITED NATIONS. **Harmony with Nature – Report of the Secretary-General A/75/266** (28 July 2020a). Disponível em: https://docs.un.org/en/A/75/266 Acesso em: 27 set. 2025.

UNITED NATIONS. **Report of the Secretary-General - Roadmap for Digital Cooperation** (June 2020b). Disponível em: https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_

Digital_Cooperation_EN.pdf Acesso em: 27 set. 2025.

VERBEEK, Peter-Paul. Designing the Public Sphere: Information Technologies and the Politics of Mediation. In: FLORIDI, Luciano (ed.). **The Onlife Manifesto**: Being Human in a Hyperconnected Era. Springer Open, 2015. p. 217-227.

VIEIRA, Giovana Batisti. A Sociedade da Transparência: Distopia ou Realidade? In: FREITAS, Cinthia Obladen de Almendra; OLIVEIRA, Dânton Hilário Zanetti de (org.). **Sociedade informacional e a lei geral de proteção de dados pessoais**: diálogos contemporâneos entre direito e tecnologia. Rio de Janeiro: Lumen Juris, 2022. p. 161-181.

WIMMER, Miriam. Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia. **Revista Brasileira de Políticas Públicas**, v. 11, n. 1, p. 123-142, abr. 2021.

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

Capítulo 7

ASSEMBLEIAS VIRTUAIS NO METAVERSO: UMA EXPRESSÃO CONTEMPORÂNEA DA SOCIEDADE TECNOLÓGICA DE RISCO

Marina Schmidlin Sponholz[1]

1 Introdução

Com a evolução tecnológica, em especial após o advento das Tecnologias de Informação e Comunicação (TICs), verificou-se o surgimento de novos riscos globais que passaram a permear a vida e o cotidiano da humanidade de tal forma que a sua própria existência digna passou a estar ameaçada. Riscos estes muitas vezes invisíveis e imperceptíveis ou até mesmo ocultos em promessas de oportunidade e comodidade de tal forma que os indivíduos demoraram para se dar conta – se é que já tenham se dado conta - de sua existência.

A busca incessante pelo aprimoramento das experiências dos indivíduos com as tecnologias, apoiada pelo modelo econômico capitalista, fez com que o mundo passasse a buscar evoluir do digital para o virtual tanto como uma forma de resposta às demandas da humanidade quanto também como uma oportunidade de geração de lucro e produtividade. E foi justamente neste cenário que surgiu o Metaverso, como um ambiente repleto de oportunidades, de praticidade, de inovação e de experiências que prometem utilizar a tecnologia para beneficiar a humanidade de uma maneira diferente de todas já vistas.

Ocorre que o Metaverso, assim como qualquer tecnologia, traz consigo riscos que não podem ser desprezados e precisam ser gerenciados para que ele cumpra com todas as promessas que ele faz. No contexto atual onde os riscos possuem proporções e consequências desconhecidas, não

1 Mestre em Direito pelo Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná (PUCPR). Advogada. Membro relatora da Comissão de Direito Digital e Proteção de Dados da OAB/PR. L.L.M em Direito Empresarial pela Fundação Getúlio Vargas FGV-Rio. Bacharela em Direito pelo Centro Universitário Curitiba. Associada do Instituto Brasileiro de Direito de Família (IBDFAM). Membro do Instituto dos Advogados do Paraná. Email marinasponholz@gmail.com

possuem limitação de tempo nem de espaço, se faz necessário que toda a ação praticada – inclusive nos negócios - envolva um gerenciamento dos riscos envolvidos, sob pena da dignidade da humanidade acabar sendo não apenas ameaçada, mas violada de uma forma irreparável.

E sabendo-se que um dos pontos principais dos negócios que o Metaverso tem impactado é a realização de assembleias – entendidas como quaisquer assembleias de acionistas, de sócios e de associados, inclusive as gerais, que compõem o processo decisório e de governança de vários tipos societários – as quais passam a ser realizadas também em ambientes virtuais e não apenas nos digitais, se faz necessária uma análise pormenorizada da viabilidade e segurança de sua adoção. Afinal, considerando que o Metaverso é um ambiente típico da sociedade tecnológica de risco, a realização de assembleias virtuais nele não pode ser tratada da mesma forma que as realizadas no ambiente físico, pois está submetida a novos riscos, específicos e que precisam de um tratamento jurídico e tecnológico específico.

Diante disto, por meio do método hipotético-dedutivo e a partir da pesquisa bibliográfica e documental, o analisa-se o contexto atual de sociedade tecnológica de risco e se o Metaverso - na expectativa de proporcionar uma experiência imersiva que aprimora a comunicação à distância e a forma como as assembleias remotas são realizadas – junto com oportunidades cria novos riscos aos negócios. Para tal, parte-se da hipótese de que o Metaverso é um ambiente típico da sociedade tecnológica de risco e que a realização de assembleias virtuais nele expressa um risco que deve ser gerenciado não apenas por dispositivos legais, mas também por ferramentas tecnológicas.

A texto possui 03 (três) tópicos, sendo que no primeiro é estruturada a noção de uma sociedade tecnológica de risco por meio de uma conexão entre a Teoria do Risco Global de Ulrich Beck e as transformações oriundas do advento de novas tecnologias, em especial das TICs. No segundo tópico é analisado como o Metaverso representa uma evolução do meio ambiente digital para o meio ambiente virtual e como as transformações que ele trouxe para a sociedade não representam apenas o surgimento de oportunidades, mas também de riscos. Por fim, no terceiro tópico examina-se a possibilidade de realização de assembleias virtuais no Metaverso e discorre-se sobre a necessidade de que, além do cumprimento dos requisitos legais, seja também adotado um ferramental

técnico relacionado a cibersegurança e Segurança da Informação para que haja um efetivo gerenciamento de riscos.

2 O surgimento de uma sociedade tecnológica de risco

Em meados de 1986, com a publicação da primeira versão da sua obra Sociedade de Risco, Ulrich Beck iniciou uma reflexão sobre como as diversas transformações proporcionadas pela globalização estavam fazendo surgir uma nova sociedade, na qual as pessoas estavam mais conectadas entre si, mas na qual ao mesmo tempo surgiam novas situações de ameaça com as quais as instituições até então existentes não eram suficientes para enfrentar. Ou seja, a partir do trabalho de Beck evidenciou-se que a pós-modernidade trouxe também consigo problemas, pois novos riscos que foram criados pela própria humanidade (BECK, 2010).

Um dos grandes marcos da teoria de Beck é a compreensão de que riscos, em que pese tenham as características de incerteza, relação com a probabilidade, conexão com futuro, se diferem dos perigos por serem fruto de atividades humanas e escolhas sociais do presente (FERREIRA, 2016, p. 112-114). E ao conferir uma dimensão racional ao risco, Beck (2002, p. 114) confere uma responsabilidade à humanidade pelas ameaças que ela mesma enfrenta, pelo surgimento de uma sociedade de risco global, uma vez que ela surge automaticamente em decorrência dos processos autônomos de modernização que desprezam consequências e perigos.

Segundo Heline Sivini Ferreira (2016, p. 117-122) os principais elementos que configuram a sociedade de risco são que os riscos passaram a não ter mais limitações de tempo e espaço - o que faz com que seus efeitos não sejam apenas instantâneos, mas possam também se projetar para o futuro -, se desconhece o seu potencial de destruição – levando à descrença de que existam instituições preparadas para controlá-los e/ou prevê-los – e, além disto, os riscos são globais, porque passaram a ser compartilhados por todos os povos, mesmo que em diferentes níveis.

Portanto, conforme o tempo foi passando e a sociedade foi evoluindo para uma sociedade de risco foram surgindo novos riscos, também mais "avançados" que acabaram sendo um grande marco da nova realidade trazida pela pós-modernidade. E, para a configuração desta chamada sociedade de risco, houve grande contribuição da ciência e da tecnologia, que passaram a ser usadas, junto com o conhecimento científico, com

vistas a fundamentar interesses específicos, principalmente mercadológicos (FERREIRA, 2016, p. 123-127).

Para Beck, o progresso tecnológico e suas consequências, adquirem caráter de bens coletivos na sociedade de risco, e, portanto, as decisões sobre eles se tornam um problema coletivo. Mas, infelizmente, nem sempre o debate público ocorre como deveria e as decisões sobre riscos aceitáveis acabam transformadas em lutas de poder. Perde-se o foco nos riscos em si e passa a se debater as posições, dimensões e características sobre os responsáveis e afetados por eles (BECK, 2002, p. 130-131).

Sob a perspectiva do avanço tecnológico, desenvolveu-se uma nova sociedade, a sociedade tecnológica, que trouxe consigo novos desafios a serem enfrentados e novos riscos, reconfigurando aquela sociedade de risco global trabalhada por Beck (2002) ao novo cenário de disseminação de TICs e de inovação tecnológica. Por isso, Freitas, Ferreira & Cavedon (2020, p. 200) afirmam que "*Dentre os riscos abstratos criados pela modernidade avançada, encontram-se aqueles decorrentes do emprego de novas tecnologias [...]*".

Em especial com o advento do paradigma que Greenfield (2006, p. 09-11) denomina de *everyware*, segundo o qual as tecnologias estão tão presentes na vida das pessoas, em todo lugar e tempo, várias noções dos sujeitos têm sido transformadas. Justamente porque não se pode conceber, atualmente, um mundo sem tecnologia, na sociedade contemporânea marcada pela velocidade, mobilidade e acessibilidade, e na qual "*fronteira, presença, matéria, território, distância, tempo e informação são palavras que mudaram seus próprios significados* [...]" (FREITAS; ROSSI, 2020, p. 14).

Ao trazerem consigo um potencial de ressignificação de aspectos essenciais à vida dos indivíduos e, inclusive, alterando a distinção entre o que configura público ou privado (FREITAS; ROSSI, 2020, p. 16), as tecnologias afetam a própria forma de viver da humanidade. O "ser" humano é transformado pelas tecnologias, em especial as de comunicação e informação, e pela computação ubíqua e pervasiva (FREITAS; ROSSI, 2020, p. 14-15), pois mesmo sem perceber e parecendo que estas interações são naturais e espontâneas, a sua forma de existir passa a ser moldada pela sua interação com elas.

De acordo com Floridi (2015) a humanidade hoje não consegue mais viver dissociada das tecnologias, por isso ele afirma que se vive uma *onlife*, não apenas uma vida, mas uma vida *online*, constantemente hiperconectada às tecnologias. Portanto, as TICs não são meras ferramentas,

mas sim forças ambientais que impactam radicalmente a vida humana, gerando grandes transformações que trazem consigo grandes impactos à condição humana ao modificarem a própria forma dos indivíduos viverem (FLORIDI, 2015, p. 03), não havendo como se ignorar que diversos problemas surgem.

Ao mesmo tempo em que temos uma hiperexposição dos indivíduos, uma intensificação da transparência (HAN, 2017, p. 09), também há um obscurecimento do espaço público (FREITAS; ROSSI, 2020, p. 03). A privacidade e o livre desenvolvimento da personalidade adquirem novos contornos ao mesmo tempo em que cresce o individualismo e a participação e interação social se focam em egos, demonstrando que a exposição, como bem trata Byung-Chul Han ao analisar a sociedade da transparência, não contribui para formar comunidades (HAN, 2017, p. 108-114). Desta maneira,

> A realidade digital está tomando conta e redefinindo tudo que é familiar, antes mesmo de termos tido a chance de ponderar e decidir sobre a situação. Nós celebramos o mundo conectado por causa das muitas maneiras pelas quais ele enriquece nossas capacidades e perspectivas, mas ele gerou novos grandes territórios de ansiedade, perigo e violência conforme o senso de um futuro previsível se esvai por entre nossos dedos (ZUBOFF, 2020, p. 18).

Por esta razão, se pode afirmar que hoje vivemos uma nova fase da sociedade de risco global na qual as tecnologias - que se tornaram ubíquas e pervasivas de tal modo que não se pode mais viver sem elas (FLORIDI, 2015, p. 43) - trouxeram consigo novos problemas criados pela própria humanidade. Assim, considerando que, com o surgimento das tecnologias, surgiram também novos riscos, invisíveis, transfronteiriços, transtemporais e globais, pode-se dizer que a sociedade tecnológica se configura também uma sociedade de risco global na qual a humanidade - em que pese muitas vezes não perceba - está extremamente vulnerável e refém de suas próprias escolhas.

Então, mesmo sendo a tecnologia de modo geral uma grande aliada para que a sociedade se desenvolva, é fato que existem algumas situações nas quais algumas tecnologias - em especial dependendo do contexto - podem apresentar grandes riscos à sociedade os quais devem ser estudados e avaliados para evitar a ocorrência de danos muitas vezes irreversíveis (VIEIRA, 2022, p. 162).

Assim como na teoria de Ulrich Beck (2002) os riscos da modernidade avançada são produtos de decisões e escolhas dos indivíduos,

o mesmo ocorre na sociedade tecnológica: os indivíduos escolheram dar à tecnologia um papel de protagonismo em suas vidas, e a escolha de abrir mão de parte do controle de suas vidas em favor da tecnologia possui consequências sobre o seu modo de viver e inclusive sobre a sua existência. Ou seja, assim como na sociedade de risco trabalhada por Beck (2002), na sociedade tecnológica de risco os riscos que surgem são decorrentes de escolhas humanas e possuem um elemento racional que os origina, porque a humanidade determina o valor das coisas na sociedade.

Da mesma forma como Beck (2012, p. 18-19) pontua a importância da reflexividade e da reflexão sobre os riscos da modernidade avançada e sobre as consequências da sociedade de risco, a compreensão e consciência da existência de uma sociedade tecnológica de risco é essencial para que a humanidade enxergue as tecnologias como elas devem ser vistas: como instrumentos que visam facilitar a vida humana e trazer uma série de benefícios, mas que ao mesmo tempo precisam ser tratados e usados com a devida cautela, pois trazem consigo novos riscos, desconhecidos, que ameaçam a humanidade em escala global e que as instituições tradicionais não são suficientes para enfrentar.

Se com o surgimento da sociedade de risco houve uma mudança na forma de viver dos indivíduos provocada por um processo de individualização e de desintegração das fontes de significado coletivas ao mesmo tempo em que cresce uma interdependência entre todos (BECK, 2012, p. 19-21; 30-31; 33-34), com a evolução para a sociedade tecnológica de risco esta individualização é agravada. Isto, porque as mudanças trazidas pelas tecnologias criam um cenário extremamente favorável a consolidação ao modelo mais individualista de estruturação da sociedade uma vez que os tomadores de decisão "não conseguem pensar de forma estratégica sobre as forças de ruptura e inovação que moldam o nosso futuro" (SCHWAB, 2016, p. 12).

Assim como na sociedade de risco concebida por Beck todos individualmente fazem escolhas e são agentes individuais e planejadores (2012, p. 33-34), mas acaba sendo toda a sociedade afetada (2002, p. 113), com o advento de uma sociedade tecnológica, trazendo várias tecnologias que permitem que a sociedade permaneça fragmentada e conectada, há um agravamento do individualismo que acaba favorecendo a desumanização da vida social, que acaba se afastando de valores humanos e coletivos.

Além disto, o próprio uso das tecnologias em si pode trazer consigo riscos à direitos fundamentais para uma existência digna. Direitos como,

por exemplo, privacidade, autodeterminação informacional e liberdade podem ser seriamente ameaçados caso as tecnologias são sejam usadas com a devida cautela e planejamento. A grande questão é a forma como as tecnologias são usadas, a forma como os seres humanos que estão por trás delas acabam as utilizando. Os riscos surgem conforme a destinação que os indivíduos dão às tecnologias, pois "*a tecnologia não é uma força externa, sobre a qual não temos nenhum controle*" (SCHWAB, 2016, p. 13).

Como bem coloca Manuel Castells (2015, p. 10) "*a volatilidade, a insegurança, a desigualdade e a exclusão social andam de mãos dadas com a criatividade, a inovação, a produtividade e a criação de riqueza nesses primeiros passos do mundo baseado na Internet*". Mas, quando falamos em tecnologias de realidade virtual e realidade ampliada, por exemplo, falamos em ferramentas tecnológicas que, além de trazerem consigo os riscos intrínsecos a elas mesmas, ao criarem um novo ambiente ampliam também o espaço no qual podem surgir ameaças. Portanto, além de surgirem novos riscos, surgem também novos ambientes nos quais tais riscos podem se manifestar, surgem novos lugares nos quais a dignidade da pessoa humana deve ser assegurada e os riscos da modernidade devem ser gerenciados - já que não podem ser eliminados.

Por esta razão, tal como na sociedade de risco global de Beck já se falava da importância da consciência da humanidade para o gerenciamento dos riscos da modernidade avançada, na sociedade tecnológica de risco, também se faz necessário que a humanidade perceba que são as suas escolhas que determinam os riscos e ameaças que deseja enfrentar e que com o advento das tecnologias, o meio ambiente no qual há a sua exposição é muito amplo, envolvendo os espaços digitais e virtuais. Afinal, "*Moldar a quarta revolução industrial para garantir que ela seja empoderadora e centrada no ser humano – em vez de divisionista e desumana – não é uma tarefa para um único interessado ou setor, nem para uma única região, ou indústria ou cultura*" (SCHWAB, 2016, p. 14).

3 Meio ambiente virtual, metaverso e a evidenciação de um novo meio das pessoas viverem e interagirem

Como visto, com o advento das tecnologias, houve também uma ampliação dos espaços nos quais os riscos podem surgir. Os perigos que antes se restringiam ao espaço físico, passaram também a se manifestar em ambientes que foram criados pelas próprias tecnologias. Surgiu um "novo

mundo" que desconhece fronteiras de tempo e de espaço, e que reflete nitidamente a lógica de globalização que impera. Este novo espaço de interação entre indivíduos não é físico-territorial, mas virtual (FREITAS; ROSSI, 2020, p. 07).

Assim, no decorrer da evolução tecnológica viu-se também a necessidade de uma evolução na compreensão da expressão meio ambiente, que compreenda que as tecnologias do mundo físico, digital e biológico estão se fundindo (SCHWAB, 2016, p. 11) e que não deixe à margem de uma proteção jurídica diversos ambientes nos quais a vida humana transformada pela Quarta Revolução Industrial se desenvolve.

Desta forma, o advento de uma sociedade tecnológica e a evolução das tecnologias fizeram com que passasse a ser reconhecida a existência de um meio ambiente digital que deve ter assegurado o seu equilíbrio e desenvolvimento, bem como onde a dignidade da pessoa humana e as garantias fundamentais devem ser salvaguardadas (FREITAS; FERREIRA, CAVEDON, 2020, p. 204). Ou seja, por meio das tecnologias surgiu um espaço que merece ser tutelado e resguardado juridicamente por se tratar de um local em que a humanidade vive, participa, interage, trabalha e realiza as mais diversas ações, e no qual, portanto, ela precisa ter a sua dignidade e integridade preservadas (FREITAS; FERREIRA, CAVEDON, 2020, p. 204).

Portanto, conceber a existência de um meio ambiente digital, significa considerar que existe um todo indivisível muito maior do que o que era tido antes do advento das tecnologias que precisa ser protegido e tutelado. Que a partir do momento em que o homem passou a atuar em outro meio que não apenas o físico, o meio ambiente digital deve ser visto como parte indissociável do conceito jurídico de meio ambiente previsto no artigo 3º da Lei 6.938/1981 (BRASIL, 1981), devendo "estar a serviço do desenvolvimento sustentável" e devendo "considerar o imperativo de proteção ambiental" (FREITAS; FERREIRA, CAVEDON, 2020, p. 203-204).

Desta forma, o conceito de meio ambiente evoluiu (FREITAS; FERREIRA, CAVEDON, 2020, p. 204) – e continua evoluindo – junto com as inovações tecnológicas. E se já houve um processo de evolução do físico para o eletrônico e posteriormente para o digital, hoje se pode afirmar que está sendo enfrentado um processo de evolução do digital para o virtual e consequentemente do meio ambiente digital para o meio ambiente virtual.

O digital, que se trata de uma representação do físico em um sistema binário, começa a ceder espaço para o virtual que cria uma imersão de tal modo que os indivíduos sentem que é real por meio de técnicas e métodos que experiências mais imersivas e autênticas que se assemelham uma realidade física (informação verbal[2]). É como se a humanidade buscasse a criação de uma nova realidade, muito próxima da física, para atender aos seus anseios quando não mais consegue satisfazer as suas necessidades apenas no meio físico[3].

No entanto, quando um sistema de comunicação gera virtualidade real ele se trata de um sistema "em que a própria realidade [...] é inteiramente captada, totalmente imersa em uma composição de imagens virtuais no mundo do faz de conta, no qual as aparências não apenas se encontram na tela comunicadora da experiência, mas se transformam na experiência." (CASTELLS, 2022, p. 455). É como se toda a experiência humana fosse absorvida pela tecnologia, pois a realidade na Era Digital compreende a transformação para o virtual (LÉVY, 1998).

Por esta razão que, com o avanço tecnológico, o próprio meio ambiente, enquanto um todo indivisível passou a ter uma concepção mais ampla para poder abranger também os ambientes digitais e virtuais de modo que se compreenda que se tratam de espaços que fazem parte de um todo indivisível e interdependente que precisa ser equilibrado (FREITAS; FERREIRA, CAVEDON, 2020, p. 201-204) e que, assim como todo o resto, também possuem problemas que precisam ser enfrentados e tutelados.

Segundo Manuel Castells (2022, p. 441-443), as comunidades virtuais que surgiram com a evolução tecnológica oferecem um novo contexto e suscitam várias reflexões, especialmente sobre a forma como as pessoas – individualmente - se relacionam com a sociedade em geral. No entanto, com base em estudos de Barry Wellman, ele afirma que as comunidades virtuais são comunidades reais (situadas em outro plano da realidade que não o físico) e que com elas surgem modelos de comunicação e interação que são diferentes dos das comunidades físicas.

E justamente neste sentido, marcando a evolução do digital para o virtual, que surgiu o chamado Metaverse[4], que consiste em "uma rede de

2 Fala da Professora, Doutora em Informática, Cinthia Obladen de Almendra Freitas na disciplina Questões Tecnológicas e Sociedades, do Programa de Pós Graduação em Direito da PUCPR, em 08 de agosto de 2022.

3 Sobre a busca de refúgio no virtual vide CASTELLS, 2022, p. 441.

4 Cumpre pontuar que há quem defenda que o Metaverso ainda não existe, pois o que existe são

mundos virtuais interligados, sobrepostos a realidades físicas, que facilita uma experiência imersiva para conhecer, interagir e transacionar sem limitações geográficas" (BRICE; GOH, 2022, p. 03, tradução nossa). Se trata um universo virtual, de "um espaço online compartilhado onde as realidades física, aumentada e virtual convergem" (RASHID et al., 2022, p. 266).

Este universo que vai além do físico, "retrata uma ampla mudança na forma como interagimos com a tecnologia através da convergência de recursos físicos, virtuais, aumentados ou mesmo de realidade mista que abraçam a emergente tecnologia Web 3.0" (BRICE; GOH, 2022, p. 03, tradução nossa) evidenciando como tecnologias de experiências imersivas e autênticas têm o potencial de impactar as interações sociais eliminando limites físicos. Por esta razão, há quem sustente que o Metaverso[5] constitui um novo horizonte para a própria existência da humanidade (CHANDRASEKAR, 2022, p. 08).

O Metaverso se trata, portanto, de "uma tecnologia que se constitui no ciberespaço e se "materializa" por meio da criação de Mundos Digitais Virtuais em 3D – MDV3D, no qual diferentes espaços para o viver e conviver são representados em 3D, propiciando o surgimento dos "mundos paralelos" contemporâneos" que se modificam em tempo real à medida que os usuários interagem com eles (SCHLEMMER; BACKES, 2008, p. 522).

Assim, o Metaverso se trata de um ambiente de total imersão viabilizada por recursos de Realidade Virtual (SCHLEMMER; BACKES, 2008, p. 523) e como cria-se uma experiência muito mais personalizada e interativa, limites geográficos e de tempo acabam sendo significativamente mitigados, proporcionando enorme comodidade ao acesso de bens, serviços e até oportunidades de emprego (BRICE; GOH, 2022, p. 03). Por esta razão que se afirma que ele representa um universo de novas oportunidades a serem oferecidas (MOY; GADGIL, 2022, p. 03), mas que ao criar uma nova realidade ele também traz consigo riscos (UNITED NATIONS DEVELOPMENT PROGRAMME, 2022).

Com as pessoas passando mais tempo em ambientes digitais e virtuais (UNITED NATIONS DEVELOPMENT PROGRAMME,

aspectos dele, mas como estes aspectos não estão conectados não se pode afirmar que ele exista efetivamente. *In:* CHANDRASEKAR, 2022, p. 02.

5 No presente artigo será usado o termo Metaverso como tradução livre da expressão *Metaverse*, para representar a tecnologia de forma genérica.

2022), talvez a expressão *onlife* de Floridi nunca tenha feito tanto sentido. A busca de experiências mais imersivas e próximas da realidade física comprova que o Metaverso não apenas terá, mas já está tendo um papel transformador na forma como as pessoas vivem e interagem entre si. Ao mesmo tempo, na condição de parte integrante do meio ambiente, como uma expressão de meio ambiente virtual, se trata de uma obrigação não apenas constitucional, mas humanitária, garantir que ele seja um ambiente sadio, justo e que respeite os valores fundamentais da humanidade.

Segundo Klaus Schwab (2016, p. 56) as tecnologias que sustentam a Quarta Revolução Industrial influenciam como as empresas são lideradas, organizadas e administradas. E, com relação ao Metaverso, isto não foi diferente, mas grande parte do foco sobre ele se centra nas expectativas de oportunidade que ele cria e em como as empresas e negócios podem explorá-lo de forma proveitosa (MOY; GADGIL, 2022, p. 01).

Ocorre que, ao ser visto apenas sob a ótica da oportunidade, alguns aspectos de grande relevância e importância acabam sendo deixados de lado. O encantamento pela novidade e inovação, cega a humanidade para problemas e faz os indivíduos acharem que o Metaverso é apenas benéfico e promissor. Quando, na verdade, assim como as outras tecnologias, ele também tem o potencial de ser bom ou ruim, de ser usado para o bem ou para a destruição, seguindo a emblemática reflexão de David Bohm (PARISER, 2012, p. 145).

O Metaverso precisa ser desmistificado, pois mesmo trazendo mudanças benéficas e oportunidades, seu surgimento também traz riscos que precisam ser gerenciados para evitar danos digitais e exacerbação das desigualdades (UNITED NATIONS DEVELOPMENT PROGRAMME, 2022). Deve ser analisado na medida das transformações que ele provoca na existência humana e na sociedade e seu potencial só poderá ser efetivamente explorado quando todos em qualquer lugar puderam acessá-lo e quando ele se comprovar seguro (UNITED NATIONS DEVELOPMENT PROGRAMME, 2022).

Não se duvida que o Metaverso traz consigo promessas encantadoras e com o potencial de contribuir inclusive para o desenvolvimento sustentável da sociedade. No entanto, deve-se pontuar que o seu surgimento e desenvolvimento traz preocupações válidas e potenciais sobre privacidade, abuso de direitos humanos, agravamento de desigualdades, perpetuação de preconceitos sociais e até mesmo preocupações ambientais sobre o uso de energia (UNITED NATIONS DEVELOPMENT

PROGRAMME, 2022). "O futuro do Metaverso é promissor, mas traz seu próprio conjunto de desafios" e é essencial que a sociedade esteja ciente deles (CHANDRASEKAR, 2022, p. 13, tradução nossa).

Apesar do potencial de mercado e das oportunidades, o Metaverso ainda está se desenvolvendo e existem riscos sobre os quais as pessoas devem estar cientes (BRICE; GOH, 2022, p. 12). Não basta só se pensar na evolução e no desenvolvimento do Metaverso, mas também se deve buscar que ele seja um ambiente de inovação que além de significativo também seja seguro e não agrave problemas que já assolam a sociedade, de modo que se possa conciliar o gerenciamento de seus riscos com as oportunidades que ele promete (UNITED NATIONS DEVELOPMENT PROGRAMME, 2022).

O Metaverso proporciona uma nova vida, virtual, mas que possui as mais diversas repercussões jurídicas na vida real física, portanto em que pese seja um cenário com diversas oportunidades, junto com elas também surgem desafios que demandam uma especial atenção do Direito. Por esta razão, ainda são necessárias mais pesquisas de planejamento e construção do Metaverso (RASHID *et al.*, 2022, p. 266), bem como sobre sua manutenção e regulação.

4 Assembleias virtuais no metaverso: desafios ao gerenciamento de riscos no meio ambiente virtual

Desde o advento da Internet, com o surgimento de uma nova economia - informacional, global e em rede (CASTELLS, 2022, p. 135) – "cada vez mais capaz de aplicar seu progresso em tecnologia, conhecimentos e administração na própria tecnologia, conhecimentos e administração", os negócios foram severamente impactados. Uma das grandes transformações é o fato de as tecnologias estarem diretamente associadas não apenas às empresas, mas aos seus negócios em si. Se antes as tecnologias, como a Internet, eram desenvolvidas no âmbito das universidades, centros de pesquisa e instituições governamentais (CASTELLS, 2015, p. 27-28), hoje elas são o próprio objeto de muitos negócios e também integram de modo indispensável o cotidiano de empresas.

Ocorre que os avanços tecnológicos já vinham ocorrendo, foram propulsados a outro patamar com a ocorrência da pandemia da COVID-19. A partir de 2020, negócios que não dependiam de tecnologias de informação e comunicação para se desenvolverem foram compelidos

a aderirem a elas para que pudessem se manter ativos. Todos, negócios grandes ou pequenos, tinham a necessidade de conciliar seu funcionamento com o distanciamento social. O mundo precisou encontrar meios de não parar e a interação por meio das tecnologias passou a ser uma necessidade para a sobrevivência da humanidade e dos negócios:

> A pandemia do COVID-19 estimulou o desenvolvimento da tecnologia da informação, que substituiu parcialmente o ser humano como ser social, a necessidade de comunicação física e troca de informações entre grupos de pessoas. É possível dizer que as restrições forçadas das atividades cotidianas tradicionais contribuíram para a mudança para a realidade virtual do metaverso das relações sociais com a imitação da funcionalidade física. Videoconferência, comunicação por vídeo e transmissão de vídeo se exauriram, precisamente porque não podem fornecer totalmente o efeito de presença e comunicação interpessoal visual, verbal e tátil com papéis sociais tradicionais (KOSTENKO, 2022, p. 03).

Assim, a aceleração que a pandemia provocou na Revolução Digital, acabou também levando o debate sobre a realização de assembleias virtuais a outro patamar, ou melhor dizendo, a outro universo. Enquanto a realidade de reuniões *online* ainda está sendo compreendida por grande parte da população, existem algumas empresas que, no desejo de mostrar o seu engajamento com a cultura digital e visando diminuir gastos com local e estrutura para a realização da reunião, bem como ampliar e melhorar a interação entre os participantes e de se destacar perante seus concorrentes, estão realizando suas assembleias (de sócios, acionistas etc.) no Metaverso.

No Brasil, a discussão ganhou força com uma consulta feita em julho de 2022 pela Associação Brasileira das Companhias Abertas (Abrasca) à Comissão de Valores Mobiliários (CVM), onde se requereu que a autarquia avaliasse a possibilidade de adequação das normas da Resolução 81, de março de 2022 (que já trata da realização de assembleias de modo digital), para realização de assembleias gerais no Metaverso (ASSOCIAÇÃO BRASILEIRA DAS COMPANHIAS ABERTAS, 2022a). Em agosto de 2022 a CVM respondeu à consulta, por meio do parecer técnico 146, informando que "não vê óbice à realização de assembleias de acionistas no espaço imersivo Metaverso, desde que atendidos todos os requisitos estabelecidos na Lei 6.404/76 e na Resolução CVM 81/22, além de outras normas eventualmente aplicáveis" (ASSOCIAÇÃO BRASILEIRA DAS COMPANHIAS ABERTAS, 2022b).

O entendimento da CVM, em que pese se restrinja às companhias abertas, possibilita que seja feita uma analogia para as companhias fechadas, sociedades limitadas e sociedades cooperativas, que não possuem nenhuma diretiva a respeito, mas que – como no caso das companhias abertas – possuem legislação específica autorizando a realização de assembleias à distância.

Desde do advento da Lei nº 12.431 de 2011 - com a inclusão do parágrafo único no artigo 121 da Lei nº 6.404 de 1976 - foi permitido em companhias abertas que o acionista participasse e votasse à distância em assembleia geral, "*nos term*os da regulamentação da Comissão de Valores Mobiliários" (BRASIL, 2011). Mas, somente com o advento da Medida Provisória nº 931 de 2020 e, posteriormente, com a nova redação dada pela Lei nº 14.030 de 2020 ao parágrafo único do artigo 121 da Lei nº 6.404 de 1976, passou a ser possível que tanto nas companhias abertas como nas fechadas os acionistas pudessem "participar e votar a distância em assembleia geral, nos termos do regulamento da Comissão de Valores Mobiliários e do órgão competente do Poder Executivo federal, respectivamente." (BRASIL, 1976). Além disto, a modalidade digital de assembleia geral de companhias abertas e fechadas passou a constar expressamente no texto da Lei 6.404 de 1976, somente após a inclusão do § 2º-A no artigo 124 feita pela Lei nº 14.030 de 2020 (BRASIL, 1976).

No caso das sociedades limitadas, há autorização expressa no artigo 1.080-A do Código Civil, incluído pela Lei nº 14.030 de 2020 para a realização não apenas de assembleias, mas também de reuniões, à distância. Sendo que o parágrafo único do referido artigo proclama que as reuniões e assembleias das referidas sociedades podem ser realizadas inclusive na modalidade digital desde que "respeitados os direitos legalmente previstos de participação e de manifestação dos sócios e os demais requisitos regulamentares" (BRASIL, 2002).

Já na hipótese das sociedades cooperativas, a realização tanto de reuniões como de assembleias a distância foi possível a partir da Medida Provisória nº 931 de 2020 e, posteriormente, a partir da Lei nº 14.030 de 2020 passou a estar expressamente autorizada na Lei nº 5.764 de 1971 no seu artigo 43-A a possibilidade de sua realização em meio digital "nos termos do regulamento do órgão competente do Poder Executivo federal". No caso das assembleias gerais, o parágrafo único do artigo 43-A da Lei nº 5.764 de 1971 impõe como condição para a sua realização no meio digital que sejam "respeitados os direitos legalmente previstos de participação e

de manifestação dos associados e os demais requisitos regulamentares." (BRASIL, 1971).

Assim, se pode afirmar que, como as leis não restringem a modalidade de realização das assembleias a distância, se os requisitos legais forem respeitados, da mesma forma como a CVM entendeu no caso das companhias abertas, se pode afirmar que não há óbice legal à realização de assembleias, inclusive as gerais, no Metaverso, podendo ser considerado ele um ambiente de imersão que se configura juridicamente adequado para a realização de reuniões. No entanto, o Metaverso, assim como as demais tecnologias, traz consigo riscos que precisam ser levados em consideração para se analisar se tecnicamente ele é um ambiente seguro para a realização de assembleias, inclusive as gerais e que, sob a lógica da criação de pontes de Eli Pariser (2012, p. 21), permitam a existência de um contexto no qual os indivíduos criem profundas conexões uns com os outros de modo que resolvam problemas além de seus interesses pessoais e alcancem melhores soluções.

A questão dos riscos fica muito evidente quando se verifica que a Organização Internacional de Polícia Criminal - INTERPOL - já ingressou no Metaverso para assegurar que junto com a exploração de suas oportunidades também haja conscientização sobre as ameaças deste "novo mundo", afinal "os criminosos já estão começando a explorar o Metaverso" e "golpes de engenharia social, extremismo violento e desinformação podem ser desafios particulares.". Isto sem contar o fato de que pode haver um grande desafio de aplicação da lei pelo fato de que "nem todos os atos que são criminalizados no mundo físico são considerados crimes quando cometidos no mundo virtual" (INTERPOL, 2022, tradução nossa).

Por esta razão que se faz extremamente importante identificar os riscos do Metaverso desde o início, para que se possa "trabalhar com as partes interessadas para moldar as estruturas de governança necessárias e cortar futuros mercados criminais antes que eles estejam totalmente formados" (INTERPOL, 2022, tradução nossa). Ou seja, juntamente com o cumprimento dos requisitos legais, é essencial que haja a adoção de mecanismos que gerenciem os riscos que envolvem o Metaverso para que se possa efetivamente defender que assembleias podem ocorrer lá de forma não apenas jurídica, mas tecnicamente segura.

Ocorre que, a segurança no Metaverso vai muito além de assegurar um ambiente seguro com relação à prática de crimes, mas consiste também em assegurar a proteção dos indivíduos e de sua integridade por meio da

proteção de seus dados. A construção de um ambiente digital (e agora também virtual) equilibrado, saudável e no qual a dignidade da pessoa humana seja preservada passa por assegurar a tutela correta aos seus dados pessoais, especialmente após o advento da Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018), que passou a exigir no Brasil, a adoção de medidas de segurança que garantam a proteção e o uso adequado de dados pessoais[6].

Portanto, quando a realização de assembleias no Metaverso envolver alguma das hipótese previstas no artigo 3º da LGPD, como - por exemplo - o tratamento de dados de indivíduos que se localizam no território brasileiro, ou quando os dados pessoais objeto do tratamento tenham sido coletados no território nacional, além do cumprimento dos requisitos previstos na legislação brasileira no que tange à formalidade de sua realização, também devem ser observadas regras relativas à proteção de dados pessoais, o que envolve adotar técnicas de Segurança da Informação. Afinal, cibersegurança, que tanto tem sido buscada na atualidade, passa pela área da Segurança da Informação (ISO, 2022a).

Desta maneira, os aspectos tecnológicos da proteção de dados pessoais trouxeram uma importância ainda maior para a área de Segurança da Informação, a qual, mesmo não tendo como objetivo específico proteger dados, tem o potencial de contribuir tecnicamente para a implantação da LGPD por meio de suas normas e boas práticas (FREITAS; SANTOS; PASINATO, 2020, p. 235-239; 243), pois há "um ciclo tecnológico que se estabelece a partir da LGPD visando a proteção de dados com base na segurança da informação. Este ciclo é composto pelas seguintes etapas: prevenção, coleta, tratamento, registro, prestação de contas." (FREITAS; SANTOS; PASINATO, 2020, p. 243).

Por esta razão que com a aceleração da transformação tecnológica a norma ISO/IEC 27001 (ISO, 2022b) e a norma de suporte ISO/IEC 27002 (ISO, 2022c) foram revisadas em 2022 para atualizar os tipos de controle de segurança e adicionar novos que se demonstram melhores. A atualização das normas é essencial para que as normas de gestão da segurança ISO/IEC se mantenham como a melhor prática global definitiva (BSI, 2022).

Segundo Freitas, Santos & Pasinato (2020, p. 244-245) as normas técnicas de referência global ISO/IEC 27001, 27002 e 27701 "fornecem orientação e direção de como uma organização, independentemente de

6 Vide artigo 1º, artigo 6º, inciso VII, artigo 46, artigo 47, artigo 49 e artigo 50 da LGPD.

seu porte e setor, deve gerenciar a segurança das informações e abordar os riscos de segurança das informações" e desta forma podem ser consideradas ferramentas de planejamento tecnológico muito importante para a proteção de dados. Afinal, se os riscos a dados pessoais e sensíveis decorrem de "fraquezas em sistemas, processos e organizações" (FREITAS; SANTOS; PASINATO, 2020, p. 245), o cumprimento das normas corporativas globais pode ser considerado como uma garantia de cumprimento dos preceitos da LGPD (CARVALHO, 2019, p. 627).

As normas ISO/IEC da família 27000 foram desenvolvidas para aprimorar um Sistema de Gerenciamento de Segurança da Informação (FREITAS; SANTOS; PASINATO, 2020, p. 242-243). Portanto, como as normas de referência global são ferramentas importantíssimas para a proteção de informações, elas se demonstram também relevantes para a proteção de dados pessoais (FREITAS; SANTOS; PASINATO, 2020, p. 240), podendo contribuir para mitigação de riscos do negócio e para que as oportunidades relacionadas a ele sejam melhor exploradas.

Ocorre que para a proteção da Informação ser alcançada se faz necessária a avaliação dos riscos (FREITAS; SANTOS; PASINATO, 2020, p. 251-253) e o estabelecimento e implementação "de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware". Além de ser essencial também que estes controles sejam "monitorados e analisados criticamente" e "constantemente revisados para melhorias e alterações" (FREITAS; SANTOS; PASINATO, 2020, p. 248).

Por este mesmo motivo também é de extrema relevância a adoção de modelos de boas práticas:

> A implementação de boas práticas no tratamento de dados pessoais possui estrondoso potencial para auxiliar no atendimento aos comandos gerais da lei de acordo com as particularidades de determinados agentes econômicos, bem como prevenir a ocorrência de violações aos direitos dos titulares, na medida em que permite orientar os agentes de tratamento, traduzindo para suas atividades cotidianas as premissas principiológicas da LGPD e concretizando vários dos seus *standards* e conceitos abertos (FRAZÃO; OLIVA; ABILIO, 2019, p. 682).

A adoção de programas de *compliance*, por exemplo, se trata de um valioso instrumento para promoção do viés operacional e preventivo da LGPD (FRAZÃO; OLIVA; ABILIO, 2019, p. 682). Principalmente quando se considera que estes programas possibilitam uma organização com procedimentos e controles internos compatíveis com o risco da

atividade (FRAZÃO; OLIVA; ABILIO, 2019, p. 689) assegurando que se iniba a prática de atos ilícitos.

Por isso que é importante não se falar apenas de adequação às normas ISO/IEC, mas também de se buscar outros meios favoráveis a proteção de informações (e dados) e consequentemente ao gerenciamento de riscos. Afinal, "Em um cenário de mudanças tão robustas, o recurso ao estabelecimento de procedimentos de boas práticas pelos agentes econômicos privados torna-se passo fundamental para propiciar a adequação à nova realidade com alguma segurança." (FRAZÃO; OLIVA; ABILIO, 2019, p. 694).

Se "as organizações são dinâmicas e a segurança da informação deve e precisa evoluir junto com a organização" (FREITAS; SANTOS; PASINATO, 2020, p. 253) sabendo-se que o Metaverso simboliza uma mudança significativa não apenas na forma das empresas negociarem, mas também na forma de elas se organizarem, é importante que a sua adoção pelas empresas venha acompanhada de cautela e planejamento, de modo que os eventuais riscos que surgem sejam gerenciados da melhor maneira possível e que se assegure que a adesão a tecnologia não provoque violações a direitos

Existem diversos modelos de boas práticas, inclusive direcionados à área de Tecnologia da Informação, e normas de padrão internacional que têm condições de melhorar a segurança das informações (e dos dados) e assim garantir uma maior proteção – ou ao menos um gerenciamento de riscos – na realização de assembleias no Metaverso. A partir do momento em que se verifica, conforme já exposto, que o Metaverso é uma expressão da sociedade tecnológica de risco, a superação ou ao menos o gerenciamento dos riscos é essencial para que se possa assegurar que a experiência de realização de assembleias neste ambiente seja realmente positiva e que se construam pontes entre os indivíduos (PARISER, 2012, p. 20-21). E isto somente é possível se além de ser exigido o cumprimento dos requisitos legais para a realização de assembleias, também forem adotadas técnicas de Segurança da Informação e cibersegurança.

Portanto, permitir a realização de assembleias no Metaverso sem preocupar-se com a segurança das informações (e dos dados) e com cibersegurança seria possibilitar que se perpetue a lógica da sociedade em rede de desenvolver tecnologias apenas para buscar a lucratividade e o aumento de valor das ações, sem uma preocupação com a inovação e com a melhora das condições de vida da humanidade (CASTELLS, 2022, p.

150-151). Seria utilizar a tecnologia apenas para criar ligações, mas não genuínas pontes entre os indivíduos (PARISER, 2012, p. 21).

5 conclusão

A pesquisa apresentou como as transformações trazidas pelas novas tecnologias, em especial as TICs, foram profundas e trouxeram consigo novos riscos, globais, transfronteiriços, transtemporais e de potencial desconhecido que impactam a forma de viver e de existir da humanidade de tal forma que evidenciam que a sociedade de risco trabalhada por Beck hoje se transfigurou em uma sociedade tecnológica de risco na qual as ameaças enfrentadas de forma global são decorrência das escolhas de todos os indivíduos.

Além disto, discutiu-se como o Metaverso representa um novo patamar da evolução tecnológica que expressa a transição do meio ambiente digital para o meio ambiente virtual, que possui um potencial gigantesco e promete várias oportunidades, mas que como qualquer tecnologia também traz consigo novos riscos – inclusive aos negócios – que precisam ser enxergados, compreendidos e gerenciados de modo que a escolha humana de ingresso neste "novo mundo" seja consciente e responsável.

Por fim, analisou-se como a realização de assembleias virtuais no Metaverso se trata de um tema que já possui algumas diretrizes e bases jurídicas para a sua implementação, mas que não pode ser resolvido apenas pelo Direito, pois necessita de um ferramental tecnológico para tal. Ponderou-se que se faz necessário não apenas o cumprimento dos requisitos legais de realização de assembleias à distância, mas que também precisa existir uma conjugação de técnicas de cibersegurança e de Segurança da Informação para que se possa assegurar que os riscos deste ambiente sejam mitigados.

O Metaverso é uma expressão da sociedade tecnológica de risco e como tal não pode ser tratado da mesma forma que o ambiente físico, pois precisa que seus riscos sejam vistos, enfrentados e gerenciados, de modo que o encantamento pela novidade e inovação, não cegue a humanidade com relação a ameaças à sua própria existência digna. Conclui-se que em razão de todos estes riscos, a realização de assembleias virtuais neste ambiente não pode depender apenas do cumprimento dos requisitos legais para realização de assembleias à distância, sendo imprescindível a adoção de um ferramental tecnológico (em especial técnicas de cibersegurança e Segurança

da Informação) para que se garanta que a assembleia, tal qual preconizada no Direito Cooperativo, seja realizada de forma ciberneticamente segura tanto para os negócios como para os indivíduos envolvidos.

Referências

ASSOCIAÇÃO BRASILEIRA DAS COMPANHIAS ABERTAS. **Abrasca consulta CVM sobre possibilidade de realização de AGO no espaço metaverso**. 04 jul. 2022a. Disponível em: https://www.abrasca.org.br/noticias/sia-cia-1605-abrasca-consulta-cvm-sobre-possibilidade-de-realizacao-de-ago-no-espaco-metaverso Acesso em: 27 set. 2025.

ASSOCIAÇÃO BRASILEIRA DAS COMPANHIAS ABERTAS. **Em resposta à consulta da Abrasca, CVM diz que não vê empecilho na realização de AGOs no espaço metaverso**. 08 ago. 2022b. Disponível em: https://www.abrasca.org.br/noticias/sia-cia-1610-em-resposta-a-consulta-da-abrasca-cvm-diz-que-nao-ve-empecilho-na-realizacao-de-agos-no-espaco-metaverso Acesso em: 27 set. 2025.

BECK, Ulrich. A reinvenção da política: rumo a uma teoria da modernidade reflexiva. *In*: GIDDENS, Anthony; LASH, Scott; BECK, Ulrich. **Modernização reflexiva**: política, tradição e estética na ordem social moderna. São Paulo: UNESP, 2012.

BECK, Ulrich. **La sociedad del riesgo global**. Espanha: Siglo Veintiuno, 2002.

BECK, Ulrich. **Sociedade de Risco**: rumo a uma outra modernidade. São Paulo: Editora 34, 2010.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm Acesso em: 27 set. 2025.

BRASIL. **Lei nº 12.431, de 24 de junho de 2011**. Dispõe sobre a incidência do imposto sobre a renda nas operações que especifica; altera as Leis nºs 11.478, de 29 de maio de 2007, 6.404, de 15 de dezembro de 1976, 9.430, de 27 de dezembro de 1996, 12.350, de 20 de dezembro de 2010, 11.196, de 21 de novembro de 2005, 8.248, de 23 de outubro de 1991, 9.648, de 27 de maio de 1998, 11.943, de 28 de maio de 2009, 9.808, de 20 de julho de 1999, 10.260, de 12 de julho de 2001, 11.096, de 13 de janeiro de 2005, 11.180, de 23 de setembro de 2005, 11.128, de 28 de junho de 2005, 11.909, de 4 de março de 2009, 11.371, de 28

de novembro de 2006, 12.249, de 11 de junho de 2010, 10.150, de 21 de dezembro de 2000, 10.312, de 27 de novembro de 2001, e 12.058, de 13 de outubro de 2009, e o Decreto-Lei nº 288, de 28 de fevereiro de 1967; institui o Regime Especial de Incentivos para o Desenvolvimento de Usinas Nucleares (Renuclear); dispõe sobre medidas tributárias relacionadas ao Plano Nacional de Banda Larga; altera a legislação relativa à isenção do Adicional ao Frete para Renovação da Marinha Mercante (AFRMM); dispõe sobre a extinção do Fundo Nacional de Desenvolvimento; e dá outras providências. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12431.htm Acesso em: 27 set. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 27 set. 2025.

BRASIL. **Lei nº 5.764, de 16 de dezembro de 1971**. Define a Política Nacional de Cooperativismo, institui o regime jurídico das sociedades cooperativas, e dá outras providências. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l5764.htm Acesso em: 27 set. 2025.

BRASIL. **Lei nº 6.404, de 15 de dezembro de 1976**. Dispõe sobre as Sociedades por Ações. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l6404consol.htm Acesso em: 27 set. 2025.

BRASIL. **Lei nº 6.938, de 31 de agosto de 1981**. Dispõe sobre a Política Nacional do Meio Ambiente, seus fins e mecanismos de formulação e aplicação, e dá outras providências. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l6938.htm Acesso em: 27 set. 2025.

BRICE, Steve; GOH, Audrey. **Enter the Metaverse**. Standard Chartered, 01 abr. 2022. Disponível em: https://podcasts.apple.com/us/podcast/talking-thematics-the-metaverse/id1553038083?i=1000555778947 Acesso em: 27 set. 2025.

BSI. **ISO/IEC 27001 Gestão de Segurança da Informação**. 2022. Disponível em: https://www.bsigroup.com/pt-BR/products-and-services/standards/iso-iec-27001-information-security-management-system/ Acesso em: 27 set. 2025.

CARVALHO, Angelo Gamba Prata de. Transferência internacional de

dados na lei geral de proteção de dados – Força normativa e efetividade diante do cenário transnacional. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana e OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Revista dos Tribunais, 2019. p. 621-645.

CASTELLS, Manuel. **A Galáxia Internet**: reflexões sobre a internet, os negócios e a sociedade. Tradução: Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2015.

CASTELLS, Manuel. **A sociedade em rede** – A era da informação: economia, sociedade e cultura. Tradução: Roneide Venancio Majer. 24. ed. Rio de Janeiro: Paz e Terra, 2022.

CHANDRASEKAR, Dinesh. **The Metaverse: A New Horizon in Digital Reality**. Pactera Edge, 2022. Disponível em: https://www.centific.com.cn/sites/default/files/2022-06/The%20Metaverse%20-%20A%20New%20Horizon.pdf Acesso em: 27 set. 2025.

FERREIRA, Heline Sivini. A dimensão ambiental da teoria da sociedade de risco. *In*: FERREIRA, Heline Sivini; FREITAS, Cinthia Obladen de Almendra (org.). **Direito Socioambiental e Sustentabilidade**: Estados, Sociedades e Meio Ambiente. Curitiba: Letra da Lei, 2016. p. 108- 158.

FLORIDI, Luciano (ed.). **The Onlife Manifesto**: Being Human in a Hyperconnected Era. Springer Open, 2015.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Viviane da Silveira. Compliance de dados pessoais. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana e OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Revista dos Tribunais, 2019. p. 677-715.

FREITAS, Cinthia Obladen de Almendra; FERREIRA, Heline Sivini; CAVEDON, Ricardo. A Bolha Informacional e os Riscos dos Mecanismos de Busca na Personalização do Usuário de Internet: reflexões sobre o direito à autodeterminação informacional. **Revista Brasileira de Direito IMED**, v. 16, n. 3, p. 01-24, set./dez. 2020.

FREITAS, Cinthia Obladen de Almendra; ROSSI, Amélia do Carmo Sampaio. Releitura dos Espaços Público e Privado frente às TICS. **Revista Direito, Estado e Sociedade**, Ahead of Print, n. XX mês/mês 2020.

FREITAS, Cinthia Obladen de Almendra; SANTOS, Henrique Guilherme; PASINATO, Rita. A Segurança da Informação como

ferramental técnico da proteção de dados pessoais. *In*: FARIA, Mariana Pereira; SILVA, Rafael Aggens Ferreira da; GOMES, Rhodrigo Deda (coord.). **Direito e inovação**, v. 3, Curitiba: OABPR, 2020. p. 233-265.

GREENFIELD, Adam. **Everyware**: The dawning age of ubiquitous computing. Berkeley-CA: AIGA, 2006.

HAN, Byung-Chul. **Sociedade da Transparência**. Tradução: Enio Paulo Giachini. Petrópolis, RJ: Vozes, 2017.

INTERPOL. **INTERPOL launches first global police Metaverse**. 20 out. 2022. Disponível em: https://www.interpol.int/en/News-and-Events/News/2022/INTERPOL-launches-first-global-police-Metaverse Acesso em: 27 set. 2025.

ISO. **ISO/IEC 27001: What's new in IT security?**. 25 out. 2022a. Disponível em: https://www.iso.org/contents/news/2022/10/new-iso-iec-27001.html Acesso em: 27 set. 2025.

ISO. **ISO/IEC 27001:2022b. Information security, cybersecurity and privacy protection — Information security management systems** — Requirements. Disponível em: https://www.iso.org/standard/27001 Acesso em: 27 set. 2025.

ISO. **ISO/IEC 27002:2022c. Information security, cybersecurity and privacy protection — Information security controls**. Disponível em: https://www.iso.org/standard/75652.html Acesso em: 27 set. 2025.

KOSTENKO, O. V. Electronic Jurisdiction, Metaverse, Artificial Intelligence, Digital Personality, Digital Avatar, Neural Networks: Theory, Practice, Perspective. **World Science**, 1 (73), Jan. 2022, p. 01-13.

LÉVY, Pierre. **Becoming Virtual**: reality in the Digital Age. Translation: Robert Bononno. New York: Plenum Trade, 1998.

MOY, Christine; GADGIL, Adit. **Opportunities in the metaverse: How businesses can explore the metaverse and navigate the hype vs. reality**. J. P. MORGAN, 18 jan. 2022. Disponível em: https://www.jpmorgan.com/content/dam/jpm/treasury-services/documents/opportunities-in-the-metaverse.pdf Acesso em: 27 set. 2025.

PARISER, Eli. **O filtro invisível**: o que a internet está escondendo de você. Tradução: Diego Alfaro. Rio de Janeiro: Zahar, 2012.

RASHID, Md Mamunur *et al*. Emergence of the Metaverse: How Blockchain, AI, AR/VR, and Digital Transformation Technologies will change the Future World. *In*: International Conference on Multimedia

Information Technology and Applications (MITA), 18., 2022, Jeju, Korea. **Proceedings [...]**. Jeju: JEJU SHINHWA WORLD, 2022. p. 266-268.

SCHLEMMER, Eliane; BACKES, Luciana. METAVERSOS: novos espaços para construção do conhecimento. **Revista Diálogo Educacional**, PUCPR, v. 8, n. 24, maio/ago. 2008, p. 519-532.

SCHWAB, Klaus. **A Quarta Revolução Industrial**. Tradução: Daniel Moreira Miranda. São Paulo: Edipro, 2016.

UNITED NATIONS DEVELOPMENT PROGRAMME. **Traversing the metaverse whilst managing risks with opportunities**. 19 jul. 2022. Disponível em: https://www.undp.org/blog/traversing-metaverse-whilst-managing-risks-opportunities Acesso em: 27 set. 2025.

VIEIRA, Giovana Batisti. A Sociedade da Transparência: Distopia ou Realidade? *In*: FREITAS, Cinthia Obladen de Almendra; OLIVEIRA, Dânton Hilário Zanetti de (org.). **Sociedade informacional e a lei geral de proteção de dados pessoais**: diálogos contemporâneos entre direito e tecnologia. Rio de Janeiro: Lumen Juris, 2022. p. 161-181.

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

Capítulo 8

TUTELA COLETIVA, PROTEÇÃO DE DADOS E INTELIGÊNCIA ARTIFICIAL: DESAFIOS DA SOCIEDADE DE RISCO DIGITAL

Rafael Almeida Oliveira Reis[1]

1 Introdução

A LGPD institui, a partir de fundamentos (art. 2º) e princípios (art. 6º), um sistema normativo robusto de proteção de dados pessoais, cujo alcance ultrapassa a mera descrição de regras e impõe deveres organizacionais de governança, prevenção e responsabilização (DE LUCCA; MACIEL, 2019).

A conformidade regulatória, especialmente em proteção de dados, governança corporativa e regulação da IA, exige mais do que políticas formais: requer práticas efetivas de diligência e evidências documentadas (relatórios de impacto[2], registros decisórios, treinamentos, protocolos de incidentes). Tais medidas dialogam com os princípios do art. 6º da LGPD (prevenção, segurança, transparência e accountability) e com os fundamentos do art. 2º, reforçando a mitigação de riscos e a capacidade de demonstrar conformidade.

Tais medidas não apenas reforçam a transparência e a credibilidade institucional, mas também funcionam como instrumentos estratégicos de mitigação de riscos. Em eventual cenário de fiscalização ou investigação, a existência de tais registros permite comprovar a adoção de medidas preventivas e a seriedade do comprometimento organizacional com as

1 Doutorando em Direito Socioambiental pela PUCPR. Mestre em Direito pela PUCPR. Advogado. Fundador da RRA_. Pós-graduado em Direito Digital e Compliance pelo IBMEC e LLM em Direito Empresarial pela FGV/Rio. Presidente do Instituto Nacional de Proteção de Dados (INPD). Atualmente coordena a Pós-Graduação em Legal Operations e Inteligência Artificial da Pós PUCPR Digital.

2 Relatórios de impacto podem ser utilizados tanto no contexto da Lei Geral de Proteção de Dados, como uma documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais (art. XVII, LGPD), mas também no contexto de relatórios de impactos algorítmicos, especialmente em se tratando de ferramentas de inteligência artificial (BRASIL, 2018).

normas aplicáveis. Assim, a construção de evidências consistentes e a atuação preventiva configuram uma das formas mais eficazes de reduzir a carga de participação e responsabilidade, seja perante processos administrativos, seja em demandas judiciais.

Nesse sentido, observa-se que a responsabilidade administrativa e judicial não se restringe à ocorrência de um incidente, mas também à postura adotada pelo agente regulado antes, durante e após o evento. A aplicação de sanções, como previsto na Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018), e no Regulamento Geral de Proteção de Dados (RGPD), leva em conta a demonstração de boa-fé[3], proporcionalidade e cooperação, o que reforça a importância de práticas preventivas e reativas bem estruturadas.

A aplicação de sanções considera condutas antes, durante e após o incidente (LGPD, art. 52), incluindo boa-fé, proporcionalidade e cooperação. A ação imediata para conter danos, a comunicação transparente a titulares e autoridades, e a cooperação com a ANPD (art. 55-J) reduzem a possibilidade de reprimendas mais gravosas, especialmente quando acompanhadas de registros auditáveis.

Assim, a diligência não deve ser entendida apenas como um requisito formal, mas como um processo contínuo de gestão de riscos, que envolve tanto a adoção de mecanismos de segurança preventiva quanto a capacidade de resposta ágil e transparente diante de crises. Ao comprovar a existência de medidas técnicas e organizacionais adequadas, a ação imediata para conter danos, a comunicação clara com autoridades e titulares, a cooperação efetiva e a implementação de medidas corretivas, a organização fortalece sua posição de defesa e minimiza a probabilidade de sanções mais severas. Dessa forma, evidencia-se que a conformidade, quando acompanhada de registros e comprovações robustas, não apenas atende às exigências legais, mas constitui estratégia indispensável para reduzir a carga de responsabilidade e participação em processos administrativos e judiciais.

Com o constante avanço tecnológico, o cenário contemporâneo pode ser compreendido à luz da chamada sociedade de risco[4], conceito

3 Art. 6º, LGPD: As atividades de tratamento de dados pessoais deverão observar a boa-fé[...].

4 A teoria da Sociedade de Risco, desenvolvida por Ulrich Beck a partir da década de 1980, parte da constatação de que a modernidade industrial produziu não apenas progresso científico e econômico, mas também novos tipos de ameaças globais. Para o sociólogo, os riscos característicos da sociedade contemporânea diferenciam-se dos perigos tradicionais, pois não se limitam mais a eventos naturais ou localizados; são riscos fabricados socialmente, derivados

desenvolvido por Ulrich Beck para descrever o contexto em que os riscos produzidos pela própria modernidade se tornam globais, invisíveis e dificilmente controláveis. Contemporaneamente, a consolidação de novos paradigmas tecnológicos, especialmente aqueles vinculados à inteligência artificial generativa, acentua a complexidade desses riscos, expandindo de maneira inédita as formas de coleta, tratamento e utilização de dados pessoais. Os modelos de IA generativa, ao operarem em larga escala e de modo opaco, potencializam riscos relacionados à assimetria informacional, à discriminação algorítmica e à perda de controle dos titulares sobre seus próprios dados, reforçando a vulnerabilidade dos consumidores frente a conglomerados tecnológicos globais que concentram poder econômico e informacional sem precedentes.

Diante desse contexto, o presente estudo busca compreender como os mecanismos de tutela coletiva previstos no Código de Defesa do Consumidor (CDC) (BRASIL, 1990) podem ser empregados como instrumentos de concretização de direitos fundamentais, particularmente para a proteção dos titulares de dados pessoais diante dos novos paradigmas da IA generativa. Considera-se que a tutela coletiva, concebida originariamente para a prevenção e reparação de danos de pequena expressão econômica individual, ganha especial relevo no ambiente da sociedade de risco, uma vez que os danos informacionais, ainda que difusos e muitas vezes intangíveis, possuem impacto social amplo e cumulativo. A própria Lei Geral de Proteção de Dados (LGPD), em seu art. 22, ao prever a tutela coletiva do titular, reforça essa necessidade de instrumentos que não apenas compensem lesões individuais, mas que sejam capazes de atuar preventivamente frente a riscos sistêmicos.

Assim, defende-se que a utilização da ação coletiva para a defesa de direitos difusos, coletivos e individuais homogêneos representa uma via indispensável de efetividade normativa, harmonizando os dispositivos da LGPD com o CDC e demais diplomas correlatos. Mais do que um mecanismo processual, a tutela coletiva revela-se como expressão do próprio direito fundamental à proteção de dados pessoais no contexto da sociedade de risco, integrando o ferramental protetivo do Estado Democrático de Direito e ampliando a legitimidade do sistema jurídico diante dos desafios trazidos pela tecnologia.

Por fim, antes de adentrar na análise prática da aplicação dos instrumentos de tutela coletiva na reparação de danos por violações ao

da própria lógica de desenvolvimento tecnológico, industrial e científico (BECK, 2015).

sistema de proteção de dados, impõe-se revisitar o arcabouço jurídico dos direitos metaindividuais no Brasil, remodelado a partir da Constituição de 1988 e consolidado com o CDC, como base indispensável para compreender a articulação entre risco, direitos fundamentais e proteção coletiva no ambiente digital como, por exemplo, o direito fundamental à proteção de dados pessoais.[5]

2 A construção normativa da tutela coletiva no Brasil: da constituição de 1988 À LGPD

Nas palavras do ministro Luis Fux, o direito brasileiro conta com uma espécie de "microssistema de tutela dos interesses transindividuais", destinado a tutelar os interesses coletivos, difusos e individuais homogêneos (STJ, REsp 1.085.218/RS, 2009). No plano infraconstitucional, esse sistema tem como pilar o CDC e a Lei da Ação Civil Pública (BRASIL, 1985), que definem os principais vetores para tutela coletiva no direito brasileiro, embora outras normas também tenham pontos de contato com o assunto, como a própria LGPD, a Lei da Proteção das Pessoas Portadoras de Deficiência (Lei 7.853/89), o Sistema Brasileiro de Defesa e Concorrência (Lei 12.529/11), o Estatuto do Torcedor (Lei 10.671/2003) e a Lei da Ação Popular (BRASIL, 1965).

A Constituição Federal de 1988 elevou os interesses difusos e coletivos ao patamar constitucional, reforçando o princípio da efetividade da tutela jurisdicional. Nesse sentido, consagrou expressamente diversos direitos de natureza transindividual, como o direito ao meio ambiente ecologicamente equilibrado (art. 225, caput) e o direito à defesa do consumidor (art. 170, V), entre outros. Além disso, ampliou o alcance da Ação Civil Pública, atribuindo-lhe a função de proteger um rol mais abrangente de direitos difusos e coletivos (art. 129, III). A Carta também fortaleceu os instrumentos de participação popular na defesa desses interesses, ao prever a ação popular para a tutela de direitos de ordem difusa

5 O congresso nacional reconheceu o direito fundamental à proteção de dados pessoais com a aprovação da proposta de emenda à Constituição (PEC) 17/2019. Não obstante, parcela significativa da doutrina já reconhecia esse direito conforme uma interpretação sistemática do ordenamento jurídico brasileiro, conforme considerações de Danilo Doneda: "No panorama do ordenamento brasileiro, o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, porém da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada (DONEDA, 2010)."

(art. 5º, LXXIII) e ao admitir o mandado de segurança coletivo como mecanismo de proteção de direitos coletivos e individuais homogêneos (art. 5º, LXIX e LXX). Dessa forma, consolidou um sistema jurídico-processual voltado não apenas à proteção de direitos individuais, mas também à salvaguarda de bens jurídicos de relevância coletiva e difusa, em sintonia com as demandas de uma sociedade cada vez mais complexa.

Já o CDC tutela todo direito ou interesse transindividual no contexto das relações do consumo. Ada Pellegrini Grinover destaca que a legislação consumerista "foi além da dicotomia dos interesses difusos e coletivos", criando "a categoria dos chamados interesses individuais homogêneos, que abriram caminho às ações reparatórias dos prejuízos individualmente sofridos (correspondendo, no sistema norte-americano, às *class actions for damages*[6]) (GRINOVER, 2004 apud BERGSTEIN, 2020).

3 Categorias jurídicas de tutela metaindividual e sua reinterpretação na sociedade de risco digital

Em uma sociedade cada vez mais complexa, caracterizada por riscos globais, impactos coletivos e relações assimétricas — como ocorre no campo ambiental, nas relações de consumo ou, mais recentemente, na proteção de dados pessoais e no uso de tecnologias disruptivas como a inteligência artificial —, torna-se indispensável buscar ferramentais jurídico-normativos para a tutela dos titulares de direitos. Nesse sentido, os direitos difusos, coletivos e individuais homogêneos são construções normativas que buscam superar a limitação da tutela tradicional centrada no indivíduo, oferecendo mecanismos de proteção adequados a interesses compartilhados por grupos, classes ou pela coletividade como um todo.

Nos próximos parágrafos, serão apresentados os conceitos normativos que definem os direitos difusos, coletivos e individuais homogêneos, com o objetivo de diferenciá-los de forma clara, evidenciando

6 Segundo Laís Bergstain, "O mecanismo das ações coletivas brasileiras assemelha-se substancialmente às class actions norte-americanas, ordenadas pela rule 23 das Federal Rules of Civil Procedure. São elencados os seguintes pré-requisitos para a certificação de uma class action federal norte-americana, de modo que: um ou mais membros de uma classe podem processar ou ser processados como partes representativas em nome de todos os membros somente se: (1) a classe é tão numerosa que a junção de todos os membros é impraticável; (2) há questões de direito ou fato comuns à classe; (3) as reivindicações ou defesas das partes representativas são típicas das reivindicações ou defesas da classe; e (4) as partes representantes protegerão de forma justa e adequada os interesses da classe. É especificamente no inciso b.3 da regra 2358 que se encontra o regime jurídico aplicável à damage class action " (BERGSTEIN, 2020).

suas particularidades e pontos de interseção, bem como sua relevância para a consolidação de um sistema de tutela coletiva efetivo no Brasil.

3.1 Direitos difusos e os novos riscos coletivos da inteligência artificial

Os direitos difusos são definidos pelo art. 81 do Código de Defesa do Consumidor como direitos metaindividuais, de natureza indivisível, titularizados por pessoas indeterminadas que se encontram ligadas entre si por circunstâncias de fato.[7] A lei consumerista, portanto, adota como critério central a indeterminação dos titulares, afastando a necessidade de um vínculo jurídico prévio entre eles. Por possuírem natureza indivisível, esses direitos são compartilhados em igual medida por toda a coletividade atingida, não sendo possível fracioná-los em parcelas individuais

Tradicionalmente, a doutrina e a jurisprudência reconhecem como exemplos clássicos de direitos difusos o direito ao meio ambiente ecologicamente equilibrado, o patrimônio histórico-cultural, a qualidade de vida nas cidades, a defesa do consumidor e a proteção da saúde pública. No entanto, no contexto contemporâneo, marcado pela economia digital e pela chamada sociedade de risco digital (REIS, 2023), surgem novas manifestações desses direitos, especialmente no campo da proteção de dados pessoais e da regulação tecnológica.

A LGPD, por exemplo, apresenta múltiplas situações de tutela difusa. Quando consumidores titulares de dados pessoais são afetados pelo tratamento realizado por empresas ou pela administração pública, o impacto é coletivo e, muitas vezes, contínuo, transcendendo a esfera individual de controle dos dados.[8] Assim, pedidos judiciais que buscam impedir que um controlador realize determinado tratamento lesivo (obrigação de não fazer) têm natureza difusa, pois beneficiam indistintamente toda a coletividade de titulares. O mesmo ocorre em pedidos que visam modificar a forma de

7 Art. 81. A defesa dos interesses e direitos dos consumidores e das vítimas poderá ser exercida em juízo individualmente, ou a título coletivo. Parágrafo único. A defesa coletiva será exercida quando se tratar de: I - interesses ou direitos difusos, assim entendidos, para efeitos deste código, os transindividuais, de natureza indivisível, de que sejam titulares pessoas indeterminadas e ligadas por circunstâncias de fato; (BRASIL, 1990, art. 81)

8 Nesse sentido, a LGPD prevê direitos que poderão ser exercidos pelos titulares de dados tanto na esfera administrativa, como os direitos dos titulares estabelecidos a partir do capítulo III da referida lei, como na judicial.

tratamento de dados (obrigação de fazer), como, por exemplo, a exigência de maior transparência em processos de tomada de decisão automatizada.[9]

No campo da inteligência artificial, os direitos difusos tornam-se ainda mais relevantes. Pode-se citar, por exemplo: (i) o direito coletivo de que sistemas de IA generativa não sejam utilizados para disseminar desinformação em massa; (ii) o direito difuso de proteção contra a discriminação algorítmica sistêmica, quando modelos de IA reproduzem vieses que impactam grupos sociais inteiros; (iii) a exigência de que bases de dados utilizadas para treinar algoritmos respeitem padrões mínimos de proteção à privacidade, beneficiando tanto os titulares atuais quanto aqueles que futuramente possam ter seus dados utilizados; e (iv) a proteção coletiva contra práticas abusivas de monitoramento em larga escala, como sistemas de vigilância biométrica em espaços públicos, que atingem indistintamente todos os cidadãos submetidos ao controle (BESSA; NUNES, 2021, p. 676).

No campo eleitoral, os riscos se intensificam, sobretudo com o uso de IA para manipulação de imagens, sons e vídeos, por meio das chamadas *deepfakes*, capazes de gerar descrédito público de pessoas, em especial das politicamente expostas, mas também de lideranças empresariais e de agentes da administração pública. Reconhecendo essa ameaça, o Tribunal Superior Eleitoral (TSE) inovou em 2024 ao regulamentar, de forma inédita, o uso da IA na propaganda eleitoral. Entre as medidas, estão a proibição expressa do uso de *deepfakes*, a obrigação de informar claramente quando conteúdos forem produzidos por IA, a vedação do uso de robôs para simular diálogos com candidatos e a responsabilização das grandes plataformas digitais que não removerem imediatamente conteúdos falsos ou desinformativos. Além disso, o TSE incluiu na Resolução nº 23.610/2019 o art. 9º-C, que veda a utilização de conteúdos fabricados ou manipulados para difundir fatos inverídicos ou descontextualizados com potencial de comprometer a integridade do pleito, sob pena de cassação do registro ou do mandato, além da apuração de responsabilidades civis e penais.

Essas inovações demonstram que a tutela de direitos difusos diante da inteligência artificial se projeta também sobre a esfera democrática, buscando assegurar o equilíbrio das eleições, a proteção da opinião pública contra manipulações tecnológicas e a preservação da integridade institucional. Nesse sentido, a utilização de IA em contextos eleitorais

9 A LGPD estabelece como direito dos titulares de dados a revisão de decisão automatizada, conforme art. 20 da referida lei.

conecta-se diretamente à noção de risco coletivo e difuso, já que seus efeitos ultrapassam a esfera individual, atingindo indistintamente toda a sociedade e, em última instância, a própria legitimidade do regime democrático.

Em todos esses casos, observa-se que a tutela jurisdicional não se limita a reparar danos individuais, mas busca proteger a coletividade enquanto tal, garantindo a efetividade de direitos fundamentais diante dos riscos difusos que emergem na era da inteligência artificial.

3.2 Direitos coletivos e os impactos determináveis da tecnologia

Os direitos e interesses coletivos são, também segundo conceituação do art. 81 do Código de Defesa do Consumidor, transindividuais, de natureza indivisível, mas, diferentemente dos direitos e interesses difusos, são pertencentes a um grupo determinável de pessoas, ligadas entre si ou com a parte contrária por uma relação jurídica comum.[10] Essa ligação pode ocorrer em torno de uma entidade associativa, como um sindicato ou associação de consumidores, ou diretamente em relação ao fornecedor, como no caso de lesão a um grupo específico de consumidores de um mesmo produto ou serviço, conforme previsto no parágrafo único, II, do art. 81 do CDC.

A principal diferença, portanto, está no fato de que, nos direitos coletivos, os titulares são determináveis, ainda que não individualmente identificados no momento da ação (BESSA; NUNES, 2021, p. 676). Um exemplo clássico é o do sindicato que ingressa com ação coletiva para impedir determinado tratamento de dados pessoais sensíveis dos colaboradores de uma organização. Nesse caso, serão beneficiados todos os funcionários que mantenham vínculo contratual com a empresa, formando um grupo claramente delimitado.

Outro exemplo, agora na seara consumerista, encontra-se nas demandas coletivas propostas por associações civis de proteção ao consumidor. É o caso da Ação Civil Pública movida pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) contra a ViaQuatro, concessionária da

10 Art. 81. A defesa dos interesses e direitos dos consumidores e das vítimas poderá ser exercida em juízo individualmente, ou a título coletivo. Parágrafo único. A defesa coletiva será exercida quando se tratar de:
[...] II - Interesses ou direitos coletivos, assim entendidos, para efeitos deste código, os transindividuais, de natureza indivisível de que seja titular grupo, categoria ou classe de pessoas ligadas entre si ou com a parte contrária por uma relação jurídica base (BRASIL, 1990, art. 81, II);

linha amarela do metrô de São Paulo, em virtude da instalação de Portas Interativas Digitais que captavam imagens dos usuários para um sistema de reconhecimento de emoções associado à publicidade (CASTRO, 2023). A ação, fundamentada no CDC e no Código de Defesa dos Usuários de Serviços Públicos[11], questionou a legalidade da prática por violar direitos de privacidade e dignidade dos passageiros. Em decisão cautelar, o Tribunal de Justiça de São Paulo determinou a suspensão do sistema sob pena de multa, beneficiando diretamente os usuários daquele serviço público específico.

No campo da inteligência artificial, multiplicam-se os exemplos de ferramentas tecnológicas que podem gerar riscos coletivos e afetar grupos determináveis de pessoas. Plataformas digitais, por exemplo, utilizam sistemas de IA para avaliar o desempenho de motoristas de aplicativo e realizar bloqueios automáticos de contas, muitas vezes sem transparência ou possibilidade de recurso, o que compromete a subsistência de trabalhadores de uma mesma categoria. Em ambientes educacionais, sistemas de vigilância algorítmica têm sido empregados para monitorar expressões faciais e padrões de comportamento de professores e alunos durante aulas virtuais, interferindo diretamente na autonomia docente e no ambiente de ensino.

Outro risco coletivo surge com a utilização, sem consentimento ou remuneração, de obras de jornalistas, escritores e artistas em bases de dados destinadas ao treinamento de modelos de IA generativa, afetando de modo específico categorias profissionais. Também se destacam os algoritmos de recomendação empregados por plataformas de comércio eletrônico, que podem adotar práticas discriminatórias, favorecendo determinados perfis de consumidores em detrimento de outros, dentro de um mesmo universo de usuários.

Esses exemplos demonstram como a aplicação da IA pode produzir efeitos que, embora não atinjam toda a coletividade indistintamente, impactam grupos sociais claramente determináveis, reforçando a necessidade de instrumentos de tutela coletiva para enfrentar as novas formas de risco digital.

11 Apesar da demanda versar sobre proteção de dados pessoais, à época dos fatos, a LGPD ainda não estava em vigor.

3.3 Direitos individuais homogêneos e os danos massificados no ambiente digital

Por fim, os direitos individuais homogêneos são definidos pelo art. 81, parágrafo único, III, do CDC, como aqueles decorrentes de origem comum.[12] Trata-se, segundo Ada Pellegrini Grinover, de "verdadeiros direitos subjetivos tradicionais", passíveis tanto de tratamento processual individual quanto de tutela coletiva, em razão de sua homogeneidade e origem comum. A proteção desses interesses busca assegurar o ressarcimento de danos pessoalmente sofridos por indivíduos em decorrência de um mesmo fato lesivo, inspirando-se nas *class actions for damages* do direito norte-americano (BESSA; NUNES, 2021, p. 677).

Por essa razão, conclui-se que os direitos individuais homogêneos podem ser considerados "acidentalmente coletivos", enquanto os direitos difusos e coletivos são "essencialmente coletivos", conforme destaca Laís Bergstein (BERGSTEIN, 2020):

> Os direitos individuais homogêneos são, nesse sentido, "acidentalmente coletivos". Isso enquanto os direitos difusos e coletivos são "essencialmente coletivos", na medida em que transcendem a esfera individual (daí a expressão transindividuais no Código de Defesa do Consumidor), são chamados superindividuais e "não pertencem a uma pessoa física ou jurídica determinada, mas a uma comunidade amorfa, fluida e flexível, com identidade social, porém sem personalidade jurídica." A natureza dos direitos individuais homogêneos "não é difusa, nem puramente individual, mas sim coletiva stricto sensu ou individual homogênea."

Enquanto estes últimos transcendem a esfera individual, projetando-se como direitos transindividuais ou superindividuais, aqueles mantêm natureza individual, mas se prestam à tutela coletiva em razão da repetição massificada de condutas que têm a mesma origem.

Segundo Leonardo Roscoe Bessa e Ana Luisa Tarter Nunes, a instrumentalização dos direitos individuais homogêneos ocorre, em regra, em duas fases processuais: primeiramente, com a ação coletiva ajuizada pelo legitimado, em que se busca o reconhecimento e a declaração do dever de indenizar; em seguida, na fase de execução, com a habilitação dos

12 Art. 81. A defesa dos interesses e direitos dos consumidores e das vítimas poderá ser exercida em juízo individualmente, ou a título coletivo. Parágrafo único. A defesa coletiva será exercida quando se tratar de:
[...] III - interesses ou direitos individuais homogêneos, assim entendidos os decorrentes de origem comum. (BRASIL, 1990, art. 81, III)

beneficiados, que promovem a satisfação da dívida reconhecida (BESSA; NUNES, 2021, p. 677). Esse modelo permite a racionalização processual e evita que inúmeros processos individuais sobrecarreguem o Judiciário.

No campo da sociedade de risco digital, a importância dessa modalidade de tutela cresce de forma exponencial. A responsabilidade civil do agente que trata dados pessoais de forma irregular continua a ser apurada individualmente, mas quando tais condutas atingem centenas ou milhares de titulares em um mesmo contexto — como vazamentos massivos de dados, falhas de segurança cibernética ou usos indevidos de informações em processos de treinamento de algoritmos de inteligência artificial — a via coletiva para a reparação dos danos individuais homogêneos revela-se indispensável.

A inteligência artificial, em especial a generativa, amplia os riscos pela possibilidade de usos danosos em larga escala, por exemplo a utilização de dados biométricos coletados em plataformas digitais para alimentar sistemas de reconhecimento facial, sem base legal adequada, impactando grupos determinados de usuários, ou ainda a manipulação automatizada de perfis de consumo para práticas abusivas de discriminação de preços, em que consumidores em idêntica posição contratual sofrem prejuízos homogêneos em decorrência da mesma lógica algorítmica.

Nesses casos, embora cada lesado sofra um dano individual, a homogeneidade da origem — ligada a uma mesma prática tecnológica — justifica a tutela coletiva como instrumento de efetividade e dissuasão (BESSA; NUNES, 2021, p. 677). A indenização coletiva por danos individuais homogêneos impede que condutas nocivas de agentes econômicos sejam mantidas pela aposta na inércia das vítimas ou na inviabilidade econômica de litígios individuais de baixa monta.

Assim, no contexto da economia digital, o fornecedor ou controlador de dados deve adotar postura preventiva e criteriosa na implementação de sistemas algorítmicos, sob pena de responder de forma ampla pelos danos homogêneos causados. A tutela coletiva, nesse sentido, funciona não apenas como instrumento reparatório, mas também como mecanismo regulatório indireto, incentivando o cumprimento de padrões mais elevados de proteção de dados pessoais e de governança de sistemas de inteligência artificial (BESSA; NUNES, 2021, p. 677).

4 Legitimidade ativa e pertinência temática na tutela coletiva de dados e IA

Para diferenciar os direitos difusos, coletivos e individuais homogêneos, deve-se considerar os direitos subjetivos que foram violados (BERGSTEIN, 2020). É o exemplo do art. 22 da LGPD[13]. Trata-se, portanto, de uma violação aos direitos subjetivos dos titulares de dados pessoais, constando expressamente a opção do legislador pela possibilidade de sua defesa individual ou coletiva, em linha com o que dispõe o art. 81 do CDC.

Em relação à legitimidade para promover ações coletivas em defesa dos titulares de dados pessoais e consumidores, concorrem o Ministério Público, a União, os Estados, os Municípios e o Distrito Federal, a Agência Nacional de Proteção de Dados (ANPD), outros órgãos da administração pública que defendem os interesses dos titulares de dados pessoais e de consumidores, além das associações legalmente constituídas há pelo menos um ano e que tenham como fim institucional a proteção de dados pessoais[14] e/ou a defesa dos interesses dos consumidores (BRASIL, 1990, art. 82).

Esse panorama revela um ecossistema diversificado de atores da litigância coletiva em proteção de dados, que se consolidou no Brasil após a entrada em vigor da LGPD e que reflete a lógica da sociedade de risco digital. O Ministério Público (MP) exerce papel proeminente, sendo legitimado para a propositura de Ações Civis Públicas.

As organizações da sociedade civil (OSCs) e associações têm igualmente papel central. Essas entidades não apenas ajuízam ações coletivas, mas também fomentam o debate público e mobilizam a sociedade em torno da proteção de dados. Essa prática encontra paralelo em experiências internacionais, como a decisão do *Bundesgerichtshof* (BGH) (BUNDESGERICHTSHOF, 2025), na Alemanha, que reconheceu às associações de consumidores legitimidade para litigar em casos de violação de dados, reforçando uma tendência de fortalecimento da sociedade civil na tutela coletiva de dados pessoais.

---

13 "defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva."

14 É o exemplo do Instituto Nacional de Proteção de Dados (INPD), que tem como um dos seus objetivos estatutários a promoção da proteção de dados pessoais no Brasil. Mais informações em: <https://www.inpd.com.br/sobreoinpd>.

Outro ator relevante são os Procons, que, embora historicamente voltados à defesa do consumidor tradicional, expandiram sua atuação para a área de dados pessoais em razão da interseção entre o CDC e a LGPD. Esses órgãos podem instaurar investigações, impor multas administrativas e promover conciliações, exercendo papel complementar à atuação judicial. A própria ANPD, por sua vez, atua no plano administrativo, com foco na conformidade regulatória, na prevenção de danos e na aplicação de sanções como advertências, multas ou bloqueio de operações de tratamento de dados.

Não obstante a definição legal dos legitimados e dos direitos subjetivos violados, é indispensável considerar, como observa Laís Bergstein, a afinidade entre o legitimado e o objeto do litígio — a chamada pertinência temática. A efetividade da tutela coletiva depende diretamente da capacidade técnica e institucional do órgão ou entidade legitimada em conduzir e fomentar a ação coletiva. A ausência de expertise ou de instrumentos adequados pode comprometer o resultado útil do processo, inviabilizando sua função protetiva:

> A efetividade do litígio de massa está diretamente relacionada à capacidade do órgão, entidade ou pessoa legitimada à propositura, à condução e ao fomento da ação coletiva. A ausência de condições técnicas ou de instrumentos para a persecução do direito reclamado durante as fases de tramitação do processo judicial pode prejudicar (até inviabilizar) o seu resultado útil.[15]

Ademais, o art. 83 do CDC confere ao magistrado a possibilidade de adotar qualquer ação capaz de propiciar a tutela efetiva dos direitos e interesses dos consumidores titulares de dados pessoais, seja de natureza coletiva ou individual. O art. 84 do mesmo diploma acrescenta que o juiz poderá conceder tutela específica da obrigação ou determinar providências que assegurem o resultado prático equivalente ao adimplemento, inclusive com a possibilidade de conversão da obrigação em perdas e danos. Tal hipótese é particularmente relevante no campo da proteção de dados pessoais, em situações em que há impossibilidade técnica de reversibilidade. Imagine, por exemplo, um caso de vazamento massivo em que não há

15 Concluí a autora que "O informativo de jurisprudência 570 do Superior Tribunal de Justiça indica que "a Lei, ao estabelecer os legitimados para promover a ação coletiva, presumivelmente reconheceu a correlação destes com os interesses coletivos a serem tutelados", ressaltando que "o controle judicial da adequada representatividade, especialmente em relação às associações, consubstancia importante elemento de convicção do magistrado para mensurar a abrangência e, mesmo, relevância dos interesses discutidos na ação." A falta da adequada representatividade permite que o Magistrado obste o prosseguimento do feito "em observância ao princípio do devido processo legal à tutela jurisdicional coletiva." (BERGSTEIN, 2020)

interesse ou viabilidade prática em obter a obrigação de não-fazer — como impedir a perpetuação da circulação indevida de informações já expostas. Nesses casos, a conversão em perdas e danos, nos termos do art. 248 do Código Civil, constitui a alternativa mais adequada para a reparação.

Esse quadro evidencia que a litigância coletiva em proteção de dados no Brasil é marcada por um arranjo institucional multifacetado, no qual Ministério Público, ANPD, Procons e associações civis atuam de forma cooperativa e complementar. Essa arquitetura não apenas amplia os canais de defesa dos titulares de dados, mas também se insere na lógica da sociedade de risco digital, na qual a tutela coletiva se revela como mecanismo indispensável de enfrentamento a riscos estruturais e massificados gerados pela inteligência artificial e pelo tratamento de dados em larga escala.

5 Dano moral informacional e os desafios reparatórios na sociedade de risco digital

Embora a Lei Geral de Proteção de Dados (LGPD), em seu art. 42, assegure a reparação de danos ao titular que sofre algum prejuízo decorrente de atividade de tratamento de dados pessoais — ainda que exclusivamente moral —, a experiência prática demonstra que, sob a ótica da reparação individual, há pouco ou nenhum incentivo para que o consumidor busque o Judiciário em casos relacionados à proteção de dados. Essa dificuldade decorre, em parte, da baixa expressão econômica individual desses danos, que, embora relevantes no plano da dignidade, raramente justificam, em termos de custo-benefício, o investimento de tempo e recursos necessários para um processo judicial ou até mesmo para procedimentos de mediação e conciliação.

Sob essa perspectiva, pode-se presumir que, sobretudo no campo consumerista, um número expressivo de organizações viola diariamente princípios e normas de proteção de dados, gerando prejuízos difusos a uma massa de consumidores. Contudo, tais violações permanecem, em grande medida, invisíveis e não contestadas judicialmente, o que favorece a inércia dos fornecedores. A ausência de uma resposta individualizada eficaz acaba por premiar condutas ilícitas e desincentivar investimentos em segurança da informação e em conformidade regulatória.

A esse cenário soma-se a emergência da computação ubíqua, na qual dispositivos, plataformas e algoritmos operam de forma integrada e invisível no cotidiano. A opacidade dos sistemas tecnológicos gera novos

obstáculos à responsabilização: consumidores lesados frequentemente desconhecem como seus dados foram coletados, tratados ou utilizados, e têm dificuldade em identificar quem são os agentes ofensores. A chamada "caixa-preta algorítmica"[16] fragiliza o exercício da ação individual, ao tornar incerta a autoria, a extensão do dano e até mesmo a comprovação de nexo causal.

Essa falta de transparência amplia os desafios já presentes no modelo tradicional da responsabilidade civil, que se baseia na clara definição dos elementos de conduta, dano e nexo causal. Em casos envolvendo novas tecnologias autônomas, como robôs dotados de sistemas de IA ou plataformas de tomada de decisão automatizada, ainda não existem respostas claras sobre como repartir responsabilidades entre fabricantes, desenvolvedores, provedores de dados e usuários. A dúvida quanto a quem deve responder — se o programador do algoritmo, o controlador de dados, a empresa que disponibiliza a solução ou mesmo o próprio fornecedor de infraestrutura tecnológica — fragiliza o sistema reparatório clássico e coloca em evidência a necessidade de repensar os marcos normativos da responsabilidade civil no contexto digital.

Nesse cenário, o dano moral individual de pequena expressão econômica não deve ser compreendido apenas como um problema de acesso à justiça, mas como um elemento estrutural da sociedade de risco digital. A ausência de incentivos para a litigância individual abre espaço para práticas abusivas em massa, em que os custos sociais são distribuídos difusamente entre milhões de consumidores, enquanto os benefícios econômicos permanecem concentrados nas mãos de fornecedores que exploram dados pessoais de forma irregular.

Não obstante, o ordenamento já oferece instrumentos que buscam atenuar essa assimetria. O Código de Defesa do Consumidor (CDC)

16 Segundo Cinthia Obladen de Almendra Freitas, "[...] algoritmos mal projetados, desenvolvidos ou testados podem produzir resultados potencialmente discriminatórios ou prejudiciais aos indivíduos. Um exemplo a ser citado é a seleção de candidatos/as à entrevista para uma vaga de emprego, em que o algoritmo pode ser desenvolvido com viés para não selecionar mulheres ou pessoas de determinada região ou bairro. E, se o sistema for uma "caixa-preta" (black-box), o que dificulta ainda mais uma IA Explicável, pode ser muito difícil compreender por que motivos determinadas candidatas foram rejeitadas, dificultando a identificação e o tratamento de vieses. Há que se esclarecer que sistemas "caixa-preta" não são sempre discriminatórios ou possuem vieses, mas a falta de transparência em si pode dificultar a capacidade daqueles/as que são afetados/as por decisões automatizadas, de modo a não entender a lógica subjacente e seu impacto potencial. Outro exemplo é a caracterização de perfil (profiling) por meio da aplicação do credit score (avaliação de crédito) a partir de modelos de IA usados para aprovação ou não de crédito, sendo que os clientes bancários podem não ter um entendimento completo e correto sobre as decisões automatizadas que afetam suas vidas financeiras." (FREITAS, 2025)

estabelece, como princípio da Política Nacional das Relações de Consumo, o incentivo à criação, pelos fornecedores, de meios eficientes de controle de qualidade e segurança de produtos e serviços. Além disso, a LGPD, ao prever expressamente a possibilidade de tutela coletiva, abre caminho para a compensação de danos homogêneos, mitigando a barreira econômica que desestimula ações individuais e ampliando o alcance protetivo da responsabilidade civil no ambiente digita (BERGSTEIN, 2020)l.

Assim, a compreensão do dano moral em matéria de proteção de dados não pode ser limitada ao plano da reparação individual. Ele deve ser interpretado como parte de um mecanismo mais amplo de responsabilização coletiva, capaz de induzir práticas preventivas, assegurar maior transparência no uso de tecnologias baseadas em IA e enfrentar os riscos estruturais da economia digital, onde a lesão individual tende a ser pulverizada e invisível, mas o dano social é profundo e difuso.

6 Tutela coletiva do consumidor entre dados pessoais e inteligência artificial

Essa dificuldade de reparação econômica individual do consumidor titular de dados é um dos pressupostos para a relevância da tutela coletiva na LGPD, mas não só isso. Segundo Rafael Zanatta e Michel Souza, há um fracasso do modelo contratualista na teoria da privacidade de aviso-e-consentimento (*notice-and-consent*). Os autores abordam, entre outros estudos, o trabalho da filósofa Helen Nissenbaum, responsável pela redefinição da teoria da privacidade no Estados Unidos da América nos últimos anos. Sua obra *Privacy in Context: technology, policy and the integrity of social life* pela *Stanford University Press* foi uma verdadeira revolução, redefinindo as abordagens até então predominantes da privacidade baseada no consentimento pelo titular de dados pessoais para afirmar que "o direito à privacidade não é nem um direito ao segredo e tampouco um direito ao controle, mas um direito a um fluxo apropriado das informações pessoais."[17]

17 Em síntese, a autora afirma que não faria sentido uma distinção entre o privado e o público, mas sim nos fluxos e poderes que decorrem do uso dos dados pessoais. Nesse sentido, "o direito à privacidade não é nem um direito ao segredo e tampouco um direito ao controle, mas um direito a um fluxo apropriado das informações pessoais." Com essas premissas, Nissenbaum afirma que consumidores não são atores racionais e suas interações no ambiente digital não deveriam se basear em uma verificação contratualista baseada em termos de uso, consentimentos e demais informações disponibilizadas ao titular de dados pessoais no momento do aceite, mas sim em uma análise da "integridade contextual" que demandará uma análise ética e jurídica do caso concreto. (NISSENBAUM, 2010, p. 127).

Nesse sentido, a dimensão coletiva da proteção de dados pessoais também é uma evolução do modelo tradicional individualista e contratualista de tutela à privacidade, especialmente num contexto de sociedade informacional onde técnicas de *profiling* e *Big Data* tratam dados pessoais de uma grande massa de consumidores, muitas vezes não identificados diretamente, mas indiretamente por meio das suas pesquisas, preferências, características etc.[18] Essas operações de tratamento normalmente acontecem de forma ubíqua, como, por exemplo, utilizando cookies[19] armazenados nos navegadores dos titulares de dados e que são acessados por empresas com a finalidade de marketing direto.

Essa nova (e necessária) abordagem coletiva da proteção de dados foi especialmente enfatizada pela LGPD. Aliada a um sistema jurídico já habituado à tutela dos interesses coletivos por entidades como o Ministério Público e órgãos de defesa do consumidor, a nova legislação de proteção de dados representa uma importante ferramenta de proteção aos consumidores no Brasil, somando-se as ferramentas já citadas na introdução do presente trabalho como o CDC e a Lei de Ação Civil Pública.

Como já anteriormente mencionado, a LGPD faz menção expressa a possibilidade de defender "os interesses e dos direitos dos titulares de dados, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva" (art. 22, LGPD). Da leitura do artigo podemos concluir que tanto os interesses quanto os direitos dos titulares serão tuteláveis pelo poder judiciário, individual ou coletivamente. Sobre essa última possibilidade, teceremos algumas considerações.

Ao mencionar "a defesa dos interesses" dos titulares de dados, nos parece que o legislador se referiu a qualquer interesse que possa afetar o titular em sua esfera patrimonial, lhe ocasionando algum dano financeiro direto como, por exemplo, o vazamento de dados de cartão de crédito que ocasione o seu uso não autorizado. Não obstante, a esfera moral do titular de dados também é especialmente tutelada pela LGPD, vez que o direito à privacidade, também entendido como direito à proteção de dados[20],

18 A Lei Geral de Proteção de Dados define dado pessoal como qualquer informação relacionada a pessoa natural identificada ou identificável (art. 5º, I, LGPD).

19 Segundo o google, Cookies são "pequenos arquivos salvos nos computadores que ajudam a armazenar as preferências pessoais e outras informações que são utilizadas nos sites visitados". (GOOGLE, 2025)

20 Segundo Anderson Schreiber, "O direito à privacidade abrange, hoje, não apenas a proteção à vida íntima do indivíduo, mas também a proteção de seus dados pessoais. Em outras palavras: o direito à privacidade hoje é mais amplo que o simples direito à intimidade. Não se limita

compõe a esfera dos direitos da personalidade. Assim, o mero tratamento indevido de dados pessoais será, conforme essa interpretação, um dano moral, ofendendo, portanto, os interesses dos titulares de dados pessoais.

Não obstante, conforme a eminente obra que inaugurou a temática da proteção de dados sob a ótima do direito do consumidor, Laura Schertel Mendes afirma que o próprio "Código de Defesa do Consumidor permite, a partir dos princípios e direitos nele consagrados, além da tutela econômica, uma tutela consistente da personalidade do consumidor" (MENDES, 2014).

Há que ser considerado, no entanto, que, no judiciário brasileiro, os danos morais geram indenizações de pequena monta, o que desestimula o consumidor em buscar a compensação de danos na esfera judicial. A tutela coletiva assume, nesse contexto, especial via de atuação para além da indenização de um titular lesado em específico, gerando um efeito preventivo nos fornecedores que tratam dados pessoais de uma massa de consumidores. Esses poderão, em caso de responsabilização, indenizar ou compensar os danos individuais e/ou coletivos que tenham causado no exercício da atividade de tratamento de dados pessoais.

O art. 22 da LGPD menciona, além da "defesa dos interesses" dos titulares de dados, a defesa dos seus "direitos". O uso dessa expressão parece estar conectado com os direitos previstos a partir do art. 17 da LGPD, que, entre outras questões, assegura à toda pessoa natural "a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade". Em relação aos demais direitos previstos a partir do art. 18, o titular poderá requisitar diretamente ao fornecedor/controlador dos seus dados direitos como a confirmação de existência de tratamento, acesso aos dados, revogação do consentimento, eliminação etc. Não satisfeito, também pode peticionar em relação aos seus dados perante a Agência Nacional de Proteção de Dados (ANPD), cuja principal função é zelar pela proteção dos dados pessoais[21], ou pleitear perante organismos de defesa do consumidor.[22]

---

ao direito de cada um de ser "deixado só" ou de impedir a intromissão alheia na sua vida íntima e particular. Transcende essa esfera doméstica para alcançar características físicas, código genético, estado de saúde, crença religiosa e qualquer outra informação pertinente à pessoa. Nesse sentido, a privacidade pode ser definida sinteticamente como o direito ao controle da coleta e da utilização dos próprios dados pessoais. (SCHREIBER, 2014, p. 138-139)

21 Art. 55-J, LGPD.

22 § 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor. (Art. 18, § 8º, LGPD).

Em cenários de tomada de decisão automatizada, a tutela dos direitos do titular envolve, além do art. 18, a disciplina do art. 20 da LGPD (direito à revisão de decisões e à informação sobre critérios), relevante para opacidade algorítmica e para o ônus dinâmico da prova (art. 42, §2º), sobretudo quando a complexidade técnica impeça o consumidor de demonstrar o nexo causal.

Apesar das extensas possibilidades de resolução de conflito pelas vias administrativas, o judiciário também pode ser provocado para aferir a responsabilidade de fornecedores controladores ou operadores de dados pessoais que tenham violado a legislação de proteção de dados (art. 42, caput e §3º, da LGPD), inclusive com possibilidade de inversão do ônus da prova (art. 42, §2º, LGPD), tal qual ocorre nas demandas que envolvem o direito do consumidor, embora na LGPD ela não seja automática, mas dependente do exame objetivo do juiz quanto à presença dos pressupostos da verossimilhança e hipossuficiência do titular (BESSA; NUNES, 2021, p. 668). O controlador só não será responsabilizado quando provar que não realizou o tratamento de dados, que não houve ofensa à legislação ou em caso de culpa exclusiva do titular de dados ou de terceiro (art. 43, LGPD).

Para além da proteção de dados pessoais prevista na LGPD, a tutela coletiva do consumidor deve alcançar também o uso de dados em processos de treinamento de sistemas de inteligência artificial, prática que acarreta impactos significativos e de difícil aferição individual. A coleta massiva de dados, muitas vezes realizada sem transparência ou consentimento adequado, viabiliza o desenvolvimento de algoritmos que, posteriormente, podem reproduzir vieses discriminatórios ou gerar efeitos lesivos sobre categorias inteiras de consumidores. Nesses casos, a dimensão coletiva se impõe, uma vez que a irregularidade não se manifesta em danos isolados, mas em prejuízos difusos ou homogêneos.

Sistemas baseados em tratamento automatizado de dados, com ou sem IA embarcada, são capazes de processar informações pessoais em tempo real e em múltiplos contextos, escapando ao controle consciente dos consumidores. Essa falta de transparência dificulta não apenas a compreensão do dano sofrido, mas também a identificação do agente responsável, tornando ineficaz a lógica tradicional da responsabilidade civil fundada em relações bilaterais claramente delimitadas. Nesse cenário, a tutela coletiva assume função essencial, pois desloca o foco da reparação individual para a contenção estrutural de riscos.

Ademais, a utilização generalizada de ferramentas de IA em relações de consumo cria riscos que extrapolam a esfera da proteção de dados pessoais. Algoritmos de recomendação que reforçam práticas de discriminação de preços, sistemas de atendimento automatizado que induzem a decisões contratuais desvantajosas, ou ainda mecanismos de vigilância biométrica que monitoram consumidores em espaços físicos, todos exemplificam situações em que os direitos da coletividade estão em jogo. A tutela coletiva, nesse contexto, torna-se o instrumento mais adequado para reequilibrar a relação entre fornecedores de tecnologia e consumidores, impondo padrões de conduta que impeçam a perpetuação de práticas abusivas em larga escala.

Dito isso, há uma extensa gama de opções ao consumidor titular de dados pessoais em caso de violação à legislação de proteção de dados ou mesmo futuras legislações que visam regulamentar o uso e aplicação de Inteligência Artificial no Brasil[23], qual seja: na via administrativa (reclamações ao controlador; petição à ANPD; órgãos de defesa do consumidor) e na via judicial (reparação de danos patrimoniais e morais, individual ou coletivamente).

Por fim, para além da mera reparação de danos já ocorridos, em relação à possibilidade de tutela coletiva em caso de um ilícito em curso e que haja urgência na decisão, Rafael Zanatta e Michel Souza defendem que, interpretando a Lei da Ação Civil Pública e o Código de Defesa do Consumidor:

> [...] as leis que trazem os "vetores de princípios básicos" da tutela coletiva brasileira, juntamente com o Art. 64, da LGPD, temos que poderá ser proposta ação civil pública não somente para que seja realizado o devido ressarcimento pelos danos causados, mas também para que seja tutelada na forma específica os eventuais ilícitos que estejam sendo cometidos, ou seja, aplicando-se também uma tutela inibitória coletiva". (ZANATTA, Rafael A. F.; SOUZA, Michel R. O. A tutela coletiva na proteção de dados pessoais: tendências e desafios, in: DE LUCCA, Newton; ROSA, Cíntia. Direito & Internet IV: Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019).

Dessa forma, poderão os instrumentos de tutela coletiva, já previstos no ordenamento jurídico brasileiro, serem utilizados para fazer cessar lesão ou ameaça aos direitos dos titulares de dados, desde que

23 É o caso do Projeto de Lei nº 2338/2023, que dispõe sobre o uso da inteligência artificial. (BRASIL, 2023)

presentes os requisitos da tutela inibitória, impedindo, assim, que a ameaça se concretize ou que haja a prática de um ilícito continuado.

7 Conclusão

A Lei Geral de Proteção de Dados (LGPD) consagra, entre seus fundamentos estruturantes, a segurança dos dados pessoais, a prevenção e a responsabilização dos agentes de tratamento (art. 2º). Em diálogo com o Código de Defesa do Consumidor (CDC), que garante como direito básico a proteção contra riscos decorrentes de práticas abusivas de fornecimento de produtos e serviços (art. 6º), verifica-se uma relação de complementaridade que impõe a leitura integrada desses diplomas. Ambos convergem para reforçar a tutela da dignidade do consumidor em uma sociedade marcada pelo fluxo constante de informações e pelo protagonismo de novas tecnologias digitais.

O consumidor titular de dados pessoais permanece, em regra, em posição de acentuada vulnerabilidade, pois seus dados circulam em múltiplos contextos e são processados por fornecedores sem transparência suficiente quanto a finalidades e riscos. Esse quadro se intensifica diante da utilização de ferramentas de inteligência artificial e da lógica da computação ubíqua, em que informações são captadas, cruzadas e processadas em escala massiva, dificultando o controle efetivo pelo indivíduo. Nessas circunstâncias, multiplicam-se práticas que violam direitos da personalidade, expondo milhões de consumidores a danos invisíveis ou de difícil comprovação.

Considerando a realidade do Judiciário brasileiro, em que a fixação de indenizações individuais por danos morais tende a valores de baixa expressão econômica, resta evidente que a tutela exclusivamente individual não é capaz de inibir condutas abusivas nem de promover uma reparação satisfatória. A ausência de incentivo à litigância individual gera um desequilíbrio estrutural: de um lado, consumidores desestimulados a buscar reparação; de outro, fornecedores que internalizam os custos da violação como parte do negócio.

Nesse cenário, a tutela coletiva emerge como instrumento indispensável de recomposição e de prevenção. Por meio de ações civis públicas, demandas coletivas propostas por entidades da sociedade civil e a atuação de órgãos como o Ministério Público, Procons e a própria ANPD, é possível superar a dispersão dos danos individuais e assegurar compensações coletivas que, além de reparar, funcionam como mecanismo

de dissuasão e conformidade regulatória. No campo das tecnologias digitais e da IA, isso significa não apenas reparar os danos sofridos, mas também induzir mudanças estruturais em fornecedores e desenvolvedores, impondo padrões de segurança, transparência e governança.

Os caminhos futuros passam pela utilização estratégica da responsabilidade civil coletiva em casos de tratamento irregular de dados, viés algorítmico, discriminação automatizada e uso abusivo de sistemas de IA generativa. Ações coletivas podem buscar não apenas a reparação em pecúnia, mas também a adoção de obrigações de fazer ou não fazer, como a suspensão de sistemas lesivos, a exigência de avaliações de impacto algorítmico e a implementação de medidas de *accountability* e *compliance by design*.

Em conclusão, o sistema brasileiro já dispõe de um arcabouço jurídico robusto para proteger o consumidor frente aos desafios tecnológicos contemporâneos. Cabe, agora, potencializar o uso da tutela coletiva como forma de garantir que violações não sejam tratadas como meros custos operacionais, mas como práticas passíveis de sanção efetiva. A integração entre LGPD, CDC e demais diplomas protetivos, somada ao fortalecimento da atuação institucional e da sociedade civil, revela-se o caminho mais promissor para assegurar que os direitos difusos e coletivos dos consumidores sejam efetivamente preservados diante da crescente complexidade das ferramentas tecnológicas e da inteligência artificial.

Em paralelo, propostas regulatórias sobre IA (como o PL 2338/2023) reforçam vetores de gestão de risco, transparência e governança algorítmica, oferecendo pontos de contato com a tutela coletiva prevista em CDC/LGPD. Em litígios massivos envolvendo IA, a proteção do consumidor deve combinar reparação pecuniária com tutelas estruturais (obrigações de fazer/não fazer, avaliações de impacto, monitoramento independente), prevenindo recorrência e recalibrando incentivos econômicos.

Referências

BERGSTEIN, Lais. Pequenos grandes danos: A relevância da tutela coletiva do consumidor face aos danos de pequena expressão econômica. Revista de Direito do Consumidor, São Paulo, vol. 129/2020, p. 341 – 368, julho de 2020.

BESSA, Leonardo Roscoe; NUNES, Ana Luisa Tarter. Instrumentos Processuais de Tutela Individual e Coletiva: Análise do Art. 22 da LGPD.

In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; JUNIOR, Otavio Luiz Rodrigues. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021.

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. Civilistica.com. Rio de Janeiro, a. 9, n. 3, 2020. Disponível em: http://civilistica.com/responsabilidade-civil-na-protecao-de-dados-pessoais/ Acesso em: 27 set. 2025.

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

BUNDESGERICHTSHOF. Im Namen des Volkes. Urteil I ZR 186/17 vom 27. März 2025. Disponível em: https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=141179&pos=0&anz=1 Acesso: 27 set. 2025.

BRASIL. Lei 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados – LGPD. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm Acesso em: 27 set. 2025.

BRASIL. Projeto de Lei nº 2.338/2023. Dispõe sobre o uso da inteligência artificial. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233 Acesso em: 27 set. 2025.

CASTRO, Grasielle. Via Quatro é condenada em R$ 500 mil e proibida a coletar dado de passageiros do Metrô: TJSP identificou uso indevido de câmeras de segurança para captação de imagens de usuários com fins comerciais e publicitários. JOTA, 11 maio 2023. Disponível em: https://www.jota.info/justica/via-quatro-e-condenada-em-r-500-mil-e-proibida-a-coletar-dado-de-passageiros Acesso em: 27 set. 2025.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm Acesso em: 27 set. 2025.

BRASIL. Lei nº 4.717, de 29 de junho de 1965. Regula a ação popular. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l4717.htm Acesso em: 27 set. 2025.

BRASIL. Lei nº 7.347, de 24 de julho de 1985. Disciplina a ação civil

pública. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm Acesso em: 27 set. 2025.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078.htm Acesso em: 27 set. 2025.

BRASIL. Tribunal Superior Eleitoral (TSE). Resolução nº 23.610, de 18 de dezembro de 2019. Dispõe sobre propaganda eleitoral… (indicar art. 9º-C e a resolução que o incluiu em 2024). Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23610-de-18-de-dezembro-de-2019 Acesso em: 27 set. 2025.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota. Direito & Internet IV: Sistema de Proteção de Dados Pessoais (De acordo com a Lei nº 13.709, de 14 de agosto de 2018, e a lei nº 13.853, de 08 de julho de 2019, que converteu em lei a Medida Provisória nº 869, de 27 de dezembro de 2018). São Paulo: Quartier Latin, 2019.

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

ENDC. A proteção de dados pessoais nas relações de consumo. Elaboração Danilo Doneda. Brasília: DPDC, 2010 (destacando o papel da Senacon na tutela desses direitos fundamentais). Disponível em: http://www.justica.gov.br/seus- direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf Acesso em: 27 set. 2025.

GOOGLE. Cookie: Definition. Google Ads Help. Disponível em: https://support.google.com/google-ads/answer/2407785?hl=en Acesso em: 27 set. 2025.

FREITAS, Cinthia Obladen de Almendra. Enviesamento em sistemas de inteligência artificial e seus reflexos no direito. RRDDIS – Revista Rede de Direito Digital, Intelectual & Sociedade, Curitiba, v. 5, n. 9, p. 173-198, 2025.

GRINOVER, Ada Pellegrini. Da class action for damages à ação de classe brasileira: os requisitos de admissibilidade. São Paulo, Revista de Processo, v. 101, p. 11-27, jan.-mar. 2001.

GRINOVER, Ada Pellegrini. Novas tendências na tutela jurisdicional dos interesses difusos, Revista da Faculdade de Direito da Universidade de São Paulo, v. 79, 1984, p. 284.

GRINOVER, Ada Pellegrini. Rumo a um sistema ibero-americano de tutela de interesses transindividuais. In: GIDI, Antonio; MAC-GREGOR, Eduardo Ferrer (coords.). La tutela de los derechos difusos, colectivos e individuales homogéneos: hacia un Código modelo para Iberoamérica. 2. ed. México: Editorial Porrúa, 2004, p. XLVI.

MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. Revista de Direito do Consumidor, v. 79, p. 45-81, 2011.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. Editora Saraiva: São Paulo, 2014.

NISSENBAUM, Helen. Privacy in Context: technology, policy and the integrity of social life. Stanford: Stanford University Press, 2010.

PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD). São Paulo: Saraivajur, 2018.

REIS, Rafael Almeida Oliveira. Sociedade de risco digital. Rio de Janeiro: Lumen Juris, 2023.

SCHERTEL, Laura Mendes; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. São Paulo: Revista dos Tribunais, vol. 120/2018, p. 469 – 483, Nov - Dez/2018.

SCHREIBER, Anderson. Direitos da Personalidade. 3ª ed. Atlas Jurídico: São Paulo, 2014.

BECK, Ulrich. Sociedade de risco mundial: em busca da segurança perdida. Rio de Janeiro: Edições 70, 2015.

Superior Tribunal de Justiça (STJ). REsp 1.085.218/RS, 1ª Turma, Rel. Min. Luiz Fux, DJe 06 nov. 2009.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, L 119, 4 mai. 2016.

ZANATTA, Rafael A. F. Agentes de tratamento de dados, atribuições e diálogo com o Código de Defesa do Consumidor. In: Coletânea do Instituto de Tecnologia e Sociedade sobre a Lei Geral de Proteção de Dados Pessoais. São Paulo: Revista dos Tribunais, 2019.

ZANATTA, Rafael A. F.; SOUZA, Michel R. O. A tutela coletiva na proteção de dados pessoais: tendências e desafios, in: DE LUCCA,

Newton; ROSA, Cíntia. Direito & Internet IV: Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019.

Capítulo 9

PROBLEMAS JURÍDICOS NO ENFRENTAMENTO AO USO DE INTELIGÊNCIA ARTIFICIAL GENERATIVA PARA CRIAÇÃO DE CONTEÚDO DE ABUSO INFANTOJUVENIL

Thiago Pereira Lima[1]

1 Introdução

A sociedade que vivemos atualmente, aqui chamando atenção ao especial tocante da proteção de crianças e adolescentes em ambiente virtual, já não é mais a mesma de ontem, quiçá de 2008, ano do advento da Lei 11.829/2008, que atualizou os tipos penais vinculados ao abuso infantojuvenil em ambientes virtuais.

A referida lei, visando "aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet.", atualizou alguns tipos penais previstos na Lei 8069/90, o Estatuto da Criança e do Adolescente.

> Atualmente, na chamada 4 Revolução industrial, vivencia-se uma "transformação radical dos processos de produção por novas tecnologias que eliminam as barreiras entre as realidades física, digital e biológica, tais como robótica, inteligência artificial, nanotecnologia, computação quântica, computação em nuvem, biotecnologia, internet das coisas, veículos autônomos, dentre outros avanços disruptivos." (ANDRADE; MAGRO, 2024, p. 576).

E essa radical transformação - e aceleração – de processos e interações sociais por novas tecnologias, que de certa forma nublam a fronteira entre o real e o virtual, além de fomentar virtudes e melhorias, também pode

1 Delegado da Polícia Civil do Estado do Paraná no Setor de Crimes Patrimoniais do NUCIBER - PCPR. Bacharel em Direito pela Universidade Positivo. Mestre em Direitos Humanos e Políticas Públicas pela PUCPR. Doutorando em Direito Econômico e Socioambiental pela PUCPR. Professor da Escola Superior da Polícia Civil do Paraná. Email thiago.pereiralima@gmail.com

ser empregada para novas formas de cometer velhos crimes, especialmente nos chamados cibercrimes impróprios, em que computadores e redes são utilizados como instrumentos para prática de condutas criminosas já existentes no ambiente físico.

É necessário explorar e pensar no uso das Inteligências Artificiais generativas para criação de materiais fotográficos e vídeos de abuso infantojuvenil com assustadora aparência de realidade, em contextos mais "seguros" aos criminosos, que dispensariam condutas físicas presenciais, mais arriscadas e mais maior grau de punição jurídico penal, para criação desse material no conforto de suas "*work stations*".

> A IA tem sido saudada como uma revolução na forma em que vivemos e trabalhos, oferecendo avanços notáveis em campos tão diversos quanto a medicina, finanças e transporte. No entanto, essa mesma tecnologia que promete nos levar a uma nova era de eficiência e personalização também tem o potencial de ser deturpada. O lado sombrio da IA é raramente discutido na esfera pública, principalmente quando se trata de tópicos delicados e potencialmente polarizadores como a exploração de menores (MENDES, 2025).

Desta feita, dada a complexidade e interdisciplinariedade da temática ora proposta, é necessário refletir em inúmeras frentes acerca dessa sensível e cara temática, seja pensando sobre (in)adequação típica dessas novas condutas em face dos tipos penais atualmente previstos no Estatuto da Criança e do Adolescente, maneiras de identificar, coibir e prevenir condutas criminosas desse cariz, visando, como norte, a constitucionalmente prevista proteção de crianças e adolescentes nesse novo mundo em que estão chegando e vivendo.

É preciso lançar novos olhares para esses novos modelos de exploração e abusos de crianças e adolescentes, potencializado pelo uso das Inteligências Artificiais generativas.

2 Inteligência artificial generativa e os chamados *deep fakes* e *deep nudes* aplicados à material de abuso infantojuvenil

Os últimos e recentes anos têm presenciado passos gigantescos nas capacidades de tecnologias empregadas em ferramentas de Inteligência Artificial, particularmente com a introdução sucessiva de sistemas de Inteligência Artificial generativa que ingerem imensa quantidade de dados, aprendem padrões estatísticos que permitem aos modelos criarem conteúdos novos e inéditos, tipicamente baseados em comandos dados em

linguagem natural. Esses modelos podem gerar uma gama numerosa de produtos, como textos, imagens, áudios e vídeos. (MORRIS, 2023)

Esses modelo de inteligência artificial generativa podem produzir essa vasta gama de material, a exemplo de vídeos, com simples comandos de textos emitidos pelos usuários, sem a necessidade do uso de linguagens de programação, criação de algoritmos ou outras ações técnicas especializada da área.

São serviços que podem ser utilizados por usuários médios de ferramentas computacionais, sem formações ou *background* na área. Basta que saibam redigir frases de comando ao sistema com linguagem natural, os chamados *prompts*.

Sistemas de Inteligência Artificial consistem em sistemas computacionais que usam algoritmos para replicar habilidades humanas com certo grau de autonomia. Muito embora existe uma variedade de sistemas de IA, os mais conhecidos são baseados em algoritmos de aprendizado de máquina (*machine learning*) que aprendem com exemplos, e não com instruções humanas específicas. Enquanto sistemas de Inteligência Artificial estão em desenvolvimento há décadas, a Inteligência Artificial generativa entrou em escala pública em 2022, com o lançamento do OpenAI's ChatGPT, um *chatbot* e assistente virtual baseado em LLMs (*large language models*).

O que separa a IA generativa dos outros ramos de IA é o fato de gerarem conteúdo novo, inédito. IA generativa tem em sua base o chamado *deep learning* (aprendizado profundo), uma poderosa capacidade derivada de *machine learning* (aprendizado de máquina) baseada em sistemas neurais. IA generativa pode produzir muito mais do que textos. Os modelos podem criar imagens e vídeos com sequenciamento de pixels randômicos. (UNICRI, 2024)

Especificamente com LLMs (*large language models*), comandos de linguagem humana natural são executados pelos sistemas de Inteligência Artificial desenhados para esse tipo de finalidade. Os resultados ou saídas desses sistemas, variam desde textos e imagens e vídeos. A efetividade dos conteúdos gerados artificialmente pelas LLM (*large language models*) é relacionado a sua habilidade de processar linguagem natural, sintetizando e arrazoando fatos, e bem como resolvendo problemas em tópicos abstratos. Sistemas de Inteligência Artificial que usam LLM compreendem o contexto e significado prováveis da linguagem natural adotada nos comandos ou *prompts*. (PANATTONI, 2025)

Em outras palavras, com comandos que consistem em frases simples emitidos por usuários comuns, os modelos terão aptidão para gerar material altamente complexo e de alta qualidade gráfica e verossimilhança.

Conforme WACHTER (2021), os benefícios são claros. Elas podem nos ajudar a tomar decisões mais eficientes, baratas e consistentes. Ao mesmo tempo, elas podem introduzir novos riscos e agravar riscos antigos.

> O avanço da tecnologia e das interações na rede mundial de computadores possibilitou a criação de novas realidades com enfoque artístico. A partir dessas vertentes de criação digital, surgiram as chamadas *deep fakes*, que, no cenário hodierno, tornam cada vez mais desafiador distinguir o que é artístico do que é real. *Deepfake* é uma técnica que utiliza inteligencia artificial para criar vídeos falsos, porem realistas, de pessoas fazendo coisas que efetivamente nunca fizeram. O termo *deepfake* é uma combinação das palavras "*deep learning*" (aprendizado profundo) e "*fake*" (falso). Essa tecnologia se baseia em algoritmos de aprendizado de máquina para analisar e sintetizar imagens e sons, permitindo a substituição de rostos e vozes em vídeos de forma convincente. …]
>
> Percebe-se o crescente terreno fértil para criação artificial de imagens, áudios e vídeos contendo abuso sexual infantil. (LIMA; LIMA, 2024).

Inteligência Artificial generativa pode criar diretamente ou ser programada para criar conteúdos ofensivos ou mesmo criminosos, cuja própria criação ou disseminação podem ser criminalizadas por sistemas de justiça criminal. A gama de conteúdos que pode ser criada é significativamente grande, a exemplo de imagens de abuso sexual infantil. Nesse tocante, reside um grande risco nos chamados *deep nudes*, como são chamados os *deep fakes* criados para perpetração de crimes de pornografia não consentida.

> Em um mundo cada vez mais permeado pela tecnologia, onde a inteligência artificial (IA) já faz parte de nosso cotidiano, surgem questões éticas e jurídicas de uma complexidade inédita. Imagine a capacidade de criar imagens, vídeos e vozes indistinguíveis da realidade; agora imagine que essas criações podem ser usadas para fins nefastos, como a simulação de conteúdo pedófilo. Este não é um cenário distópico de um filme de ficção científica, mas uma realidade iminente que nosso ordenamento jurídico não está preparado para enfrentar. (Além da realidade, artigo).

De fato, é necessário refletir se a legislação nacional referente à temática, com sua última atualização datada do ano de 2008, pode servir

como ferramenta atual(izada) de combate a esse novo meio de praticar crimes de abuso infantil, ou se já trata-se de uma ferramenta obsoleta e deficitária.

Ademais, diante desse novo e desafiador cenário, é importante também pontuar a proteção de dados (ou ausência dela), nas imagens empregadas pelos referidos modelos.

Um relatório da *Human Rights Watch* conseguiu rastrear imagens usadas pelo LAION-5B para crianças específicas no Brasil, mostrando que muitas das fotos usadas nos modelos de produção foram tiradas de blogs pessoais de família. Embora não seja diretamente material de abuso infantojuvenil, as imagens dessas crianças, quando combinadas com pornografia adulta ou material de pornografia infantil já gerado, poderiam treinar um modelo sobre como criar material abusivo gerado por IA. Ficou claro para os criminosos que, desde o início, essas tecnologias tinham o potencial de gerar material de abuso infantil (UNICRI, 2024)

Portanto, para além da análise do tratamento penal das referidas condutas, escopo aqui abordado, é necessário refletir sobre as fontes que esses modelos se utilizam, nos tocantes à utilização de dados pessoais sem consentimento do titular, nos termos do art.7, I, da Lei 13.709/2018.

Verifica-se que não se trata apenas do problema do emprego das ferramentas na criação de material abuso, mas também sobre a proteção e identificação de quais bases de dados esses sistemas se utilizam para dar seus *outputs* aos usuários.

3 Adequação típica para o Direito

É preciso pontuar, inicialmente, que, de fato, "o impacto da informática criou uma nova estrutura social" (SYDOW, 2021, p.39).

Ressalte-se, desde já, que novo esse momento social exige respostas sempre atualizadas e atualizáveis.

> A sociedade da informação teve sua potência elevada com a popularização das maquinas e suas conexões, levando à boa parte da população o acesso a um cotidiano com características próprias, e que tem arquivos e dados intangíveis como mote de sua existência e sustentabilidade. A rede mundial de computadores trouxe velocidade de relacionamentos (comerciais, negociais, humanos, internacionais, etc) e dissolveu fronteiras físicas, permitindo que o usuário internauta experimentasse liberdade em grau antes inimaginável. O acesso às informações, vídeos, fotos, filmes, a potencialização da possibilidade

> de comunicação e a sensação de segurança fizeram com que houvesse massiva popularização da virtualidade. Certamente, todavia, a evolução tecnológica trouxe consigo sacrifícios e problemas (SYDOW, 2021, p.33).

Os crimes virtuais certamente estão inseridos nos problemas advindos da evolução tecnológica, aqui aplicado ao (mal) uso das ferramentas de Inteligência Artificial generativa para potencial criação de imagens e vídeos de abusos infantojuvenis.

Assim sendo, também exige celeridade na abertura do catálogo jurídico protetivo, na medida em que as antigas proteção não são mais bastantes.

O Estatuto da Criança e do Adolescente previu as seguintes condutas típicas:

> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente: (Redação dada pela Lei nº 11.829, de 2008)
>
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (Redação dada pela Lei nº 11.829, de 2008)
>
> § 1º Incorre nas mesmas penas quem: (Redação dada pela Lei nº 14.811, de 2024)
>
> I - agencia, facilita, recruta, coage ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no **caput** deste artigo, ou ainda quem com esses contracena; (Incluído pela Lei nº 14.811, de 2024)
>
> II - exibe, transmite, auxilia ou facilita a exibição ou transmissão, em tempo real, pela internet, por aplicativos, por meio de dispositivo informático ou qualquer meio ou ambiente digital, de cena de sexo explícito ou pornográfica com a participação de criança ou adolescente.
>
> Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Redação dada pela Lei nº 11.829, de 2008)
>
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (Redação dada pela Lei nº 11.829, de 2008)
>
> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008)

> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
>
> § 1 º Nas mesmas penas incorre quem: (Incluído pela Lei nº 11.829, de 2008)
>
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo; (Incluído pela Lei nº 11.829, de 2008)
>
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)
>
> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008)
>
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
>
> Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual: (Incluído pela Lei nº 11.829, de 2008)
>
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. (BRASIL, 1990).

Note-se que todos os tipos penais acima citados e relacionados à temática utilizam as seguintes elementares normativas: cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente.

O espectro protetivo dos citados tipos penais incriminadores é largo. Varia desde o agente que produz o material abusivo diretamente, passando por quem transmite, vende, divulga ou armazena. Ainda, em padrões de pena mais brandos, o artigo 241-C pune a simulação por montagem ou modificação de fotografia e video, de cena envolvendo abuso infantojuvenil.

Todavia, é importante que se frise que a última atualização dos mencionados institutos legais de repressão penal foi realizada no ano de 2008.

Referido ano foi marcado pela então CPI da Pedofilia, que promoveu mudanças legislativas que culminaram nos tipos penais acima colacionados. E partindo dessas atualizações, o legislador objetivava obstar, prevenir e reprimir criminalmente a utilização da internet e seus mecanismos de fácil

distribuição de conteúdo, quando empregada em ações voltadas ao abuso infantojuvenil. (SYDOW, 2021, p.595/597).

Impõe-se refletir, todavia, que naquele momento, as tecnologias de Inteligência Artificial generativas não existiam – e não apresentavam risco aos bens jurídicos que se desejava a proteção legal – no momento de elaboração e desta última atualização legislativa. Claramente, aplicavam-se no caso de crianças e adolescentes humanos figurassem como vítimas nos materiais de abuso. As novas Inteligências Artificiais têm capacidade de produzir materiais de altíssima qualidade gráfica e aparência de realidade. Assim, estaria o arcabouço jurídico atual capaz de reprimir e punir condutas em que não exista um vítima humana "criança ou adolescente"? (MENDES, 2023)

De modo que, se a cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente for criada por ferramenta de inteligência artificial, é necessário refletir juridicamente, se haveria tipicidade criminal diretamente aplicada a esse tipo de conduta.

Um material contendo crianças ou adolescentes criados artificialmente, inseridos em uma cena de abuso igualmente criada artificialmente por mecanismo de inteligência artificial, enquadra-se nos atuais tipos penais do Estatuto da Criança e do Adolescente?

> visualiza-se que o tipo penal não especifica se a criança ou adolescente deve ser real ou um avatar criado por Inteligência Artificial. No entanto, o artigo 2 do ECA prevê que "considera-se criança, para os efeitos da Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade". Assim, entende-se que abranger um ser criado, virtualmente, não correspondente a uma pessoa, seria clássico caso de analogia *in malam partem* (LIMA; LIMA, 2024).

O autor remete à questão da tipicidade levantando um alerta de que os tipos penais aqui remetidos, quando utilizados em situação de material de abuso produzido por Inteligência Artificial, poderiam suscitar questionamentos acerca da impossibilidade de utilização por 1) analogia in malam parte e 2) carência de tipicidade (formal).

> A maior parte das funções que a doutrina atribui à tipicidade formal, de regra, são atendidas pela pretensão conceitual de relevância. Ele efetivamente atende à função político criminal, ou de garantia, já que representa a expressão do princípio da legalidade, posto que limita o âmbito do punível ao indicar o que, exatamente, pode ser objeto de imputação (BUSATO, 2017, p. 299).

E tratando do princípio da legalidade, continua o autor mencionando que, para que determinada conduta seja considerada adequada formalmente à norma penal incriminadora e, assim, seja típica para o direito, ela deve preencher a forma expressa do princípio da legalidade, ou seja, deve haver exata adequação entre a conduta praticada e a descrição legal que a incrimina (BUSATO, 2017, p.286).

E a improvisação do uso de novas condutas em tipos penais antigos pode acarretar em analogia *in malam partem*, vedada pelo Direito, o que, em termos práticos, inviabiliza a punição de autores de crimes por violação do princípio da legalidade.

No tocante à proibição da analogia in malam partem, ressalte-se que:

> A analogia, como método de pensamento comparativo de grupos de casos, significa aplicação da lei penal a fatos não previstos, mas semelhantes aos fatos previstos. (…) como analogia prejudicial ao réu é absolutamente proibida pelo direito penal (SANTOS, 2008, p.23).

Impõe-se assim a reflexão de que, ao aplicarmos analogicamente uma lei que é lacunosa quanto à criação de conteúdo artificial com crianças e adolescentes igualmente artificiais, seria uma potencial analogia in malam parte que, ao fim e ao cabo, prejudicaria e persecução desse novo método de criminalidade, impedindo a responsabilização das novas condutas delitivas com base em antigos dispositivos penais.

Entretanto, é necessário igualmente pensar no mandamento constitucional de que:

> Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão (BRASIL, 1988).

É certo que a proteção deficitária de condutas que envolvem a criação artificial de material contendo crianças e adolescentes abusadas viola a Constituição Federal na obrigação de salvaguardar e proteger em face de exploração. Ainda, perpetradores desse tipo de crime não podem ficar protegidos por lacunas legislativas que poderiam criar campos cinzentos de (a)tipicidade e impunidade.

E no tocante a lacunas legislativas nessa temática, é imperativo citar o Decreto 11.491 de 12 de abril de 2023, que promulgo – e implantou - no ordenamento jurídico a Convenção de Budapeste sobre o Crime Cibernético, na qual os países signatários, Conscientes das profundas mudanças desencadeadas pela digitalização, interconexão e contínua globalização das redes informáticas, assinaram conjuntamente o ato normativo que norteia o combate à criminalidade e aos crimes cibernéticos. Segundo a referida Convenção,

> Título 3 - Crimes relacionados ao conteúdo da informação
>
> Artigo 9 - Pornografia infantil
>
> 1. Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, as seguintes condutas, quando cometidas dolosamente e de forma não autorizadas:
>
> a. produzir pornografia infantil para distribuição por meio de um sistema de computador;
>
> b. oferecer ou disponibilizar pornografia infantil por meio de um sistema de computador;
>
> c. distribuir ou transmitir pornografia infantil por meio de um sistema de computador;
>
> d. adquirir, para si ou para outrem, pornografia infantil por meio de um sistema de computador;
>
> e. possuir pornografia infantil num sistema de computador ou num dispositivo de armazenamento de dados de computador (BRASIL, 2023).

E de forma mais profunda e atualizada na temática, propõe que:

> 2. Para os fins do parágrafo 1, "pornografia infantil" inclui material pornográfico que represente visualmente:
>
> a. um menor envolvido em conduta sexual explícita;
>
> b. uma pessoa que pareça menor envolvida em conduta sexual explícita;
>
> c. imagens realísticas retratando um menor envolvido em conduta sexual explícita (BRASIL, 2023).

O importante item c parece ser um grande indicativo para atenção legislativa interna dos países signatários, acerca da necessidade de tipificar crimes que envolvam a criação artificial de material realístico que retrate pornografia envolvendo crianças e adolescentes.

Além do mandamento incriminador contido na mencionada Convenção, esse normativo também estabelece como pornografia ou material de abuso infantojuvenil, imagens realísticas retratando menores em condutas sexuais explícitas, o que parece preencher a lacuna que é ora tratada.

4 Projetos de lei em trâmite

Além do direcionamento dado pelo Decreto que promulgou a Convenção de Budapeste, tramitam nas casas legislativas brasileiras dois projetos de Lei sobre a temática aqui tratada, que merecem destaque.

O primeiro deles, o Projeto de Lei 2338 de 2023, de abordagem mais panorâmica e generalista, diz respeito ao estabelecimento de

> normas gerais de caráter nacional para o desenvolvimento, implementação e uso responsável de sistemas de inteligência artificial (IA) no Brasil, com o objetivo de proteger os direitos fundamentais e garantir a implementação de sistemas seguros e confiáveis, em benefício da pessoa humana, do regime democrático e do desenvolvimento científico e tecnológico (BRASIL, 2023).

Já o segundo Projeto está umbilicalmente ligado ao uso específico de Inteligência Artificial generativa para criação de *deep nudes*, ou seja, imagens de conteúdo pornográfico criadas criminosamente por ferramentas de IA.

O Projeto de Lei 3821 de 2024 prevê a criação de um novo tipo penal no Código Penal brasileiro com o seguinte texto:

> Art. 216-C. Manipular, produzir ou divulgar, por qualquer meio, conteúdo de nudez ou ato sexual falso, gerado por tecnologia de inteligência artificial ou por outros meios tecnológicos com a finalidade de humilhação pública, vingança, intimidação ou constrangimento social:
>
> Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa, se o fato não constituir crime mais grave. (BRASIL, 2024).

O poder legislativo caminha, acertadamente, para preencher lacunas legais deixadas pelo escalada no (ab)uso da Inteligência Artificial generativa e sua potencialidade para cometimento de crimes e violação de direitos.

5 Conclusão

É notório que o uso massivo de ferramentas de Inteligência Artificial generativa é uma realidade cada mais abundante, próxima e constante em inúmeras atividades e campos da sociedade. Ainda, é importante que se diga, já de antemão, que "Tecnologia não é boa e também não é má, mas também não é neutra. Ou seja, como toda ferramenta, o que a define é seu utilizador." (SYDOW, 2021, p. 22).

No entanto, conforme exposto nos fundamentos e reflexões aqui apresentadas, novas ferramentas tecnológicas que empregam a Inteligência Artificial generativa têm grande potencial de criarem artificialmente material de abuso infantojuvenil, ou, usando os termos da Convenção de Budapeste, pornografia infantil.

É necessário pontuar, do ponto de vista jurídico, que problemas residem no tocante a aplicar uma legislação que não acompanhou a evolução tecnológica, e não prevê expressamente as novas situações fática e condutas que se pretende proibir e incriminar.

É dizer que, no caso dos crimes previstos no Estatuto da Criança e do Adolescente no que tange à exploração de material de abuso sexual infantojuvenil em todas as suas formas (produzir, vender, divulgar, armazenar, dentre outros verbos nucleares dos tipos penais), a própria lei prevê o termo "*cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente*".

Todavia, impõe-se refletir que, sob o prisma do princípio da legalidade e da tipicidade formal, os tipos penais do ano de 2008 não parecem estar normativamente preparados e capazes de abarcar condutas envolvendo a criação de fotos e vídeos pornográficos artificiais, criados por Inteligência Artificial e empregando imagens de crianças e adolescentes artificialmente criados com dados constantes nas bases de dados das ferramentas.

A discussão torna mais corpo ao pensar-se que, por lacunas legislativas, é possível que essas novas e graves condutas, com imenso potencial lesivo e potencial produtivo maior ainda, possam ter sua repressão e punição deficitárias e inválidas, pois ausente uma legislação tecnicamente atual e capaz de englobar taxativamente os crimes envolvendo material de abuso sexual infantojuvenil produzido por inteligência artificial.

E se trata de uma temática que toca inúmeros campos que circundam tanto a persecução penal como a proteção de dados pessoas.

As empresas detentoras das soluções de Inteligência Artificial generativa tem transparência em suas bases de dados? O produto de suas ferramentas são auditáveis e possuem dotação de códigos *hash* para identificação de responsáveis pela produção e as demais cadeias de distribuição e uso desses produtos?

Em caso de apreensões de materiais, com quais padrões periciais se dará a identificação de conteúdo potencialmente criminoso?

São inúmeros campos que circundam a temática ora proposta, que precisam acompanhar a evolução tecnológica visando dar efetivas e satisfatórias respostas à

> A violência sexual contra crianças e adolescentes talvez sempre tenha permeado a humanidade, mas ganhou um grande impulso nas últimas décadas com o avanço da tecnologia, principalmente com a internet, com a popularização dos equipamentos de captura de imagens e também a modernização de meios de comunicação (VELHO, 2016, p. 247).

Um desses campos, em cujo foco reside o presente artigo, é a atualização legislativa, a exemplo dos projetos de Lei mencionados anteriormente. O tratamento jurídico da Inteligência Artificial generativa deve ser inter e multidisciplinar e, sobretudo, atualizado, sob pena do atraso gerar impunidade e fomentar ações criminosas.

Referências

ANDRADE, Landolfo; MAGRO, Américo Ribeiro. **Manual de Direito Digital**. 4.ed. São Paulo: Juspodivm, 2024.

BRASIL. Constituição Federal (1988). **Constituição da República Federativa do Brasil**. Brasília, DF, 4 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm Acesso em: 27 set. 2025.

BRASIL. Lei 8.069 de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial da União,** Brasília, DF, 13.jul.1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm Acesso em: 27 set. 2025.

BRASIL. Decreto n. 11.491 de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. **Diário Oficial da União,** Brasília, DF, 12 abr. 2023. Disponível em: https://

www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm Acesso em: 27 set. 2025.

BRASIL. Lei 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União,** Brasília, DF, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 27 set. 2025.

BRASIL. Senado Federal. Projeto de Lei 2338 de 2023. Dispõe sobre o uso da Inteligência Artificial. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1738768169771&disposition=inline Acesso em: 27 set. 2025.

BRASIL. Câmara dos Deputados. Projeto de Lei 3821 de 2024. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e a Lei nº 9.504, de 30 de setembro de 1997 (Lei das Eleições), para tipificar o crime de manipulação digital de imagens por inteligência artificial, e agravar a pena em casos de crimes contra mulheres e candidaturas em período eleitoral, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2461213 Acesso em: 27 set. 2025.

BUSATO, Paulo César. **Direito penal: parte geral**. V.1. São Paulo: Atlas, 2017.

LIMA, Anderson Rodrigo Andrade de; LIMA, Eduardo Pacheco de Mello. A (a)tipicidade da criação artificial de conteúdo abusivo: protegendo a dignidade infantil na era da inteligência artificial. In Anais do 7 Congresso Internacional de Direito e Contemporaneidade: midias e direitos da sociedade em rede. 2024. Disponível em: https://www.ufsm.br/app/uploads/sites/563/2024/12/3.5.pdf Acesso em: 27 set. 2025.

MENDES, Cleylton. Além da realidade: IA, menores e o espaço cibernético inexplorado. In Revista Consultor Jurídico. 2023. Disponível em: https://www.conjur.com.br/2023-nov-08/cleylton-mendes-alem-realidadeia-menores-espaco-cibernetico/ Acesso em: 27 set. 2025..

MORRIS, Meredith Ringel. Scientists' Perspectives on the Potential for Generative AI in their Fields. In Arxiv.org – Cornell University. 2023. Disponível em: https://arxiv.org/abs/2304.01420 Acesso em: 27 set. 2025.

PANATTONI, Beatrice. Generative AI and criminal law. In *Cambridge Forum on AI: Law and Governance*. 2025. Disponível

em: https://www.cambridge.org/core/journals/cambridge-forum-on-ai-law-and-governance/article/generative-ai-and-criminal-law/CFBB64250CAC6A338A5504F0F41C54AB Acesso em: 27 set. 2025.

SANTOS, Juarez Cirino dos. **Direito penal: parte geral**. 3.ed. Curitiba: Lumen Iuris, 2008.

SYDOW, Spencer Toth. **Curso de Direito Penal Informático**.2.ed. Salvador: Juspodivm, 2021.

UNICRI (United Nations Interregional Crime and Justice Research Institute). Generative AI: A New Threat for Online Child Sexual Exploitation and Abuse. 2024. Disponível em: https://unicri.org/sites/default/files/2024-09/Generative-AI-New-Threat-Online-Child-Abuse.pdf Acesso em: 27 set. 2025.

VELHO, Jesus Antonio (org.). **Tratado de computação forense**. Campinas: Millenium, 2016.

WACHTER, Sandra. How fair AI can make us richer. In European data protection law review. 2021. Disponível em <https://edpl.lexxion.eu/article/edpl/2021/3/5> Acesso em 10/03/2025.

Capítulo 10

A LGPD E AS POLÍTICAS DE PRIVACIDADE NO ÂMBITO DOS JOGOS *MOBILE*

Willian Ryutaro Kobe[1]

1 Introdução

Para contextualizar, destaca-se que o mercado de jogos e aplicativos *mobile*, de maneira semelhante ao mercado clássico de *games* (jogos eletrônicos), vêm se mostrando promissor e extremamente rentável, demonstrando crescimento significativo ao longo dos últimos anos.

Para fins de demonstração, no ano de 2018, o mercado global de jogos *mobile* contava com 1,28 bilhão de usuários, com estimativa de crescimento para 1,65 bilhão até 2023. Consequentemente, com aumento de consumidores, estima-se que as receitas do mercado aumentarão de 46,7 bilhões de dólares para 55,48 bilhões, até o referido ano de 2023 (Clement, 2021). Outrossim, a indústria dos jogos eletrônicos, segundo estudos publicados pela *GameScan* (2020) e *SuperData* (2019), a aludida indústria se mostra como a mais rentável e lucrativa do ramo do entretenimento, superando, em expressão econômica, a indústria musical e cinematográfica (Wakka, 2021).

Outrossim, diferentemente do mercado tradicional, o qual abrange os consoles e computadores, o mercado *mobile* tende ao maior uso de modelos de oferta classificados como *barter.* O referido modelo, como meio de remuneração ou monetização do produto ou serviço, utiliza de coleta de dados (incluindo dados pessoais) e informações, em contraprestação dos bens ofertados, dados estes que podem ser alienados ou utilizados para outros fins econômicos (Mcgrath, 2010), propiciando a veiculação, por exemplo de publicidade direcionada especificamente ao jogador, como contraprestação de um serviço ou produto ofertado sem cobranças de valores.

1 Bacharel em Direito pela PUCPR, advogado licenciado, mestre em Direito pela PUCPR. Email william.taro@gmail.com

Tal modelo negocial tende a ser adotado justamente pela democratização de acesso proporcionada pelos dispositivos *mobiles*, característica esta que propicia o consumo por um público-alvo maior, abrangendo diversas faixas etárias e classes econômicas distintas, justamente pela fácil aquisição de dispositivos celulares (Silva et al. 2016), de modo que, inevitavelmente, conclui-se pela praticidade do modelo *barter*, neste ramo industrial, uma vez que incentiva o consumo de seus produtos sem onerar diretamente o consumidor final, ao mesmo tempo que proporciona uma receita ao fornecedor.

O problema surge quando se verifica que, mesmo diante das vantagens do aludido modelo, dados pessoais do jogador são coletados para a finalidade publicitária, ou outras ainda desconhecidas, caracterizando, ao menos aparentemente, uma operação de coleta de dados, a qual é regida, hoje, por lei própria, consistente na Lei 13709/2018, ou Lei Geral de Proteção de Dados Pessoais, doravante referida como LGPD.

A LGPD, estabelece diversas disposições acerca da coleta e tratamento de dados pessoais, conforme tratado no presente artigo, e busca regular essas operações com o fim de proteger o direito fundamental à privacidade, o qual possui, além da envergadura constitucional, previsão em normas internacionais de Direitos Humanos, o que, também, encontra-se desenvolvido e explicado no Tópico 2.

Portanto, surgem diversos questionamentos acerca destes mecanismos de coleta e tratamento de dados pessoais, tendo em vista que os dispositivos móveis são capazes de fornecerem diversos dados pessoais, tais como localização, imagens, conteúdo de memória interna, e-mail, contatos telefônicos e de redes sociais, bem como diversos outros conteúdos informacionais de cunho financeiro. Logo, pela entrada em vigor da nova LGPD, a qual, conforme já destacado, instituiu diversos deveres e condições de coleta e tratamentos de dados pessoais, impende analisar se ocorre o efetivo cumprimento das disposições legais e, caso haja violações, as eventuais consequências jurídicas.

Ao seu turno, a atualidade da pesquisa se torna evidente, vez que, diante do cenário de pandemia vivenciado atualmente pela sociedade, a demanda por jogos eletrônicos, como meio de entretenimento durante o período de isolamento e distanciamento social aumentou expressivamente (Borges, 2020), logo, com o aumento do consumo em uma indústria que já era extremamente expressiva, aumenta-se, consequentemente, o número

de pessoas sujeitas à eventual coleta e tratamento irregular de dados pessoais.

Por sua vez, a relevância, igualmente, se mostra presente pela expressividade da indústria e o elevado número de jogadores afetados pela prática, de modo que, pela recente entrada em vigor da Lei Geral de Proteção de Dados, o acervo epistemológico sobre a temática ainda se encontra em construção, sendo relevante, à comunidade jurídica, pesquisas que busquem analisar situações e problemas concretos da atualidade, se mostrando oportuno o estudo sobre as práticas adotadas pelas desenvolvedoras desses jogos, visto que seus produtos e serviços estão se incorporando à rotina dos indivíduos modernos, em especial pelos efeitos decorrentes da sociedade de informação aliado à acessibilidade dos jogos *mobile*, decorrente da difusão social dos aparelhos celulares.

Desta forma, denota-se que o objetivo geral do presente trabalho consiste na análise de termos de política de privacidade e a respectiva verificação de adequação às disposições da LGPD no contexto de Direitos Humanos e Empresas, uma vez que há a necessidade de se compreender as responsabilidades.

Como metodologia, método dedutivo e procedimentos bibliográficos, realizou-se a leitura e análise de obras bibliográficas e artigos científicos. Claramente, o trabalho se pautou em pesquisas teóricas, para tanto, utilizou-se a base de dados da Pontifícia Universidade Católica do Paraná (*Pergamum*) e *Google* Acadêmico, bem como bases de dados de acesso restrito, tais como Revista dos Tribunais e Portal de Periódicos da CAPES, sem prejuízo de obras em mídia física

Cabe, ainda, destacar as contribuições do grupo de pesquisa: "Das possibilidades de responsabilização de estados e de empresas por violações de Direitos Humanos", as quais foram essenciais ao desenvolvimento do presente trabalho, seja por meio de auxílio direto, em forma de aulas, ou por meio de indicação bibliográfica. Por fim, como resultado esperado, busca-se estabelecer os conceitos aplicáveis à relação de consumo de jogos *mobile* e aplicá-los na análise dos referidos termos de política de privacidade, sob um olhar das responsabilidades das empresas fornecedoras/desenvolvedoras de jogos eletrônicos.

2 A possibilidade de violação horizontal do direito à privacidade

O Direito à Privacidade, mesmo possuindo tutela infraconstitucional pela LGPD, consiste em direito fundamental de envergadura constitucional, conforme art. 5º, XII, da CRFB (Brasil, 1988), ao passo que, também, possui previsão em norma internacional de direitos humanos, conforme art. 12 da Declaração Universal de Direitos Humanos (ONU, 1948), demandando uma análise mais rigorosa e técnica para sua proteção e, por se tratar de relações entre empresa e consumidor que são ambos particulares, deve ser analisada, inclusive, com base na eficácia horizontal dos direitos fundamentais para efetivar sua proteção.

A despeito da conceituação do Direito à Privacidade, em que pese a complexidade e abrangência técnica deste instituto, é possível defini-lo, segundo as lições de Sarlet (2021), nos seguintes termos:

> Assim, não se coloca em causa que o direito à vida privada consiste, a exemplo do que emblematicamente já se disse no direito norte-americano, no direito de se estar só e de se ser deixado só (*the right to be let alone*), no sentido, portanto, de um direito a viver sem ser molestado pelo Estado e por terceiros no que toca aos aspectos da vida pessoal (afetiva, sexual etc.) e familiar. Em causa, portanto, está o controle por parte do indivíduo sobre as informações que em princípio apenas lhe dizem respeito, por se tratar de informações a respeito de sua vida pessoal, de modo que se poderá mesmo dizer que se trata de um direito individual ao anonimato.

Ao seu turno, quanto à Privacidade como um dos Direitos Humanos, previsto na Declaração Universal de Direitos Humanos de 1948, de acordo com Piovesan (2018, p. 238), cabe destacar as seguintes considerações:

> Por isso, como já aludido, a Declaração Universal tem sido concebida como a interpretação autorizada da expressão 'direitos humanos', constante da Carta das Nações Unidas, apresentando, por esse motivo, força jurídica vinculante. Os Estados-membros das Nações Unidas têm, assim, a obrigação de promover o respeito e a observância universal dos direitos proclamados pela Declaração. Nesse sentido, estabelece o art. 28 da Declaração que todos têm direito a uma ordem social e internacional em que os direitos e liberdades sejam plenamente realizados.

Desta forma, quanto à conceituação e eficácia do Direito à Privacidade, observa-se que se trata de norma de mais elevado status no

ordenamento interno, ao passo que é pacificamente reconhecido pela comunidade internacional, devendo sua proteção ser efetivada, inclusive, contra violação de terceiros particulares, e não somente de eventuais ingerências estatais.

Estabelecidas breves conceituações sobre o aludido instituto normativo, cabe adentrar na explicação sobre a possibilidade de violação horizontal (eficácia horizontal), ou violação nas relações privadas, deste direito, assim como pode ocorrer com qualquer outro de natureza semelhante.

Acerca da eficácia horizontal e sua respectiva possibilidade de violação, cabe destacar que esta corrente se originou junto à década de 1950, na Alemanha, tendo sua autoria creditada ao *Hans Carl Nipperdey* (Carvalho, 2015, p. 17). Quanto ao seu conteúdo, a referida corrente estabelece que as normas de direitos fundamentais podem ser oponíveis à parte adversa de uma relação privada, não se restringindo somente às relações com o Estado, devendo ser aplicados princípios constitucionais diretamente ao caso (Carvalho, 2015, p. 17), neste sentido:

> Assim, com a aplicação da teoria direta dos direitos fundamentais às relações privadas, a Constituição pode demonstrar sua eficácia de forma dúplice ou binária, pois esse método se concretiza quando o Poder Judiciário, em sua atuação típica, resolve o caso concreto utilizando-se da legislação ordinária (em um método de aplicação indireta), mas ao mesmo tempo, aplica também, em razão de sua normatividade, de forma direta, os princípios constitucionais ao caso concreto.

Ao seu turno, destaca-se que o fundamento da aludida corrente, apesar de não expressa na redação constitucional, decorre da hermenêutica constitucional, dentre outros aspectos normativos, decorrente do comando do art. 5º, §1º, CRFB (Brasil, 1988), neste sentido, cabe citar:

> Apesar de, como dito anteriormente, não existir no Texto Constitucional pátrio, norma expressa que preveja a vinculação dos particulares aos direitos fundamentais, isso não é empecilho para que se desenvolva construção jurídico-normativa para chegar a tal conclusão. E isso porque a Carta Magna, apesar de não prever expressamente, por outro lado, (i) não proíbe a vinculação dos particulares, (ii) é possível que se chegue a tal conclusão de forma mediata, (iii) observa-se, em algumas normas, que, estruturalmente, os direitos fundamentais têm como destinatários os particulares, e (iv) alguns autores defendem que a norma do § 1º do artigo 5º prevê a 'máxima otimização' das normas definidoras de direitos fundamentais. (Nakahira, 2007, p. 95)

Portanto, feitas breves considerações a respeito do direito à privacidade, sua oponibilidade em face aos particulares, inclusive na relação entre titulares de dados e empresas, bem como demonstrada sua envergadura constitucional e de Direitos Humanos, prossegue-se no desenvolvimento do tema, agora, sob a óptica dos institutos da LGPD.

3 Normas da lgpd aplicáveis ao consumo de jogos *mobile*

Inicialmente, cabe destacar que, diante do cenário atual de desenvolvimento tecnológico, aliado à dinamicidade dos meios de comunicação digital, "revela-se impossível cogitar de proteção integral à liberdade, à privacidade e ao desenvolvimento da pessoa natural sem que se lhe garanta eficaz defesa e controle de seus próprios dados – o que se traduz na expressão autodeterminação informativa." (Frazão, 2019, p. 678)

Conforme já mencionado anteriormente, em que pese a natureza de direito constitucional e de direitos humanos, o direito à privacidade, em seu aspecto de proteção de dados pessoais, passou a contar com regulamentação infraconstitucional por meio da LGPD, a qual, por sua vez, introduziu diversos novos institutos ao ordenamento jurídico e estabeleceu regime próprio para tutela do referido bem jurídico, os quais serão analisados neste capítulo. Neste sentido, assevera Miragem (2019, p. 20) que:

> A eficácia da proteção dos interesses do titular dos dados, segundo a técnica legislativa adotada pela LGPD implica reconhecer e assegurar os direitos fundamentais de liberdade, de intimidade e de privacidade, de acordo com a estrutura normativa definida pela lei (art. 17). Nos mesmos termos, define uma série de direitos subjetivos específicos do titular de dados, em relação aos quais corresponde ao controlador uma situação jurídica passiva, do dever de realizar seu conteúdo.

Visando à definição da relação jurídica regulada pela mencionada lei, cabe destacar a redação do art. 3º, da LGPD, o qual estabelece que esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: (I) "a 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 (II) "os dados pessoais objeto do tratamento tenham sido coletados no território nacional". Observa-se,

nesta disposição, que para incidência da LGPD (Brasil, 2018), é suficiente o preenchimento de qualquer uma das hipóteses descritas para sua aplicação.

Quanto aos sujeitos envolvidos e bem jurídico tutelado, o art. 5º, I, V, VI, VII e IX, preveem, respectivamente, que para os fins desta Lei, considera-se a) "dado pessoal: informação relacionada a pessoa natural identificada ou identificável"; ao passo que b) "titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento"; bem como c) "controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais"; ainda, d) "operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador"; e, por fim, e) "agentes de tratamento: o controlador e o operador". Constata-se que todas as figuras subjetivas se fazem presente na relação de consumo de jogos *mobile*, sendo o titular dos dados pessoais o consumidor, e empresa fornecedora, e seus prepostos, os agentes de tratamento de dados.

Em relação à operação de tratamento de dados, consta do art. 7º, I, V e IX, O tratamento de dados pessoais somente poderá ser realizado a) "mediante o fornecimento de consentimento pelo titular"; ou, também, b) "quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados", ou, então, c) "quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais". Quanto ao consentimento, nos termos do art. 8º, este deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

Outrossim, se mostra imperioso destacar a redação integral do art. 9º, como ponto essencial para o desenvolvimento do próximo capítulo, pois o dispositivo institui regras sobre a facilitação do acesso à informação sobre o tratamento de dados pessoais: "Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso"[2]

2 I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do

Acerca do art. 9º e comentários acerca de seus incisos, cabe citar Marcacini (2020, p. 160):

> Algumas dessas informações são meras indicações que não exigem maiores comentários. É direito do titular conhecer quem é o controlador (inc. III) e como entrar em contato com ele (inc. IV). As 'responsabilidades' dos agentes de tratamento também devem ser descritas ao titular de dados (inc. VI), texto este que merece um breve comentário. […] Mais relevantes são as informações que o titular há de receber acerca do disposto nos incisos I, II e V, pois são essas que permitem compreender que uso será feito dos seus dados pessoais.

Inobstante a previsão do art. 9º, verifica-se que, em seu inciso VII, ocorre alusão ao art. 18 da mesma lei (Brasil, 2018), o qual apresenta a seguinte redação: "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição"[3].

Oportuno, também, destacar as disposições relevantes sobre transferência internacional de dados, previstas no art. 33 (Brasil, 2018): "a transferência internacional de dados pessoais somente é permitida nos seguintes casos"[4].

Em relação à segurança e sigilo dos dados, dispõe o art. 46 (Brasil, 2018) que os agentes de tratamento "devem adotar medidas de segurança,

---

titular, com menção explícita aos direitos contidos no art. 18 desta Lei. […] § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

3 I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

4 I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei; II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de: a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos; […] VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

Ao seu turno, oportuno destacar o incentivo à boas práticas de governança, contido o art. 50 autoriza com 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 (Brasil, 2018).

Por sua vez, impende destacar a disposição do art. 22 (Brasil, 2018), o qual estabelece que "a defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente", bem como a disposição do art. 42 (Brasil, 2018), o qual estipula que o "controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo", ao passo que o art. 52 (Brasil, 2018) estabelece penas administrativas às eventuais infrações das disposições da Lei.

Portanto, em resumo das disposições apresentadas, a relação de consumo de jogos *mobile* ostenta todos os elementos caracterizadores da relação jurídica objeto da LGPD (Brasil, 2018), estando presente a figura do titular de dados pessoais, dos agentes de tratamento, a coleta de dados é realizada em território nacional, por meio dos dispositivos móveis, ao passo que, também, se destina ao oferecimento de bens e serviços ao sujeito do mesmo local, de modo que deverá atender aos deveres e condições dos artigos 7º, 9º, 18, 33 e 46, sob penas da aplicação do disposto nos artigos 22, 42 e 52.

Inobstante a breve exposição dos institutos normativos pertinentes, cabe ainda destacar a correlação da proteção de dados pessoais com as disposições de direito consumerista, como forma de dialogar com ambas as fontes e conferir proteção efetiva aos usuários de jogos *mobile*, objeto de análise do presente trabalho, motivo pelo qual destaca-se:

Contudo, antes da finalização do tópico, impende destacar algumas lições de Miragem (2019, p. 18), o qual assevera acerca da essencialidade da manifestação de vontade para permissão de tratamento de dados, conforme segue:

> O art. 5º, XII, da LGPD, em clara influência do Regulamento Geral europeu sobre proteção de dados, define o consentimento como 'manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada'. A rigor, seu significado se identifica com os requisitos que se exigem para a manifestação de vontade do consumidor capaz de vincular-lhe juridicamente. Sabe-se que nos negócios jurídicos de consumo, o silêncio não caracteriza anuência, tampouco convalida o abuso ou a ilicitude. A aceitação do consumidor sempre deve ser expressa, ainda que se possa interpretar, naquilo que não se lhe seja oneroso ou determine prejuízo, o consentimento tácito, segundo os usos. No caso do consentimento, para o tratamento de dados (art. 7º, I, da LGPD) observam-se requisitos substanciais e formais.

Ademais, ainda a respeito do consentimento, considerando que o direito à privacidade também possui uma dimensão de direito da personalidade, cabe salientar que o consentimento deve ser analisado sob o prisma substancial, de modo que a mera existência de um consentimento formal não autoriza tratamentos abusivos e violações legais, de modo que se deve interpretar as normas acerca do consentimento à luz da principiologia que rege os direitos da personalidade, devendo, de acordo com o caso, se encontrar um equilíbrio entre a liberdade negocial e a proteção dos direitos inerentes ao ser humano, neste sentido:

> A compreensão de que o fluxo informacional é (in)apropriado envolve, portanto, a limitação do consentimento, verificando-se qual é o impacto do trânsito das informações pessoais nas relações sociais do seu titular, em particular para o livre desenvolvimento da sua personalidade. Daí por que o consentimento do titular dos dados pessoais não deve ser um recurso para legitimar os mais abusivos e invasivos tipos de tratamentos de dados pessoais, coisificando-o. Essa interpretação está de acordo com a matriz normativa do CC que impõe limites à autonomia privada, em especial, na seara dos direitos da personalidade. […] A limitação voluntária dos direitos da personalidade é admitida em uma perspectiva de disponibilidade relativa por seu titular. No entanto, o grande desafio é parametrizar qual deve ser o sentido dessa liberdade, notadamente, quais são os limites impostos a tal esfera de autonomia relativa. Do seminal caso de arremesso de anão, passando-se pelos contratos vitalícios de patrocínio, do direito sobre o próprio corpo (body-art), da convicção religiosa em conflito com o direito à

> vida (testemunhas de jeová), dos programas de reality show, verifica-se que há uma tensão permanente em preencher o significado da referenciada disponibilidade relativa dos direitos da personalidade e, em especial, na maioria dos casos, dos limites da natureza negocial do consentimento dos seus titulares sobre a circulação comercial dos seus bens da personalidade (Bioni, 2021, p. 207-210).

Por sua vez, assevera Bruno Miragem que o tratamento de dados deve estar adstrito à finalidade específica e bem delimitada, esclarecida, consoante se observa:

> Da mesma forma há exigência legal expressa de que a manifestação de consentimento deve se dar em vista de finalidades determinadas para a utilização dos dados, sendo nulas as manifestações que se caracterizem como autorizações genéricas para o tratamento de dados (art. 8º, § 4º, da LGPD). Deste modo é correto entender que a declaração de vontade do titular dos dados vincula-se expressamente a certas e determinadas finalidades (Miragem, 2019 p. 18).

Por fim, vale asseverar que a LGPD (Brasil, 2018), dentre outros princípios, é regida pelo princípio da boa-fé, conforme art. 6º, caput, sem, no entanto, que seu conteúdo seja conceituado pela aludida lei, de modo que se mostra conveniente aplicar a teoria do diálogo das fontes, no sentido de convivência e aproveitamento, superando-se o paradigma de divisórias entre as normas, viabilizando o intercâmbio de conceitos, conforme prelecionado por Benjamin (2018, p. 27). Ato contínuo, nos ensinamentos de Tartuce (2021, p. 51), a boa-fé, no âmago do Código de Defesa do Consumidor se estabelece como um princípio essencial: a boa-fé objetiva, delineada detalhadamente no artigo 4º, inciso III. Este preceito fundamental da Política Nacional das Relações de Consumo visa a conciliação dos interesses dos envolvidos, equilibrando a proteção ao consumidor com o imperativo do desenvolvimento econômico e tecnológico, em conformidade com os princípios da ordem econômica estabelecidos no artigo 170 da Constituição Federal. Assim, é imprescindível que as relações comerciais no contexto consumerista se pautem pela busca constante de equilíbrio e harmonia entre consumidores e fornecedores durante todas as fases da transação.

Deste modo, à luz do diálogo das fontes e definição de boa-fé, evidencia-se a necessidade de adoção de conduta proba por parte dos fornecedores de jogos *mobile*, na constância da coleta e tratamento de dados, visando ao respeito das disposições, não somente da LGPD, como também de comandos normativos de demais áreas jurídicas, inclusive da principiologia constitucional.

Portanto, feitas as considerações necessárias acerca da LGPD, bem como de outros institutos normativos aplicáveis, voltada ao âmbito da pesquisa, além de apresentados institutos normativos relevantes ao desenvolvimento do trabalho, cabe adentrar à análise dos termos de política e privacidade das empresas fornecedoras de jogos eletrônicos.

4 Análise de políticas de privacidade sob a perspectiva da LGPD

Para fins de análise, diante do vasto repertório de jogos *mobile* e necessidade de delimitação da análise, elegeu-se, dentre os jogos com maior alcance de público, 02 (dois) títulos relevantes no mercado, a saber: *CANDY CRUSH SAGA*[5] e *POKÉMON GO*[6].

4.1 Política de privacidade de Candy Crush[7]

Em seu termo de política e privacidade, o qual, de acordo com o próprio documento disponibilizado pela fornecedora King, responsável pelo jogo Candy Crush, consta que a referida política se aplica "a todos os nossos jogos, sejam eles jogados em nosso site www.king.com, em dispositivos móveis, computadores ou em outras plataformas, como o Facebook. Também se aplica às nossas atividades de Marketing e Publicidade em todas as plataformas e outros serviços que podemos fornecer a você de tempos em tempos", logo em suas disposições introdutórias intituladas como "Jogando nossos jogos' apresenta quais dados serão coletados:

- detalhes sobre como você usa e interage com nossos jogos, publicidade e outros Serviços (por exemplo, informações sobre como e quando você joga nossos jogos ou visita nosso(s) site(s), qual dispositivo você usa para acessar nossos jogos e serviços ou detalhes sobre visitas de perfil, conforme estabelecido no Perfil King e jogando socialmente);
- informações que você nos fornece ao preencher formulários, responder a perguntas ou completar pesquisas usando qualquer um dos nossos Serviços, ao criar uma conta conosco, incluindo e-mail, ou ao convidar seus amigos a usarem nossos jogos e Serviços;

5 Documentação disponível por meio da página da loja de aplicativos da Google, conforme link adiante. Disponível em: https://play.google.com/store/apps/details?id=com.king.candycrushsaga

6 Documentação disponível por meio da página da loja de aplicativos da Google, conforme link adiante. Disponível em: https://play.google.com/store/apps/details?id=com.nianticlabs.pokemongo

7 Disponível em: https://www.king.com/pt_BR/privacyPolicy

- o conteúdo das mensagens enviadas usando nosso bate-papo e sistemas de mensagens;
- informações de uso caso participe em ferramentas de bate-papo por vídeo com outros usuários (conforme veremos mais adiante em Bate-papo por vídeo);
- se você entrar em contato conosco, por exemplo, através dos canais de atendimento ao cliente King Care, ou responder às mensagens e comunicações enviadas por nós, podemos manter um registro de tais correspondências;
- suas interações conosco em nossos canais de mídias sociais;
- informações que coletamos através de cookies e outras tecnologias similares, conforme explicado abaixo;
- informações conforme definidas nesta Política de Privacidade, incluindo o Perfil King e jogando socialmente, Marketing e Publicidade;
- informações que coletamos sobre você com outras empresas do grupo ou outras empresas terceiras que têm seu consentimento ou outro direito legal para compartilhar tais informações conosco (incluindo plataformas, parceiros de publicação, plataformas de publicidade, parceiros de publicidade e agregadores de dados). Isso pode incluir atributos sobre você e seus interesses, assim como outros jogos e serviços que você usa, informações demográficas e de localização geral. Nós utilizaremos essas informações conforme descrito nesta Política de privacidade e sujeito a quaisquer limitações na política de privacidade da empresa que coletou as suas informações.

Neste aspecto, observa-se o respeito às disposições dos artigos 7º e 9º, LGPD, vez que se encontram bem delimitados os dados que serão coletados, sua necessidade contratual, de forma específica e clara, possibilitando a compreensão dos objetos da coleta.

Ao seu turno, a aludida Política esclarece que a finalidade da coleta de dados consiste em:

- para permitir que forneçamos nossos jogos e outros Serviços a você, garantir que quaisquer compras realizadas sejam verificadas em nossos servidores e ativadas nos jogos e fornecer a você o suporte ao jogador, caso seja necessário;
- para permitir que possamos otimizar nossos jogos para você e para o dispositivo que utiliza, assim como fornecer eventos em jogo, ofertas e promoções personalizados;

> • Para outros fins, conforme definidos nesta Política de privacidade, incluindo fins de Marketing e Publicidade; e
>
> • para permitir que cumpramos com as leis que se aplicam a nós, evitar fraudes, garantir a conformidade com nossos termos de serviço ou, quando necessário, defender, exercer ou estabelecer nossos direitos legais conforme nossos Termos de serviço (https://king.com/termsAndConditions).

Novamente, se observa a adequação ao disposto no art. 9º, I, LGPD, diante da delimitação das finalidades da coleta dos dados.

Em continuidade, a fornecedora, ainda, afirma que "*também podemos compartilhar suas informações com editores terceiros que desenvolvem e fornecem jogos e outros Serviços para você, em seu nome*". Tal disposição, assim como as demais, necessita de consentimento, o qual é melhor abordado no desenvolver do texto.

Ademais, consta expressamente do referido documento mais disposições acerca do compartilhamento:

> Podemos usar as informações que mantemos sobre você para promover os próprios Serviços da King ou da Activision Blizzard, Inc ("Activision Blizzard") de diversas maneiras. Isso pode incluir:
>
> • publicidade em sites de terceiros, aplicativos e dispositivos de conexão à Internet;
>
> • exibir promoções para outros jogos da King ou da Activision Blizzard nos jogos que você joga; ou
>
> • enviar materiais de marketing por e-mail.

Nota-se que o compartilhamento, indicado no trecho supra, se refere tanto a terceiros como empresas do mesmo grupo econômico, o que, como qualquer atividade de tratamento, demanda um nível adequado de segurança, em especial quando os dados são transferidos para terceiros, diante da troca de base de dados, no entanto, os mecanismos de segurança adotados não são claros, conforme se explicará mais adiante.

Prosseguindo, a fornecedora dispõe sobre informações que serão utilizadas para marketing da seguinte forma:

> Usamos informações sobre você para tentar garantir que você veja apenas marketing nosso que possa ser do seu interesse. Isso inclui o uso de informações que possamos ter sobre você, como:
>
> • identificadores de anúncios e outras informações não pessoais coletadas do seu dispositivo. Para mais informações, veja Identificadores de anúncios, cookies e tecnologias similares;

- os jogos que você joga e informações sobre como você interage com nossos jogos e Serviços;
- sua idade, país ou região e sexo; e
- outras informações que possamos adquirir de nossos parceiros de marketing ou outros terceiros que obtiveram seu consentimento ou tiverem algum outro direito legal de compartilhar informações conosco.

Observa-se que no terceiro item, se explicita a uso, dos dados já coletados, acerca de idade e sexo, o que se mostra como dados sensíveis, haja vista que, na dicção do art. 5º, I, da LGPD, se definem como sensíveis aqueles dados sobre "dado genético ou biométrico, quando vinculado a uma pessoa natural", o que exige, nos termos do art. 11, I, o consentimento "de forma específica e destacada, para finalidades específicas", o que pode vir a se confrontar com as disposições da analisada política, especialmente, no que concerne ao consentimento, conforme se verifica adiante.

Quanto aos parceiros da fornecedora, bem como acerca do compartilhamento de dados com estes, consta que:

> Quando comercializamos nossos jogos em mídia publicada por outras empresas, usamos vários parceiros de marketing terceirizados para nos auxiliar em nosso nome, e poderemos compartilhar informações que coletamos sobre você com tais terceiros para esses propósitos.
>
> Nossos parceiros de marketing podem nos ajudar a direcionar anúncios para você ao combinar essas informações com dados que eles coletaram sobre você em outros lugares. Essas informações são coletadas quando você usa os serviços ou os sites e serviços de terceiros. Nossos parceiros usam essas informações para fazer suposições sobre os tipos de publicidade que você prefere ver. Se eles determinarem que você estaria interessado em ver um anúncio para os jogos ou Serviços da King, eles exibirão um anúncio da King enquanto você estiver usando outros sites e serviços.
>
> Ao aceitar esta Política de Privacidade e fazer o download ou continuar a jogar nossos jogos, e a menos que você escolha siar de anúncios baseados em interesse, como explicado nessa seção, você consente que nossos parceiros de marketing coletem e usem informações sobre você para aprimorar os sistemas de anúncios, direcionamento e medições como descrito em suas políticas de privacidade.

Quanto aos parceiros, logo adiante das disposições supra, a fornecedora disponibiliza a relação dos parceiros com os quais serão compartilhados dados do usuário, o que, nesta parte, se mostra em consonância com o art. 18, VII, LGPD, vez que é obrigação do controlador

indicar as entidades privadas com as quais ocorrer o compartilhamento. Incumbe destacar a obrigação instituída pelo § 6º do mesmo art. 18, o qual prevê que ao responsável pelo tratamento de dados incumbirá "informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional".

Por sua vez, no tópico denominado como "*Os seus direitos*", a fornecedora prevê os seguintes direitos ao usuário/titular de dados: a) Direito de acesso; b) Direito de corrigir informações pessoais; c) Eliminação de dados; d) Desativação da conta; e) Portabilidade de dados; f) Restrição de processamento; g) Direito de objeção; h) Desativar o marketing direto; i) Direito de optar por não participar (Califórnia, EUA). Logo, considerando que o último direito elencado não se aplica aos residentes em território nacional, constata-se a existência de 08 (oito) direitos, ao passo que o art. 18 da LGPD estipula 09 (nove), de modo que o único direito não previsto, nesta seção, corresponde ao direito de "confirmação da existência de tratamento", elencado junto ao art. 18, I, da LGPD. Cabe destacar que o referido direito deixado de lado é tão importante quanto os demais, impedindo que os titulares tenham a efetiva confirmação sobre o tratamento de seus dados pessoais.

A despeito da segurança dos dados, a fornecedora afirma que:

> A King adota medidas técnicas e de segurança adequadas para proteger as suas informações contra acesso não autorizado, perda e uso indevido. Além disso, solicitamos que nossos fornecedores que processam informações pessoais em nosso nome adotem uma série de medidas de segurança projetadas para ajudar a proteger as suas informações pessoais e manter um nível adequado de segurança. No entanto, não podemos garantir a segurança absoluta das suas informações online e offline, pois a Internet, por sua natureza, não é um ambiente seguro e a natureza dos riscos de segurança está em constante evolução. Como tal, você deve sempre tomar cuidado ao compartilhar suas informações online.

Deste modo, observa-se que a fornecedora não especifica quais medidas, exatamente, são adotadas para propiciar essa segurança para proteger os dados dos usuários, o que se mostra como uma violação ao art. 6º, caput e seu inciso VII, visto que a fornecedora não procede de boa-fé ao se limitar no esclarecimento dos procedimentos de segurança adotados, o

que, se devidamente esclarecido, possibilitaria controle e questionamento por parte dos usuários, vez que a segurança dos dados é essencial à proteção do direito à intimidade daqueles que se submetem aos serviços ofertados pela empresa, seus colaboradores e parceiros. Tal omissão não se justifica, vez que existem padrões, tais como as certificações da família ISO/IEC 2700,[8] que, caso já não estejam sendo adotados pela empresa (o que permanece como uma incógnita diante da não especificação pela fornecedora), poderão ser adotados e demonstrados para tentar garantir um padrão de segurança de qualidade, atendendo ao mencionado princípio da boa-fé, tendo em vista que, por expressa disposição do termo analisado, o aplicativo utiliza transferência internacional dos dados[9], o que, pela sua própria natureza, exige um padrão de segurança adequado e transparência/informação (decorrente da boa-fé e se consubstanciam como deveres laterais, conforme destacado por Gonçalves, 2020, p. 63) para com o consumidor/titular de dados, tendo em vista que as irregularidades no processo de transferência internacional podem ensejar violação ao art. 33, LGPD.

Por fim, como último aspecto relevante, a fornecedora aborda o consentimento do usuário da seguinte forma:

---

8 As normas da família ISO/IEC 2700 " *tratam da Segurança da Informação*", de modo que a norma ISO 27001 "*trata dos requisitos do Sistema de Gestão de Segurança da Informação (SGCI)*", e se destina à empresa, e não ao seu pessoal, sendo necessário que "*Para a obtenção da certificação, todas as áreas do SGSI devem estar em conformidade, de acordo com as diretrizes estabelecidas para fins de auditoria*", ao passo que, baseada em "*Plan-Do-Check-Act*" sua aplicação abrange "*todo e qualquer conteúdo e formato de dados*"; quanto à norma ISO 27002, esta "*estabelece as boas práticas de gestão e implementação de um sistema que objetiva garantir a Segurança da Informação, cuja questão também é tratada pela LGPD*", e "*pode ser utilizada pelas empresas como um parâmetro de garantia da gestão da segurança da informação e da proteção dos dados pessoais no âmbito da LGPD*", sendo que sua estruturação se subdivide em "*11 (onze) seções de controles de segurança da informação, que juntas totalizam 39 (trinta e nove) categorias principais de segurança, gestão e tratamento de riscos*"; Por fim, a norma ISO 27701, destinada à "*aprimorar o SGSI já existente nas organizações, com requisitos adicionais e que tratam especificamente da privacidade de dados*", viabiliza com que "*controladores e operadores, agentes de tratamento de dados (art. 5º., inciso VI a VIII) possam estabelecer mecanismos de controles de privacidade e redução de riscos de violação aos direitos da privacidade*", de modo que a aludida norma "*define os requisitos extras para um SGSI, a fim de proteger a privacidade e tratamento do que é denominado na norma de Personally identifiable information*", ultrapassando a mera proteção de dados com intuito de defender o direito à privacidade dos titulares dos dados pessoais. (FREITAS et al, 2020, p. 244-256). Assim, estas breves explicações evidenciam a importância de adoção de mecanismos de segurança par proteção dos dados pessoais coletados pelas empresas fornecedoras.

9 Extraído do termo analisado: "Podemos transferir suas informações para entidades afiliadas ou terceiros para jurisdições fora do EEE. Observe que estes países fora do EEE podem não ter as mesmas leis de proteção de dados que a sua jurisdição. Tomamos medidas para assegurar que existam salvaguardas e mecanismos adequados em vigor (incluindo o uso de cláusulas-modelo da UE) para permitir a transferência das suas informações para fora das fronteiras do EEE."

> Consentimento. Isto é usado como uma base legal nos seguintes contextos: (i) a coleta de dados armazenados em seu dispositivo por nós e nossos parceiros de anúncios, incluindo informações do dispositivo, endereço IP, país e região. Você consente a esta coleta quando concorda em instalar nosso jogo e pode revogar esse consentimento ao desinstalar nossos jogos; (ii) o armazenamento de dados em seu dispositivo por nós e nossos parceiros de anúncios, incluindo através do uso de cookies. Ao acessar e usar nossos Serviços, você concorda com esse armazenamento e você pode revogar esse consentimento ao atualizar suas configurações de cookie; e (iii) o uso de seus dados por nós e nossos parceiros para propósitos de anúncios direcionados (para mais informações, veja Marketing e Anúncios, acima). Você concorda com essa coleta quando aceita esta Política de Privacidade e você pode revogar esse consentimento a esse processamento ao seguir os passos em Como ajustar suas preferências para anúncios baseados em interesse. Onde pedirmos por seu consentimento para usar seus dados para qualquer outro propósito, iremos deixar isso claro no momento da coleta e também deixaremos claro como você poderá revogar seu consentimento.

Observa-se que, predominantemente, é interpretado pela fornecedora que houve o consentimento com o simples uso do serviço, isto é, com a instalação e inicialização do aplicativo, ocorre que, conforme destacado nos tópicos anteriores, o consentimento deve ser expresso, salvo, em situações excepcionais, e que não gerem prejuízo ao consumidor titular dos dados, em que se admite a manifestação tácita. No entanto, a possível controvérsia pode se manifestar em relação ao prejuízo ao consumidor, visto que, de início, o simples processo de coleta e tratamento de dados não poderia, em tese, ser interpretado como algo prejudicial ao titular, porém, na ocorrência de eventuais perdas, vazamentos ou subtração destes dados, com ou sem algum grau de culpa do fornecedor, é possível indagar: qual seria a validade daquele consentimento, se o processo de coleta se inicia com a simples instalação e inicialização (Sendo que, logicamente, a instalação é ato obrigatório para se desfrutar do serviço).

Portanto, encerrando a análise dessa política de privacidade, se verificou o cumprimento de várias disposições da LGPD, no entanto, também, se contatou algumas inadequações e obscuridades, as quais são relevantes e devem ser questionadas, diante do caráter fundamental do direito à privacidade, que, novamente, merece atenção e proteção jurídica adequada.

4.2 Política de privacidade de Pokemon GO[10]

Logo em suas disposições introdutórias, a fornecedora *Niantic*, responsável pelo software Pokemon GO, estabelece o controlador dos dados coletados por meio de seu produto:

> A Niantic, Inc. (1 Ferry Building Suite 200, São Francisco, CA 94111) é geralmente a controladora de dados responsável pela tomada de decisões sobre como usamos as suas informações pessoais. Se, no entanto, você estiver localizado no Reino Unido (RU), na Rússia ou no Espaço Econômico Europeu (EEE), o seu controlador de dados é a Niantic International Limited no RU (11º Andar, Whitefriars, Lewins Mead, Bristol ,Reino Unido, BS1 2NT).

Neste aspecto, observa-se que a controladora se encontra sedeada em território estrangeiro, apresentando indícios de necessidade de transferência internacional dos dados coletados.

Adiante, a fornecedora informa os dados que serão objeto de coleta durante a utilização de seus serviços:

> Você deve ter uma conta com um serviço externo suportado de logon único para utilizar nossos Serviços. Dessa forma, os Dados Pessoais que coletamos dependem também das contas externas que você escolhe usar, da política de privacidade dessas contas e daquilo que as suas definições de privacidade com esses serviços nos permitem ver quando você usa seus serviços para acessar os Serviços Niantic. Se você optar por vincular sua conta do Google aos Serviços, iremos coletar o seu endereço de e-mail do Google e um token de autenticação fornecido pelo Google. Se você optar por vincular sua conta no Facebook aos serviços, nós iremos coletar uma ID única de usuário fornecida pelo Facebook e, se autorizado por você, o seu e-mail registrado no Facebook. Se você optar por vincular sua conta da Apple aos Serviços, coletaremos seu endereço de e-mail arquivado com a sua conta Apple ID ou um endereço de e-mail retransmitido privado se você usar a opção Ocultar Meu E-mail fornecida pela Apple. Dependendo do Serviço específico no qual você se inscrever, podemos suportar outros serviços externos de logon único e deles coletar Dados Pessoais adicionais. Para mais detalhes, leia as Divulgações de Jogos Específicos no final desta Política de Privacidade. Alguns fornecedores externos podem notificá-lo de que nos disponibilizam informações adicionais, tais como o seu perfil público, quando você usa os serviços de logon único desses fornecedores. Nós não coletamos essas informações deles.

10 Disponível em: https://nianticlabs.com/privacy/pt_br/

Acerca dos dados e seus respectivos modos de coleta, conforme disposições supra, constata-se que a fornecedora faz uso de mecanismos de terceiros para autenticação e acesso ao serviço/produto, o que sujeita o processo de coleta de dados à políticas desses outros fornecedores, de modo que, conforme destacado anteriormente, a depender de qual serviço será utilizado pelo titular, o citado processo de coleta pode sofrer alterações quanto ao seu objeto e meios, sem, no entanto, que sejam especificadas e devidamente esclarecidas consequências de tais intercorrências.

Outrossim, destacam, ainda, a fornecedora que a se faz necessária coleta de informações sobre a localização dos usuários, coma finalidade de cumprir com as disposições do termo de uso, neste sentido:

> Nós coletamos e usamos informações de localização do seu dispositivo conforme você usa nossos Serviços (e, se você opta por ativar o rastreamento em segundo plano para nossos Serviços, enquanto você não está interagindo diretamente com os Serviços), incluindo a forma como você se locomove e eventos que ocorrem durante o jogo. Nossos serviços incluem jogos baseados em localização, cuja funcionalidade principal é fornecer uma experiência de jogo vinculada à sua localização no mundo real, então precisamos saber onde você está para operar estes jogos para você e para planejar a localização de recursos no jogo (por exemplo, PokéStops dentro do Pokémon GO). Nós identificamos sua localização usando uma série de tecnologias, incluindo GPS, os pontos de WiFi por meio dos quais você está acessando o Serviço e triangulação de torres de celular.

Quanto à disposição em epígrafe, nota-se que o meio para coleta de informação de localização do usuário é bem contumaz, não restando dúvida da precisão na coleta, justamente, pelas tecnologias empregadas, o que culmina, praticamente, no mapeamento da rotina de locomoção de um indivíduo e, indiretamente, na fixação e previsão de suas preferências e necessidades, ostentando potencial ofensivo ao direito à privacidade. Logo, essa espécie de dado, ainda que não seja considerado como sensível, possui um caráter extremamente relevante, merecendo proteção adequada por parte da fornecedora, a qual deve prezar por sua segurança.

Por sua vez, no tópico subsequente, a fornecedora prevê que, respaldada em legítimo interesse, dentre outras finalidades inerentes à prestação de serviço, os dados pessoais poderão ser utilizados para:

> Para personalizar os anúncios que você vê em nossos aplicativos para torná-los mais relevantes para você, e para mostrar mensagens de presentes patrocinados e/ou ofertas de nossos anunciantes relevantes para a sua vizinhança no mapa do jogo. Você pode optar por não

> receber presentes patrocinados visitando as configurações do aplicativo. Você pode optar por cancelar os anúncios personalizados visitando as configurações do seu dispositivo e ativando "Limitar o Rastreamento de Anúncios" em dispositivos Apple ou ativando "Cancelar a Personalização de Anúncios" em dispositivos Android.

Incumbe destacar que esta previsão corrobora com a afirmação dos parágrafos anteriores, de modo que reforça a necessidade de propiciar mecanismos adequados de segurança desses dados, pois, conforme já salientado, são informações que traçam um perfil do titular de dados, evidenciando aspectos inerentes à intimidade daquele indivíduo.

Ao seu turno, a fornecedora destaca quais serão os dados coletados, bem como seus modos, de acordo com consentimento do titular, sendo estes: a) rastreamento de atividade em segundo plano (anteriormente citado); b) amigos usuários do Facebook; c) dados de atividade física; dentre outros. Impende analisar, com maior acurácia, a disposição acerca da coleta de dados de atividade física, em conjunto à disposição acerca do consentimento do titular, o qual não possui regulamentação específico no documento analisado, de modo que não constam, exatamente, o modo pelo qual ocorrerá tal manifestação de vontade, diferente do que se observou no termo de política e privacidade de *Candy Crush*, anteriormente examinado. Inobstante a ausência de disposição sobre o consentimento, observa-se que, acerca da coleta de dados sobre atividade física, a fornecedora estipula que:

> Com a sua permissão, usamos o app de saúde do seu dispositivo (HealthKit Apple, se você usar um dispositivo Apple, ou Google Fit, se você usar um dispositivo Android) para coletar seus dados de atividade física: nós lemos e/ou gravamos os seus dados de atividade física no app de saúde do seu dispositivo para operar o rastreamento de atividade em segundo plano e para garantir que você obtenha "crédito" no app de saúde do seu dispositivo por toda a caminhada que você faz enquanto joga os nossos jogos. Nós não utilizamos os dados coletados por meio do Health Kit ou do Google Fit para fins de marketing ou publicidade. Nossos Serviços não podem ler ou gravar no app de saúde do seu dispositivo sem o seu consentimento. Você pode mudar de ideia e desabilitar nosso acesso a qualquer tipo de dado de atividade física a qualquer momento nas suas configurações do app Apple Health ou Google Fit no seu dispositivo.

Logo, observa se tratar de um dado pessoal sensível, previsto pelo art. 5º, II, LGPD, de modo que deve ser coletado, nos termos do art. 11, I, deve ser consentido "de forma específica e destacada", no entanto,

conforme já mencionado, não constam previsões sobre como este tipo de consentimento, nem de outros, ocorrerá, acarretando violação às disposições da LGPD.

Quanto ao compartilhamento dos dados, afirma a fornecedora que, em suma, não serão compartilhados dados pessoais, exceto nos seguintes casos: a) Informações Compartilhadas com nossos Prestadores de Serviços; b) Informações Compartilhadas com Outros Jogadores; c) Informações Compartilhadas com Terceiros; d) Informações Divulgadas para Nossa Proteção e a Proteção de Terceiros; e) Informações Divulgadas no tocante a Transações Comerciais. No entanto, de acordo com próprio documento, não constam disposições acerca do consentimento específico, tampouco sobre respaldo em eventual hipótese legal de dispensa do consentimento. Outrossim, nos termos do art. 7º, §5º, da LGPD,[11] existe a necessidade de consentimento específico do titular para compartilhamentos de dados, exceto nos casos previstos em lei, o qual não é previsto pelo referido termo, remetendo ao problema da ausência de regulamentação do consentimento, de modo que, novamente, em razão da ausência de previsão do modo como ocorrerá este consentimento específico, bem como sua efetivação, gera violação à disposição da LGPD. Ademais, nos termos do art. 18, §2º, mesmo em se tratando de eventual hipótese de dispensa de consentimento, diante do descumprimento das disposições da aludida Lei, o titular poderá se opor ao tratamento realizado.

Avançando pela análise, em relação à transferência de dados, dispõe a fornecedora que:

> A Niantic opera seus Serviços em todo o mundo. Seus Dados Pessoais provavelmente serão transferidos e armazenados em um país fora de seu país de origem, incluindo os Estados Unidos da América, para os fins descritos nesta Política de Privacidade, na medida permitida pelas leis aplicáveis. As leis de proteção de dados nesses países podem não ser as mesmas que no seu país de origem. Se nós transferirmos seus Dados Pessoais do RU ou do EEE para outros países, incluindo os Estados Unidos da América, nós garantimos que será dado aos seus Dados Pessoais um grau de proteção semelhante ao do RU ou do EEE, conforme aplicável, assegurando que pelo menos uma das seguintes salvaguardas seja implementada […]

11 § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

Nesta disposição, se constata um grave confronto com as previsões da LGPD, visto que a fornecedora não garante que o país destinatário da transferência possui o mesmo, ou superior, nível de proteção, nem são oferecidas garantias contratuais pela fornecedora, de modo a violar o disposto no art. 33, LGPD. Por sua vez, cabe se atentar que disposições semelhantes às exigências do art. 33 estão previstos somente aos residentes junto ao RU e EEE, em que pese a plena aplicabilidade da LGPD, diante da coleta em território nacional, evidenciando, assim, o desrespeito à Lei brasileira.

Adiante, a respeito da segurança dos dados coletados, a fornecedora afirma, tão somente, que:

> Nós temos medidas de segurança legais, organizacionais e técnicas adequadas para evitar que seus Dados Pessoais sejam perdidos acidentalmente, usados ou acessados de forma não autorizada ou alterados ou divulgados indevidamente. Nós também limitamos o acesso aos seus Dados Pessoais a funcionários, agentes, contratados e outros terceiros que tenham necessidade comercial de conhecê-los. Eles somente processarão os seus Dados Pessoais de acordo com as nossas instruções e estarão sujeitos a um dever de confidencialidade. Colocamos em prática procedimentos para lidar com qualquer suspeita de violação de Dados Pessoais e iremos notificar você e qualquer regulador aplicável de uma violação quando estivermos legalmente obrigados a fazê-lo.

Deste modo, observa-se que a fornecedora, assim como a fornecedora do tópico anterior, não especifica quais medidas, exatamente, são adotadas para propiciar essa segurança aos dados dos usuários, o que se mostra como uma violação ao art. 6º, caput e seu inciso VII, visto que a *Niantic*, igualmente, não procede de boa-fé ao se limitar no esclarecimento dos procedimentos de segurança adotados, o que, se devidamente esclarecido, possibilitaria controle e questionamento por parte dos usuários, vez que a segurança dos dados é essencial à proteção do direito à intimidade daqueles que se submetem aos serviços ofertados pela empresa, seus colaboradores e parceiros. Tal omissão, também, não se justifica, vez que existem padrões, como mencionado anteriormente, tais como normas da família ISO/IEC 2700, que, caso já não estejam sendo adotados pela empresa (o que permanece como uma incógnita diante da não especificação pela fornecedora), poderão ser adotados e demonstrados para tentar garantir um padrão de segurança e qualidade, atendendo ao mencionado princípio da boa-fé, vez que o tratamento de dados pessoais, pela sua própria natureza, exige um padrão de segurança adequado e

transparência/informação (decorrente da boa-fé e se consubstanciam como deveres laterais, consoante Gonçalves, 2020, p. 63).

Por fim, cabe analisar o cumprimento da disposição do art. 9º, VII, o qual obriga que o fornecedor faça constar, de forma clara, os "direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei". A despeito da questão, a fornecedora prevê que:

> Você pode: Solicitar acesso aos Dados Pessoais que temos sobre você, enviando um e-mail para privacy@nianticlabs.com. Deletar ou corrigir seus Dados Pessoais. A forma mais fácil de atualizar as informações da sua conta é através das suas configurações de aplicativo. Você também pode enviar uma solicitação de suporte ao cliente através de nosso site de suporte aqui para Pokémon Go, aqui para Ingress, ou aqui para Harry Potter: Wizards Unite. Solicitar-nos que paremos de processar seus Dados Pessoais, incluindo para fins diretos promocionais e de publicidade, como recompensas personalizadas, promoções e outras ofertas, enviando um e-mail para opt-out@nianticslabs.com. No entanto, esteja ciente de que às vezes precisamos utilizar seus Dados Pessoais para fornecer os Serviços para você). Ter seus Dados Pessoais transferidos para outra organização (quando isso for tecnicamente viável). Reclamar para um regulador. Nós apreciaríamos a oportunidade de lidar com suas preocupações diretamente, então preferimos que você fale conosco primeiro. No entanto, se você estiver localizado no RU ou no EEE e acreditar que nós não cumprimos a legislação de proteção de dados, você pode reclamar com sua autoridade fiscalizadora local. A lei prevê exceções a esses direitos em determinadas circunstâncias. Quando você não puder exercer um desses direitos devido a uma tal exceção, nós iremos explicar-lhe o porquê. Oferecemos a você opções relativamente à coleta, utilização e compartilhamento dos seus Dados Pessoais e respeitaremos as escolhas que você fizer. Observe que se você decidir não nos fornecer os Dados Pessoais que solicitamos, você pode não ser capaz de acessar todos os recursos dos Serviços. Depois de entrar em contato conosco, você receberá um e-mail para verificar sua solicitação. Temos o objetivo de fornecer as informações ou de concluir o resultado que você solicitar no prazo de 30 dias, ou um período de tempo mais curto, conforme previsto pelas leis de sua jurisdição.

Observa-se que não foram respeitados os incisos I, IV, VII, do art. 18, os quais, respectivamente preveem que é direito do titular: a) "confirmação da existência de tratamento"; b) "anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei" e c) "informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados", de modo a violar o art. 9º, VII, anteriormente mencionado. Portanto, verificou-se

diversas violações à LGPD, contidas no termo de política e privacidade da fornecedora *Niantic*, responsável pelo jogo *Pokemon GO*.

5 Conclusão

Diante do desenvolvimento da temática, em especial pela análise das políticas de privacidade, em dois jogos eletrônicos: *Candy Crush* e *Pokémon GO*, observou-se que ainda subsistem inadequações nas práticas adotadas pelas fornecedoras analisadas, de modo que incumbe, a estas, alterações e adaptações aos comandos normativos anteriormente destacados, tendo em vista que, inegavelmente, se sujeitam à LGPD, nos termos de seu art. 3º, o que as obrigam ao atendimento das exigências legais e seus deveres anexos, sob pena de sua responsabilização.

Outrossim, constatou-se que, com a regulamentação da LGPD, o direito à privacidade passou a contar com proteção mais eficiente, voltada, principalmente à sociedade da informação e novas tecnologias que, inevitavelmente, ameaçam um dos direitos mais importantes ao ser humano. Como efeito, o Brasil, em termos jurídicos, se posiciona ao encontro de estado estrangeiros que buscam tutelar a proteção de dados, tal como a comunidade europeia, por meio da GRPD.

Deste modo, frente às violações da LGPD que, por sua vez, regulamenta o Direito constitucional à Privacidade e encontra lastro junto à Declaração Universal de Direitos Humanos, enseja a responsabilização das empresas sob o olhar aludidas normas, ensejando aplicação de sanções administrativas pela ANPD, tais como multas, visando à efetivação dos direitos dos jogadores em solo brasileiro.

Por sua vez, as penalidades administrativas não eximem as empresas da responsabilização judicial, a qual poderá ser carreada por meio de tutelas coletivas, tais como Ação Civil Pública (art. 1º, II e IV c/c art. 5º, Lei 7.347/85) (Brasil, 1985) e Ações Cíveis pautadas no art. 81 e seguintes do CDC (Brasil, 1990), ocasiões em que poderão ser exigidos valores a título de indenização e imposição de obrigação de fazer, consubstanciados na retificação da políticas das empresas destinadas à adequação e conformidade com as disposições da LGPD.

Ademais, com a ultimação do presente trabalho, atingiram-se os objetivos, inicialmente estipulados, ao passo que se logrou êxito no aprofundamento da problemática introduzida nos tópicos inaugurais,

sendo razoável concluir que o presente trabalho cumpriu com sua finalidade.

Por fim, convêm apontar que, diante da vastidão do mercado de jogos *mobile*, se mostra oportuno continuar, em ocasiões futuras, a análise das práticas adotadas pelas empresas do ramo, visto que, conforme reiteradamente destacado, o direito à privacidade é extremamente relevante ao ser humano e merece proteção justa e adequada.

Referências

BENJAMIN, Antônio Herman; MARQUES, Cláudia Lima. A Teoria do Diálogo das Fontes E Seu Impacto no Brasil: Uma Homenagem a Erik Jayme. Revista de Direito do Consumidor. Vol. 115. ano 27. p. 21-40. São Paulo: Ed. RT, jan.-fev. 2018.

BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. – 3. ed. – Rio de Janeiro: Forense, 2021.

BORGES, Diego. Pandemia faz consumo de jogos disparar e mercado procura profissionais. TECMUNDO. 2020. Disponível em: https://www.tecmundo.com.br/voxel/207292-pandemia-consumo-jogos-disparar-mercado-procura-profissionais.htm Acesso em: Acesso em: 27 set. 2025.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm Acesso em: 27 set. 2025.

BRASIL. Lei nº 7.347, de 24 de julho de 1985. Lei de Ação Civil Pública. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm Acesso em: Acesso em: 27 set. 2025.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm Acesso em: 27 set. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 27 set. 2025.

CANDY CRUSH SAGA; Google Play, 2021. Disponível em: https://play.google.com/store/apps/details?id=com.king.candycrushsaga&pli=1 Acesso em: 27 set. 2025.

CARVALHO, Alexander Perazo Nunes de; LIMA, Renata Albuquerque de. A eficácia horizontal dos direitos fundamentais. Revista Opinião Jurídica (Fortaleza), v. 13, n. 17, p. 11-23, 2015.

CLEMENT, Jessica. *Mobile* games publishers - Statistics & Facts. Statista. 2021. Disponível em: https://www.statista.com/topics/4104/mobile-games-publishers/ Acesso em: 27 set. 2025.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E SUAS REPERCUSSÕES NO DIREITO BRASILEIRO. 1ª ed. São Paulo. Revista dos Tribunais. 2019.

FREITAS, Cinthia Obladen de Almendra; SANTOS, Henrique Guilherme; PASINATO, Rita. A SEGURANÇA DA INFORMAÇÃO COMO FERRAMENTAL TÉCNICO DA PROTEÇÃO DE DADOS PESSOAIS. Direito e inovação. - Curitiba: OABPR, 2020.

GAMINGSCAN. 2020 Gaming Industry Statistics, Trends & Data. Disponível em: https://www.gamingscan.com/gaming%20-%20statistics/ Acesso em: 27 set. 2025.

GONÇALVES, Carlos Roberto. Contratos e atos unilaterais. Coleção Direito civil brasileiro volume 3 – 17. ed. – São Paulo: Saraiva Educação, 2020.

MARCACINI, Augusto Tavares Rosa. Comentários à lei geral de proteção de dados: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019 / coordenadora Cíntia Rosa Pereira de Lima. – São Paulo: Almedina, 2020.

MCGRATH, Rita. Business Models: A Discovery Driven Approach, 2010, Long Range Planning, v.43, pp. 247- 261.

MIRAGEM, Bruno. A LEI GERAL DE PROTEÇÃO DE DADOS (LEI 13.709/2018) E O DIREITO DO CONSUMIDOR. Revista dos Tribunais, vol. 1009/2019, p. 173 – 222, nov/ 2019.

NAKAHIRA, Ricardo. Eficácia horizontal dos direitos fundamentais. Dissertação Mestrado. Pontifícia Universidade Católica De São Paulo. São Paulo. 2007.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos, 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos Acesso em: 26 maio 2025.

PIOVESAN, Flávia. Direitos humanos e o direito constitucional

internacional. – 18. ed., rev. e atual. – São Paulo: Saraiva Educação, 2018.

POKÉMON GO, Google Play, 2021. Disponível em: https://play.google.com/store/apps/details?id=com.nianticlabs.pokemongo Acesso em: 27 set. 2025.

SARLET, Ingo Wolfgang. Curso de direito constitucional/Ingo Wolfgang Sarlet, Luiz Guilherme Marinoni, Daniel Mitidiero. – 10. ed. – São Paulo: Saraiva Educação, 2021.

SILVA, Leonardo Ferreira; PINHEIRO, Matheus Dias; SANTOS, Rick Rodrigues dos; SCHIMIGUEL, Juliano. O CRESCIMENTO DOS JOGOS NO MERCADO *MOBILE* E SUAS ACESSIBILIDADES. Revista Caribeña de Ciencias Sociales. Fev, 2016.

SUPERDATA, A NIELSEN COMPANY. Data is great. A game plan is even better. Disponível em: https://www.nielsen.com/pt/insights/2021/the-future-of-video-gaming-is-bright-even-as-real-experiences-return/ Acesso em: 27 set. 2025.

TARTUCE, Flávio. Manual de Direito do Consumidor: direito material e processual, volume único. – 10. ed. – Rio de Janeiro: Forense; Método, 2021.

WAKKA, Wagner. Mercado de games agora vale mais que indústrias de música e cinema juntas. CANALTECH. 2021. Disponível em: https://canaltech.com.br/games/mercado-de-games-agora-vale-mais-que-industrias-de-musica-e-cinema-juntas-179455/ Acesso em: 27 set. 2025.

CONSIDERAÇÕES FINAIS

O GEDDIG, desde a sua origem, reconhece que as discussões sobre o Direito Digital não se reduzem à aplicação de normas ou à leitura literal de leis recentes. A área exige um exercício constante de interpretação, crítica e criação — uma hermenêutica da Era Digital. Os estudos reunidos neste livro são frutos desse movimento coletivo de pensamento que busca dar nome às incertezas e sentido aos riscos.

Ao refletirmos sobre o Direito Digital, reconhecemos que o verdadeiro desafio não está apenas em regular tecnologias, mas em compreender o que elas revelam sobre nós: nossas vulnerabilidades, nossos desejos, nossa relação com o poder e com o espaço e o tempo. A Inteligência Artificial, a vigilância algorítmica, o consumo de dados e a mediação total da vida pelas plataformas são expressões de uma sociedade que espelha suas próprias contradições no meio ambiente digital.

Muito embora a tecnologia seja um elemento presente na trajetória evolutiva da raça humana, não sendo esta estranha ao Direito, a ciência jurídica e sua eterna função de regular as relações sociais, cada vez mais se funde ao elemento tecnológico, inspirando a criação e formatação deste novo ramo, o Direito Digital. E, nesse sentido, buscaram os autores contribuir para que as relações sociais, em meio às inovações tecnológicas, encontrem reflexos éticos e morais positivos, capazes de conduzir tais relações a um platô de bem-estar social, digno e humano.

Deste modo, temos aqui um conjunto de considerações finais que, para além de estabelecer um panorama do livro, oferecem um fechamento e uma conexão entre os artigos. Os artigos têm como ponto central um aporte teórico que se debruça sobre as interações entre as sociedades informacional e tecnológica, por meio de todos os aparatos e dispositivos eletrônicos, digitais e móveis disponíveis na sociedade contemporânea e acessíveis por uma gama variada de usuários e consumidores com diferentes níveis de conhecimento e letramento digital, *digital literacy*.

Consideramos, assim, a construção de um ecossistema digital a partir deste universo de dispositivos interconectados não apenas entre si, mas que também se conecta e influi nas relações humanas, de modo profundo. Por isto, o Direito Digital passa a conceber um novo estágio de organização social que pode ser identificado como o "Socioambientalismo Digital", ou seja, a integração plena entre as Sociedades que tradicionalmente

conhecemos por meio do desenvolvimento das relações humanas no mundo e ecossistema natural em que vivemos, agregando-se, ainda, o elemento tecnológico que lhe introduz o meio ambiente digital.

A interação entre as sociedades informacional e tecnológica, vale ressaltar, oferece riscos que desafiam o próprio compreender destas sociedades, de modo a se propor uma nova leitura da sociedade de risco agora em meio digital, não mais somente sob os aspectos ambientais. Há que se compreender a sociedade de risco digital. E, é nesta sociedade que urge pensar em um ciberespaço de não-coisas, diante da complexidade dos algoritmos ora aplicados nas mais diversas áreas visando a solução de problemas do dia a dia do ser humano, o qual vive imerso em *bits* (zeros e uns).

Ao se tratar sobre riscos, o livro apresenta também uma discussão sobre *robots* (*bots*) e o contexto dos usuários-consumidores no que se refere a *bots* maliciosos que oferecem riscos, uma vez que a atuação desses agentes automatizados, com capacidade de disseminar informações enganosas e manipular decisões de compra, evidencia um cenário de vulnerabilidade que compromete princípios fundamentais do Código de Defesa do Consumidor – CDC, especialmente os direitos à informação verídica e à proteção contra práticas abusivas.

Não há como dissociar o Direito Digital dos direitos informacionais, da proteção de dados pessoais, da necessidade de regulação e da proteção efetiva aos direitos fundamentais que estão primariamente conectados à dignidade da pessoa humana, especialmente dos mais vulneráveis. Aqui a preocupação recai sobre as crianças e adolescentes, que para além dos direitos da criança e da proteção jurídica necessitam de um olhar de cuidado especialmente diante de questões relacionadas à pornografia infantil, ao aliciamento e abuso infanto-juvenil para que se alcance o disposto no Estatuto da Criança e do Adolescente (ECA) sem discriminação de nascimento, situação familiar, idade, sexo, raça, etnia ou cor, religião ou crença, deficiência, condição pessoal de desenvolvimento e aprendizagem, condição econômica, ambiente social, região e local de moradia ou outra condição que diferencie as pessoas, as famílias ou a comunidade em que as crianças e os adolescentes vivem.

Entre as temáticas urgentes e necessárias ao Direito Digital não se poderia esquecer do tema de Inteligência Artificial. Os sistemas de Inteligência Artificial estão estabelecendo uma nova camada na sociedade contemporânea, ou seja, a sociedade de algoritmos. E algoritmos não

faltam, estão no reconhecimento facial aplicado na área de Segurança Pública, nos jogos *mobile* que estabelecem políticas de privacidade que violam o direito à proteção de dados pessoais e em *deepfakes* e *deep nudes* envolvendo crianças e adolescentes. Há que se lançar mão da Lei Geral de Proteção de Dados Pessoais (LGPD), sem esquecer de outros instrumentos do ordenamento jurídico brasileiro, a exemplo de: Constituição Federal, Código Civil, Código de Defesa do Consumidor (CDC), Marco Civil da Internet, Estatuto da Criança e do Adolescente (ECA), entre outros.

O contexto de mudanças e adaptações gerou também a necessidade de transformação digital nas cooperativas, as quais, diante da pandemia de COVID-19, precisaram realizar as assembleias gerais de modo virtual, mantendo ao mesmo tempo os princípios cooperativos. Em verdade, a aceleração da transformação digital provocada pela pandemia de COVID-19 não foi um processo apenas benéfico, visto apresentar riscos, agravando riscos já existentes, expandindo deste modo a sociedade risco para os aspectos tecnológicos e digitais.

Cabe, portanto, ao Direito Digital questionar: que Internet é esta que permite acesso e conectividade sem limites, mas que, por outro lado, está saturada de conteúdos automatizados, diminuindo a autenticidade das interações e criando uma esfera digital artificial e manipuladora? Questionou-se: A *web* está morta? Se não há pessoas gerando conteúdo, mas em sua maioria são os robôs - *bots* (programas automatizados que interagem de maneira autônoma com usuários *online*) que geram os conteúdos, o que está acontecendo com as interações humanas? Será que o humano ainda está a sobressair ao Metaverso?

Há quem diga que o Metaverso morreu, visto que o humano não deseja viver e conviver em representações, em modelos ou em mundos paralelos. O ser humano ainda almeja viver e conviver com outros seres humanos em sociedade. E eis aqui o maior desafio da participação cívica e da inclusão social que precisa ser contrabalanceado pela necessidade de regulação e responsabilidade no meio ambiente digital diante de uma cibercultura fundada por meio de não-espaço, de não-coisas.

Ainda há esperança?

Sim, precisa haver esperança. E o Direito Digital desempenhará, cada vez mais, um importante papel no que se refere à regulação das novas tecnologias e à mitigação de riscos, sempre considerando os impactos nos seres humanos.

Finalmente, sem ter resposta conclusiva, mas permitindo um exercício epistemológico, há que se questionar: Será o Direito Digital o ramo do Direito que possibilitará a efetiva interseção entre o código lei e o código fonte, de modo a se estabelecer o código-lei-fonte? Caberá aos estudiosos seguir desbravando este caminho, por vezes tortuoso e desconhecido, mas com certeza desafiador e necessário.

Direito Digital: Temáticas Urgentes e Necessárias reúne textos produzidos no âmbito do Grupo de Estudos em Direito Digital (GEDDIG), espaço dedicado à análise crítica das transformações jurídicas provocadas pelo avanço das Tecnologias de Informação e Comunicação (TIC) e, mais recentemente, da Inteligência Artificial. Compreendendo o Direito Digital como campo que regula normas, processos e relações surgidos da interação entre indivíduos, tecnologias e o ambiente digital, o grupo investiga temas que atravessam a sociedade contemporânea, marcada pela informação, vigilância, transparência, algoritmos e riscos tecnológicos. Nesse cenário, conceitos como ciberespaço, não-coisas, dados digitais e hiperconectividade desafiam noções tradicionais de materialidade, territorialidade, temporalidade e pessoalidade, exigindo novas leituras do Direito e de suas instituições. Desde sua criação, o GEDDIG acompanha debates sobre proteção de dados, direitos fundamentais, segurança da informação, Inteligência Artificial, responsabilidade civil e os impactos da sociedade de algoritmos. Suas atividades incluem reuniões de estudo, eventos científicos e produção acadêmica que fortalecem o diálogo interdisciplinar e ampliam o entendimento jurídico sobre fenômenos digitais cada vez mais complexos. Este livro apresenta resultados dessas reflexões e propõe ao leitor uma travessia pelos desafios que emergem da interseção entre Direito e Tecnologia. Mais do que interpretar o presente, a obra convida a pensar novos paradigmas jurídicos necessários para um mundo estruturado por dados, códigos, fluxos informacionais e relações que se constroem e se transformam no ciberespaço.

ISBN 978-656135204-8

EDITORA
ILUSTRAÇÃO