Brasília 2025

ISBN: 978-85-7267-234-4

Direito, Tecnologia e Inovação:
Estudos e Perspectivas Contemporâneas da Era Digital

Organização: Bárbara Ohanna dos Santos Veloso

CEUB

ISBN: 978-85-7267-234-4

CEUB

Direito, Tecnologia e Inovação:
Estudos e Perspectivas Contemporâneas da Era Digital

Organização: Prof. Bárbara Ohanna dos Santos Veloso
Arte: Joelson Araujo Silva dos Santos
Assistência: Milene da Silva Costa

Brasília
2025

CENTRO UNIVERSITÁRIO DE BRASÍLIA - CEUB

Reitor
Pio Pacelli Moreira Lopes

Coordenador do curso de Direito
Daniel Amin Ferraz

Dados Internacionais de Catalogação na Publicação (CIP)

Direito, tecnologia e inovação: estudos e perspectivas contemporâneas da era digital / organizador, Bárbara Ohanna dos Santos Veloso – Brasília: CEUB, 2025.

609 p.

ISBN 978-85-7267-234-4

1. Direito digital. I. Centro Universitário de Brasília. II. Título.

CDU 34:004.02

Ficha catalográfica elaborada pela Biblioteca Reitor João Herculino

APRESENTAÇÃO

O acelerado avanço tecnológico tem transformado de maneira irreversível a dinâmica social, econômica e jurídica da contemporaneidade. A integração de tecnologias digitais à vida cotidiana, seja por meio de sistemas algorítmicos, inteligência artificial, plataformas digitais, big data ou dispositivos inteligentes, deixou de ser uma tendência futura para se tornar uma realidade concreta e estruturante das relações humanas. Em um mundo cada vez mais conectado, no qual decisões são mediadas por dados, códigos e automação, torna-se indispensável compreender os efeitos sociais e jurídicos que emergem desse novo ecossistema digital.

É nesse contexto que se insere o livro Direito, Tecnologia e Inovação, Estudos e Perspectivas Contemporâneas da Era Digital, elaborado pelos estudantes do curso de Direito do UniCEUB, Centro Universitário de Brasília, como resultado das atividades acadêmicas desenvolvidas na disciplina Direito, Tecnologia e Inovação (DTI). A obra reúne um conjunto de artigos produzidos ao longo do semestre, que refletem não apenas o rigor teórico e a análise normativa exigida pelo campo jurídico, mas também as inquietações, percepções e contribuições pessoais dos discentes diante das transformações tecnológicas em curso.

Cada capítulo aborda, sob diferentes perspectivas, os desafios regulatórios, éticos e constitucionais que permeiam temas como proteção de dados pessoais, cibersegurança, inteligência artificial, governança digital, algoritmos, desinformação, economia digital, plataformas, responsabilidade civil e penal no ambiente virtual, entre tantos outros fenômenos que impactam diretamente direitos fundamentais e estruturas democráticas. A produção aqui apresentada demonstra não apenas domínio conceitual, mas também sensibilidade crítica diante dos riscos e oportunidades produzidos pela inovação tecnológica.

Assim, este livro cumpre dupla função, de um lado, contribui para o debate acadêmico e jurídico sobre os rumos da sociedade digital, diante do olhar pessoal dos autores, de outro, reafirma o compromisso com uma formação jurídica

contemporânea, interdisciplinar e alinhada às demandas reais de um mundo em constante transformação. Ao reunir diferentes olhares sobre um mesmo cenário, a obra evidencia que compreender a tecnologia é compreender o avanço do Direito e da sociedade, e que pensar juridicamente o futuro exige dialogar com as mudanças que já moldam o presente.

Que esta leitura inspire reflexões, provoque novos debates e construção de soluções jurídicas inovadoras, éticas e socialmente responsáveis. Afinal, o Direito, ao lado da tecnologia, continua sendo uma das ferramentas mais potentes para a promoção de justiça, inclusão e cidadania em um mundo cada vez mais digital.

Professora: Bárbara Ohanna dos Santos Veloso

AUTORES

Ágatha Ruiz Pinheiro Torres de Florambel
Alana Karoline Andrade
Allana Almeida de Oliveira
Alicia Alexandre de Sousa
Amanda Muniz Godoy Modesto
Ana Beatriz Amaral
Ana Beatriz Soares Lima
Ana Júlia Sarauza Castro
Ana Júlia Silva
Ana Thereza Santana Pessoa
Anne Louise Morais Gomes
Ariely Vitória Lopes Lima
Barbara Moon
Bruna Aquino
Bruno Vinicius Carvalho
Carlos Abraão Zimmerman Araújo
Carolina Almeida Alavrenga
Cibely Maria Pires de Oliveira
Cláudio da Silva Souza
Daniel Martins Moreira Lana
Daniela de Brito Olinto
Eduardo Ceolin da Silva Menna Barreto
Eduardo Rodrigues Miranda Martins
Emilly de Alcântara Cordeiro
Enrico Rizotto Senedese
Éryn Sousa Aguiar
Felipe Martins Obliziner
Filipe Moura da Silva
Gabriel Machado Oliveira Fagundes
Gabriela França da Costa
Gabriela Teixeira Honorato
Giovana Andressa Leite Alves
Giovana Brito Carrijo Costa
Giovana Gomes Barros
Gustavo Cauã Alves de Oliveira
Gustavo Gonçalves de Castro Marques
Heráclito Frederico Crisnamurth de Jesus
Iasmin Soares
Isabela Saraiva Faria
João Francisco Santana Madella
João Henrique Escobar Costa
João Pedro Garcia de Araújo Gomes
Joelson Araujo Silva dos Santos
Jussey Marcos Vargas Monterio
Kalyne Aryane Melo Xavier
Karen Menéndez
Kauann Gabriel Silva Alves
Kemille Christine Araújo de Sousa
Laís Carla Conceição Bezerra
Laís Eduarda Leal da Fonseca
Larissa Maria de Figueiredo
Letícia Silva Costa
Letícia Sol Barbosa
Lorena Portilho Bruno
Lucca de Sousa Ribeiro
Lucas Caetano Leão
Lucas Krisney Lima de Oliveira
Lucas Limone
Luciana Geralda Silva Duarte
Luisa Lopes Margato
Luísa Helena Pereira dos Santos
Luiz Arthur Batista de Figueiredo
Maísa Anaisse Ribeiro
Maira Heloísa Amarante Silveira
Maria Clara Tamashiro Bego
Maria Eduarda França
Maria Fernanda Siebra da Silva
Maria Luísa Barbosa Guerra
Maria Luísa de Castro Queiroz
Mariana Marques
Marina Lara Parreira
Marcus Vinícius de Oliveira Bastos Goulart
Matheus Caiado Tosta
Max Efraim Bianchi Godoy
Melissa Braga
Naylani James
Natália Sousa Maciel
Nicole Lopes Marinho Bandeira
Nicolle de Castro Oliveira
Nilsa Antonia de Oliveira
Pedro Henrique de Souza Mertins
Rafael Tadeu Simões Barreto
Ramon Santana Morel Gomes de Oliveira
Rodrigo Moreira de Oliveira
Sofia Fortes Soares Dutra Moraes
Sofia Viana do Vale
Stephanie da Fonseca Soares
Thiago Max Diego Xavier Silva
Victor Matias Andrade Monteiro
Vinicius Augusto de Oliveira Feitoza

SUMÁRIO

PARTE I – INTELIGÊNCIA ARTIFICIAL, RESPONSABILIDADE E DIREITOS FUNDAMENTAIS.....12

A CONSTITUCIONALIDADE DO EMPREGO DE INTELIGÊNCIA ARTIFICIAL NA JUSTIÇA CRIMINAL: RISCOS DE VIOLAÇÃO AO DEVIDO PROCESSO LEGAL E À IMPARCIALIDADE.....13
Daniel Martins Moreira Lana

IA E A CRIAÇÃO DE CONTEÚDO ILÍCITO: DESAFIOS NA PROTEÇÃO DE MENORES.....34
Luisa Lopes Margato

O USO DA INTELIGÊNCIA ARTIFICIAL E A ATRIBUIÇÃO DE RESPONSABILIDADE NO COMBATE AO PLÁGIO.....47
Anne Louise Morais Gomes; Maria Clara Tamashiro Bego; Kalyne Aryane Aryane Melo Xavier

INTELIGÊNCIA ARTIFICIAL E ALGORITMOS: O NOVO DESAFIO PARA O DIREITO DA CONCORRÊNCIA.....58
Ramon Santana Morel Gomes de Oliveira

PROTEÇÃO DE DADOS E INTELIGÊNCIA ARTIFICIAL: ENTRE A INOVAÇÃO E A TUTELA DOS DIREITOS FUNDAMENTAIS NA ERA LGORÍTMICA.....68
Eduardo Rodrigues Miranda Martins

INTELIGÊNCIA ARTIFICIAL E PROTEÇÃO DE DADOS SENSÍVEIS EM DOCUMENTOS SIGILOSOS E RESTRITOS: O PAPEL DA LGPD NO SETOR PÚBLICO E PRIVADO.....94
João Pedro Garcia de Araujo Gomes

COMO ESTÁ A REGULAÇÃO DE IA NO BRASIL?.....110
Cláudio da Silva Souza; Heráclito Frederico Crisnamurth de Jesus Miranda; Júlio César Alves Lima; Rodrigo Moreira de Oliveira; Thiago Max Diego Xavier Silva

RESPONSABILIDADE CIVIL NAS VIOLAÇÕES AO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS: UMA ANÁLISE DA JURISPRUDÊNCIA BRASILEIRA.....124

Alicia Alexandre de Sousa; Ana Júlia Sarauza Castro; Gabriel Machado Oliveira Fagundes; Lucca de Sousa Ribeiro

PARTE II – PROTEÇÃO DE DADOS PESSOAIS, PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO.....144

SEÇÃO 2.1 – FUNDAMENTOS E DESAFIOS ESTRUTURANTES DA LGPD.....145

A IMPORTÂNCIA DA PROTEÇÃO DE DADOS PESSOAIS PARA O EXERCÍCIO DA CIDADANIA DIGITAL NO ESTADO DEMOCRÁTICO DE DIREITO: ANÁLISE DO CENÁRIO CONTEMPORÂNEO.....146
Allana Almeida de Oliveira

A COLETA DE DADOS PESSOAIS E OS DESAFIOS ENVOLVENDO PRIVACIDADE E SEGURANÇA.....158
Lucas Krisney Lima de Oliveira

CONSENTIMENTO OU COERÇÃO? UMA LEITURA CRÍTICA DA LGPD: ENTRE AUTONOMIA, ARQUITETURA DE ESCOLHAS, PROPORCIONALIDADE E GOVERNANÇA.....174
Felipe Martins Obliziner; Larissa Maria de Figueiredo

***DATA BROKERS* E PROTEÇÃO DE DADOS PESSOAIS: UMA ANÁLISE PRINCIPIOLÓGICA.....190**
Melissa Braga; Rafael Tadeu Simões Barreto

ENGENHARIA SOCIAL E VULNERABILIDADES HUMANAS: COM A LEI GERAL DE PROTEÇÃO DE DADOS CONTRIBUI PARA A CIBERSEGURANÇA.....213
Nicolle de Castro Oliveira; Victor Matias Andrade Monteiro

SEÇÃO 2.2 – LGPD EM SETORES ESPECÍFICOS.....223

A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NO SETOR DA SAÚDE BRASILEIRA: DESAFIOS E IMPLICAÇÕES.....224
Gabriela França da Costa; Gabriela Teixeira Honorato; Isabela Saraiva Faria; Matheus Caiado Tosta

PROTEÇÃO DE DADOS SENSÍVEIS NA SAÚDE SUPLEMENTAR SOB A ÓTICA DA LGPD: OS LIMITES DO TRATAMENTO DE INFORMAÇÕES PELOS PLANOS DE SAÚDE DIANTE DA FINALIDADE CONTRATUAL E DA VEDAÇÃO À PRÁTICAS ABUSIVAS E DISCRIMINATÓRIAS.....238

Kemille Christine Araújo de Sousa; Luciana Geralda Silva Duarte; Sofia Fortes Soares Dutra Moraes; Stephanie da Fonseca Soares

A OPACIDADE NOS PLANOS DE SAÚDE PRIVADOS: DESAFIOS AO ACESSO DO BENEFICIÁRIO À INFORMAÇÃO À LUZ DA LGPD E DA LAI.....257
Luísa Helena Pereira dos Santos

ANÁLISE DA COLETA DE FOTOS EM CADASTRO PARA ACESSO A LOCAIS PÚBLICOS SEGUNDO OS FUNDAMENTOS E PRINCÍPIOS DA LGPD.....265
Éryn Sousa Aguiar; Filipe Moura da Silva; Giovana Gomes Barros; Melissa Braga

RECONHECIMENTO FACIAL EM CONDOMÍNIOS: LIMITES E RISCOS À LUZ DA LGPD.....283
Enrico Rizotto Senedese

O TRATAMENTO DE DADOS PESSOAIS PELO FISCO: CONVERGÊNCIAS NORMATIVAS, TENSÕES CONSTITUCIONAIS E DESAFIOS PRÁTICOS NA COMPATIBILIZAÇÃO ENTRE LGPD E O SIGILO FISCAL.....295
Maísa Anaisse Ribeiro

CONSTRUINDO CONFIANÇA SOCIAL: COMO OS ÓRGÃOS DE EMERGÊNCIA PODEM DIVULGAR SUAS AÇÕES RESPEITANDO A LGPD.....309
Lucas Caetano Leão; Nilsa Antonia de Oliveira

MEU INSS: FACILIDADE DIGITAL OU FONTE DE INSEGURANÇA NO PLANEJAMENTO DA APOSENTADORIA?.....322
Daniela de Brito Olinto

PARTE III – DIREITO DIGITAL, CIBERCRIMINALIDADE E SEGURANÇA.....328

CRIMES CIBERNÉTICOS: A EFICÁCIA DAS LEGISLAÇÕES BRASILEIRAS.....329
Bárbara Moon

CIBERCRIME CONTRA CRIANÇAS E ADOLESCENTES: ADULTIZAÇÃO.....344
Karen Menéndez; Leticia Sol Barbosa; Mariana Marques

A PEDOFILIA NAS REDES SOCIAIS CONTRA CRIANÇAS E ADOLESCENTES DO SEXO FEMINO.....358
Carolina Almeida Alavrenga; Letícia Silva Costa

GOLPES CONTRA IDOSOS A PARTIR DE INFORMAÇÕES PROCESSUAIS PÚBLICAS.....372
Laís Eduarda Leal da Fonseca

A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NAS ATIVIDADES DE INVESTIGAÇÃO POLICIAL.....385
Ana Thereza Santana Pessoa

DIREITO E TECNOLOGIA: A RESPONSABILIDADE DAS PLATAFORMAS, O DEVER DE CUIDADO E O ENFRENTAMENTO AOS CIBERCRIMES, COM ÊNFASE NA PROTEÇÃO INTEGRAL DE CRIANÇAS E ADOLESCENTES.....397
Ariely Vitória Lopes Lima; Bruna Aquino Carvalho; Maria Luísa Barbosa Guerra; Naylani James de Oliveira; Sofia Viana do Vale

***DEEPFAKE* E O DIREITO BRASILEIRO: DESAFIOS CONTEMPORÂNEOS DA MANIPULAÇÃO DIGITAL E DA TRANSFORMAÇÃO TECNOLÓGICA.....424**
Maria Fernanda Siebra da Silva; Natália Sousa Maciel; Nicole Lopes Marinho Bandeira

PARTE IV – TRANSPARÊNCIA, PUBLICIDADE E GOVERNO DIGITAL.....443

A TENSÃO ENTRE A PUBLICIDADE DOS ATOS PROCESSUAIS E A PROTEÇÃO DE DADOS PESSOAIS.....444
Ana Júlia Guimarães Ferreira da Silva; Anna Beatriz Dias Amaral; Iasmin de Freitas Soares; Maria Eduarda França Fernandes Beserra

ACESSO E REGULAMENTAÇÃO DAS INFORMAÇÕES PÚBLICAS: OS IMPACTOS DA LEI 12.527/2011 NOS ATOS DE GESTÃO PÚBLICA.....458
Luiz Arthur Batista de Figueiredo; Max Efraim Bianchi Godoy

O "PL DA DEVASTAÇÃO" E O USO DE DADOS.....471
Giovana Brito Carrijo Costa; Laís Carla Conceição Bezerra; Marina Lara Parreira; Pedro Henrique de Souza Mertins; Lorena Portilho Bruno

O USO DA INTELIGÊNCIA ARTIFICIAL NO PODER JUDICIÁRIO.....504
Eduardo Ceolin da Silva Menna Barreto; Lucas Limone

DIREITO ELEITORAL E DIGITAL NO COMBATE À DESINFORMAÇÃO.....518
Maria Luísa de Castro Queiroz; João Francisco Santana Madella

PARTE V – ECONOMIA DIGITAL, CONSUMO E COMÉRCIO ELETRÔNICO.....529

LGPD E COMÉRCIO ELETRÔNICO: PROTEÇÃO DO CONSUMIDOR EM AMBIENTE DIGITAL.....530
Ana Beatriz Soares Lima; Bruno Vinicius Carvalho; Gustavo Gonçalves de Castro Marques

E-COMMERCE E SEUS DESAFIOS NA COLETA E ARMAZENAMENTO DE DADOS DE CLIENTES.....542
Emilly de Alcântara Cordeiro

EXCLUSÃO DIGITAL: A NOVA FACE DA DESIGUALDADE SOCIAL NO BRASIL.....557
Ágatha Ruiz Pinheiro Torres de Florambel; Alana Karoline Andrade; Giovana Andressa Leite Alves

PARTE VI – APOSTAS ESPORTIVAS, TECNOLOGIA E REGULAÇÃO..574

APOSTAS ESPORTIVAS, MANIPULAÇÃO DE RESULTADOS E RESPONSABILIDADE PENAL: UMA ANÁLISE À LUZ DOS CASOS PAQUETÁ E BRUNO HENRIQUE E OS DESAFIOS JURÍDICOS DIANTE DA INOVAÇÃO TECNOLÓGICA NAS "BETS".....575
Amanda Muniz Godoy Modesto; Cibely Maria Pires de Oliveira; Gustavo Cauã Alves de Oliveira; João Henrique Escobar Costa; Kauann Gabriel Silva Alves; Marcus Vinícius de Oliveira Bastos Goulart Cruz; Vinicius Augusto de Oliveira Feitoza e Leite de Oliveira

REGULAÇÃO, VÍCIO E IMPACTOS SOCIAIS: APOSTAS ESPORTIVAS DIGITAIS NO BRASIL.....584
Carlos Abraão Zimmerman Araújo B.; Maira Heloísa Amarante Silveira;
Jussey Marcos Vargas Monterio

A REGULAMENTAÇÃO DAS APOSTAS ESPORTIVAS ONLINE E A RESPONSABILIDADE DOS INFLUENCIADORES DIGITAIS NO BRASIL: UMA ANÁLISE LEGAL E PUBLICITÁRIA.....598
Joelson Araujo Silva dos Santos

PARTE I - INTELIGÊNCIA ARTIFICIAL, RESPONSABILIDADE E DIREITOS FUNDAMENTAIS

A CONSTITUCIONALIDADE DO EMPREGO DE INTELIGÊNCIA ARTIFICIAL NA JUSTIÇA CRIMINAL: RISCOS DE VIOLAÇÃO AO DEVIDO PROCESSO LEGAL E À IMPARCIALIDADE

Daniel Martins Moreira Lana[1]

RESUMO

Este trabalho investigou a compatibilidade do emprego de sistemas de inteligência artificial na justiça criminal brasileira com os princípios constitucionais do devido processo legal e da imparcialidade. O problema da pesquisa consistiu em saber se a utilização dessas tecnologias respeita às garantias constitucionais fundamentais. Partiu-se da hipótese de que a adoção não regulamentada de inteligência artificial pode violar as normas constitucionais, como o devido processo legal, a ampla defesa e a imparcialidade judicial, em razão de riscos como viés algorítmico e opacidade decisória. A metodologia empregada foi a abordagem qualitativa, com análise dedutiva de doutrina, legislação e jurisprudência nacional e internacional. Os objetivos específicos foram: apresentar os fundamentos constitucionais do processo penal aplicáveis à análise da IA; descrever os usos e riscos da IA na justiça criminal; analisar criticamente sua compatibilidade com a Constituição e propor diretrizes para uma regulamentação adequada.

Palavras-chave: Inteligência Artificial; Processo Penal; Constitucionalidade; Imparcialidade; Transparência Algorítmica.

Sumário: Introdução. 1. Fundamentos constitucionais do processo penal. 2. Inteligência artificial na justiça criminal: usos e riscos. 2.1. Conceito de inteligência artificial e justiça preditiva. 2.2. Experiências internacionais no uso da IA no processo penal. 2.3. Primeiras iniciativas de uso de IA na justiça brasileira. 2.4. Riscos de discriminação algorítmica no processo penal. 2.5. O problema da opacidade dos algoritmos e a crise da transparência. 3. A constitucionalidade do uso de inteligência artificial no processo penal. 3.1. A compatibilidade da IA com o princípio da imparcialidade. 3.2. O risco de violação ao princípio da ampla defesa e do contraditório. 3.3. A inconstitucionalidade do uso de sistemas opacos e não auditáveis. Considerações finais. Referências.

---

[1] O autor é aluno do Centro Universitário de Brasília - UniCEUB e cursa o 10º semestre de Direito; endereço eletrônico: daniel.lana@sempreceub.com. Trabalho apresentado como exigência para aprovação na disciplina Direito, tecnologia e inovação.

1 INTRODUÇÃO

A ascensão da inteligência artificial (IA) tem provocado transformações significativas em diversos setores da sociedade, inclusive no Judiciário, onde se observa a crescente incorporação dessa tecnologia na tomada de decisões e na gestão processual. No cenário jurídico, observa-se uma crescente incorporação de sistemas de IA para fins de apoio à tomada de decisões judiciais, otimização de processos e previsão de comportamentos.

Segundo Laurent Alexandre (2018), a inteligência artificial inaugurou uma era de profundas reconfigurações sociais, políticas e jurídicas, exigindo reflexão crítica sobre seus impactos em direitos fundamentais. No entanto, quando se trata da esfera criminal, essas inovações levantam preocupações específicas, sobretudo quanto à preservação dos direitos e garantias assegurados pela Constituição Federal de 1988 e pelos instrumentos normativos que regem o processo penal brasileiro.

O emprego da inteligência artificial no processo penal suscita questionamentos relevantes sobre sua compatibilidade com princípios estruturantes do Estado Democrático de Direito, como o devido processo legal, a ampla defesa, o contraditório, a presunção de inocência e a imparcialidade do julgador. Conforme alerta Virgílio Afonso da Silva (2017), “qualquer inovação que toque o processo penal deve ser cuidadosamente filtrada pelos princípios constitucionais, sob pena de comprometer a legitimidade da persecução penal.”

A automatização de decisões judiciais em matéria penal, sem o devido controle constitucional, pode gerar violações graves aos direitos individuais e coletivos, além de reproduzir ou até ampliar desigualdades sociais preexistentes, como demonstrado por Virginia Eubanks (2018)[2] em suas análises sobre algoritmos e marginalização.

Nesse contexto, a presente pesquisa se justifica pela necessidade de se refletir criticamente sobre a constitucionalidade da utilização da IA na justiça criminal, analisando os riscos de violação a princípios processuais penais fundamentais.

[2] Livro de Virginia Eubanks: "Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor"

Conforme destaca Pedro Lenza (2022), "o princípio do devido processo legal é cláusula pétrea do ordenamento jurídico brasileiro, sendo intolerável qualquer forma de mitigação ou flexibilização de garantias processuais em nome da eficiência ou da inovação tecnológica."

Delimita-se, portanto, como objeto de estudo, a investigação acerca do uso da inteligência artificial especificamente na justiça criminal, não abrangendo sua aplicação em áreas cíveis, trabalhistas, administrativas ou outras. A análise se concentrará no impacto da IA no processo penal, avaliando em que medida essa tecnologia pode comprometer ou fortalecer a efetividade dos direitos fundamentais no âmbito do processo criminal.

A partir dessa delimitação, formula-se a seguinte pergunta de pesquisa: O emprego de sistemas de inteligência artificial na justiça criminal brasileira é compatível com o devido processo legal e a imparcialidade exigidos pela Constituição Federal? Busca-se, assim, analisar criticamente a constitucionalidade dessas ferramentas à luz dos princípios processuais penais e dos direitos fundamentais, identificando riscos e propondo caminhos para uma utilização juridicamente adequada da tecnologia.

Quanto à metodologia, a pesquisa será desenvolvida por meio de abordagem qualitativa, com base em levantamento e análise de fontes doutrinárias nacionais e internacionais, legislação vigente, bem como em decisões judiciais que envolvam o tema. Será utilizado o método dedutivo, partindo da análise das normas constitucionais e processuais para a avaliação dos impactos da inteligência artificial no processo penal.

Por fim, a estrutura do trabalho está dividida em três capítulos. No primeiro capítulo, serão apresentados os fundamentos constitucionais que regem o processo penal, com enfoque nos princípios do devido processo legal, ampla defesa, contraditório, presunção de inocência e imparcialidade. No segundo capítulo, será abordada a aplicação prática da inteligência artificial na justiça criminal, seus usos, riscos e implicações processuais.

No terceiro capítulo, proceder-se-á à análise crítica da constitucionalidade da utilização da IA no processo penal, considerando possíveis violações e sugerindo

diretrizes para uma regulamentação compatível com a ordem constitucional. O trabalho se encerra com a conclusão, na qual serão sintetizados os resultados obtidos e apresentadas considerações finais sobre a pesquisa.

2 FUNDAMENTOS CONSTITUCIONAIS DO PROCESSO PENAL

O processo penal brasileiro é estruturado a partir de princípios constitucionais fundamentais que visam proteger os direitos dos indivíduos diante do poder punitivo estatal.

Esses princípios não apenas moldam o rito processual, mas servem como garantias de justiça, equidade e imparcialidade, especialmente importantes em um contexto de crescente automação das decisões judiciais por meio de sistemas de inteligência artificial. Assim, compreender essas bases constitucionais é essencial para avaliar a compatibilidade da aplicação de tecnologias com os direitos fundamentais previstos na Constituição Federal de 1988.

O princípio do devido processo legal, insculpido no artigo 5º, inciso LIV, da Constituição Federal, estabelece que "ninguém será privado da liberdade ou de seus bens sem o devido processo legal". Trata-se de uma cláusula essencial que garante ao indivíduo a possibilidade de ser processado e julgado conforme um conjunto prévio de regras legítimas e imparciais.

Segundo José Afonso da Silva (2014), o devido processo legal apresenta uma dupla dimensão: formal, referida à necessidade de respeito a procedimentos previamente estabelecidos; e material, que impõe a razoabilidade e a justiça das próprias leis.

Ambas as dimensões são fundamentais quando se analisa o emprego de sistemas de IA no processo penal, pois algoritmos que decidem questões penais de forma automática, sem transparência e possibilidade de controle, podem comprometer a legitimidade do processo.

Luigi Ferrajoli (2002) reforça que, no Estado Democrático de Direito, o processo penal deve atuar como uma barreira contra o exercício arbitrário do poder

punitivo. O uso da IA sem mecanismos de controle rigorosos pode ameaçar essa barreira, já que decisões automatizadas podem escapar ao controle humano efetivo, violando a exigência de um devido processo substantivamente justo.

O contraditório e a ampla defesa, previstos no artigo 5º, inciso LV, são instrumentos indispensáveis para assegurar o equilíbrio processual. A ampla defesa inclui o direito de o acusado ser assistido por advogado, enquanto o contraditório implica o direito de participar ativamente da formação da prova e da decisão.

Ada Pellegrini Grinover (2001) ressalta que o contraditório não se limita ao conhecimento dos atos processuais, mas também compreende a possibilidade de influenciar a formação do convencimento do juiz. Quando sistemas de IA são utilizados para gerar decisões ou recomendações no processo penal sem que as partes possam compreender e questionar seus fundamentos, há uma violação direta desses princípios.

Daniel Sarmento (2007) alerta para os riscos da "opacidade algorítmica" no processo judicial, uma vez que decisões baseadas em sistemas de IA, especialmente aqueles classificados como “caixa-preta”, impedem a atuação efetiva da defesa, restringindo a possibilidade de impugnar fundamentos ou contestar a validade das decisões.

Assim, para que a adoção de IA no processo penal esteja em conformidade com os princípios constitucionais, é indispensável que seus mecanismos sejam auditáveis, transparentes e passíveis de contestação pelas partes.

A presunção de inocência, assegurada pelo artigo 5º, inciso LVII, da Constituição, estabelece que ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória. Trata-se de uma das garantias mais importantes do processo penal democrático. Guilherme de Souza Nucci (2017) destaca que a presunção de inocência não é apenas uma regra probatória, mas também um princípio que exige um tratamento respeitoso e não discriminatório ao acusado em todas as fases do processo.

Em um contexto de uso de inteligência artificial, a preocupação com a presunção de inocência é ainda mais evidente. Ferramentas preditivas, como os

algoritmos de avaliação de risco de recidiva, podem induzir julgamentos antecipados sobre a periculosidade ou culpabilidade do réu, com base em dados estatísticos e não em provas concretas individualizadas.

Michele Taruffo (2002) ressalta que a prova penal deve ser individualizada e construída de forma racional, não podendo se basear em generalizações estatísticas que, embora possam ser eficientes em outros ramos da ciência, não atendem às exigências da verdade processual penal.

O princípio da imparcialidade do julgador e o princípio do juiz natural, previstos nos incisos XXXVII e LIII do artigo 5º da Constituição Federal, garantem que as partes serão julgadas por autoridade competente, previamente estabelecida por lei e isenta de interesses no conflito. Para Michele Taruffo (2002), a imparcialidade é um componente essencial da legitimidade do processo. A confiança na justiça depende da percepção de que o julgador não tenha vínculos ou preferências em relação às partes.

No contexto do uso de IA, a imparcialidade pode ser afetada por vieses algorítmicos presentes nos dados de treinamento ou incorporados nos próprios modelos de decisão. Luciana Boiteux (2020) alerta que algoritmos utilizados no sistema de justiça criminal podem reforçar discriminações históricas e comprometer a neutralidade necessária às decisões judiciais, caso não sejam cuidadosamente auditados e supervisionados.

Além disso, o uso de inteligência artificial não elimina a necessidade do juiz humano responsável por validar e fundamentar as decisões, respeitando as garantias processuais e evitando a delegação irrestrita da função jurisdicional a sistemas automatizados.

A igualdade, princípio basilar da ordem constitucional brasileira, está expressa no artigo 5º, caput, da Constituição Federal, e exige tratamento igualitário a todos que se encontram na mesma situação jurídica. Para Ingo Wolfgang Sarlet (2019), “a igualdade formal deve ser complementada pela igualdade material, reconhecendo e combatendo desigualdades fáticas que afetam o exercício de direitos fundamentais”.

No processo penal, a tutela da igualdade implica combater práticas discriminatórias, especialmente aquelas que, de forma velada, podem surgir através do uso de novas tecnologias. Cathy O'Neil (2016) demonstra como algoritmos, ao serem treinados em dados históricos contaminados por preconceitos, tendem a perpetuar discriminações raciais, socioeconômicas e de gênero, agravando desigualdades estruturais.

Nesse sentido, a adoção de sistemas de IA no processo penal deve ser precedida de rigorosa análise de impacto discriminatório, exigindo-se transparência nos critérios de decisão e mecanismos de correção de eventuais distorções.

3 INTELIGÊNCIA ARTIFICIAL NA JUSTIÇA CRIMINAL: USOS E RISCOS

A ascensão da inteligência artificial (IA) no cenário jurídico, especialmente no âmbito do processo penal, representa uma transformação sem precedentes, ao mesmo tempo promissora e desafiadora. A aplicação da IA na justiça criminal busca trazer maior eficiência, celeridade e previsibilidade às decisões, mas, por outro lado, suscita sérias preocupações quanto à proteção dos direitos fundamentais, à imparcialidade e à transparência do processo. Este capítulo examina essas dinâmicas, oferecendo um panorama conceitual, prático e crítico do uso da inteligência artificial na justiça penal.

A inteligência artificial pode ser conceituada, segundo Russell e Norvig (2010), como "o ramo da ciência da computação que se ocupa da construção de agentes inteligentes, sistemas que percebem seu ambiente e tomam ações para maximizar suas chances de sucesso em determinado objetivo". Essa definição destaca a autonomia decisória das máquinas e sua capacidade de adaptar-se a diferentes cenários.

No contexto jurídico, e especificamente no processo penal, a IA tem sido empregada principalmente em ferramentas de justiça preditiva, que buscam antecipar comportamentos futuros, como a probabilidade de reincidência de um réu, a tendência a descumprir medidas cautelares ou o risco de periculosidade.

Daniel Limongi França (2020) explica que a justiça preditiva consiste na utilização de algoritmos para analisar grandes volumes de dados jurídicos e formular previsões sobre decisões ou comportamentos, oferecendo aos operadores do Direito elementos que podem auxiliar na tomada de decisão. Entretanto, a natureza probabilística da justiça preditiva entra em tensão com princípios constitucionais essenciais, como a presunção de inocência, a ampla defesa e a individualização da pena.

Ademais, como pontua André de Carvalho Ramos (2021), o sistema penal democrático brasileiro é orientado pelo princípio da culpabilidade, que exige a responsabilização com base em atos concretos e não em riscos futuros hipotéticos. Assim, o uso da IA para prever comportamentos pode implicar um grave retrocesso, transformando o processo penal de um instrumento de garantias em um mecanismo de controle preventivo.

Em síntese, a IA aplicada à justiça criminal busca aumentar a eficiência, mas levanta importantes dilemas éticos e jurídicos, principalmente relacionados à segurança jurídica, ao contraditório, ao devido processo legal e à proteção contra decisões automatizadas injustas.

3.1 Experiências internacionais no uso da ia no processo penal

Diversos países têm experimentado o uso de sistemas automatizados no âmbito criminal. Um dos exemplos mais discutidos é o software COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), desenvolvido pela empresa norte-americana Northpointe (atualmente Equivalent).

O COMPAS é utilizado para avaliar o risco de reincidência de réus criminais e orientar decisões de liberdade condicional e sentenças. No entanto, estudos realizados pela organização ProPublica (2016) revelaram que o COMPAS apresentava viés racial, superestimando o risco de reincidência entre pessoas negras e subestimando entre pessoas brancas. Julia Angwin e colegas mostraram que "os algoritmos que deveriam ser neutros replicaram e ampliaram discriminações já existentes no sistema" (Angwin et al., 2016).

Outro exemplo é o uso de algoritmos de "risk assessment" em estados como Kentucky e Arizona, nos EUA. Apesar da promessa de decisões mais objetivas e eficientes, Danielle Citron (2016) alerta que a falta de transparência e a impossibilidade de questionamento dos critérios de decisão violam direitos fundamentais, como o devido processo legal e o contraditório.

Na União Europeia, o Regulamento Geral sobre a Proteção de Dados (GDPR) exige que indivíduos sejam informados sobre a lógica envolvida em decisões automatizadas que os afetem, além de garantir o direito à intervenção humana, o que reflete uma maior preocupação com a proteção de direitos em face da inteligência artificial.

Essas experiências internacionais servem de alerta para os riscos do uso acrítico de tecnologias similares no Brasil, onde as desigualdades raciais e sociais são ainda mais acentuadas, podendo resultar na amplificação de injustiças históricas.

3.2 Primeiras iniciativas de uso de IA na justiça brasileira

No Brasil, o uso de inteligência artificial no Judiciário ainda é incipiente, mas vem crescendo, impulsionado pelo Programa Justiça 4.0, lançado pelo Conselho Nacional de Justiça (CNJ) em 2020. Esse programa busca modernizar a Justiça brasileira por meio da utilização de tecnologias emergentes, como big data, IA e automação de processos.

Entre os exemplos mais relevantes está o sistema Victor, utilizado no Supremo Tribunal Federal (STF), que realiza a triagem de processos relacionados à repercussão geral, identificando precedentes que possam ser aplicáveis. Outro projeto é o Sinapses, desenvolvido em Santa Catarina, que visa sugerir alternativas à prisão preventiva durante audiências de custódia.

Contudo, na esfera penal, essas iniciativas ainda são predominantemente experimentais e limitadas. Como alertam Lemos e Silva (2021), o uso de IA no processo penal brasileiro ainda carece de regulamentação específica que assegure padrões de transparência, auditabilidade e respeito aos direitos fundamentais.

Além disso, o próprio CNJ reconhece, por meio da Resolução nº 332/2020, a necessidade de que os sistemas de IA observem princípios constitucionais, em especial a dignidade da pessoa humana, a não discriminação, a transparência e a responsabilidade, indicando que o uso dessas tecnologias deve ser acompanhado de cautela e de salvaguardas jurídicas robustas.

3.3 Riscos de discriminação algorítmica no processo penal

Um dos principais perigos da utilização de IA no processo penal é a chamada discriminação algorítmica, que consiste na replicação e até amplificação de preconceitos existentes na sociedade por meio de decisões automatizadas.

> "A falta de cuidado com a regulamentação do tema no Brasil pode gerar o inadmissível dataveillance racial, consistente no desequilíbrio na utilização da técnica especial de coleta de metadados em desfavor de pessoas historicamente excluídas no contexto brasileiro." (QUINTIERE, 2021, p. 8)"

Virginia Eubanks (2018), em "Automating Inequality", evidencia que sistemas de IA utilizados em contextos de risco social ou criminal tendem a penalizar desproporcionalmente populações pobres, negras e marginalizadas. Segundo a autora, "os algoritmos frequentemente tratam desigualdades históricas como dados objetivos, reforçando injustiças em nome da eficiência".

No caso brasileiro, considerando a forte desigualdade racial e socioeconômica, o risco de discriminação algorítmica é ainda mais grave. Silvio Almeida (2019) ensina que o racismo estrutural permeia todas as instâncias sociais, inclusive o sistema de justiça, de modo que a adoção acrítica de tecnologias de IA, sem mecanismos corretivos, pode reforçar práticas discriminatórias.

Para enfrentar esse problema, é imprescindível que as ferramentas de IA sejam desenvolvidas com base em princípios de justiça social e que se implementem medidas de "debiasing" — técnicas que visam identificar e corrigir vieses nos dados e nos algoritmos —, além de processos de auditoria externa independentes.

3.4 O problema da opacidade dos algoritmos e a crise da transparência

Outro desafio crucial é a opacidade dos algoritmos, ou seja, a dificuldade ou impossibilidade de compreender como os sistemas de IA chegam às suas conclusões.

A opacidade algorítmica representa um dos principais desafios para a preservação do devido processo legal no uso de tecnologias de inteligência artificial na justiça criminal. Como aponta Andrew Ferguson (2017, p. 03), professor e especialista em big data policing, os chamados "dados pretos" ilustram os perigos ocultos dessa tecnologia:

> "Este livro ilumina os 'dados brutos' resultantes do policiamento que utiliza 'big data': 'pretos' no sentido de opacos, porque os dados existem extensivamente escondidos dentro de algoritmos complexos; 'pretos' no sentido de codificados racialmente, porque os dados impactam diretamente comunidades não brancas; 'pretos' no sentido da próxima novidade, dada a legitimidade e proeminência decorrentes da percepção de que qualquer coisa orientada por dados é legal, bem recebida — em termos tecnológicos — e futurista; e, finalmente, 'pretos' no sentido de deturpadores, criando sombras legais e lacunas constitucionais em áreas nas quais a lei costumava enxergar nitidamente. Dados pretos importam porque têm impactos no mundo real."

A advertência de Ferguson demonstra que os sistemas de decisão baseados em inteligência artificial não apenas carecem de transparência, mas também introduzem riscos concretos de discriminação e de erosão dos direitos fundamentais, fatores que exigem especial cautela na sua adoção no âmbito processual penal brasileiro.

Cathy O'Neil (2016), em "Weapons of Math Destruction", critica duramente o fato de que algoritmos são muitas vezes tratados como entidades "neutras" e "objetivas", quando, na realidade, operam segundo lógicas que podem ser enviesadas, injustas e invisíveis ao público.

Essa falta de transparência compromete diretamente o contraditório e a ampla defesa no processo penal, pois impede que as partes conheçam e questionem os fundamentos das decisões. Como sustenta Danielle Citron (2008), a governança algorítmica exige não apenas transparência formal, mas explicações significativas que permitam a contestação substantiva das decisões automatizadas.

No Brasil, o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) estabelecem princípios de transparência e autodeterminação informativa que devem orientar também o uso de algoritmos no processo penal. No entanto, a falta de regulamentação específica sobre IA na Justiça Criminal cria lacunas que podem comprometer a proteção efetiva dos direitos fundamentais.

Portanto, garantir a transparência, a auditabilidade e a explicabilidade dos algoritmos utilizados é condição indispensável para assegurar que a introdução da inteligência artificial no processo penal não venha a representar uma ameaça à ordem jurídica democrática.

4 A CONSTITUCIONALIDADE DO USO DE INTELIGÊNCIA ARTIFICIAL NO PROCESSO PENAL

A evolução tecnológica, notadamente com o advento da inteligência artificial (IA), trouxe à tona desafios complexos no campo do processo penal. Se, por um lado, as inovações prometem maior eficiência, redução de erros humanos e celeridade, por outro, colocam em risco garantias constitucionais fundamentais que estruturam o processo penal democrático. Assim, impõe-se uma análise crítica sobre a compatibilidade da IA com os princípios constitucionais brasileiros, especialmente à luz do devido processo legal, do contraditório, da ampla defesa, da publicidade e da imparcialidade judicial.

O devido processo legal, consagrado no artigo 5º, inciso LIV, da Constituição Federal, é mais do que uma formalidade procedimental: é um princípio que assegura a proteção dos direitos fundamentais no âmbito processual. Conforme José Afonso da Silva (2010), o devido processo legal implica um "processo regular, conduzido por juiz imparcial e observando-se todas as garantias do contraditório, ampla defesa e fundamentação".

A introdução da IA no processo penal só será legítima se compatível com a dimensão substancial do devido processo legal. Como assinala Ferrajoli (2002), o processo penal deve ser o "lugar da máxima proteção do indivíduo contra o arbítrio estatal", e não um meio de eficiência inquisitorial. Se os algoritmos utilizados forem

incapazes de respeitar os direitos fundamentais, como o direito de ser ouvido, de participar ativamente do processo e de influenciar a decisão, haverá clara violação constitucional.

> O objetivo do princípio analisado consiste em "proteger o indivíduo contra excessos cometidos pelo Estado, na persecução penal, incluindo-se nele o resguardo contra violências físicas e morais, empregadas para compelir o indivíduo a cooperar na investigação e apuração de delitos, bem como contra métodos proibidos no interrogatório, sugestões e dissimulações" (QUEIJO, 2003, p. 54-55).

Um exemplo emblemático que ilustra essa tensão é o caso State v. Loomis (Suprema Corte de Wisconsin, EUA, 2016). Neste caso, o réu Eric Loomis contestou o uso do software preditivo COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) na fixação de sua pena. Ele argumentou que a falta de transparência sobre como o COMPAS calculou seu "score de risco" violava seu direito ao devido processo legal, pois ele não podia entender ou contestar a base da recomendação utilizada pela corte.

Embora a Suprema Corte de Wisconsin tenha validado o uso do software como ferramenta auxiliar (e não decisória exclusiva), a controvérsia destacou como a opacidade de sistemas algorítmicos pode comprometer a capacidade do réu de se defender e de ter um processo cujo fundamento é compreensível e auditável, aspectos essenciais do devido processo legal.

No Brasil, o Conselho Nacional de Justiça (CNJ) recomenda que o uso de IA respeite as garantias fundamentais e que jamais substitua a análise humana em atos decisórios (Resolução nº 332/2020). Essa recomendação, embora não seja lei, reforça que o uso da IA no processo penal deve sempre se subordinar aos postulados do devido processo legal em sua dupla dimensão: formal e substancial, garantindo que a tecnologia não se torne uma "caixa-preta" incontrolável que prejudique a justiça do processo.

Adicionalmente, a dimensão substantiva do devido processo legal exige que as medidas estatais que afetem direitos fundamentais sejam adequadas e necessárias para atingir uma finalidade legítima, em um exercício de proporcionalidade.

O STF, na análise da Medida Cautelar na ADI 6387, que versava sobre o compartilhamento de dados de usuários de telefonia, assentou que:

> "Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades".

Este entendimento da Suprema Corte é diretamente aplicável ao uso de IA no processo penal. A falta de transparência sobre como um algoritmo opera e para qual finalidade específica ele é utilizado (por exemplo, se para sugerir prisão preventiva ou auxiliar na dosimetria da pena) impede a avaliação de sua adequação e necessidade para a finalidade judicial legítima, violando o devido processo legal em sua substância.

4.1 A compatibilidade da IA com o princípio da imparcialidade

A imparcialidade é condição essencial para a legitimidade do julgamento penal, assegurada tanto pela Constituição Federal (art. 5º, XXXVII) quanto pelos instrumentos internacionais ratificados pelo Brasil, como o Pacto de San José da Costa Rica.

Entretanto, a inteligência artificial, ao ser treinada com dados históricos carregados de preconceitos raciais, socioeconômicos ou de gênero, pode reforçar vieses inconscientes. Como pontua Cathy O'Neil (2016), algoritmos são "armas de destruição matemática" quando operam sem transparência e replicam injustiças sociais em escala massiva.

Assim, a utilização de IA no processo penal exige rigorosos mecanismos de controle para evitar discriminações sistemáticas. Daniel Sarmento (2017) destaca que a imparcialidade judicial demanda também "imparcialidade estrutural", ou seja, a ausência de discriminações sistêmicas no próprio arcabouço institucional.

O caso COMPAS, já mencionado, ilustra perfeitamente esse risco. Estudos realizados pela organização jornalística ProPublica (Angwin et al., 2016) revelaram

que o algoritmo utilizado nos EUA para avaliar o risco de reincidência apresentava viés racial significativo: superestimava o risco de reincidência para réus negros em comparação com réus brancos com histórico criminal semelhante.

Essa discriminação algorítmica viola diretamente os princípios da igualdade e da imparcialidade. Ao apresentar ao juiz uma "nota de risco" enviesada, o sistema pode induzir o julgador a tomar decisões (sobre fiança, liberdade condicional, sentença) que perpetuam a discriminação racial já existente no sistema de justiça criminal.

Portanto, a compatibilidade da IA com a imparcialidade judicial somente será possível se houver controle rigoroso sobre os dados de treinamento, revisão contínua dos algoritmos para identificar e corrigir vieses, e a manutenção da supervisão humana em todas as fases do processo decisório, de forma que o juiz não seja um mero "carimbador" de recomendações algorítmicas discriminatórias.

4.2 O risco de violação ao princípio da ampla defesa e contraditório

O contraditório e a ampla defesa constituem pilares do processo penal democrático, assegurando às partes o direito de influenciar o convencimento judicial. De acordo com Aury Lopes Jr. (2022), "o contraditório não é apenas uma formalidade, mas a garantia de poder participar ativamente da formação da decisão".

A IA, ao operar com modelos opacos — os chamados sistemas "caixa-preta" —, dificulta ou impede o pleno exercício do contraditório. Se a parte não puder entender como o algoritmo chegou a determinada conclusão, não poderá contestá-la adequadamente.

Essa preocupação foi endossada pelo Supremo Tribunal Federal na ADI 6387, que discutiu o uso de reconhecimento facial para fins de segurança pública. Ainda que não tenha declarado a tecnologia inconstitucional per se, o STF ressaltou que seu uso deve respeitar a transparência e a possibilidade de contestação de resultados equivocados, sob pena de violação dos direitos fundamentais.

Assim, no âmbito do processo penal, a utilização de IA que não permita auditoria, contestação e explicação compreensível viola diretamente o contraditório e a ampla defesa, ensejando a nulidade do ato processual.

A experiência com o sistema HART (Harm Assessment Risk Tool), utilizado no Reino Unido, serve como um exemplo. O HART era um algoritmo usado para avaliar o risco de dano que um indivíduo poderia causar. Críticas severas surgiram devido à falta de transparência sobre os fatores que o algoritmo considera e como eles eram ponderados para gerar a avaliação de risco. Essa opacidade impediu que advogados de defesa efetivamente contestam as avaliações de risco usadas em decisões judiciais, comprometendo o direito ao contraditório e à ampla defesa.

No Brasil, o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) estabelecem princípios de transparência e autodeterminação informativa que devem orientar também o uso de algoritmos no processo penal. No entanto, a falta de regulamentação específica sobre IA na Justiça Criminal cria lacunas que podem comprometer a proteção efetiva desses direitos.

A exigência de transparência e explicabilidade não é meramente técnica; é um requisito fundamental para que o contraditório e a ampla defesa possam ser exercidos de forma significativa diante do uso de ferramentas de IA.

4.3 A inconstitucionalidade do uso de sistemas opacos e não auditáveis

A Constituição exige que os atos do Poder Judiciário sejam públicos, transparentes e fundamentados (art. 93, IX, CF). O uso de IA opaca, sem possibilidade de auditoria, contraria frontalmente esse mandamento constitucional. O Relatório Ethics Guidelines for Trustworthy AI da Comissão Europeia (2019) defende que a IA deve ser explicável, justa, robusta e auditável, especialmente no contexto judicial.

No Brasil, a Resolução nº 332/2020 do CNJ estabelece que os sistemas de IA utilizados pelo Judiciário devem obedecer aos princípios da explicabilidade e da auditabilidade. Sem auditabilidade, não há contraditório efetivo, nem controle jurisdicional ou social. Como destaca Gustavo Badaró (2019), "não existe processo

penal democrático onde não se possa compreender, questionar e contestar as decisões judiciais". Dessa forma, sistemas opacos, que inviabilizam o controle externo, são incompatíveis com o Estado Democrático de Direito e, consequentemente, inconstitucionais.

A opacidade não é apenas um problema técnico; é um vício que contamina a validade do ato processual baseado na ferramenta de IA, tornando-o potencialmente inconstitucional. Sistemas que não permitem auditoria externa independente e que não são capazes de gerar explicações compreensíveis de suas conclusões violam diretamente os princípios da publicidade, da fundamentação das decisões judiciais, do devido processo legal, do contraditório e da ampla defesa.

Portanto, sistemas opacos, que inviabilizam o controle externo e interno, são incompatíveis com o Estado Democrático de Direito e, consequentemente, inconstitucionais para uso em decisões que afetem a liberdade ou os direitos fundamentais no processo penal.

Diante dos riscos identificados através da análise dos princípios constitucionais e das experiências internacionais (como COMPAS, que evidenciou vieses; HART, que mostrou o problema da opacidade; e a abordagem cautelosa do Canadá), torna-se imperioso estabelecer critérios claros para a utilização da inteligência artificial no processo penal brasileiro.

A falta de controle, exemplificada pelo uso massivo e opressivo da IA em sistemas de vigilância e controle social na China, serve como um alerta máximo sobre os perigos de uma implementação sem salvaguardas democráticas. É fundamental que haja regulamentação legal específica e robusta, que vá além das recomendações do CNJ. Essa regulamentação deve definir limites objetivos para o uso da IA no processo penal, garantindo a transparência, a auditabilidade e os direitos de revisão humana em todas as etapas.

5 CONSIDERAÇÕES FINAIS

A presente pesquisa teve como objetivo investigar a compatibilidade do emprego de sistemas de inteligência artificial na justiça criminal brasileira com os princípios constitucionais do devido processo legal e da imparcialidade.

Partiu-se da hipótese de que, embora a inteligência artificial possa trazer eficiência e celeridade ao processo penal, sua aplicação desregulada e sem salvaguardas adequadas representa uma séria ameaça às garantias processuais constitucionais. Para examinar essa hipótese, adotou-se uma metodologia qualitativa, com análise doutrinária, legislativa, jurisprudencial e estudo de experiências internacionais e nacionais.

A análise realizada confirmou que o uso indiscriminado de inteligência artificial no processo penal implica riscos concretos de violação a direitos fundamentais. A opacidade dos algoritmos, a dificuldade de compreensão dos critérios decisórios e o risco de reprodução de discriminações históricas revelam-se incompatíveis com o modelo de processo penal garantista adotado pela Constituição Federal de 1988.

O estudo demonstrou que sistemas opacos e não auditáveis comprometem o devido processo legal (art. 5º, LIV e LV, da CF), especialmente a dimensão substancial, ao impedir o controle democrático das decisões judiciais.

Além disso, foi constatado que a presença de vieses algorítmicos viola os princípios da igualdade (art. 5º, caput) e da imparcialidade (art. 5º, XXXVII), ao perpetuar discriminações sistêmicas sob a aparência de neutralidade tecnológica. Da mesma forma, a impossibilidade de compreender e contestar decisões automatizadas atinge o núcleo essencial do contraditório e da ampla defesa (art. 5º, LV).

A pesquisa também evidenciou que a utilização de inteligência artificial preditiva — baseada em riscos futuros e não em provas concretas — tenciona perigosamente o princípio da presunção de inocência (art. 5º, LVII), colocando em risco a própria lógica do processo penal democrático.

Frente a esses achados, conclui-se que a utilização da inteligência artificial no processo penal, nas condições atuais, não é compatível com o ordenamento constitucional brasileiro.

Sua utilização apenas poderá ocorrer de forma legítima caso sejam observados requisitos rigorosos, tais como: a regulamentação legal específica que imponha padrões obrigatórios de transparência, auditabilidade e explicabilidade dos algoritmos; a obrigatoriedade da supervisão humana, garantindo que a decisão judicial seja sempre fundamentada por juiz natural e capaz de se afastar das recomendações algorítmicas injustas;

A implementação de mecanismos robustos de identificação, mitigação e correção de vieses discriminatórios e a garantia de direitos procedimentais específicos para que as partes possam contestar decisões baseadas em inteligência artificial também são requisitos rigorosos para legitimar a aplicação da IA.

A ausência de regulamentação adequada representa grave ameaça ao Estado Democrático de Direito, podendo comprometer a efetividade das garantias processuais e ampliar desigualdades já presentes no sistema de justiça criminal.

Assim, reafirma-se que a tecnologia, no campo penal, deve ser sempre um instrumento a serviço dos direitos fundamentais e não um fator de erosão das garantias constitucionais arduamente conquistadas. O avanço tecnológico, embora inevitável, não pode prescindir da centralidade dos valores constitucionais que estruturam o processo penal brasileiro.

Portanto, a inteligência artificial, quando empregada sob rígido controle normativo e judicial, poderá contribuir para a realização da justiça. Fora desse marco, seu uso representa sério risco de arbitrariedade, desigualdade e violação dos direitos humanos, incompatível com os princípios do Estado Constitucional de Direito.

REFERÊNCIAS

ALMEIDA, Silvio. **Racismo estrutural**. São Paulo: Pólen, 2019.

ANGWIN, Julia; LARSON, Jeff; MATTU, Surya; KIRCHNER, Lauren. **Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks**. *ProPublica*, 2016. Disponível em: https://apublica.org/2016/06/software-que-avalia-reus-americanos-cria-injusticas-na-vida-real. Acesso em: 10 nov. 2025.

BADARÓ, Gustavo. **Processo penal e garantismo**. 2. ed. São Paulo: Atlas, 2019.

BOITEUX, Luciana. **Justiça criminal e inteligência artificial: desafios para o processo penal**. *Revista Brasileira de Ciências Criminais*, v. 162, 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988.

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: 15 out. 2024.

CRAWFORD, Kate. **Artificial Intelligence and Life in 2030**. *One Hundred Year Study on Artificial Intelligence: Report of the 2015–2016 Study Panel*, Stanford University, 2016.

EUBANKS, Virginia. **Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor**. Nova York: St. Martin's Press, 2018.

ETZIONI, Oren. **Como regular a inteligência artificial**. Disponível em: https://www.dtibr.com/post/2018/10/08/como-regular-a-inteligencia-artificial-por-oren-etzion. Acesso em: 4 nov. 2025.

FERRAJOLI, Luigi. **Direito e razão: teoria do garantismo penal**. 6. ed. São Paulo: Revista dos Tribunais, 2002.

GARAPON, Antoine. **La justice prédictive: Un état des lieux**. Paris: Dalloz, 2021.

LENZA, Pedro. **Direito constitucional esquematizado**. 28. ed. São Paulo: Saraiva Educação, 2022.

O'NEIL, Cathy. **Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy**. Nova York: Crown Publishing Group, 2016.

PELLEGRINI GRINOVER, Ada. **As nulidades no processo penal**. 6. ed. São Paulo: Revista dos Tribunais, 2001.

PHAM, Hoang; DEHMAN, Amira. **The California Racial Justice Act of 2020, explained**. Disponível em: https://law.stanford.edu/2024/04/22/the-california-racial-justice-act-of-2020-explained/. Acesso em: 10 nov. 2025.

QUINTIERE, Víctor Minervino. **A persecução penal das sociedades pós-industriais: análise da expansão do direito penal à luz do dataveillance e seu impacto na interpretação do direito ao silêncio (nemo tenetur se detegere) e da**

privacidade digital. 2021. 306 f. Tese (Doutorado em Direito) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP, Brasília, 2021.

RUSSELL, Stuart; NORVIG, Peter. **Artificial Intelligence: A Modern Approach**. 3. ed. Upper Saddle River: Prentice Hall, 2010.

SARMENTO, Daniel. **Direitos fundamentais e relações privadas**. Rio de Janeiro: Lumen Juris, 2007.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 37. ed. São Paulo: Malheiros, 2014.

SMITH, John. **AI and Legal Research: The Canadian Approach**. *Canadian Journal of Law and Technology*, v. 15, n. 3, p. 234-245, 2020.

VIEIRA, Leonardo Marques. **A problemática da inteligência artificial e dos vieses algorítmicos: caso COMPAS**. Disponível em: https://lcv.fee.unicamp.br/images/BTSym-19/Papers/090.pdf. Acesso em: 10 nov. 2025.

IA E A CRIAÇÃO DE CONTEÚDO ILÍCITO: DESAFIOS NA PROTEÇÃO DE MENORES

Luisa Lopes Margato[1]

RESUMO

O objetivo deste artigo é analisar os desafios éticos, jurídicos e sociais decorrentes do uso da Inteligência Artificial (IA) na criação e disseminação de conteúdos ilícitos que envolvem menores de idade, com ênfase nas deepfakes e em outras formas de manipulação digital. A pesquisa busca compreender como essas tecnologias têm sido utilizadas para produzir materiais falsos de natureza sexual, difamatória ou abusiva, bem como avaliar os impactos sobre a proteção da imagem, da dignidade e da privacidade infantil. O estudo se baseia em uma revisão bibliográfica de autores da área do Direito Digital, da Psicologia e da Tecnologia da Informação, além de examinar legislações vigentes, como o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD) e o Estatuto da Criança e do Adolescente (ECA). Observa-se que o avanço rápido da IA tem superado a capacidade de resposta das normas jurídicas, exigindo uma atualização legislativa e o fortalecimento das políticas públicas de prevenção, educação digital e responsabilização penal. Conclui-se que a proteção integral de menores no ambiente digital depende da cooperação entre Estado, plataformas tecnológicas, famílias e sociedade civil, de modo a equilibrar inovação e segurança ética no uso da IA.

Palavras-chave: Inteligência Artificial; Deepfake; Conteúdo ilícito; Proteção de menores; Direito Digital.

ABSTRACT

The objective of this article is to analyze the ethical, legal, and social challenges arising from the use of Artificial Intelligence (AI) in the creation and dissemination of illicit content involving minors, with an emphasis on deepfakes and other forms of digital manipulation. The research aims to understand how these technologies have been used to produce false materials of a sexual, defamatory, or abusive nature, as well as to assess their impact on the protection of children's image, dignity, and privacy. The study is based on a literature review of authors in the fields of Digital Law, Psychology, and Information Technology, in addition to

[1] Estudante de direito do UniCEUB- Centro Universitário de Brasília, fluente em inglês e apaixonada pela língua portuguesa. E-mail: margatoluisa@gmail.com

examining current legislation such as the Brazilian Internet Bill of Rights (Marco Civil da Internet), the General Data Protection Law (LGPD), and the Child and Adolescent Statute (ECA). It is observed that the rapid advancement of AI has outpaced the legal system's ability to respond, requiring legislative updates and the strengthening of public policies focused on prevention, digital education, and criminal accountability. It is concluded that the comprehensive protection of minors in the digital environment depends on cooperation among the State, technology platforms, families, and civil society, in order to balance innovation with ethical safety in the use of AI.

Keywords: Artificial Intelligence; Deepfake; Illicit content; Child protection; Digital Law.

SUMÁRIO: 1. Introdução; 2. O que são Deepfakes?; 3. Riscos e desafios na proteção de menores; 4. Aspectos jurídicos e regulatórios; 5. ECA Digital; 6. Perspectiva ética e social; 7. Conclusão; 8. Referências.

1 INTRODUÇÃO

A popularização da Inteligência Artificial (IA) tem promovido transformações significativas em diversos setores da sociedade, ampliando as possibilidades de automação, personalização e otimização de processos. No entanto, junto aos benefícios trazidos por essa tecnologia emergem também riscos e desafios complexos, especialmente relacionados ao seu uso indevido, já que se trata de algo extremamente atual. Entre as aplicações mais controversas da IA, destacam-se as deepfakes: Produções digitais criadas a partir de algoritmos de aprendizado de máquina e redes neurais profundas, capazes de gerar imagens, áudios e vídeos altamente realistas e, muitas vezes, indistinguíveis da realidade. Embora estas possam ser utilizadas de maneira legítima em áreas como o cinema, a publicidade, o entretenimento e até mesmo a educação, o seu uso indevido tem se tornado uma preocupação crescente. O potencial de manipulação dessas tecnologias abre espaço para a criação e disseminação de conteúdos ilícitos, falsificações de identidade e violações de direitos fundamentais, especialmente quando envolvem crianças e adolescentes. Nessas situações, a exposição de menores em contextos falsos ou de caráter sexual não apenas configura crime, mas também causa danos psicológicos e sociais profundos, comprometendo seus direitos fundamentais[2].

[2] "Os direitos fundamentais funcionam como uma reserva mínima de justiça aplicável a todas as pessoas. Característica essencial dos direitos fundamentais é que eles são oponíveis às maiorias políticas. Vale

Diante desse cenário, surge a necessidade de refletir sobre as implicações éticas, jurídicas e sociais do uso da IA na produção de conteúdos ilícitos e sobre a urgência de medidas preventivas que assegurem a proteção integral de menores no ambiente digital. Este artigo tem como objetivo discutir os riscos associados às deepfakes ilícitas, os desafios que elas impõem ao Direito e à sociedade, bem como propor estratégias de enfrentamento que envolvam a atuação conjunta do Estado, das plataformas digitais e da sociedade civil na construção de um espaço virtual mais seguro e ético.

2 O QUE SÃO DEEPFAKES?

As deepfakes são conteúdos digitais, como vídeos, áudios ou imagens, gerados ou alterados por meio de técnicas de Inteligência Artificial, especialmente por redes neurais profundas e algoritmos de aprendizado de máquina. O termo vem da junção de deep learning (aprendizado profundo) e fake (falso), e descreve materiais em que rostos, vozes ou corpos são manipulados para parecerem autênticos. Essa tecnologia é capaz de criar simulações extremamente realistas, nas quais uma pessoa pode ser mostrada dizendo ou fazendo algo que nunca aconteceu.

Quando utilizadas de forma ética e responsável, essa tecnologia pode trazer benefícios relevantes em diversos campos, como por exemplo: No entretenimento e no cinema é possível empregá-las para recriar personagens, dublar falas com maior precisão ou revitalizar obras muito antigas. Na educação, podem ser usadas para simular experiências históricas ou científicas de modo imersivo, tornando o aprendizado mais dinâmico e interessante aos alunos. Pode-se ir mais fundo e citar, também, aplicações legítimas na publicidade e até em pesquisas médicas, onde a IA auxilia na criação de imagens para treinar sistemas de diagnóstico e visualizar melhor o corpo humano.

Entretanto, o mesmo potencial que torna essa tecnologia promissora também a transforma em uma ferramenta perigosa quando utilizada de má-fé. O uso indevido das deepfakes tem se expandido para a produção de conteúdos falsos, difamatórios e,

dizer: eles funcionam como limites ao legislador e mesmo ao poder constituinte reformador." (BARROSO, 2015)

sobretudo, de natureza sexual, sem o consentimento das pessoas envolvidas. Em especial, observa-se o agravante da criação de conteúdos falsos que envolvem a sexualização de menores de idade, prática extremamente grave que viola direitos fundamentais da criança e do adolescente, como a dignidade, a privacidade e a integridade psicológica, dificultando, também, que esse menor de idade não consiga viver e construir um futuro de forma plena.

Essas manipulações digitais podem não apenas gerar danos irreparáveis às vítimas, como também facilitar o acesso de predadores sexuais a conteúdos simulados de exploração infantil, ampliando o ciclo de abuso e estimulando a circulação desse tipo de material em ambientes virtuais, comprometendo a segurança pública e o bem estar social. Além disso, a dificuldade em distinguir o que é real do que é artificial cria um cenário de insegurança informacional, no qual a confiança pública nas imagens e nos vídeos é enfraquecida, prejudicando toda a sociedade.

3 RISCOS E DESAFIOS DAS DEEPFAKES NA PROTEÇÃO DE MENORES

Entre os principais riscos associados às deepfakes, destaca-se a produção e disseminação de conteúdo sexual falso envolvendo crianças e adolescentes, caracterizando novas formas de abuso digital. Tais práticas configuram uma violação grave dos direitos fundamentais, afetando diretamente a dignidade, a imagem e a integridade psicológica das vítimas, direitos previstos no artigo 5º da Constituição Federal. O ponto principal do problema consiste, justamente, na dificuldade crescente em diferenciar o que é real do que é artificial, o que potencializa a vulnerabilidade das vítimas e dificulta ações rápidas de contenção e responsabilização.

Sabendo disso, é evidente a influência do avanço tecnológico na definição de novas necessidades jurídicas, fazendo surgir, assim, o Constitucionalismo Digital, que é uma corrente teórica do Direito Constitucional entendida a partir de normas que protegem, reconhecem e reafirmam os direitos fundamentais no contexto do ciberespaço, promovendo o reequilíbrio de poderes na governança do ambiente digital (Mendes; Fernandes, 2020). Num diálogo sobre o Direito Digital, entendemos

que a evidenciação das garantias individuais e coletivas como um bem jurídico é um assunto delicado, pois, apesar da força normativa vinculada à sua proteção, a sua violação apresenta um nível alto de fragilidade e facilidade, devido ao crescente avanço da tecnologia. Ironicamente, o aprimoramento científico-tecnológico foi acompanhado de uma hiper valorização do relativismo e das questões subjetivas que envolvem o conhecimento e a verdade (Salgado, 2002), já que isso se tornou parte do cotidiano da sociedade, criando uma espécie de conformismo .

Manuel Castells, em sua obra A Sociedade em Rede, explica que as transformações tecnológicas do final do século XX não foram pautadas apenas na letra do conhecimento, mas sim na sua aplicação vivemos em uma era informacional na qual "a linha que separa o real do artificial se torna progressivamente tênue", abrindo espaço para manipulações que confundem o olhar humano e fragilizam a confiança social. Essa ambiguidade é explorada de forma perversa quando aplicada à criação de deepfakes com conteúdo sexualizado de menores, tornando-se uma forma contemporânea de violência simbólica e psicológica.

Para Zuboff (2019, p. 112), o atual contexto de "capitalismo de vigilância" amplia a coleta e o uso indevido de dados e imagens, convertendo a intimidade em mercadoria e expondo indivíduos, nesse caso, crianças, a dinâmicas de exploração invisíveis e difíceis de controlar. Nesse sentido, o uso ilícito de deepfakes reforça estruturas de poder desiguais, em que a tecnologia é instrumentalizada para fins de controle, dominação e lucro, em detrimento da proteção e da privacidade infantil.

Do ponto de vista jurídico, Doneda (2020, p. 89) destaca que a legislação brasileira ainda se mostra insuficiente diante das transformações tecnológicas, reagindo "de forma fragmentada e tardia" às novas modalidades de violação de direitos. Apesar da proteção prevista na Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e no Estatuto da Criança e do Adolescente (Lei nº 8.069/1990), a aplicação prática dessas normas encontra obstáculos diante da velocidade com que o conteúdo digital é produzido e disseminado, criando uma lacuna na lei. Sabendo disso, como observa Bauman (2007, p. 18), vivemos em uma sociedade "líquida", marcada pela efemeridade dos vínculos e pela fragilidade das responsabilidades éticas. No ambiente virtual, essa liquidez se manifesta na naturalização de práticas

violentas, no compartilhamento inconsequente de conteúdos e na ausência de empatia em relação às vítimas. Esse cenário intensifica o sofrimento psicológico de crianças e adolescentes que têm sua imagem falsificada ou exposta, gerando impactos emocionais duradouros.

4 ASPECTOS JURÍDICOS E REGULATÓRIOS

Do ponto de vista legal, o ordenamento jurídico brasileiro já possui dispositivos importantes que podem ser aplicados aos casos de uso ilícito de deepfakes envolvendo crianças e adolescentes. O Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) prevê, em seu artigo 241-A, que é crime "produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente". A legislação também tipifica como infração a divulgação, publicação e armazenamento de tais conteúdos, independentemente de se tratar de material real ou manipulado digitalmente. Assim, a criação e disseminação de deepfakes com conotação sexual envolvendo menores se enquadra diretamente nas hipóteses de exploração sexual infantil previstas no ECA, ainda que as imagens sejam sintéticas.

Além disso, o Marco Civil da Internet (Lei nº 12.965/2014) estabelece princípios fundamentais sobre liberdade, privacidade e responsabilidade na rede, mostrando, em seu artigo 19, a responsabilização de provedores de aplicações caso não retirem conteúdos ilícitos após notificação judicial, reforçando a importância da atuação das plataformas digitais na prevenção e contenção de materiais produzidos por meio de deepfakes. Essa norma cria um elo entre a liberdade de expressão e a proteção dos direitos fundamentais, inclusive de crianças e adolescentes.

Outro instrumento essencial é a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), que garante a proteção de dados sensíveis e estabelece diretrizes para o tratamento de informações pessoais. O artigo 14 dispõe sobre o tratamento de dados de crianças e adolescentes, exigindo consentimento específico e proteção reforçada, reconhecendo-os como grupo vulnerável. A manipulação de imagens e vídeos para fins ilícitos, como no caso de deepfakes, constitui uma clara violação desses princípios, sujeitando os responsáveis às sanções previstas na legislação.

Apesar dessas previsões normativas, a efetiva responsabilização dos autores de crimes envolvendo deepfakes ainda enfrenta obstáculos devido à dimensão transnacional da internet, que dificulta a identificação da origem dos conteúdos e a aplicação das leis nacionais, o que demanda cooperação internacional e mecanismos mais eficazes de rastreamento, para se aproximar da realidade em que diversos países e organismos multilaterais têm avançado na tipificação específica do uso ilícito dessas tecnologias. Nos Estados Unidos, alguns estados já aprovaram leis que criminalizam a criação de deepfakes com fins difamatórios ou sexuais. A União Europeia, por meio do Regulamento Geral sobre a Proteção de Dados (GDPR), reforça a proteção de dados pessoais, impondo sanções severas para usos abusivos de tecnologias de manipulação de imagem. Percebe-se, então, que esses movimentos indicam uma tendência global de fortalecimento da regulação, buscando equilibrar a liberdade de inovação tecnológica com a salvaguarda dos direitos humanos. Assim, os aspectos jurídicos e regulatórios relacionados às deepfakes evidenciam a necessidade de atualização e integração de instrumentos legais no plano nacional. A proteção de crianças e adolescentes no ambiente digital não depende apenas da existência de leis, mas da efetividade de sua aplicação, da cooperação internacional e de mecanismos tecnológicos que permitam identificar e responsabilizar autores de abusos.

5 ECA DIGITAL

A discussão sobre os aspectos jurídicos e regulatórios relacionados às deepfakes envolvendo crianças e adolescentes ganha novos contornos com a promulgação do chamado ECA Digital, instituído pela Lei nº 15.211, de 17 de setembro de 2025. Essa legislação complementa o Estatuto da Criança e do Adolescente tradicional ao estabelecer diretrizes específicas para a proteção de menores no ambiente digital, fortalecendo o arcabouço jurídico existente para lidar com situações de manipulação sintética de imagens e vídeos. A sanção da nova lei foi acompanhada da edição do Decreto nº 12.622/2025, que atribuiu à Autoridade Nacional de Proteção de Dados (ANPD) a competência para regulamentar e fiscalizar as disposições do ECA Digital. Ademais, a Medida Provisória nº

1.319/2025 reduziu o prazo de vacância da norma para seis meses, reforçando a urgência da proteção infantojuvenil diante da crescente complexidade dos riscos digitais.

Com o ECA Digital, a ANPD foi transformada em agência reguladora independente, ampliando seu papel institucional no enfrentamento de violações de direitos de crianças e adolescentes na internet. A autoridade passou a ser responsável pela elaboração de normas complementares, pela orientação das plataformas digitais e pela fiscalização das condutas dos provedores. Segundo declarações oficiais, a ANPD iniciou a revisão de sua agenda regulatória 2025-2026 para incorporar prioritariamente temas relacionados à proteção de menores e preparar um mapa de fiscalização voltado para os desafios emergentes do ambiente digital, incluindo a detecção e mitigação de conteúdos sintéticos ilícitos.

A nova legislação estabeleceu obrigações específicas para plataformas digitais, reforçando o dever de proteção integral previsto no ordenamento jurídico brasileiro. Entre as medidas previstas está a exigência de mecanismos confiáveis de verificação de idade, superando modelos baseados apenas na autodeclaração do usuário. Além disso, as plataformas deverão disponibilizar ferramentas de supervisão parental eficazes, com controles que permitam limitar contato, compartilhamento, tempo de uso e exposição a conteúdos potencialmente prejudiciais. Em conformidade com o princípio do "melhor interesse da criança", o ECA Digital determina que serviços voltados para menores adotem configurações padrão mais protetivas e implementem práticas de "design por prevenção", voltadas à antecipação de riscos decorrentes do funcionamento dos sistemas.

No que se refere ao enfrentamento de conteúdos ilícitos, a lei determinou a remoção célere de materiais que violem direitos fundamentais de crianças e adolescentes, especialmente aqueles ligados à exploração sexual. Esse ponto é particularmente relevante no contexto das deepfakes, uma vez que a manipulação sintética de imagens de menores para fins sexuais, ainda que sem registro real de abuso, enquadra-se nas hipóteses de crimes previstos no ECA e enseja a responsabilização dos agentes envolvidos. Ao mesmo tempo, a legislação passou a prever sanções administrativas mais severas para as plataformas que descumprirem

as obrigações impostas, incluindo multas elevadas, suspensão de atividades e, em casos extremos, a proibição de funcionamento no território nacional.

O ECA Digital também estabeleceu limites expressos às práticas de vigilância conduzidas por plataformas digitais, proibindo formas de monitoramento massivo ou indiscriminado dos usuários, tendo em vista que essa previsão que busca equilibrar a proteção à privacidade com as necessidades de segurança não pode ocorrer por meio de violações generalizadas a direitos fundamentais. A regulamentação futura da ANPD deverá detalhar como as empresas poderão conciliar mecanismos de detecção de riscos, como deepfakes, com a garantia de proteção de dados pessoais.

Nesse cenário, a incidência dessas tecnologias com conotação sexual envolvendo crianças e adolescentes passa a estar diretamente abrangida por um sistema regulatório mais robusto e integrado. As obrigações de verificação de idade, supervisão parental, detecção precoce de riscos, mecanismos de proteção por design e remoção rápida de conteúdos ilícitos criam uma estrutura preventiva mais eficaz, além de que a existência de sanções administrativas severas tende a pressionar plataformas a adotar tecnologias mais avançadas para identificação e bloqueio de deepfakes, contribuindo para reduzir a circulação desses materiais.

Entretanto, apesar dos avanços, permanecem desafios relacionados à natureza global da internet e às dificuldades de cooperação transnacional na responsabilização de autores desses crimes. Assim como ocorre em outros ordenamentos, como exemplo dos Estados Unidos e da União Europeia, que têm adotado medidas específicas para regular o uso abusivo de tecnologias de manipulação de imagem, o Brasil avança no sentido de alinhar a inovação tecnológica com a proteção de direitos fundamentais. Contudo, a eficácia do ECA Digital dependerá não apenas de seu texto legal, mas também da capacidade de fiscalização da ANPD, da atuação conjunta das plataformas e da coordenação entre diferentes países no combate às violações digitais.

Esse movimento, portanto, revela a tendência contemporânea de uma regulação mais firme e estruturada sobre tecnologias digitais, especialmente no que diz respeito à proteção de crianças e adolescentes diante de práticas como o uso

ilícito de deepfakes. A atualização normativa e a integração entre os instrumentos legais existentes demonstram que a proteção infantojuvenil no ambiente digital exige não apenas leis, mas também mecanismos tecnológicos, ações coordenadas e instituições fortalecidas para garantir a efetividade desse conjunto normativo.

6 PERSPECTIVA ÉTICA E SOCIAL

A manipulação de conteúdos digitais envolvendo crianças e adolescentes ultrapassa o campo jurídico e adentra o âmbito ético e social. As deepfakes ilícitas, especialmente aquelas que exploram menores, violam diretamente a dignidade humana, a privacidade e o direito ao pleno desenvolvimento, valores que constituem a base da proteção integral prevista no artigo 227 da Constituição Federal que possui o seguinte texto:

> 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" (CONSTITUIÇÃO FEDERAL, 1988.)

Do ponto de vista ético, o uso de tecnologias capazes de falsificar imagens e vídeos de menores representa uma afronta à noção de respeito à pessoa humana. A criança, em especial, é um sujeito em formação e, portanto, particularmente vulnerável aos impactos psicológicos e sociais decorrentes da exposição digital indevida, então, quando sua imagem é manipulada ou distorcida, há uma quebra da confiança social e da segurança emocional necessárias para seu desenvolvimento saudável. Além disso, as *deepfakes* ilícitas agravam um problema social já existente: a banalização da exposição e do consumo de conteúdo sensacionalista ou sexualizado na internet. A facilidade com que essas produções circulam nas redes cria uma cultura de desinformação e de desvalorização da intimidade, torna cada vez mais difícil distinguir o que é real do que é fabricado, o que gera consequências graves não apenas para as vítimas diretas, mas também para todo o convívio social, que passa a permanecer em um ambiente digital de incerteza e descrédito.

A responsabilidade ética pela prevenção e combate a esse tipo de prática deve ser compartilhada entre diferentes atores sociais, como as famílias, que precisam orientar as crianças sobre o uso consciente da tecnologia e sobre os riscos de exposição virtual, as escolas, que têm papel essencial na educação digital, promovendo debates sobre ética, cidadania e segurança na internet e, também, as empresas de tecnologia, que, por sua vez, devem desenvolver mecanismos de verificação, denúncia e bloqueio de conteúdos falsificados, assumindo sua parcela de responsabilidade social.

Sabendo disso, é de suma importância citar o Estado, que também exerce função indispensável, tanto na fiscalização e responsabilização dos envolvidos quanto na promoção de políticas públicas de conscientização e proteção. É necessário incentivar a criação de programas de alfabetização digital, campanhas educativas e regulamentações que impeçam o uso indevido de ferramentas de inteligência artificial.

7 CONCLUSÃO

As *deepfakes* representam um dos maiores desafios contemporâneos no campo da proteção de menores, reunindo riscos tecnológicos, jurídicos, éticos e sociais em um cenário de complexidade crescente. Conforme discutido, essas tecnologias têm potencial para usos legítimos e benéficos, como na educação, no entretenimento e na comunicação digital, mas também podem ser exploradas de forma ilícita, gerando conteúdos sexuais falsos envolvendo crianças e adolescentes e práticas ilícitas, tais usos afetam diretamente a dignidade, a privacidade e o desenvolvimento emocional das vítimas, além de comprometer a confiança social e a percepção de autenticidade no ambiente digital.

No plano jurídico e regulatório, o Estatuto da Criança e do Adolescente (ECA), o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD) oferecem instrumentos importantes para coibir a produção e disseminação de *deepfakes* ilícitas. Entretanto, a dimensão transnacional da internet, aliada à velocidade de disseminação de conteúdos digitais, apresenta desafios para a identificação de responsáveis e para a aplicação efetiva das normas. Observa-se,

portanto, a necessidade de harmonização entre legislação nacional e internacional, bem como a criação de mecanismos que aumentem a responsabilização de autores e plataformas, com mais clareza e quebra do anonimato desses.

Do ponto de vista ético e social, a proteção de menores diante das *deepfakes* requer uma abordagem multidisciplinar e colaborativa. Famílias, escolas, empresas de tecnologia e o Estado devem atuar de forma integrada, promovendo educação digital, conscientização ética e medidas preventivas que reduzam a exposição e os riscos às crianças e adolescentes. A responsabilidade social não se limita à punição; envolve também a construção de uma cultura de respeito à intimidade, à dignidade e à segurança digital, expondo com que a combinação de avanços tecnológicos com vulnerabilidades sociais cria um cenário complexo que exige uma resposta coordenada e multidisciplinar. Somente por meio da atuação conjunta entre legislação, tecnologia, educação e ética será possível assegurar um ambiente digital mais seguro, no qual os direitos das crianças e adolescentes sejam efetivamente preservados, equilibrando inovação tecnológica com proteção integral e desenvolvimento saudável.

REFERÊNCIAS

BAUMAN, Zygmunt. "**Tempos líquidos**." Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2007.

BERNAL, Paul. "**Internet privacy rights: rights to protect autonomy**." Cambridge: Cambridge University, 2014.

BOBBIO, Norberto. "**A era dos direitos"**. Nova edição, Rio de Janeiro: Elsevier, 2004. Disponível em: https://www.mprj.mp.br/documents/20184/172905/a_era_dos_direitos.pdf

DONEDA, Danilo. **"Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados."** São Paulo: Thomson Reuters Brasil, 2020.

ZUBOFF, Shoshana. **"A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder. "** Rio de Janeiro: Intrínseca, 2021.

Protocolo de Direitos Humanos. Nova York, 1948. Declaração Universal dos Direitos Humanos.

DALLARI, Dalmo de Abreu. "**O que são direitos da pessoa.**" Coleção Primeiros Passos, v. 49. São Paulo: Brasiliense, 1981.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)**. Diário Oficial da República Federativa do Brasil, Brasília, DF, 15 ago. 2018.

LESSIG, Lawrence. "**Code : version 2.0**." New York: Basic Books, 2006. Disponível em: https://ia601903.us.archive.org/33/items/Code2.0/Code.pdf

SIQUEIRA, M. de; ANDRADE, E. J. de. **"Deepfake e privacidade: uma análise jurídica acerca da manipulação da imagem dos usuários"**. *Revista Foco*, v. 17, n. 8, e5679, p. 1-34, 2024. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/5679/4216

BRASIL. Lei n.º 8.069, de 13 de julho de 1990. **Estatuto da Criança e do Adolescente.** Diário Oficial da União, Brasília, 13 jul. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm

O USO DA INTELIGÊNCIA ARTIFICIAL E A ATRIBUIÇÃO DE RESPONSABILIDADE NO COMBATE AO PLÁGIO

Anne Louise Morais Gomes
Maria Clara Tamashiro Bego
Kalyne Aryane Aryane Melo Xavier

RESUMO

Este artigo trata do uso da Inteligência Artificial e a responsabilidade dos desenvolvedores na criação e progresso de sistemas de software na consolidação do conteúdo disponibilizado na internet e o combate ao plágio. O presente artigo procura expor uma análise da atual situação do desenvolvimento da Inteligência Artificial na projeção de conteúdos para a internet e a quem recai a responsabilização nos casos de plágio no Brasil, apresentando a visão de juristas quanto ao cenário e mostrando como se dá a atuação do Estado para minimizar os delitos digitais cometidos. Foi fomentado através de pesquisas em artigos acadêmicos, consulta de índices oficiais e literatura referente ao assunto. Os dados coletados permitiram que fizéssemos uma análise da realidade digital brasileira ao que tange a aplicação das normas do Direito Digital e as reincidências ao sistema operacional. As recomendações baseadas nas literaturas usadas como base para este presente artigo são direcionadas às autoridades públicas, sugerindo uma nova vertente de pensar as formas de se responsabilizar os conteúdos produzidos e sobretudo a segurança cibernética.

Palavras-chaves: Inteligência Artificial; Cibernético; Plágio; Responsabilidade, Desenvolvedores.

Sumário: 1. Introdução; 2. Cenário atual da Inteligência Artificial no desenvolvimento de sistemas no Brasil; 3. Plágio: definição e previsão legal; 4. Responsabilidade no combate ao plágio; 5. Considerações finais, Referências.

1 INTRODUÇÃO

Na atual conjuntura presente na revolução 4.0, concomitantemente ao crescimento da globalização e célere difusão de informações, estão presentes as consequências jurídicas do processo de automação proporcionado pelo uso da Inteligência Artificial.

O objetivo do presente artigo é conscientizar e apresentar uma reflexão a respeito do uso da base de dados disponibilizada na internet pela Inteligência Artificial e a responsabilização de sua utilização no combate ao plágio.

Temática essa presente em vários níveis de discussão, seja em âmbitos de reconhecimento e preservação da propriedade intelectual, assim como visando à melhor regulamentação do mundo cibernético. De tal modo, torna-se essencial discutir as implicações jurídicas do conteúdo produzido pela Inteligência Artificial e a incidência da responsabilidade ao se deparar com uma informação plagiada pelo próprio sistema operacional.

Como marco teórico, o artigo científico trará análises de desenvolvedores de software e pensadores do meio e sua relação com a sociedade; assim como as estudantes juristas adentram em outros domínios do Direito Digital.

O artigo proporcionará reflexões sobre o atual cenário cibernético e as principais implicações cotidianas do uso da Inteligência Artificial, que vêm ganhando cada vez mais espaço na sociedade, desde tarefas mais simples ao desenvolvimento mais complexo de sistemas e utilização de informações.

2 CENÁRIO ATUAL DA INTELIGÊNCIA ARTIFICIAL NO DESENVOLVIMENTO DE SISTEMAS NO BRASIL

O desenvolvimento da Inteligência Artificial no Brasil é um fenômeno que se aperfeiçoou paulatinamente ao longo de diversos anos, desde a constituição das revoluções industriais (dos anos de 1750 a 1950) à revolução técnico-científica informacional (1950 - aos dias atuais) e, por fim, à revolução 4.0 (a partir do século XXI)[1].

A globalização contribuiu para a célere difusão e utilização da Inteligência Artificial. Apesar dos avanços tecnológicos serem de intrínseca importância no cotidiano da sociedade, é necessária maior normatização do mundo cibernético, a fim de preservar a integridade de seus usuários, bem como a originalidade dos conteúdos produzidos.

[1] SCHWAB, Klaus. A quarta revolução industrial. Edipro, 2019.

O cenário de transitoriedade das relações sociais e a busca incessável pelo automatismo, fluidez e rapidez de se adquirir informações no contexto modernidade líquida, conforme os ensinamentos proporcionados pelo intelectual Zygmunt Bauman, perpetua a ininterrupta utilização da Inteligência Artificial no cotidiano social[2].

A imagem difundida de que a Inteligência Artificial otimiza diversos processos que anteriormente eram morosos para a pessoa humana em seu dia a dia, bem como automatiza numerosas tarefas em exacerbados volumes, vem atrelada, também, a uma realidade digital obscura, que, muitas vezes produz falsos conteúdos, bem como os desenvolve sem o devido reconhecimento de sua autoria e autorização.

Pode-se afirmar que, ao ser abastecida por determinada base de dados, o cenário cibernético permite sua utilização como instrumento tecnológico, que pode ser potencialmente utilizado como meio para plagiar obras e conteúdos previamente existentes na internet.

Assim, ao consolidar informações a um determinado usuário, a Inteligência Artificial faz uso de uma base de dados preexistentes, as quais, por si, derivam de conteúdos produzidos pelo intelecto humano, que são disponibilizados na internet.

Desse modo, com o crescente progresso tecnológico, os conteúdos disponibilizados na internet ficam sujeitos ao plágio não somente pela pessoa humana, mas pela consolidação de conteúdos que a Inteligência Artificial proporciona e satisfaz. Conforme o colunista e jornalista inglês Sam Leith escreveu na The Spectator[3]:

> Para produzir qualquer coisa, a inteligência artificial generativa precisa roubar material protegido por direitos autorais em escala inimaginável.

O típico e reflexivo exemplo da utilização da Inteligência Artificial é na produção de imagens imitando o estilo de pinturas criado por artistas reais. Assim, por exemplo, ao provocar a Inteligência Artificial, mediante uma foto de um usuário,

[2] BAUMAN, Zygmunt. Modernidade líquida. Rio de Janeiro: Editora Zahar, 2001.
[3] VEJA. Uma brincadeira inocente ou plágio sinistro da inteligência artificial? Disponível em: <https://veja.abril.com.br/coluna/mundialista/uma-brincadeira-inocente-ou-plagio-sinistro-da-inteligencia-artificial/>. Acesso em: 09 out. 2025.

para se produzir uma ilustração que se remete a um determinado estilo criado por um artista, não se estaria diante de um plágio?

Afinal, se um outro artista real reproduzisse a mesma técnica e estilo criado anteriormente, não seria responsabilizado por plagiar propriedade intelectual e artística de outrem?

Nesse caso, a responsabilização recairia para o artista nos termos do art. 33 da Lei nº 9.610/1998:

> Art. 33. Ninguém pode reproduzir obra que não pertença ao domínio público, a pretexto de anotá-la, comentá-la ou melhorá-la, sem permissão do autor.

A grande adversidade presente na era digital é justamente a precariedade quanto a sua regulamentação.Fato é que o desenvolvimento da Inteligência Artificial ainda é um marco recente na sociedade. No entanto, é necessário que se desenvolva mecanismos de atuação ativa para regulação de suas atividades, a fim de que se preserve a integridade das obras produzidas, bem como a propriedade intelectual de seus usuários.

Atualmente, o Direito Digital, ainda em desenvolvimento, conta com algumas regulamentações, como a Lei Geral de Proteção de Dados (LGPD - Lei 13.709/2018); Marco Civil da Internet (Lei 12.965/2014); Lei Carolina Dieckmann (Lei 12.737/2012).

Contudo, não está prevista, em uma das principais leis relacionada à proteção de dados (LGPD), o uso da Inteligência Artificial e suas limitações e resguardo da segurança das informações e usuários.

Fator esse que, acrescido a outros, contribuem para o inseguro cenário digital de quais são as possíveis consequências e efeitos na sociedade do uso e reprodução de conteúdos pela Inteligência Artificial.

3 PLÁGIO: A VIOLAÇÃO DE DIREITO AUTORAL

O plágio é o ato de apropriar-se indevidamente de propriedade intelectual e/ou imaterial que não lhe pertença, abrangendo obras literárias, artísticas e

científicas, sem que o autor seja devidamente creditado. Ele pode acontecer de maneira parcial ou integral a depender da quantidade de conteúdo afetado.

No Brasil, a violação de direito autoral é tipificada pela Lei de Direitos Autorais (Lei nº 9.610/98) que estabelece proteção às propriedades autorais e reconhece que os autores possuem direitos morais e patrimoniais sobre suas criações e que sua violação caracteriza uma infração legal, com possibilidade de repercussão na seara civil e penal. [4]

No âmbito penal, o Decreto-lei nº 2.848 de 7 de dezembro de 1940 (Código Penal), prevê possíveis sanções para os praticantes dessa conduta em seu art. 184:

> Art. 184. Violar direitos de autor e os que lhe são conexos:
>
> Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.
>
> § 1º Se a violação consistir em reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual, interpretação, execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, conforme o caso, ou de quem os represente:
>
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
>
> § 2º Na mesma pena do § 1º incorre quem, com o intuito de lucro direto ou indireto, distribui, vende, expõe à venda, aluga, introduz no País, adquire, oculta, tem em depósito, original ou cópia de obra intelectual ou fonograma reproduzido com violação do direito de autor, do direito de artista intérprete ou executante ou do direito do produtor de fonograma, ou, ainda, aluga original ou cópia de obra intelectual ou fonograma, sem a expressa autorização dos titulares dos direitos ou de quem os represente.
>
> § 3º Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente:
>
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

[4] BOAS, Sofia. Até Onde é Plágio? Definindo Limites de Apropriação de Conteúdo. Disponível em: https://www.jusbrasil.com.br/artigos/ate-onde-e-plagio-definindo-limites-de-apropriacao-de-conteudo/2802207847. Acesso em: 09 out.2025

> § 4º O disposto nos §§ 1º, 2º e 3º não se aplica quando se tratar de exceção ou limitação ao direito de autor ou os que lhe são conexos, em conformidade com o previsto na Lei nº 9.610, de 19 de fevereiro de 1998, nem a cópia de obra intelectual ou fonograma, em um só exemplar, para uso privado do copista, sem intuito de lucro direto ou indireto.

Anteriormente, a detecção e identificação desse tipo de delito dependia de uma análise criteriosa, minuciosa e até mesmo individual. Mas, com o avanço e influência crescentes da tecnologia e da IA, diversas plataformas que visam a detecção e o combate ao plágio foram criadas e desenvolvidas, como: *Turnitin*, *Grammarly*, *Copyscape e Plagscan.*[5] De certa forma, há de parecer que assim, o problema estaria resolvido, já que a própria IA encontra e cria soluções para os próprios problemas que desenvolve.

Contudo, diversos relatos de artistas têm chamado atenção com relação a plataformas de Inteligência Artificial que se apoderaram de suas obras sem dar os créditos aos seus autores originais. Ferramentas como o *DALL-E 2* da *OpenAI,* por exemplo, tem viralizado porque são capazes de gerar artes a partir de uma simples descrição textual. Em entrevista, o advogado Matthew Butterick afirma que:[6]

> Ouvimos pessoas de todo o mundo: escritores, artistas e programadores, que estão preocupados com essas AIs, que são treinadas com grandes quantidades de trabalhos protegidos por direitos autorais sem consentimento.

Ainda, o plágio com uso da Inteligência Artificial tem ido além de "criação de imagens e desenhos" e "reescrita de artigos e trabalhos científicos e acadêmicos" a partir de obras já existentes. Em 2024, dois dubladores profissionais processaram a *Lovo,* plataforma de IA que transforma texto em fala, por clonagem e venda ilegal de suas vozes.[7]

---

[5] ALVES, Ronan. Integridade Acadêmica na Era Digital: Ferramentas e Desafios da IA na Detecção de Plágio em Trabalhos Escolares. Disponível em: https://ronanalves.com.br/ia-na-deteccao-de-plagio-academico/. Acesso em: 13 out. 2025.

[6] GLOBO. Artistas processam empresas que geram arte com IA por violação de direitos autorais. Disponível em: https://g1.globo.com/tecnologia/noticia/2023/01/18/artistas-processam-empresas-que-geram-arte-com-ia-por-violacao-de-direitos-autorais.ghtml. Acesso em: 11 out.2025.

[7] LOPES, Talita. Dubladores processam empresa de IA por clonagem e venda ilegal de suas vozes.Disponível em: https://www.metroworldnews.com.br/social/2024/09/05/dubladores-processam-empresa-de-ia-por-clonagem-e-venda-ilegal-de-suas-vozes/. Acesso em: 11 out.2025.

Desse modo, fica o questionamento: e quando é a própria IA que pratica esse tipo de conduta? Ela ficaria isenta de responsabilidade? Seria possível responsabilizar os seus desenvolvedores por tal prática delituosa?

4 RESPONSABILIDADE NO COMBATE AO PLÁGIO

A propagação da inteligência artificial no mundo contemporâneo nos faz refletir sobre uma série de questões quanto à responsabilidade civil. Como pode a IA agir de forma autônoma? Gerando danos a terceiros quem detém a responsabilidade pelo prejuízo gerado, quem responderá pela reparação?

De acordo com Maria Helena Diniz (2014) a responsabilidade civil tem como dever reparar danos decorrentes de condutas que causam prejuízos a terceiros. Além disso, como aplicar a responsabilidade civil ao sistema IA tendo em vista a complexidade e a falta de legislação específica?

Vale ressaltar que no Brasil o primeiro documento aprovado oficialmente para abordar da IA foi a Estratégia Brasileira de Inteligência Artificial (EBIA) produzida pela Portaria nº 4.617 de 6 de abril de 2021, porém foi modificada pela Portaria n° 4.979 de 13 de julho de 2021, do Ministério da Ciência, Tecnologia e Inovação.

A EBIA tem como objetivos:

I. Contribuir para a elaboração de princípios éticos para o desenvolvimento e uso de IA responsáveis;

II. Promover investimentos sustentados em pesquisa e desenvolvimento em IA;

III. Remover barreiras à inovação em IA;

IV. Capacitar e formar profissionais para os ecossistemas da IA;

V. Estimular a inovação e o desenvolvimento da IA brasileira em ambiente internacional,

> VI. Promover ambiente de cooperação entre os entes públicos e privados, a indústria e os centros de pesquisas para o desenvolvimento da Inteligência Artificial.

Embora tenha iniciado a pauta sobre o avanço da IA no Congresso Nacional, por outro prisma houve pouco avanço no tocante à responsabilidade civil.

Todavia, a responsabilização civil é primordial dentro do Direito Civil o tem como propósito reparar danos causados a terceiros, assim como, assegurando que o autor do dano, ou quem detém a responsabilidade, responda pela reparação.[8]

O atual Código Civil manteve o princípio da responsabilidade com base na culpa, definindo o ato ilícito no art. 186, verbis:

> Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito".
>
> No art. 927, depois de estabelecer, no caput, que "aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo", dispôs, refletindo a moderna tendência, no parágrafo único, verbis:
>
> Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

A responsabilidade civil no código brasileiro é dividida em: responsabilidade subjetiva e responsabilidade objetiva.

Segundo GONÇALVES[9] (2025) a responsabilidade subjetiva consiste na comprovação de culpa do autor do dano, ou seja, somente se configura se agiu com dolo ou culpa. Portanto é necessário que exista: ação, omissão, nexo de causalidade, culpa ou dolo.

> Artigo. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.

Para TARTUCE (2018) a responsabilidade subjetiva, portanto, é imprescindível que se prove a culpa do agente para que ele seja obrigado a indenizar.

[8] Ministério da Ciência, Tecnologia e Inovação
[9] GONÇALVES, Carlos Roberto. Responsabilidade Civil - 24a Edição 2025. 14/02/2025: SaraivaJur, 2025.

Nos casos da responsabilidade objetiva, não exige a comprovação de culpa do agente, para que este seja responsabilizado a reparar o dano. Neste modelo, a responsabilidade processa-se pela existência de dano e de nexo de causalidade com o ato do autor, agente da ação. Para essa teoria aquele que desempenha uma atividade, cria-se um risco e com isso, deve-se arcar com as consequências, reparando os eventuais danos causados, ainda que seu ato seja isento de culpa.

Como dispõe o artigo 927, do Código Civil:

> Art. 927: Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
>
> Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

Com isso a responsabilidade objetiva torna-se relevante quanto ao assunto de inovação tecnológica, assim como nos casos dos sistemas de inteligência artificial.

Se tratando de inteligência artificial a aplicação da responsabilidade objetiva aponta como uma solução jurídica para reparação dos danos causados. A inteligência artificial exerce atividades, as quais possuem um risco elevado e consideradas a serem tratadas.

É válido que o responsável pelo desenvolvimento ou quem utiliza dessa ferramenta assuma os riscos desse exercício, sendo responsabilizado de forma objetiva pelos danos causados resultante do uso.

> Em conformidade com GOLÇALVES (2022)[10] , a responsabilidade civil é um princípio jurídico que se ocupa das implicações financeiras oriundas do não cumprimento de deveres legais ou contratuais por empresas, particularmente na prevenção ou correção de prejuízos causados a consumidores de seus produtos e serviços.

Em suma, aplicar a responsabilidade objetiva, procura proteger os indivíduos de danos gerados pela inteligência artificial, de forma que não seja necessário a comprovação de dolo ou culpa dos autores.

[10] DE CARVALHO, Lucca Tonetto; LINS, Robson Sitorski. A Aplicabilidade da Responsabilidade Civil nos Danos Causados por Inteligência Artificial. Revista Camalotes.

5 CONSIDERAÇÕES FINAIS

O atual cenário de crescente transformações tecnológicas e desenvolvimento da Inteligência Artificial no escopo social envolve enormes complexidades, desde os efeitos do uso da IA no cotidiano dos usuários à responsabilização de sua utilização no combate ao plágio.

Conforme discorrido ao longo do artigo, no Brasil, há tipificação da proteção de direitos autorais na Lei nº 9.610/98, em que se preserva as propriedades autorais, bem como seus direitos morais e patrimoniais de seus criadores que estabelece proteção às propriedades, com possibilidade de repercussão na seara civil e penal, em casos de violação.

Inúmeros são os exemplos de violações dos direitos autorais com o uso da Inteligência Artificial. Hodiernamente, no Brasil, a regulamentação das limitações do uso desse instrumento ainda é uma adversidade a ser superada e implementada cada vez mais na faceta do Direito Digital.

O dinamismo da situação permite a realização de reflexão acerca de a quem recairia a responsabilidade frente ao uso indevido da Inteligência Artificial. Ao considerar que essa ferramenta consolida bases de dados preexistentes na internet e oferece respostas a seus usuários, sem, muitas vezes, citar suas fontes, ou copiando técnicas artísticas na produção de imagens, caberia ao usuário ou aos órgãos competentes do Estado realizar essa fiscalização? Ou seria um passo anterior atribuir responsabilidade a seus desenvolvedores?

O presente artigo visa à reflexão sobre os efeitos da Inteligência Artificial no combate ao plágio, bem como a necessidade de melhor regulamentação desse cenário tão novo, mas tão expoente na sociedade. A atribuição de responsabilidade deve ser algo a ser considerado, interpretado, e atribuído a cada caso concreto, visando à manutenção da segurança dos usuários, informações e preservação dos direitos autorais.

REFERÊNCIAS

ALVES, Ronan. Integridade acadêmica na era digital: ferramentas e desafios da IA na detecção de plágio em trabalhos escolares. Disponível em: https://ronanalves.com.br/ia-na-deteccao-de-plagio-academico/. Acesso em: 13 out. 2025.

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

BOAS, Sofia. Até onde é plágio? Definindo limites de apropriação de conteúdo. Disponível em:https://www.jusbrasil.com.br/artigos/ate-onde-e-plagio-definindo-limites-de-apropriacao-de-conteudo/2802207847. Acesso em: 9 out. 2025.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. *Diário Oficial da União*, Rio de Janeiro, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 10 out. 2025.

DE CARVALHO, Lucca Tonetto; LINS, Robson Sitorski. A aplicabilidade da responsabilidade civil nos danos causados por inteligência artificial. *Revista Camalotes*, [s.l.], [s.d.].

GLOBO. Artistas processam empresas que geram arte com IA por violação de direitos autorais. Disponível em: https://g1.globo.com/tecnologia/noticia/2023/01/18/artistas-processam-empresas-que-geram-arte-com-ia-por-violacao-de-direitos-autorais.ghtml. Acesso em: 11 out. 2025.

GONÇALVES, Carlos Roberto. *Responsabilidade civil.* 24. ed. São Paulo: SaraivaJur, 2025.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. Inteligência artificial. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial. Acesso em: 17 out. 2025.

LOPES, Talita. Dubladores processam empresa de IA por clonagem e venda ilegal de suas vozes. Disponível em: https://www.metroworldnews.com.br/social/2024/09/05/dubladores-processam-empresa-de-ia-por-clonagem-e-venda-ilegal-de-suas-vozes/. Acesso em: 11 out. 2025.

SCHWAB, Klaus. *A Quarta Revolução Industrial.* Tradução: Daniel Moreira Miranda. São Paulo: Edipro, 2016. ISBN 978-85-7283-978-5.

VEJA. Uma brincadeira inocente ou plágio sinistro da inteligência artificial? Disponível em: https://veja.abril.com.br/coluna/mundialista/uma-brincadeira-inocente-ou-plagio-sinistro-da-inteligencia-artificial/. Acesso em: 9 out. 2025.

INTELIGÊNCIA ARTIFICIAL E ALGORITMOS: O NOVO DESAFIO PARA O DIREITO DA CONCORRÊNCIA

Ramon Santana Morel Gomes de Oliveira [1]

RESUMO

Este artigo realiza uma breve análise acerca do impacto da Inteligência Artificial no Direito da Concorrência, principalmente sobre as dificuldades e desafios na detecção e distinção entre comportamentos paralelos lícitos e práticas colusivas camufladas por algoritmos. O método de estudo se baseia na análise bibliográfica e em estudos de casos recentes, como o processo contra a plataforma imobiliária RealPage nos Estados Unidos e no caso de colusão entre motoristas do aplicativo Uber no Brasil. Diante das análises, os resultados indicam que as limitações atuais da legislação e das ferramentas de fiscalização criam uma "zona cinzenta" que favorece a colusão realizada com o auxílio da IA. Conclui-se que há a necessidade de uma regulamentação equilibrada da Inteligência Artificial que harmonize a segurança jurídica sem prejudicar a inovação tecnológica, com a constante supervisão humana e na transparência dos algoritmos como medidas mitigadoras essenciais, com o desenvolvimento de normas, como a PL nº 2.338/2023 no Brasil, sendo crucial para evitar que as práticas anticompetitivas se multiplique de forma indetectável.

Palavras-chave: Inteligência Artificial; Direito da Concorrência; Colusão Algorítmica; Regulamentação; CADE.

SUMÁRIO: 1. Introdução; 2. O potêncial da inovação da inteligência e a ameaça da colusão algorítmica no direito da concorrência; 3. Detecção; 4. Casos; 4.1. Estados Unidos; 4.2. Brasil; 5. Soluções; 6. Conclusão; 7. Bibliografia.

1 INTRODUÇÃO

A tecnologia durante a existência humana, sempre esteve inserida nos contextos culturais, ambientais, econômicos, políticos, sociais e comportamentais da

[1] Graduando em Direito pelo Centro Universitário de Brasília (CEUB). Lattes: https://lattes.cnpq.br/7400920348635281. Orcid Id: https://orcid.org/0009-0008-6649-0387.

sociedade[2]. É difícil manter-se distânte da interferência dos *"gadgets"*, principalmente daqueles que definem um antes e depois na sociedade, que, querendo ou não, acaba por se infiltrar em diversos âmbitos do cotidiano humano.

Com a Inteligência Artificial não foi diferente. Conhecida também pela sigla IA, se tornou mais um dos grandes marcos tecnológicos da humanidade, no sentido de modificar e influenciar vários fractais da vida humana. É uma "velha conhecida", inclusive, o termo e a tecnologia surgiram em 1956, na conferência de *Darthmouth College*, nos Estados Unidos, que reuniram cientistas e teóricos da computação, para dialogarem acerca dessa tecnologia em nascimento[3].

Entretanto, nos anos recentes pós-pandemia de COVID-19, a Inteligência Artificial ganhou maior relevância na sociedade e uma rápida evolução e ascensão tecnológica, se tornando cada vez mais aperfeiçoada, inclusive, possuindo vários concorrentes entre si, como o Chat GPT, Gemini (Google), Amazon (AWS) e entre outros entes privados do meio. O impacto da Inteligência Artificial foi tão intenso, que as pessoas buscam se qualificar no seu manuseio, igualmente ao que ocorria com a datilografia e as oficinas de informática que existiam no anteriormente.

Como todo advento de uma nova tecnologia, além de ter os seus benefícios, surgem sintomas que podem prejudicar o coletivo humano, sendo imprescindível a sua regulamentação[4]. Como debatido na filosofia do direito, o direito sempre vem depois, pois busca sempre a se adaptar aos fenômenos sociais.

No Direito da Concorrência não foi diferente. Desde 2021, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), demonstrou preocupação em relação à proteção da concorrência no mercado digital, cominando

[2] HAYNE, Luíz Augusto; WYSE, Angela Terezinha de Souza. Análise da evolução da tecnologia: uma contribuição para o ensino da ciência e tecnologia. Revista Brasileira de Ensino de Ciência e Tecnologia, v. 11, n. 3, 2018. Disponível em: https://periodicos.utfpr.edu.br/rbect/article/view/5947. p. 2.

[3] DOS SANTOS, Paulo Argôlo; SANTOS, João Almeida. Os Desafios da Regulamentação da Inteligência Artificial (IA) no Brasil em Relação a Alguns Países Desenvolvidos. Ver. FSA, Teresina, v. 21, n.6, art. 2, p. 27-45, junho de 2024. Disponível em: http://www4.unifsa.com.br/revista/index.php/fsa/article/view/2905/491494351. p. 1.

[4] DOS SANTOS, Paulo Argôlo; SANTOS, João Almeida. Os Desafios da Regulamentação da Inteligência Artificial (IA) no Brasil em Relação a Alguns Países Desenvolvidos. Ver. FSA, Teresina, v. 21, n.6, art. 2, p. 27-45, junho de 2024. Disponível em: http://www4.unifsa.com.br/revista/index.php/fsa/article/view/2905/491494351 p. 3.

na publicação de seu artigo de análise sobre negócios e finanças em 2021[5], fazendo previsões do que poderia ocorrer à longo prazo e de quais mitigações que poderiam ser realizadas para contornar os possíveis problemas, principalmente acerca das colusões e formações de monopólios por meio de algoritmos, chamados de colusão algorítmica.

No Brasil, já houve investigações sobre esses tipos de práticas por parte do Conselho Administrativo de Defesa Econômica (CADE), baseadas nos termos da Lei de Defesa da Concorrência[6]. O marco legal da Lei 12.529/2011 se adequa às colusões praticadas pelo auxílio do algoritmo. Entretanto, com as dificuldades enfrentadas durante as investigações, foi constatado, de um aspecto geral, que a Lei brasileira necessita ser atenciosa acerca da regulamentação da Inteligência Artificial.

2 O POTÊNCIAL DA INOVAÇÃO DA INTELIGÊNCIA E A AMEAÇA DA COLUSÃO ALGORÍTMICA NO DIREITO DA CONCORRÊNCIA

É inegável assumir que a Inteligência Artificial é uma ferramenta importante e de grande valia. Inclusive, podendo gerar benefícios em prol da concorrência saudável. Sendo um deles, a melhoria de previsões, otimização de operações, alocações eficazes de recursos, personalização de serviços para a sociedade e o meio ambiente e a promoção de vantagens competitivas[7] . Inclusive, a IA pode fomentar a inovação[8] , que pode garantir um ambiente concorrêncial saudável para os players.

[5] OECD (2021), OECD Business and Finance Outlook 2021: AI in Business and Finance, OECD Publishing, Paris, https://doi.org/10.1787/ba682899-en.

[6] BRASIL. Lei 12.529, de 30 de novembro de 2011. Lei que estrutura o Sistema Brasileiro da Defesa da Concorrência – SBDC e dispõe sobre a prevenção e a repressão às infrações contra a ordem econômica, orientada pelos ditames constitucionais de liberdade de iniciativa, livre concorrência, função social da propriedade, defesa dos consumidores e repressão ao abuso do poder econômico. **Planalto.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12529.htm.

[7] ADRISE, Lage de Mendonça Mendes; GRACE, Ladeira Garbaccio; LAVOURAS, Maria Matilde. Regulação da Inteligência Artificial no Âmbito da Concorrência: uma maneira de Promover ou Inibir a Inovação?. **Revista Opinião Jurídica,** Fortaleza, v. 22, n. 40, p. 162-180, maio/ago. 2024. Disponível em: https://periodicos.unichristus.edu.br/opiniaojuridica/article/view/5455. p. 8.

[8] DOS SANTOS, Paulo Argôlo; SANTOS, João Almeida. Os Desafios da Regulamentação da Inteligência Artificial (IA) no Brasil em Relação a Alguns Países Desenvolvidos. Ver. FSA, Teresina, v. 21, n.6, art. 2, p. 27-45, junho de 2024. Disponível em: http://www4.unifsa.com.br/revista/index.php/fsa/article/view/2905/491494351. p. 8.

Isso é possível caso seja utilizado com ética e responsabilidade, conforme prevê a norma européia, que foi aprovada pelo Parlamento da União Européia em 2023, que é considerado a primeira regulação da IA no Mundo, conhecida como o "AI Act".

Mesmo possuindo propósitos e funções positivas, a Inteligência Artificial pode ser um meio para realizar práticas anticompetitivas, facilitando as colusões e as formações de cartéis com métodos inovadores e discretos. Um dos desafios enfrentados atualmente pelas autoridades antitruste pelo Mundo é detecção de algorítmos. Essa forma de colusão dificulta a obtenção de provas para comprovar as práticas anticompetivas[9]. Mas como as decisões das praticas ilegais são feitas por máquinas, a tarefa de detectar os algoritmos se tornam ainda mais complicadas[10], sendo um desafio técnico extenso.

3 DETECÇÃO

As limitações das autoridades antitruste dão vantagem ao cometimento de concluio auxiliado pelas Inteligências Artificiais, facilitando os concluios e as condutas abusivas, como o monitoriamento de cartel existente, que seria uma espécie de vigilância do "companheiro de cartel", com o objetivo de, por exemplo, manter a fixação de preços que foram acordados entre os entes do cartel, buscando trazer a estabilidade do cartel; a facilitação da entrada de cartéis, que pode ser feito por acordos colusivos sem o contato direto entre os entes, pois normalmente, um dos principais meios de provas são os contatos ilícitos entre os cartéis; e a facilitação de colusão tácita, onde os preços podem ser combinados entre os entes pelas Inteligências artificais, porém, não deixando vestígios de acordo tácito explicito[11].

[9] ADRISE, Lage de Mendonça Mendes; GRACE, Ladeira Garbaccio; LAVOURAS, Maria Matilde. Regulação da Inteligência Artificial no Âmbito da Concorrência: uma maneira de Promover ou Inibir a Inovação?. **Revista Opinião Jurídica,** Fortaleza, v. 22, n. 40, p. 162-180, maio/ago. 2024. Disponível em: https://periodicos.unichristus.edu.br/opiniaojuridica/article/view/5455. p. 6.

[10] ADRISE, Lage de Mendonça Mendes; GRACE, Ladeira Garbaccio; LAVOURAS, Maria Matilde. Regulação da Inteligência Artificial no Âmbito da Concorrência: uma maneira de Promover ou Inibir a Inovação?. **Revista Opinião Jurídica,** Fortaleza, v. 22, n. 40, p. 162-180, maio/ago. 2024. Disponível em: https://periodicos.unichristus.edu.br/opiniaojuridica/article/view/5455. p. 6.

[11] BERGQVIST, Christian; RINGELING, Camilla; CAMACHO, Mariana. Concluio por inteligência artificial: devemos nos preocupar? **Revista de Defesa da Concorrência**, Brasília, v. 12, n. 2, p. 11-31.

Isso acaba por gerar uma "zona cinzenta"[12], deixando as coordenações anticompetitivas camufladas para as autoridades antitruste. Normalmente, para provar se houveram condutas abusivas, são realizadas análises de evidências econômicas acerca dos ajustes de preços entre as entidades por um certo período de tempo[13]. Nesses estudos, almeja identificar se os ajustes de preços realizado pelas entidades econômicas foram comportamentos paralelos ou colusivas[14].

O comportamento colusivo é caracterizado pelo dolo ou a intenção de eliminar o concorrente e a concorrência, por meio da restrição da competição, buscando obter mais lucros entre as empresas que deveriam competir entre si. Os entes acabam por atuar em cooperação, buscando o controle do monopólio.

Entretanto, em primeiro momento, o comportamento paralelo pode parecer um ato ilegal. Mas em outras circunstâncias, pode ser um acontecimento natural no meio da concorrência, onde os concorrentes precificam de maneira aproximada ou semelhante os seus produtos e serviços, mas de forma independente, sem a existência de acordo colusivo. Porém, as empresas podem utilizar essa prática como "fachada" para acordos colusivos, disfarçando os atos ilícitos para dificultar a atuação da autoridade antitruste.

Na União Europeia[15], uma reunião entre os concorrentes combinado com um comportamento paralelo, se tornam elementos suficientes para se configurar um acordo colusivel. Na norma dos EUA, que inspira as normas dos países latino-americanos, identificam a ação colusiva por evidências indiretas e com ampla

Disponível em: https://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/issue/view/67/89. p. 13

[12] BERGQVIST, Christian; RINGELING, Camilla; CAMACHO, Mariana. Concluio por inteligência artificial: devemos nos preocupar? **Revista de Defesa da Concorrência,** Brasília, v. 12, n. 2, p. 11-31. Disponível em: https://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/issue/view/67/89. p. 13.

[13] BERGQVIST, Christian; RINGELING, Camilla; CAMACHO, Mariana. Concluio por inteligência artificial: devemos nos preocupar? **Revista de Defesa da Concorrência,** Brasília, v. 12, n. 2, p. 11-31. Disponível em: https://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/issue/view/67/89. p. 25.

[14] BERGQVIST, Christian; RINGELING, Camilla; CAMACHO, Mariana. Concluio por inteligência artificial: devemos nos preocupar? **Revista de Defesa da Concorrência,** Brasília, v. 12, n. 2, p. 11-31. Disponível em: https://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/issue/view/67/89. p. 25.

[15] BERGQVIST, Christian; RINGELING, Camilla; CAMACHO, Mariana. Concluio por inteligência artificial: devemos nos preocupar? **Revista de Defesa da Concorrência,** Brasília, v. 12, n. 2, p. 11-31. Disponível em: https://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/issue/view/67/89. p. 29.

discricionariedade, que acabam por gerar diversas interpretações e decisões inconstantes. As vezes, a ampla subjetividade pode gerar decisões diferentes para casos que possuam circunstâncias semelhantes[16].

Porém, em um aspecto geral, os dois "mundos" possuem a mesma dificuldade de distinguir os comporamentos paralelos dos comportamentos colusivos[17], se tornando um desafio em conjunto.

4 CASOS

4.1 Estados Unidos

No ramo imobiliário dos Estados Unidos, houve o recente caso com a plataforma RealPage, Inc., que gerência por meio do seu software de algoritmos, os valores dos imóveis que são destinados para habitações de aluguel.

A RealPage foi acusada e condenada pelo Departamento de Justiça dos Estados Unidos (DOJ) em 2024[18], por formar cartel juntamente com os seus clientes, no caso, os proprietários dos imóveis, realizando a troca de informações sensíveis para fixar preços entre os outros proprietários de imóveis, com o auxilio dos algoritmos.

Devido a essa conduta anticompetitiva, não havia a variação de preços entre os imóveis, havendo a limitação de escolha de habitação e o aumento dos preços dos alugueis, reduzindo a quantidade de locatários interessados.

4.2 Brasil

[16] BERGQVIST, Christian; RINGELING, Camilla; CAMACHO, Mariana. Concluio por inteligência artificial: devemos nos preocupar? **Revista de Defesa da Concorrência,** Brasília, v. 12, n. 2, p. 11-31. Disponível em: https://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/issue/view/67/89. p. 29.

[17] BERGQVIST, Christian; RINGELING, Camilla; CAMACHO, Mariana. Concluio por inteligência artificial: devemos nos preocupar? **Revista de Defesa da Concorrência,** Brasília, v. 12, n. 2, p. 11-31. Disponível em: https://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/issue/view/67/89. p. 24.

[18] UNITED STATES. Department of Justice (DOJ). Justice Department Sues RealPage for Algorithmic Pricing Scheme that Harms Millions of American Renters. **Press Release,** 1º de novembro de 2023. Disponível em: https://www.justice.gov/archives/opa/pr/justice-department-sues-realpage-algorithmic-pricing-scheme-harms-millions-american-renters.

No Estado de São Paulo, a Associação de Motoristas Autônomos de Aplicativos (AMAA) apresentou denúncia ao CADE, alegando que os motoristas parceiros com a Uber, estariam praticando o cartel tipo *hube and spoke*, onde os motoristas estariam utilizando o aplicativo da Uber para fixar preços.

A denuncia alegava que os motoristas do aplicativo se comunicavam entre si, para propor estratégias de utilização do aplicativo, para manipular o multiplicador de preço do aplicativo, havendo o desquelibrio entre a oferta de motoristas e a demanda de passageiros, que por consequência, aumentaria a receita dos motoristas.

Entretanto, após a investigações da Superintendência Geral do CADE, não houve entendimento e identificação de prática de cartel *hube and spoke*. Além de não haver o lastro probatório suficiente para comprovar que o desligamento do aplicativo entre os motoristas não influenciava o multiplicador de preço do aplicativo, a própria ação de realizar esse desligamento não aumentava a receita dos motoristas.

O aplicativo calculava os seus preços no momento, com base ao tempo de viagem e distância da corrida. Em certos exemplos expostos na nota técnica[19], o mesmo destino final poderia variar de preço, de acordo com a distância percorrida e o tempo de viagem.

Aliás, o modo de precificação da Uber foi vista como um meio de otimizar a demanda e a oferta de transporte individual de passageiros[20], não havendo práticas anticoncorrêncial entre os outros aplicativos do mesmo ramo.

5 SOLUÇÕES

É evidente a necessidade de haver a regulação para a Inteligência Artificial no âmbito da concorrência. A IA pode ser uma ferramenta perigosa para a manutenção da concorrência, pois, pode de fato restringir que novos concorrentes

[19] Ver, CADE, Processo Preparatório nº 08700.008318/2016-29.
[20] BERGQVIST, Christian; RINGELING, Camilla; CAMACHO, Mariana. Concluio por inteligência artificial: devemos nos preocupar? **Revista de Defesa da Concorrência,** Brasília, v. 12, n. 2, p. 11-31. Disponível em: https://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/issue/view/67/89. p. 25.

possam entrar e disputar no mercado de forma justa[21]. Os novos *players* por si só já possuem desvantagens em relação aos entes já consolidados no mercado, principalmente por motivos econômicos, onde normalmente os orçamentos são mais limitados e que a consolidação dos lucros ocorre a longo prazo, como naturalmente acontece.

A regulação é importante. Porém, há o debate sobre o tema para se alcançar o equilibro dessas normas, para evitar o destimulação da inovação tecnológica da IA. O excesso e a falta de regulação podem ser negativas para o ambiente concorrencial[22]. Um dos principais argumentos sobre o excesso de regulamentação, são os efeitos colaterais da estagnação do desenvolvimento tecnológico da IA. A inovação caminha paralelamente com o desenvolvimento humano, e a falta de estímulo à inovação pode ser a decretação do fim da Inteligência Artificial. Um dos objetivos fundamentais do direito da concorrência é a busca pela inovação[23], tornando isso inviável, não há sentido do direito antitruste em colocar tantas amarras para evitar a inovação entre os concorrentes. Os legisladores, nesse sentido, buscam encontrar a harmonia da inovação com a segurança jurídica.

Acredita-se que a supervisão humana e a transparência em relação ao funcionamento desses algoritmos podem ser uma das formas de mitigar o problema da colusão[24], sendo um ponto de vista técnico, que busca evitar que todas as decisões sejam tomadas automáticamente pelas máquinas.

Já existem propostas em tramitação acerca da regulação do assunto pelo Projeto de Lei nº 2.338/2023 no legislativo brasileiro. A norma, que se encontra remetida nesse momento na Câmara dos Deputados, busca exatemente dar ênfase à

[21] ADRISE, Lage de Mendonça Mendes; GRACE, Ladeira Garbaccio; LAVOURAS, Maria Matilde. Regulação da Inteligência Artificial no Âmbito da Concorrência: uma maneira de Promover ou Inibir a Inovação?. **Revista Opinião Jurídica,** Fortaleza, v. 22, n. 40, p. 162-180, maio/ago. 2024. Disponível em: https://periodicos.unichristus.edu.br/opiniaojuridica/article/view/5455. p. 6.

[22] ADRISE, Lage de Mendonça Mendes; GRACE, Ladeira Garbaccio; LAVOURAS, Maria Matilde. Regulação da Inteligência Artificial no Âmbito da Concorrência: uma maneira de Promover ou Inibir a Inovação?. **Revista Opinião Jurídica,** Fortaleza, v. 22, n. 40, p. 162-180, maio/ago. 2024. Disponível em: https://periodicos.unichristus.edu.br/opiniaojuridica/article/view/5455. p. 6.

[23] SILVEIRA, Paulo Burnier da. Direito da Concorrência. 1. Ed. Rio de Janeiro: Editora Forense, 2021. p.3

[24] ADRISE, Lage de Mendonça Mendes; GRACE, Ladeira Garbaccio; LAVOURAS, Maria Matilde. Regulação da Inteligência Artificial no Âmbito da Concorrência: uma maneira de Promover ou Inibir a Inovação?. **Revista Opinião Jurídica,** Fortaleza, v. 22, n. 40, p. 162-180, maio/ago. 2024. Disponível em: https://periodicos.unichristus.edu.br/opiniaojuridica/article/view/5455. p. 10.

supervisão humana nos sistemas de IA, principalmente as IA's classificadas de alto risco[25]. Da mesma forma, a PL busca também garantir a proteção e direitos às pessoas que sofreram consequências pela utilização inadequada da Inteligência Artificial.

A regularização que consiga atingir o equilibro, respeitando os limites do desenvolvimento tecnológico, pode proteger a concorrência justa e o próprio desenvolvimento tecnológico. Garantindo a qualidade, a diversidade e um preço condizente para o consumidor final e a concorrência saudável entre os vendedores e fornecedores de produtos e serviços.

6 CONCLUSÃO

Conforme todo o cenário, não somente apresentado neste trabalho, mas o que acontece no cotidiano, é evidente que a Inteligência Artificial necessita de regulamentação para definir os limites de seu uso. Além de ter vindo para ficar, é uma ferramenta que possui um imenso poder, independentemente do objetivo de sua utilização.

Acredita-se que a regulamentação da IA não esteja somente focada acerca de sua utilização como um todo, mas também no âmbito da concorrência, sendo uma regularização paralela entre os dois temas e que podem ser desenvolvidas simultaneamente.

Devido à rápida evolução do sistema de IA, é necessário que a legislação consolide as normas acerca da transparência e o *compliance* na utilização do sistema. E que ao mesmo tempo, consiga conciliar as restrições impostas pela regulação com o desenvolvimento tecnológico, evitando que ocorra a ruína da Inteligência Artificial[26] Com o passar do tempo, a Inteligência Artificial tende a se tornar mais

[25] BRASIL. PL nº 2338/2023. Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. **Câmara Legislativa.** Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2868197&filename=PL%2023 38/2023 (art. 6º)

[26] ADRISE, Lage de Mendonça Mendes; GRACE, Ladeira Garbaccio; LAVOURAS, Maria Matilde. Regulação da Inteligência Artificial no Âmbito da Concorrência: uma maneira de Promover ou Inibir a

complexa, tornando mais difícil a detecção das práticas anticompetitivas pelas autoridades antitruste pelo mundo.

Desse modo, é importante e urgente o aprofundamento e a aplicação da regulação da utilização da Inteligência Artificial, para não o problema não se tornar um "bola de neve". Evitando que se multipliquem as praticas anticompetitivas e que a sua detecção não se torne uma tarefa difícil para os agentes fiscalizadores e investigadores do assunto.

REFERÊNCIAS

ADRISE, Lage de Mendonça Mendes; GRACE, Ladeira Garbaccio; LAVOURAS, Maria Matilde. Regulação da Inteligência Artificial no Âmbito da Concorrência: uma maneira de Promover ou Inibir a Inovação?. **Revista Opinião Jurídica,** Fortaleza, v. 22, n. 40, p. 162-180, maio/ago. 2024. Disponível em: https://periodicos.unichristus.edu.br/opiniaojuridica/article/view/5455.

BERGQVIST, Christian; RINGELING, Camilla; CAMACHO, Mariana. Concluio por inteligência artificial: devemos nos preocupar? **Revista de Defesa da Concorrência,** Brasília, v. 12, n. 2, p. 11-31. Disponível em: https://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/issue/view/67/89.

HAYNE, Luíz Augusto; WYSE, Angela Terezinha de Souza. Análise da evolução da tecnologia: uma contribuição para o ensino da ciência e tecnologia. Revista Brasileira de Ensino de Ciência e Tecnologia, v. 11, n. 3, 2018. Disponível em:

https://periodicos.utfpr.edu.br/rbect/article/view/5947.

OECD (2021), OECD Business and Finance Outlook 2021: AI in Business and Finance, OECD Publishing, Paris, https://doi.org/10.1787/ba682899-en.

DOS SANTOS, Paulo Argôlo; SANTOS, João Almeida. Os Desafios da Regulamentação da Inteligência Artificial (IA) no Brasil em Relação a Alguns Países Desenvolvidos. Ver. FSA, Teresina, v. 21, n.6, art. 2, p. 27-45, junho de 2024. Disponível em: http://www4.unifsa.com.br/revista/index.php/fsa/article/view/2905/491494351.

SILVEIRA, Paulo Burnier da. Direito da Concorrência. 1. Ed. Rio de Janeiro: Editora Forense, 2021.

Inovação?. **Revista Opinião Jurídica,** Fortaleza, v. 22, n. 40, p. 162-180, maio/ago. 2024. Disponível em: https://periodicos.unichristus.edu.br/opiniaojuridica/article/view/5455. p. 13.

PROTEÇÃO DE DADOS E INTELIGÊNCIA ARTIFICIAL: ENTRE A INOVAÇÃO E A TUTELA DOS DIREITOS FUNDAMENTAIS NA ERA ALGORÍTMICA

Eduardo Rodrigues Miranda Martins[1]

RESUMO

Este artigo examina a relação entre as legislações de proteção de dados — em especial a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) — e o treinamento de sistemas de Inteligência Artificial (IA), discutindo os desafios jurídicos, técnicos e éticos decorrentes do uso massivo de dados pessoais. Analisa-se princípios como finalidade, necessidade, transparência, minimização e responsabilização moldam o ciclo de vida dos dados em modelos algorítmicos. O estudo aborda temas como anonimização, vieses e governança algorítmica, responsabilidade civil, explicabilidade e bases legais para o treinamento de IA, bem como a interação entre a LGPD, o GDPR, o AI Act europeu e o Projeto de Lei nº 2.338/2023, que institui o Marco Legal da IA no Brasil. Conclui-se que a proteção de dados não constitui barreira à inovação, mas fundamento indispensável para uma IA ética, confiável e democrática.

Palavras-chave: Proteção de Dados; Inteligência Artificial; LGPD; GDPR; Governança Algorítmica; Privacidade; IA Responsável; Marco Legal da IA; Treinamento de Modelos.

SUMÁRIO: 1 Introdução; 2 Marco Legal da Proteção de Dados; 2.1 Regulamento Geral de Proteção de Dados (GDPR); 2.2 LGPD; 2.3 Convergências e Modelos Internacionais; 3 Treinamento de Modelos de IA e uso de Dados; 4 Aplicação das Leis ao Treinamento de IA; 5 Desafios Éticos e Jurídicos; 5.1 Vieses Algorítmicos; 5.2 Responsabilidade Civil; 5.3 Governança Algorítmica; 6 Perspectivas Futuras e Tendências Regulatórias da Inteligência Artificial; 6.1 o AI ACT Europeu; 6.2 Marco Regulatório da IA no Brasil; 6.3 Convergência Internacional; 6.4 Inovações Técnicas para Mitigação de Riscos; 7 Conclusão; Referências

1 INTRODUÇÃO

[1] Graduando em Direito do UniCEUB – Centro Universitário de Brasília - E-mail: eduardo2004.martins@sempreceub.com

A Inteligência Artificial (IA) consolidou-se como um dos principais vetores da transformação digital, capaz de redefinir estruturas econômicas, reorganizar dinâmicas sociais e influenciar diretamente práticas institucionais.

Seu potencial decorre, sobretudo, da capacidade de processar grandes volumes de dados, identificar padrões complexos e automatizar decisões antes restritas à intervenção humana.

Esse mesmo potencial, entretanto, expõe questões sensíveis relacionadas à privacidade, à discriminação algorítmica, à autonomia individual e à própria legitimidade das decisões automatizadas.

Em um cenário em que dados constituem o "combustível" dos sistemas de IA, a proteção de informações pessoais torna-se elemento central para o funcionamento seguro e ético dessas tecnologias.

O Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e a Lei Geral de Proteção de Dados brasileira (LGPD) emergem como marcos normativos estruturantes, destinados a equilibrar inovação e tutela de direitos fundamentais.

Seus princípios — finalidade, necessidade, adequação, minimização, transparência, segurança e responsabilização — orientam não apenas o tratamento de dados, mas também o próprio design, o ciclo de vida e a governança dos modelos algorítmicos.

A complexidade desse cenário aumenta quando se consideram as dinâmicas tecnológicas contemporâneas, como o uso de dados massivos (*big data*), o surgimento de modelos opacos de aprendizado profundo, a sofisticação das técnicas de reidentificação e o rápido avanço regulatório internacional.

A interação entre essas dimensões revela desafios que extrapolam a mera conformidade legal, exigindo abordagens interdisciplinares que integrem direito, ciência da computação, ética e políticas públicas.

Diante desse contexto, o presente artigo tem como objetivo examinar de forma sistemática a relação entre proteção de dados e Inteligência Artificial,

analisando os impactos jurídicos, técnicos e éticos decorrentes do treinamento e da operação de sistemas algorítmicos.

Para isso, discute-se o marco jurídico da privacidade e da proteção de dados, os fundamentos técnicos do uso de dados na IA, as bases legais aplicáveis ao treinamento de modelos, os riscos associados à anonimização e à reidentificação, bem como os dilemas referentes à explicabilidade, à discriminação algorítmica e à responsabilidade civil.

Além disso, avaliam-se as tendências regulatórias globais — com destaque para o AI Act europeu e para o Projeto de Lei nº 2.338/2023 no Brasil — e as inovações técnicas voltadas à mitigação de riscos, como privacidade diferencial, aprendizado federado e dados sintéticos.

Ao final, sustenta-se que a proteção de dados não representa uma barreira ao desenvolvimento tecnológico, mas um elemento estruturante de confiança, legitimidade e sustentabilidade social da Inteligência Artificial.

Assim, compreender a relação entre IA e a privacidade ser condição indispensável para assegurar que a inovação tecnológica se traduza em benefícios coletivos, compatíveis com a dignidade humana e com os direitos fundamentais na era algorítmica.

2 MARCO LEGAL DA PROTEÇÃO DE DADOS

A proteção de dados pessoais consolidou-se, nas últimas décadas, como um dos pilares normativos fundamentais para a regulação da economia digital.

Com a crescente centralidade da informação na organização das atividades econômicas e sociais, emerge a necessidade de instrumentos jurídicos capazes de assegurar a autodeterminação informativa dos indivíduos e limitar o poder de coleta, tratamento e monetização dos dados por agentes públicos e privados.

Nesse cenário, os marcos legais de proteção de dados, especialmente o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e a Lei Geral de Proteção de Dados brasileira (LGPD), assumem papel estruturante ao estabelecer

princípios, direitos e obrigações destinados a equilibrar inovação tecnológica e tutela de direitos fundamentais.

A evolução dessas legislações está diretamente relacionada ao reconhecimento de que a assimetria informacional entre titulares de dados e organizações se intensificou com o uso de tecnologias avançadas, como *big data*, *machine learning* e, mais recentemente, modelos generativos de IA.

O deslocamento das fronteiras tradicionais de privacidade — antes vinculadas ao sigilo, ao controle individual e ao consentimento — para um ambiente em que decisões automatizadas influenciam oportunidades e liberdades reforça a necessidade de um arcabouço jurídico robusto, dotado de princípios flexíveis e aplicáveis a diferentes contextos tecnológicos.

O GDPR, em vigor desde 2018, representa o marco mais expressivo dessa nova fase regulatória ao instituir um sistema abrangente, centrado na responsabilização objetiva do controlador, no fortalecimento dos direitos dos titulares e na adoção de medidas preventivas, como avaliações de impacto, *privacy by design* e *privacy by default*. Mais que um conjunto de regras, o regulamento europeu inaugura uma filosofia regulatória que combina flexibilidade tecnológica com rigor na proteção de direitos fundamentais, estabelecendo padrões globais de governança de dados e influenciando legislações em diversas jurisdições.

A LGPD, por sua vez, embora inspirada no modelo europeu, adapta-se ao contexto jurídico e institucional brasileiro ao incorporar princípios como boa-fé, adequação, necessidade, não discriminação e responsabilização, além de atribuir à Autoridade Nacional de Proteção de Dados (ANPD) competências normativas, fiscalizatórias e sancionatórias.

A criação da ANPD representa avanço institucional importante, pois garante a centralização da interpretação normativa, a padronização de práticas de conformidade e o diálogo contínuo entre Estado, setor privado, sociedade civil e comunidade científica.

Em nível internacional, observa-se um movimento de convergência regulatória baseado na necessidade de harmonizar práticas comerciais e garantir padrões mínimos de proteção.

Normas como o California Consumer Privacy Act (CCPA), o Personal Information Protection and Electronic Documents Act (PIPEDA) do Canadá, além dos princípios da OCDE, das diretrizes da UNESCO e de legislações emergentes na Ásia, evidenciam a formação de um ecossistema global de proteção de dados, ainda que com diferentes graus de rigor e abrangência.

Essa convergência ganha relevância especial no contexto da IA, em que fluxos internacionais de dados, interoperabilidade e responsabilidade transnacional constituem desafios crescentes.

Nesse ambiente multifacetado, os marcos legais de proteção de dados cumprem três funções essenciais: ***i)*** estabelecer limites e salvaguardas ao tratamento de dados pessoais; ***ii)*** promover maior transparência e responsabilidade no uso de tecnologias emergentes; e ***iii)*** fornecer diretrizes normativas para o desenvolvimento ético e seguro de sistemas de IA.

Assim, o entendimento dos fundamentos e da lógica estruturante desses marcos é requisito indispensável para analisar, nos tópicos seguintes, como suas disposições se aplicam ao treinamento de modelos algorítmicos, à governança da IA e à mitigação de riscos associados.

2.1 Regulamento Geral de Proteção de Dados (GDPR)

O Regulamento Geral de Proteção de Dados (GDPR), em vigor desde maio de 2018 na União Europeia, constitui o marco normativo mais abrangente e influente no campo da proteção de dados.

Sua relevância decorre tanto da densidade jurídica quanto da adoção de uma abordagem baseada em princípios, *accountability* e gestão de riscos, que confere ao regulamento flexibilidade para acompanhar a evolução tecnológica, incluindo sistemas avançados de Inteligência Artificial.

O GDPR estabelece um conjunto robusto de princípios — como limitação da finalidade, minimização, precisão, limitação do armazenamento, integridade e confidencialidade — que orientam todo o ciclo de vida dos dados. Sua inovação central, contudo, reside no princípio da responsabilização (accountability), que impõe ao controlador o dever de demonstrar, de forma ativa e contínua, a conformidade com o regulamento.

Essa abordagem desloca o eixo da regulação de modelos prescritivos para mecanismos de governança, transparência e prevenção.

Outro aspecto fundamental é o fortalecimento dos direitos dos titulares, como acesso, portabilidade, oposição, retificação, restrição do tratamento e apagamento.

O direito de não se submeter exclusivamente a decisões automatizadas, previsto no artigo 22, possui impacto direto sobre sistemas de IA, ao exigir explicabilidade suficiente para permitir a contestação de decisões algorítmicas, bem como intervenção humana significativa em processos de alto risco.

O GDPR também introduz instrumentos normativos específicos para atividades de risco elevado, como as Avaliações de Impacto à Proteção de Dados (DPIA), obrigatórias quando o tratamento envolve monitoramento sistemático, dados sensíveis em larga escala ou decisões automatizadas com efeitos jurídicos relevantes.

Além disso, mecanismos como *privacy by design*, *privacy by default*, registros de operações de tratamento e obrigações de segurança reforçam a incorporação da proteção de dados às fases de concepção, desenvolvimento e operação de sistemas algorítmicos.

Do ponto de vista institucional, as autoridades de proteção de dados dos Estados-Membros, articuladas pelo Comitê Europeu de Proteção de Dados (EDPB), exercem papel central no monitoramento, uniformização interpretativa e aplicação de sanções, cuja gravidade — alcançando até 4% do faturamento global — estabelece incentivos regulatórios eficazes.

O GDPR, portanto, transcende a mera regulação de privacidade ao impor padrões de governança que influenciam diretamente o design e a operacionalização de sistemas de Inteligência Artificial, especialmente aqueles de alto risco ou opacos.

2.2 LGPD

A Lei Geral de Proteção de Dados (LGPD), em vigor no Brasil desde 2020, representa a consolidação normativa da proteção de dados como direito fundamental e estabelece um arcabouço jurídico inspirado no GDPR, mas adaptado ao contexto regulatório e institucional brasileiro.

Sua estrutura baseia-se em um conjunto de princípios, direitos, bases legais e obrigações aplicáveis a agentes de tratamento públicos e privados.

Entre seus princípios mais relevantes destacam-se: finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização. Esses princípios orientam o tratamento de dados em todas as etapas, incluindo coleta, armazenamento, compartilhamento, uso e eliminação, impactando diretamente práticas técnicas e organizacionais no desenvolvimento de sistemas de IA.

A LGPD prevê dez bases legais, distribuídas entre hipóteses associadas ao consentimento e hipóteses independentes de consentimento — como cumprimento de obrigação legal, execução de contrato, tutela da saúde, proteção ao crédito e legítimo interesse.

No contexto da IA, os maiores desafios jurídicos recaem sobre a definição da base legal adequada para o treinamento de modelos com dados pessoais, especialmente quando envolve dados coletados massivamente, reutilizados ou submetidos a combinações capazes de gerar perfis extensos.

Outro ponto relevante é o tratamento de dados sensíveis, sujeito a requisitos mais rigorosos e bases legais restritas, o que impacta sistemas de IA aplicados à saúde, biometria, reconhecimento facial ou análises comportamentais.

A lei também estabelece salvaguardas adicionais para tratamento automatizado de dados, como o direito à revisão de decisões automatizadas e a exigência de informações claras sobre critérios e procedimentos adotados.

A criação da Autoridade Nacional de Proteção de Dados (ANPD) é um marco institucional significativo.

A ANPD possui competência normativa, fiscalizatória e sancionatória, atuando na interpretação da lei, na regulamentação de temas sensíveis — como bases legais, legítimo interesse, sanções, transferência internacional e critérios para anonimização — e na aplicação de sanções proporcionais à gravidade das infrações.

Por fim, a LGPD adota uma abordagem de governança similar ao GDPR, exigindo medidas técnicas e administrativas de segurança, registro das operações de tratamento, programas de compliance, boas práticas e relatórios de impacto à proteção de dados (RIPD).

Esses instrumentos reforçam a integração da proteção de dados ao ciclo de vida dos sistemas de IA e contribuem para mitigar riscos associados à opacidade algorítmica, discriminação e reidentificação.

2.3 Convergências e modelos internacionais

O avanço global das tecnologias digitais conduziu a um processo de convergência normativa em proteção de dados, motivado por três fatores centrais: ***i)*** necessidade de harmonização econômica e regulatória; ***ii)*** circulação transfronteiriça de dados; e ***iii)*** crescente preocupação com riscos emergentes associados a decisões automatizadas.

Embora existam assimetrias entre legislações, observa-se a adoção de princípios comuns derivados do GDPR, ainda que com diferentes níveis de detalhamento e rigor.

Nos Estados Unidos, o California Consumer Privacy Act (CCPA) e o California Privacy Rights Act (CPRA) representam modelos setoriais e

descentralizados, baseados em obrigações voltadas à transparência, opt-out e proteção ao consumidor, mais do que em uma lógica de direitos fundamentais.

Apesar disso, normas estaduais têm criado um mosaico regulatório que aproxima gradualmente o país de um padrão mais próximo do europeu.

No Canadá, a legislação PIPEDA adota abordagem mais flexível e orientada ao consentimento, enquanto países como Japão, Coreia do Sul, Índia e Austrália avançam em reformas que incorporam princípios de minimização, proporcionalidade e responsabilização.

Na América Latina, além do Brasil, países como Chile, Argentina e Uruguai apresentam movimentos significativos rumo à modernização de seus marcos legais, alinhando-se a padrões internacionais para facilitar transferência de dados e fortalecer direitos dos titulares.

Organizações multilaterais também influenciam a convergência global. Os Princípios da OCDE, as Diretrizes da UNESCO sobre Ética da IA e a atuação do Conselho da Europa ampliam o alcance normativo, integrando proteção de dados com governança da IA, direitos humanos e responsabilidade algorítmica.

No campo específico da IA, observa-se a consolidação de modelos regulatórios baseados em risco — como o AI Act da União Europeia e as propostas legislativas do Brasil e Estados Unidos — que tratam proteção de dados e governança algorítmica como dimensões interdependentes. Esse movimento indica que a proteção de dados está se tornando componente essencial da arquitetura normativa global de Inteligência Artificial, com reflexos diretos em conformidade técnica, governança e *accountability*.

3 TREINAMENTO DE MODELOS DE IA E USO DE DADOS

O uso de dados para o treinamento de modelos de Inteligência Artificial constitui a base funcional dessas tecnologias e, simultaneamente, representa um dos pontos de maior tensão entre avanços tecnológicos e conformidade regulatória.

Em sistemas de aprendizagem de máquina, a qualidade, a diversidade e o volume dos dados influenciam diretamente o desempenho, a precisão e a robustez do modelo.

Contudo, esses mesmos insumos também podem introduzir riscos substanciais à privacidade, à discriminação algorítmica e à segurança das informações, tornando imprescindível a adoção de salvaguardas jurídicas e técnicas que garantam conformidade com normas como o GDPR e a LGPD.

Do ponto de vista técnico, o ciclo de treinamento envolve três etapas fundamentais: coleta, processamento e modelagem.

A coleta refere-se à aquisição de dados provenientes de diferentes fontes — bancos de dados públicos ou privados, *web scraping*, sensores, bases comerciais ou interações do usuário.

O processamento envolve limpeza, normalização, anonimização, rotulagem e organização dos dados.

A modelagem compreende os algoritmos de aprendizagem utilizados para identificar padrões e gerar previsões.

Cada estágio possui implicações regulatórias específicas que determinam a escolha da base legal, o cumprimento de princípios de proteção de dados e a implementação de mecanismos de governança.

Uma das principais controvérsias é a utilização de dados pessoais, e em especial dados sensíveis, para treinar modelos.

A depender da finalidade, a atividade pode demandar bases legais específicas, justificativa técnica clara, medidas de minimização e mecanismos de segurança avançados.

Modelos treinados com grandes volumes de dados não estruturados, como aqueles utilizados em IA generativa, podem incorporar informações pessoais de forma incidental ou involuntária.

Isso eleva riscos de vazamentos por memorização (*model leakage*), em que o modelo reproduz trechos de dados pessoais presentes no conjunto de treinamento.

Tanto o GDPR quanto a LGPD impõem restrições específicas para evitar esse tipo de ocorrência, exigindo anonimização eficaz ou outra salvaguarda equivalente.

Além disso, modelos mal treinados podem reproduzir ou amplificar viéses presentes nos dados originais, gerando discriminação algorítmica em áreas como crédito, saúde, segurança pública e seleção de pessoal.

Esse risco é especialmente relevante para legislações como o GDPR (art. 22) e a LGPD (art. 20), que asseguram ao titular o direito de revisão de decisões automatizadas e estabelecem salvaguardas contra decisões discriminatórias.

Assim, práticas como auditorias de viés, testes de robustez, documentação de datasets e validação de modelos tornam-se centrais para garantir conformidade.

Outro ponto de destaque refere-se à licitude da coleta e reutilização de dados. O treinamento de IA frequentemente envolve dados obtidos de forma secundária, por exemplo, dados coletados para uma finalidade distinta daquela do treinamento.

As regulamentações como o GDPR exigem compatibilidade de finalidade, transparência e proteção reforçada quando há mudanças no propósito original. Já na LGPD, os princípios da finalidade, adequação e necessidade condicionam o tratamento, o que obriga o agente a demonstrar a legitimidade da reutilização dos dados em nova finalidade.

A transferência internacional de dados também exerce papel estratégico no treinamento de IA, sobretudo quando empresas dependem de bases de dados localizadas em diferentes jurisdições.

O GDPR possui restrições rígidas para transferência a países sem nível adequado de proteção, exigindo salvaguardas como cláusulas contratuais padrão. A LGPD segue lógica semelhante, estabelecendo hipóteses específicas de transferência, ainda em processo de regulamentação pela ANPD.

Finalmente, o uso de dados no treinamento de modelos de IA cria a necessidade de documentos e processos formais, como Relatórios de Impacto à Proteção de Dados (DPIA/RIPD), documentação da arquitetura do modelo, registro das operações de tratamento e políticas de segurança e governança de dados.

Esses instrumentos fortalecem o princípio da responsabilidade e permitem que o agente demonstre conformidade regulatória, mitigando riscos jurídicos, operacionais e éticos.

Assim, o treinamento de modelos de IA constitui uma atividade intrinsecamente multidisciplinar, que combina engenharia de dados, ciência da computação e direito. A conformidade regulatória não deve ser vista como barreira, mas como elemento estruturante de modelos mais seguros, transparentes e socialmente responsáveis — capazes de extrair valor dos dados sem violar direitos fundamentais.

4 APLICAÇÃO DAS LEIS AO TREINAMENTO DE IA

A aplicação das legislações de proteção de dados ao treinamento de modelos de Inteligência Artificial constitui um desafio normativo complexo, dada a natureza multifacetada dos fluxos informacionais envolvidos e o caráter técnico das operações algorítmicas.

Embora tanto o GDPR quanto a LGPD não tenham sido originalmente concebidos para regular especificamente a IA, seus princípios e dispositivos oferecem estrutura jurídica suficientemente abrangente para disciplinar atividades de coleta, processamento, armazenamento e uso de dados no contexto de aprendizado de máquina e IA generativa.

Em termos jurídicos, o primeiro eixo de análise refere-se à definição das bases legais que autorizam o tratamento de dados para fins de treinamento.

No GDPR, destacam-se bases como o consentimento explícito, o interesse legítimo e o cumprimento de obrigação legal ou regulatória. Entretanto, o uso do interesse legítimo como fundamento para treinamento de IA é controverso, pois requer a demonstração de que os interesses do controlador não se sobrepõem aos direitos e liberdades do titular.

Na LGPD, a lógica é semelhante, com destaque para as hipóteses de consentimento, tutela da saúde, execução de contratos e legítimo interesse, que deve ser sempre justificado e documentado conforme diretrizes da ANPD.

A compatibilidade de finalidade representa outro ponto crítico. Dados coletados para uma finalidade primária, como prestação de serviços ou análise de comportamento, nem sempre podem ser automaticamente reutilizados para treinar modelos.

Tanto o GDPR quanto a LGPD exigem que o novo propósito seja compatível com o original ou, caso contrário, demandam novo consentimento ou base legal adequada.

Esse requisito é especialmente relevante em modelos que utilizam grandes bases de dados historicamente acumuladas, cuja origem e finalidade podem estar dissociadas do uso atual.

A minimização e a necessidade são princípios centrais na aplicação das leis ao treinamento. Mesmo que o uso de dados pessoais seja autorizado, o controlador deve demonstrar que apenas os dados estritamente necessários ao desempenho do modelo estão sendo utilizados. Isso implica justificar a presença de informações sensíveis, explicar a indispensabilidade de atributos específicos e comprovar que técnicas alternativas — como anonimização, agregação ou geração sintética de dados — não seriam suficientes.

Outro aspecto essencial é a avaliação e mitigação de riscos. O GDPR impõe a obrigatoriedade de realizar Data Protection Impact Assessments (DPIAs) quando o tratamento envolve alto risco, o que inclui atividades como monitoramento sistemático, uso de dados sensíveis ou modelos que afetem significativamente indivíduos.

A LGPD prevê conceito semelhante por meio do Relatório de Impacto à Proteção de Dados (RIPD), que deve analisar riscos, medidas de mitigação e a proporcionalidade da operação.

No contexto de IA, esses relatórios tornam-se instrumentos fundamentais para documentar decisões técnicas, justificar bases legais e demonstrar conformidade regulatória perante autoridades.

A transparência e a explicabilidade também assumem papel central. As legislações exigem que titulares sejam informados de forma clara sobre o uso de seus dados, inclusive quando submetidos a decisões automatizadas.

No GDPR, o artigo 22 estabelece o direito de não se submeter exclusivamente a decisões automatizadas que produzam efeitos jurídicos ou significativos, enquanto na LGPD o artigo 20 garante o direito de revisão e a obrigação de fornecimento de informações claras sobre os critérios utilizados.

A aplicação desses dispositivos ao treinamento de IA, especialmente em modelos de deep learning com baixa interpretabilidade, demanda práticas como documentação técnica, explicações acessíveis, testes de impacto algorítmico e implementação de mecanismos de contestação.

A segurança da informação, por sua vez, exige que o controlador adote medidas técnicas e administrativas proporcionais ao risco. No treinamento de IA, isso inclui a prevenção de ataques de extração de modelo, mitigação de memorizações indevidas, controle de acesso a datasets, criptografia, segregação de ambientes e práticas rígidas de governança.

A falha em implementar tais medidas pode gerar responsabilidade civil, administrativa e até penal, dependendo da legislação aplicável.

Por fim, a responsabilização (*accountability*) se consolida como princípio transversal. Tanto o GDPR quanto a LGPD atribuem ao controlador o dever de estruturar processos, políticas e evidências que comprovem conformidade regulatória.

No âmbito da IA, isso implica manter logs, documentar decisões técnicas, registrar fluxos de dados, armazenar versões do modelo e garantir mecanismos de auditoria interna e externa.

Desse modo, a aplicação das leis ao treinamento de IA não se limita a identificar bases legais, mas abrange um conjunto articulado de obrigações que integram governança, transparência, prevenção de riscos e medidas técnicas de segurança. Modelos desenvolvidos sem essas salvaguardas enfrentam riscos significativos de ilicitude, responsabilização e danos aos titulares, enquanto aqueles

construídos em conformidade fortalecem a confiabilidade, a legitimidade e a segurança jurídica da inovação tecnológica.

5 DESAFIOS ÉTICOS E JURÍDICOS

A integração de dados pessoais em sistemas de Inteligência Artificial amplifica riscos éticos e jurídicos, especialmente quando tais sistemas operam em larga escala ou assumem papel decisório em contextos sensíveis. A seguir, são analisados os principais desafios estruturantes que emergem no cruzamento entre IA, proteção de dados e direitos fundamentais.

5.1 vieses algorítmicos

Os vieses algorítmicos constituem um dos riscos mais evidentes e persistentes no uso de IA. O problema pode se manifestar em diferentes etapas do ciclo de vida do sistema — desde a seleção de dados até o desenho do modelo e sua validação — e decorre, em grande parte, da representatividade insuficiente ou distorcida dos dados utilizados para o treinamento.

Quando os dados refletem desigualdades históricas, discriminações sistêmicas ou padrões sociais assimétricos, o modelo tende a reproduzir ou acentuar tais distorções. Esse fenômeno compromete direitos fundamentais, como igualdade, não discriminação e dignidade da pessoa humana.

Tanto o GDPR quanto a LGPD impõem limites diretos a tratamentos que resultem em discriminação ilícita, sendo que o primeiro reconhece explicitamente a "discriminação automatizada" como fator de risco que exige mitigação.

As estratégias de enfrentamento incluem auditorias algorítmicas, avaliação estatística de performance entre grupos, revisão humana contínua e técnicas de *fairness*, como balanceamento de *datasets*, regularização de equidade e métricas de impacto disparate. A adoção dessas medidas passa a ser critério de conformidade jurídica e não mero aprimoramento técnico.

5.2 Responsabilidade civil

A responsabilização por danos causados por sistemas de IA é um dos debates jurídicos mais complexos da atualidade. Modelos algorítmicos podem causar danos diretos (ex.: decisão automatizada injusta, negativa de direito) ou indiretos (ex.: vazamento de dados, reidentificação indevida, memorização de informações sensíveis).

A LGPD prevê responsabilidade objetiva para controladores e operadores quando há violação da legislação, independentemente de culpa, desde que comprovado o dano. Já o GDPR estabelece regime semelhante, exigindo demonstração de violação normativa, dano e nexo causal.

No entanto, a opacidade dos modelos "caixa-preta" dificulta a comprovação e a rastreabilidade das decisões, criando obstáculos à efetividade da responsabilização.

Esse problema levou o debate regulatório internacional a propor mecanismos complementares, tais como:

- obrigação de documentação robusta e versionamento do modelo;
- logs detalhados das decisões automatizadas;
- auditorias independentes;
- inversão parcial do ônus da prova em contextos de difícil rastreamento;
- classificação de sistemas de IA por risco (AI Act).

Em razão disso, no Brasil, vem sendo criado o Projeto de Lei (PL) 2.338/2023, a qual avança ao prever obrigações específicas de segurança, supervisão humana, mitigação de riscos e deveres de informação, aproximando-se do modelo europeu.

5.3 Governança Algorítmica

A governança algorítmica refere-se ao conjunto de processos, estruturas e mecanismos institucionais destinados a assegurar o uso ético, transparente e seguro

dos sistemas de IA. Ela integra dimensões jurídicas, organizacionais e técnicas, e constitui eixo central de conformidade regulatória.

As legislações de proteção de dados impulsionam a consolidação de modelos de governança baseados em:

a) Transparência e Documentação

Organizações devem registrar de forma sistemática:

- fontes dos dados,
- etapas do tratamento,
- critérios de decisão,
- avaliação de desempenho e risco,
- justificativas para parâmetros e hiperparâmetros,
- resultados de auditorias internas.

Esse conjunto documental sustenta o princípio da responsabilização e permite a atuação de autoridades regulatórias.

b) Supervisão Humana Significativa

A presença humana qualificada é um requisito central para garantir que sistemas automatizados não substituam integralmente a deliberação humana em decisões sensíveis. O AI Act e o PL 2.338/2023 reforçam a necessidade de supervisão contínua, intervenção em caso de falhas e capacidade de override.

c) Gestão de Riscos e Auditorias

As organizações passam a adotar frameworks estruturados, como:

- Avaliação de Impacto à Proteção de Dados (DPIA/RIPD),
- auditorias algorítmicas periódicas,
- testes de robustez, segurança e resistência a ataques adversariais,
- políticas internas de segurança e compliance.

d) Arquiteturas Técnicas orientadas à Privacidade

Incluem técnicas como:

- privacidade diferencial,
- aprendizado federado,
- controle de memorizações indesejadas,
- geração de dados sintéticos controlados,
- segregação de ambientes de desenvolvimento, teste e produção.

Esses mecanismos dialogam diretamente com o princípio do *privacy by design*, previsto tanto no GDPR quanto na LGPD.

e) Participação Social e Prestação de Contas

A governança não pode ser restrita a atores técnicos. Processos participativos, relatórios de impacto público e mecanismos de contestação garantem legitimidade democrática às decisões algorítmicas, especialmente quando afetam direitos fundamentais.

6 PERSPECTIVAS FUTURAS E TENDÊNCIAS REGULATÓRIAS DA INTELIGÊNCIA ARTIFICIAL

A rápida evolução da Inteligência Artificial tem impulsionado um movimento global de formulação de marcos regulatórios específicos para lidar com riscos emergentes, promover segurança jurídica e orientar modelos responsáveis de desenvolvimento e uso.

A convergência entre direitos fundamentais, governança algorítmica e proteção de dados pessoais situa-se no centro desse processo, que combina requisitos normativos, padrões internacionais e inovações técnico-científicas.

A seguir, analisam-se as principais tendências e perspectivas relacionadas ao cenário regulatório global e nacional.

6.1 O AI Act Europeu

O AI Act, aprovado pela União Europeia, representa o primeiro marco regulatório horizontal e abrangente dedicado exclusivamente à IA. Seu modelo estrutura-se na lógica de regulação baseada em risco, classificando sistemas de IA em categorias que variam de risco mínimo a risco inaceitável, com exigências proporcionais à criticidade de cada aplicação.

a) Classificação de risco

O AI Act estabelece quatro classes:

- Risco inaceitável: sistemas proibidos, como manipulação subliminar, pontuação social estatal e reconhecimento facial em tempo real para fins de vigilância generalizada.
- Alto risco: inclui IA em setores como emprego, crédito, educação, saúde, Justiça e aplicações de reconhecimento biométrico. Sujeitos a obrigações robustas.
- Risco limitado: exige transparência e avisos aos usuários, como chatbots ou sistemas generativos.
- Risco mínimo: liberados sem exigências adicionais.

b) Obrigações para sistemas de alto risco

Para sistemas de alto risco, o AI Act impõe:

- gestão contínua de risco;
- documentação técnica detalhada;
- qualidade, representatividade e governança dos dados;
- supervisão humana qualificada;
- avaliação de conformidade;
- registro em banco de dados europeu de sistemas de alto risco;
- monitoramento pós-mercado.

A estrutura influencia diretamente o treinamento de IA demandando rigor na seleção de *datasets*, explicabilidade e auditorias independentes.

c) IA generativa e modelos fundacionais (*foundation models*)

Uma inovação regulatória é a inclusão de modelos de uso geral e modelos fundacionais, como grandes modelos de linguagem e modelos multimodais. As obrigações incluem:

- políticas de direitos autorais e transparência;
- documentação dos dados utilizados no treinamento;
- mitigação de riscos sistêmicos;
- práticas de segurança reforçadas;
- avaliação contínua de impacto.

Essa abordagem deve servir como referência global, influenciando legislações em outros países.

6.2 Marco regulatório da IA no Brasil

O Brasil avança com o PL nº 2.338/2023, discutido no Senado, que busca instituir o Marco Legal da Inteligência Artificial. O projeto se inspira na abordagem europeia, mas adapta conceitos ao contexto brasileiro, enfatizando dignidade humana, desenvolvimento sustentável e redução de desigualdades.

a) Princípios estruturantes

O projeto adota princípios como:

- não discriminação,
- transparência,
- segurança,
- governança algorítmica,
- responsabilização,

- supervisão humana significativa,
- rastreabilidade.

b) Classificação de risco

Assim como o AI Act, o PL adota o modelo de classificação:

- IA de risco excessivo (proibida);
- IA de alto risco (obrigação de gestão de risco, supervisão humana, auditorias e RIPD);
- IA de risco moderado (transparência reforçada);
- IA de baixo risco (regras gerais de proteção de dados).

c) Convergência com a LGPD

O Marco Legal da IA dialoga diretamente com a LGPD, complementando-a ao:

- especificar obrigações para sistemas automatizados;
- estabelecer deveres de rastreabilidade e documentação;
- exigir avaliações de impacto algorítmico;
- definir regras de uso de dados para treinamento;
- disciplinar a responsabilidade civil por danos decorrentes de decisões automatizadas.

Essa integração tende a fortalecer a atuação da ANPD e estimular a criação de normas setoriais.

6.3 Convergência internacional

Observa-se crescente harmonização global em torno de princípios e parâmetros regulatórios. Organizações como OCDE, ONU, UNESCO e União Europeia têm produzido diretrizes convergentes, que destacam:

- centralidade dos direitos humanos;
- governança baseada em risco;
- transparência e explicabilidade;
- robustez técnica e segurança;
- equidade e mitigação de discriminação;
- accountability.

Países como Canadá, Japão, Austrália, Índia e Estados Unidos avançam em regulações setoriais ou diretrizes federais, especialmente voltadas a IA generativa, reconhecimento biométrico e uso governamental de algoritmos.

Essa convergência facilita a circulação internacional de modelos e produtos de IA, reduz o custo regulatório e reforça padrões mínimos de segurança e privacidade.

6.4 Inovações técnicas para mitigação de riscos

A evolução regulatória vem acompanhada por avanços técnico-científicos que buscam conciliar inovação e proteção de direitos. Entre as principais tendências, destacam-se:

a) Privacidade diferencial

Consiste na introdução controlada de ruído matemático para impedir reidentificação, garantindo que a saída do modelo não revele dados específicos de um indivíduo.

b) Aprendizado federado

Permite treinar modelos em múltiplos dispositivos ou servidores sem centralizar dados, reduzindo riscos de vazamento e exposições indevidas.

c) Geração de dados sintéticos

Criação de conjuntos de dados artificialmente produzidos que simulam padrões estatísticos reais, protegendo dados sensíveis e respeitando princípios de minimização.

d) Métodos de detecção de memorização

Técnicas que identificam quando um modelo armazenou ou reproduziu informações pessoais, garantindo conformidade com princípios de necessidade e segurança.

e) Robustez e segurança algorítmica

Inclui testes contra ataques adversariais, verificação formal de modelos e detecção de manipulação de entradas.

f) *Explainable* AI (XAI)

Desenvolvimento de ferramentas capazes de explicar decisões de modelos opacos, facilitando auditorias e garantindo direitos de informação.

Essas inovações tornam-se essenciais para atingir os padrões estabelecidos por legislações modernas e para possibilitar o uso ético e seguro da IA.

7 CONCLUSÃO

A análise realizada ao longo deste artigo demonstra que a relação entre proteção de dados e Inteligência Artificial não constitui um obstáculo ao desenvolvimento tecnológico, mas um eixo estruturante para a construção de sistemas seguros, éticos e socialmente responsáveis.

O exame dos marcos regulatórios — em especial o GDPR, a LGPD, o AI Act europeu e o PL 2.338/2023 — evidencia que a regulação orientada por princípios como finalidade, necessidade, minimização, transparência e responsabilização fornece as bases jurídicas necessárias para mitigar riscos e garantir que o uso de dados no treinamento de modelos de IA respeite direitos fundamentais.

A partir da compreensão do ciclo de vida dos dados, dos riscos associados ao tratamento automatizado, das vulnerabilidades inerentes a práticas de anonimização

e dos desafios éticos e jurídicos relacionados a vieses, discriminação e responsabilidade civil, conclui-se que a governança algorítmica e as medidas técnicas de privacidade são elementos essenciais para a conformidade normativa e para a legitimação social dessas tecnologias.

As tendências regulatórias, tanto no Brasil quanto no cenário internacional, revelam uma convergência em direção a modelos baseados em risco e em mecanismos preventivos, reforçando o entendimento de que o avanço da IA depende da articulação entre inovação, regulação e direitos humanos.

Assim, a síntese dos temas abordados confirma que a proteção de dados não apenas orienta o desenvolvimento de soluções de IA, mas constitui condição indispensável para que essas tecnologias possam contribuir, de forma segura e democrática, para a transformação digital contemporânea.

REFERÊNCIAS

AZADIAN, J. S.; FAHY, G. M. Artificial Intelligence and the Law: Navigating "KnownUnknowns". Computer & Internet Lawyer, v. 35, n. 2, p. 19–23, 2018. Disponível em: https://www.proquest.com/docview/1991583672?sourcetype=Trade%20Journals. Acesso em: 25 abr. 2024.

CAMBRAIA, Leonardo ; PYRRHO, Monique . Inteligência artificial e injustiça: para além de uma análise ética encantada dos algoritmos. Revista Iberoamericana de Bioética, n. 25, p. 1-15, 2024. Disponível em: https://www.researchgate.net/publication/382294904_Inteligencia_artificial_e_injustica_para_alem_de_uma_analise_etica_encantada_dos_algoritmos. Acesso em: 24 abr. 2024.

SILVA, Leandro Gomes da; RAMOS, Jefferson David Asevedo; PRATA, David Nadler. Inteligência Artificial e a Lei de Direitos Autorais. Revista Cereus, v. 10, n. 4, p. 137-146, 2018. Disponível em: http://ojs.unirg.edu.br/index.php/1/article/view/2348. Acesso em: 25 abr. 2024.

SILVA D'ÁVILA, Fernanda Felitti; VON HOHENDORFF, Raquel; CANTALI, Fernanda Borghetti. Inteligência artificial e direitos autorais: desafios e possibilidades no cenário jurídico brasileiro e internacional. PragMATIZES-Revista Latino-Americana de Estudos em Cultura, v. 10, n. 19, p. 249-273, 2020. Disponível em: https://periodicos.uff.br/pragmatizes/article/view/41210. Acesso em 23 abr. 2024

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. Projeto de Lei nº 2.338, de 2023. Institui o Marco Legal da Inteligência Artificial no Brasil. Senado Federal, Brasília, 2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162255. Acesso em: 17 out. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados – GDPR). Jornal Oficial da União Europeia, L119, 4 maio 2016.

UNIÃO EUROPEIA. Artificial Intelligence Act. Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas para a Inteligência Artificial. Bruxelas, 2024. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/european-ai-act. Acesso em: 17 out. 2025.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). OECD Principles on Artificial Intelligence. Paris: OECD, 2019. Disponível em: https://oecd.ai/en/ai-principles. Acesso em: 17 out. 2025.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA (UNESCO). Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO, 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000381137. Acesso em: 17 out. 2025.

FACHIN, Z.; HIRATA, A. C. A proteção jurídica dos dados pessoais sensíveis relativos à saúde. *Revista Jurídica*, [S. l.], v. 3, n. 70, p. 1–23, 2022. Disponível em: https://research.ebsco.com/linkprocessor/plink?id=62a7f1f5-57eb-3931-99f2-ce9bd378b5e1. Acesso em: 26 set. 2025.

MENDES, L. S.; FONSECA, G. C. S. da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. *Revista Estudos Institucionais*, [S. l.], v. 6, n. 2, p. 507–533, 2020. DOI: https://doi.org/10.21783/rei.v6i2.521. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/521. Acesso em: 15 set. 2025.

NETO, Gabriel de Oliveira Cavalcanti. *LGPD, cidades inteligentes e privacidade. Revista Sociedade Científica*, v. 6, n. 1, Pernambuco, 2023. Disponível em: https://revista.scientificsociety.net/wp-content/uploads/2023/06/Art00083-2023.pdf. Acesso em: 15 set. 2025.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Brasília: ANPD, 06 abr. 2023.

Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 14 out. 2025.

INTELIGÊNCIA ARTIFICIAL E PROTEÇÃO DE DADOS SENSÍVEIS EM DOCUMENTOS SIGILOSOS E RESTRITOS: O PAPEL DA LGPD NO SETOR PÚBLICO E PRIVADO

João Pedro Garcia de Araujo Gomes[1]

RESUMO

O avanço da Inteligência Artificial (IA) tem modificado de maneira profunda os processos de gestão e análise de informações, tanto na administração pública quanto nas organizações privadas. A crescente automação no tratamento de dados, especialmente quando envolve informações sigilosas e sensíveis, levanta desafios jurídicos substanciais. Nesse contexto, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), surge como norma regulatória fundamental para disciplinar o tratamento de dados no Brasil, estabelecendo princípios de transparência, segurança e finalidade (BRASIL, 2018). O presente artigo tem por objetivo analisar o papel da LGPD na proteção de dados sensíveis diante do uso da IA, com enfoque no setor público e no setor privado.

Palavras-chave: Lei Geral de Proteção de Dados Pessoais - LGPD; Administração Pública; dados pessoais; proteção; inteligência artificial.

SUMÁRIO: Introdução. 1 A Inteligência Artificial e seus desafios jurídicos; 1.1 Conceito e aplicações da Inteligência Artificial; 1.2 Os riscos da Inteligência Artificial no tratamento de dados sigilosos; 1.3. O papel da LGPD na mitigação de riscos e na governança de dados; 1.4 Diferenças de aplicação entre o setor público e o setor privado; 2 O tratamento de dados sensíveis em ambientes de Inteligência Artificial; 2.1 Desafios e perspectivas éticas no uso da Inteligência Artificial; 2.2 Técnicas de mitigação: anonimização, pseudonimização e abordagem por risco; Conclusão; Referências;

1 INTRODUÇÃO

[1] Graduando em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: joao.pedrog@sempreceub.com

A Inteligência Artificial, IA, se apresentou como uma inovação tecnológica de grande alcance, capaz de transformar rotinas administrativas, decisórias e operacionais em diferentes setores da sociedade. Seu poder de processar grandes volumes de informação trouxe grandes melhorias na eficiência de trabalho e possibilitou novas formas de prestação de serviços, porém, também ampliou a exposição de dados pessoais e sensíveis a riscos de tratamento inadequado, vazamentos e usos discriminatórios. Nessas circunstâncias, torna-se urgente a maior ligação entre inovação tecnológica e tutela de direitos fundamentais, como o da privacidade e a proteção de dados.

A proteção de dados sensíveis e a confidencialidade de documentos sigilosos tornaram-se pilares essenciais em uma sociedade cada vez mais orientada pela tecnologia e pela inteligência artificial. De acordo com o jurista brasileiro e especialista em proteção de dados, Danilo Doneda, a privacidade não seria um fim em si, mas sim um instrumento pelo qual a personalidade e, até, a dignidade humana seriam protegidas. Em suas palavras:

> a privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento indutor da autonomia, da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Nesse papel, ela é pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos (DONEDA, 2019, p. 128-129).

Nesse aspecto, a privacidade tem, como elemento central, a noção de garantia da liberdade à informação e a inviolabilidade da autodeterminação informativa. Doneda, ao citar Stefano Rodotà, reforça que a privacidade deve ser entendida como "o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada" (RODOTÀ apud DONEDA, 2019).

No Brasil, a Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), representa o marco regulatório que disciplina o tratamento de dados pessoais, inclusive nos meios digitais, "com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018). A norma estabelece princípios

como finalidade, necessidade e responsabilização, aplicáveis a qualquer operação de tratamento, tanto no setor público quanto no privado. Conforme destaca a Agência Nacional de Proteção de Dados (ANPD), a conformidade legal deve envolver "a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas" (ANPD, 2023).

No âmbito dos documentos sigilosos e restritos, o tratamento de dados sensíveis por meio de sistemas de IA demanda cuidados redobrados, especialmente diante da possibilidade de vazamentos, discriminação algorítmica ou acesso indevido. Conforme Petry e Hupffer, "sendo imprescindível, que sejam estabelecidas medidas técnicas e administrativas voltadas a garantir a funcionalidade de sistemas e proteção dos titulares de dados, garantindo-lhes seus direitos, desde a concepção até execução das atividades". Essa perspectiva reforça que tanto os entes públicos quanto as empresas privadas precisam estabelecer políticas claras de controle de acesso, anonimização e registro de atividades, de modo a assegurar a rastreabilidade das operações de IA sobre dados pessoais. (PETRY, HUPFFER, 2023)

Em âmbito internacional, organismos multilaterais têm buscado estabelecer parâmetros éticos e técnicos para o desenvolvimento de sistemas de IA confiáveis. Em seus princípios sobre Inteligência Artificial, a OCDE, afirma que os sistemas de IA devem funcionar de maneira robusta, segura e protegida ao longo de seus ciclos de vida. Os riscos em potencial devem ser avaliados e gerenciados continuamente (OCDE, 2019).

Diante desse contexto, o presente artigo tem por objetivo analisar o papel da LGPD na proteção de dados sensíveis em documentos sigilosos e restritos, com ênfase na aplicação diferenciada entre o setor público e o privado. Pretende-se demonstrar como o arcabouço jurídico brasileiro, aliado às boas práticas internacionais, pode oferecer uma base sólida para o uso ético e seguro da Inteligência Artificial, conciliando inovação com a preservação da privacidade e da dignidade humana.

2 A INTELIGÊNCIA ARTIFICIAL E SEUS DESAFIOS JURÍDICOS

O avanço da Inteligência Artificial, *Artificial Inteligence (AI)*, representa uma das transformações tecnológicas mais significativas do século XXI, trazendo consigo inúmeros benefícios, mas também novos e complexos desafios jurídicos. A IA tem sido amplamente utilizada em diversos setores, desde setores públicos até setores privados, alterando como dados e informações são processados, analisados, utilizados e tratados. Conforme define a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), "um sistema de IA é um sistema baseado em máquina que pode, para um determinado conjunto de objetivos definidos pelo homem, fazer previsões, recomendações ou tomar decisões que influenciam ambientes reais ou virtuais. Os sistemas de IA são projetados para operar com vários níveis de autonomia". (OCDE, 2019)

2.1 Conceito e aplicações da Inteligência Artificial

A Inteligência Artificial inclui técnicas e modelos computacionais que aprendem a identificar padrões em grandes volumes de dados e a executar tarefas como, classificação de documentos, análise preditiva e suporte à decisão. A aplicabilidade da IA cresceu em áreas como saúde, segurança pública, administração tributária e serviços financeiros, o que exige atenção às implicações do seu emprego sobre direitos fundamentais, em especial a privacidade. (SOUSA, GOMES, GOUVEIA, 2025)

A automação, pode, acabar por gerar dificuldades jurídicas, limitando a transparência e a responsabilização de seus usuários. Atualmente, as normas utilizadas para preencher estes vácuos legislativos, são a LGPD e a LEI Nº 12.527/2011, Lei de Acesso à Informação (LAI), incluem mecanismos próprios para lidar com este assunto, a exemplo disso o artigo 20 da LGPD indica: "O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses" (BRASIL, 2018). Essa previsão visa assegurar a possibilidade de intervenção humana e de contestação em processos decisórios automatizados.

Um exemplo da aplicação de IA, pelo Poder Público, ocorre na nossa Suprema Corte, o STF, Supremo Tribunal Federal, em conjunto com a UnB, criou

uma IA denominada como "Victor", buscando tornar mais eficiente os seus processos. Cabe, no entanto, indicar, que o "Victor" não decide recursos, mas sim apoia a análise de admissibilidade recursal, tendo seu trabalho validado ou confirmado durante a análise do caso em questão pelos Ministros. Deste modo, a IA é apenas um instrumento de auxílio de trabalho, de pré-análise, sem capacidade de gerar as decisões do tribunal. (BRASIL *apud* GONZALEZ, 2025).

2.2 Os riscos da Inteligência Artificial no tratamento de dados sigilosos

O uso da Inteligência Artificial no tratamento de informações sigilosas e sensíveis apresenta riscos significativos de vazamentos de dados, decisões automatizadas enviesadas e violação de princípios de privacidade. Estes sistemas, baseados em aprendizado de máquina, demandam grandes volumes de dados, potencializando a possibilidade de exposição indevida.

Outro risco de grande preocupação para o uso desenfreado de Inteligência Artificial, são os seus riscos de vazamentos de dados, por estes sistemas dependerem de grandes números de dados para seus usos em seu treinamento e operação, o risco de uma falha de segurança, poderá ocasionar em uma exposição de informações que deveriam ser protegidas pela LGPD. Este tisco, se intensifica quando inserimos cada vez mais agentes de tratamentos de dados e multiplicamos o uso desta tecnologia com ausência de controle rigorosos de governança e responsabilidade governamental.

Além disso, com o aumento do uso destas tecnologias e a maior ausência de supervisão humana, podemos gerar oque chamamos de discriminação algorítmica, o qual são os padrões sistemáticos de tratamento desigual, que produzem resultados enviesados ou injustos contra determinados grupos sociais, violando princípios como o da finalidade, necessidade e não discriminação previstos na LGPD, qual impõe que os agentes de tratamento "devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas" (BRASIL, 2018). Sendo assim, a governança da IA requer protocolos rigorosos de segurança e auditoria continua.

2.3 O papel da LGPD na mitigação de riscos e na governança de dados

A Lei Geral de Proteção de Dados Pessoais, constitui o principal marco legal, normativo, voltado à proteção da privacidade e ao uso legal de informações pessoais, utilizado nos contextos permeados por tecnologias automatizadas e Inteligências Artificiais. Sua função não se limita à regulação formal, mas também à criação de uma cultura de governança de dados e de responsabilidade ativa entre os agentes de tratamento. Conforme o art. 46 da LGPD, "os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas" (BRASIL, 2018).

Conforme a norma, controladores e operadores devem adotar medidas técnicas e administrativas, manter registros e elaborar Relatórios de Impacto à Proteção de Dados, notificando incidentes de risco (BRASIL, 2018). De acordo com a ANPD, a utilização de dados sensíveis em sistemas automatizados deve considerar políticas de retenção e descarte, alinhando prazos legais e mitigando riscos de exposição.

A exemplo disso, temos o Sistema Eletrônico de Informações, SEI, que gerência a criação e trâmite de processos e documentos restritos, garantindo acesso somente a usuários autorizados. A análise jurídica de documentos sigilosos combina LGPD, Lei de Acesso à Informação e normas internas para justificar limites à publicidade e medidas protetivas (BRASIL, 2018).

Em relação à Inteligência Artificial, o papel da LGPD torna-se ainda mais relevante por atuar como instrumento jurídico de mitigação de riscos algorítmicos e de preservação da dignidade humana. Isso ocorre porque, ao usar IA, no tratamento de dados para aprendizado e predição, pode incidir em práticas discriminatórias, opacas ou abusivas. Assim, princípios como os da finalidade, necessidade, transparência e responsabilização tornam-se pilares fundamentais na conformidade entre inovação tecnológica e direitos fundamentais. (DONEDA, 2019)

A aplicação da LGPD nas operações que envolvem IA se concretiza por meio de mecanismos como o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), documento que, segundo a Agência Nacional de Proteção de Dados:

> contém a descrição dos processos de tratamento de dados pessoais que podem gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados. Deve conter, ainda, as medidas, salvaguardas e mecanismos de mitigação de risco, nos termos dos artigos 5º, inciso XVII, e 38 da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD). (ANPD, 2023)

Esse documento é essencial para que controladores e operadores demonstrem a adoção de medidas preventivas e de governança, especialmente em projetos de IA voltados ao tratamento de dados sensíveis ou sigilosos.

Além disso, a norma de proteção de dados, reforça a necessidade de transparência e *accountability*, garantindo ao titular o direito de conhecer, revisar e se opor a decisões automatizadas que o afetem significativamente, previsto no art. 20 da LGPD, incluindo as decisões que definem seu perfil ou comportamento no contexto de IA. Essa garantia busca inibir o tratamento discriminatório dos dados pelas IA 's.

Dessa forma, a aplicação da LGPD estabelece uma ligação direta entre o progresso tecnológico e a ética digital, exigindo que os agentes públicos e privados cumpram a sua responsabilidade de equilibrar inovação e proteção de direitos. Em suma, a governança de dados se torna uma ferramenta indispensável para a manutenção da confiança social e da legitimidade das tecnologias baseadas em Inteligência Artificial.

2.4 Diferenças de aplicação entre o setor público e o setor privado

No setor público, a LGPD permite tratamento de dados pessoais apenas para finalidade pública e com base legal adequada, conciliando publicidade administrativa e proteção da privacidade (BRASIL, 2018). O SEI e sistemas similares adotam controles, auditorias e classificação de documentos para garantir conformidade legal e proteger dados sensíveis.

No setor privado, o uso de sistemas de Inteligência Artificial tornou-se prática cotidiana, especialmente em processos de análise de documentos, marketing, triagem de currículos e atendimento automatizado. Grandes empresas utilizam algoritmos capazes de processar dados de consumo, comportamento online e histórico financeiro, visando personalizar ofertas e prever tendências de mercado. Essa coleta massiva de informações pessoais, embora traga eficiência e competitividade, exige observância rigorosa dos princípios estabelecidos na norma legal, como o da finalidade, adequação, não discriminação, segurança e necessidade.

A LGPD atua como instrumento de regulação dessas práticas, determinando que as empresas adotem mecanismos de governança e *accountability*, demonstrando a conformidade de suas operações com a legislação. Isso implica a necessidade de elaboração de políticas de privacidade transparentes, relatórios de impacto à proteção de dados pessoais (RIPD) e procedimentos internos até mesmo por meio de corregedorias, responsáveis pelas respostas a incidentes, que buscam assegurar ao titular o direito de acesso, retificação e exclusão de suas informações. Em alguns setores, que tratam diretamente com dados sensíveis, como o bancário e o de saúde, essas medidas se tornam ainda mais relevantes nos tratamentos de dados, assegurando maior transparência para o que está acontecendo com os dados pessoais.

Por outro lado, no setor público, embora a LGPD estabeleça regras semelhantes, a administração direta e indireta enfrenta desafios adicionais, especialmente pela necessidade de equilibrar o princípio da publicidade com o dever de resguardar informações pessoais. O uso de IA em políticas públicas, como sistemas de reconhecimento facial, vigilância inteligente ou cruzamento de bases de dados governamentais, impõe o dever de adotar medidas robustas de anonimização ou pseudoaninomização dos dados compartilhados e controle de acesso, sob pena de violação de direitos fundamentais. Assim, a distinção essencial entre os dois setores está na finalidade do tratamento: enquanto o Estado deve tratar dados em nome do interesse público, as empresas privadas o fazem sob o interesse econômico, ambos, contudo, subordinados aos limites e princípios da LGPD. (BRASIL, 2018)

3 O TRATAMENTO DE DADOS SENSÍVEIS EM AMBIENTES DE INTELIGÊNCIA ARTIFICIAL

O avanço da Inteligência Artificial (IA) tem ampliado significativamente a capacidade de coleta, tratamento e análise de dados em larga escala. No entanto, essa evolução tecnológica traz consigo desafios complexos relacionados à privacidade e à proteção de dados pessoais, especialmente quando se trata de dados pessoais sensíveis, informações cuja exposição indevida pode causar danos significativos aos indivíduos.

Em ambientes automatizados, o tratamento desses dados exige atenção redobrada, pois algoritmos de IA podem identificar padrões, inferir características pessoais e tomar decisões com base em informações altamente delicadas. A ausência de salvaguardas adequadas pode resultar em violações de direitos fundamentais, como a dignidade, a igualdade e a não discriminação. (BRASIL, 2022)

3.1 Desafios e perspectivas éticas no uso da Inteligência Artificial

O emprego crescente de sistemas de Inteligência Artificial (IA) coloca no centro do debate jurídico e social questões éticas que vão além da mera conformidade normativa. Embora a LGPD ofereça um forte arcabouço jurídico para proteção de dados pessoais, muitos dos problemas éticos da IA, como vieses, discriminação, perda de autonomia e vigilância, demandam respostas que combinem regulação, governança técnica e reflexão aprofundada sobre direitos fundamentais. Nesse sentido, além dos princípios técnicos, precisamos contemplar sobre a ética do uso de IAs junto a documentos com dados sensíveis, para que a tecnologia seja utilizada com o mínimo de risco e com propriedade.

Um desafio ético de grande relevância para o uso de IAs, é o viés que o algorítmico poderá ocasionar, uma vez que os modelos de IA são treinados por meio de manipulação de base de dados, a tecnologia, tende a reproduzir e até amplificar certas desigualdades, baseando-se nestes dados, quais, não necessariamente sejam verdadeiras, ocasionando com reprodução de decisões injustas, como no caso de seu uso em campanhas de recrutamento, estudo de crédito, planos de saúde, além de

casos de racismo mascaradas como garantias à segurança. A correção desse problema exige não apenas ajustes técnicos, mas também decisões de política pública sobre quais critérios são aceitáveis em automações, em principal sobre as que afetam direitos fundamentais e norteadores dos Direitos Humanos, tal como a dignidade humana. Pesquisadores do tema, e organizações internacionais, apontam que auditorias independentes e testes de viés periódicos são práticas essenciais para mitigar discriminações algorítmicas (OCDE, 2019; DONEDA, 2019).

A transparência e os devidos esclarecimentos, sobre a manutenção e o uso de dados, configuram outro eixo ético, onde os titulares e reguladores devem compreender, como decisões automatizadas são tomadas, para se resguardar de seus possíveis malefícios. Essas exigências buscam assegurar informações sobre a finalidade dos dados utilizados e possíveis consequências das decisões automatizadas. Essa clareza aumenta a responsabilização e a confiança pública. A exemplo disto, temos as recomendações de organismos internacionais no fato de que sistemas de IA sejam explicáveis e auditáveis (OCDE, 2019; UNESCO, 2021).

A responsabilização, accountability, é outro meio importante, visando garantir que as organizações demonstrem a adoção de medidas de governança, monitoramento e mitigação de riscos. Na prática, isso envolve Relatórios de Impacto à Proteção de Dados (RIPD), políticas internas, encarregados (DPOs) e órgãos de governanças multidisciplinares, tal como as corregedorias e ouvidorias, além de demonstração, pelo Controlador ou pelo Operador, de todas as medidas eficazes e capazes de comprovar o comprimento da lei e a eficácia das medidas aplicadas. A atuação da ANPD e a construção de sanções, trazem o pesar desta responsabilização (ANPD, 2021; BRASIL, 2018).

Além disso, temos um outro desafio, referente à vigilância e à autonomia individual, em principal, o confronto do direito de privacidade, transparência e de consentimento e em relação à finalidade e necessidade deste tratamento de dados pelas tecnologias de IA, em principal frente a combinação com big data e reconhecimento biométrico, quais podem reduzir espaços de privacidade e autodeterminação. A perspectiva ética recomenda limites rigorosos ao uso de tecnologias de vigilância, exigindo bases legais claras e mecanismos de controle

democrático sobre sistemas que afetem a esfera íntima dos cidadãos. Nesse sentido, os direitos fundamentais visando a proteção da dignidade e da liberdade individual devem orientar qualquer uso de IA que envolva dados pessoais (UNESCO, 2021; BIONI, 2021).

3.2 Técnicas de mitigação: anonimização, pseudonimização e abordagem por risco

A proteção de dados sensíveis no contexto da Inteligência Artificial exige a adoção de técnicas de mitigação que reduzam o risco de vazamento de informações. Dentre essas técnicas, destacam-se a anonimização, a pseudonimização e a abordagem baseada em risco, todas alinhadas aos princípios da LGPD e às boas práticas recomendadas pela Agência Nacional de Proteção de Dados (ANPD).

A anonimização consiste em um processo técnico, por meios razoáveis e disponíveis no momento do tratamento, que torna impossível, ou altamente improvável, possibilitando que um dado perda a possibilidade de associação, direta ou indireta, a um indivíduo; Segundo a ANPD (2023),

> "a anonimização deve ser vista como processo contínuo baseado em risco possibilita que o controlador defina, de acordo com seu contexto, o compromisso entre ao grau de utilidade e o grau de anonimização que contemple a finalidade definida no tratamento e minimize o risco de reidentificação do titular."

Entre as principais técnicas de anonimização, estão a supressão, remoção de atributos identificadores ou partes dos registros, a generalização, redução do nível de detalhamento, agrupando dados em um nível mais geral, a perturbação, introdução de ruído ou pequenas alterações e permutação, consiste em reorganizar os valores dos dados dentro do conjunto de dados, de tal forma que os valores originais ainda são representados, mas geralmente não mais associado ao seu titular. Essas medidas visam tornar o dado irreversível e desconectado do indivíduo, além de, ao mesmo tempo, mantendo a sua utilidade estatística.

No entanto, a anonimização nunca é absoluta. Como destaca Bioni (2021), a irreversibilidade é sempre relativa ao estado da técnica, podendo ser comprometida pela evolução tecnológica e pelo cruzamento de bases de dados. Por essa razão, a

LGPD exige que o controlador demonstre diligência técnica e avalie continuamente os riscos de reidentificação, devendo ainda ter maior preocupação quando o dado é processado por sistemas de IAs capazes de correlacionar grandes volumes de informação.

Já a pseudonimização difere da anonimização por não eliminar completamente a possibilidade de reidentificação. Segunda a própria LGPD,

> Pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro (art. 13, § 4º, da LGPD).

Nesse processo, identificadores diretos são substituídos por chaves e códigos, de modo que apenas quem possui a chave de correspondência possa recompor a identidade do titular. Segundo Doneda (2020), a pseudonimização seria um meio intermediário de proteção, útil para reduzir riscos operacionais e limitar o acesso indevido em uma organização, mas que ainda mantém o dado como pessoal sob o regime da LGPD, logo sujeita às obrigações legais estabelecidas nesta. Esta técnica, é por sua vez muito associada com outras práticas tais como criptografia, controle de acesso baseado em papéis e tokenização, para criar múltiplas camadas de proteção contra vazamentos.

A abordagem baseada em risco, é a técnica norteadora, da governança de dados. Inspirada nas diretrizes da OCDE e da ANPD, essa indica que o nível de proteção deve ser proporcional à natureza dos dados e a sua sensibilidade, bem como à probabilidade e gravidade dos danos causados por seus vazamentos ou maus tratos. Assim, a avaliação de risco orienta o controlador na escolha das medidas técnicas e administrativas adequadas, e na elaboração de Relatórios de Impacto à Proteção de Dados, exigidos pela LGPD em operações de alto risco.

Essa prática, baseada na mitigação de riscos, é baseada em documentação, monitoramento e revisão periódica, tornando-se essencial em sistemas de IA, onde o ciclo de vida dos dados envolve múltiplos atores e ambientes computacionais, ampliando a possibilidade de vulnerabilidades, assegurando que o uso de IA permaneça compatível com a proteção da privacidade e os direitos fundamentais dos titulares destes dados.

4 CONCLUSÃO

Os avanços da tecnologia agrega inúmeros benefícios à sociedade contemporânea. Entretanto, a Inteligência Artificial, a atual material de inovação tecnologia de ponta, ocasiona por ampliar inúmeros problemas, tais como os riscos à privacidade e a transparência e finalidade do uso de dados sensíveis. Diante deste quadro de maiores riscos, percebemos uma integração entres os entes que controlam a tecnologia e o governo, visando em especial garantir para a população a proteção dos seus direitos fundamentais, com a privacidade e proteção de dados.

A LGPD emerge, nesse cenário de inovação rápida, como instrumento normativo e cultural que orienta práticas de governança, transparência e responsabilização, exigindo que controladores e operadores adotem medidas técnicas e administrativas proporcionais ao risco, como os RIPD, controles de acesso, anonimização e pseudonimização. Tornando-se indispensável para a proteção dos dados sigilosos.

Percebemos, ainda, que a LGPD se mostra não como um obstáculo à inovação, mas como um marco regulatório indispensável para a consolidação de um ecossistema digital ético e responsável. Proporcionando segurança jurídica, transparência e regras claras para agentes de tratamento, Poder Público e titulares, viabilizando o controle sobre os próprios dados e consolidando a autodeterminação informativa.

A regulação da proteção de dados pessoais proporciona segurança jurídica, transparência e regras claras para agentes de tratamento, Poder Público, privado e para os titulares dos dados, com viabilização do controle sobre os seus próprios dados.

Portanto, conclui-se que a LGPD fornece instrumentos jurídicos suficientes para compatibilizar a inovação tecnológica com a tutela dos direitos fundamentais, desde que seus princípios sejam efetivamente implementados na concepção e no uso de IAs. Assim, o equilíbrio entre tecnologia e privacidade não depende apenas da norma, mas da prática destes princípios, consolidando um modelo de

desenvolvimento tecnológico centrado na pessoa humana e na proteção de sua dignidade.

REFERÊNCIAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD). Brasília, 2023. Disponível em:https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 10 out. 2025.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). ESTUDO TÉCNICO SOBRE A ANONIMIZAÇÃO DE DADOS NA LGPD: ANÁLISE JURÍDICA. Brasília: Autoridade Nacional de Proteção de Dados, 2023.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). ESTUDO TÉCNICO SOBRE A ANONIMIZAÇÃO DE DADOS NA LGPD: UMA VISÃO DE PROCESSO BASEADO EM RISCO E TÉCNICAS COMPUTACIONAIS. Brasília: Autoridade Nacional de Proteção de Dados, 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). GUIA ORIENTATIVO: TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO. Brasília, DF: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 19 out. 2025

AJURU Pataxó: Mekukradjá. Entrevistado: Ajuru Pataxó. Apresentação: Daniel Munduruku. São Paulo: Itaú Cultural, 28 out. 2019. Podcast (23 min.). Disponível em: https://www.itaucultural.org.br/ajuru-pataxo-mekukradja. Acesso em: 14 out. 2025.

BIONI, Bruno Ricardo. PROTEÇÃO DE DADOS PESSOAIS: A FUNÇÃO E OS LIMITES DO CONSENTIMENTO. 2. ed. Rio de Janeiro: Forense, 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 out. 2025.

BRASIL. Ministério da Ciência, Tecnologia e Inovação. *Portaria MCTI nº 4.979, de 13 de julho de 2021*. Disponível em: https://antigo.mctic.gov.br/mctic/opencms/legislacao/portarias/Portaria_MCTI_n_4979_de_13072021.html. Acesso em: 12 out. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Serviços Compartilhados. Diretoria de Administração e Logística. *Usuário do Sistema Eletrônico de Informações (SEI): cartilha*. 10. ed. Brasília: MGI/SSC/DAL,

2023. Disponível em: https://www.gov.br/memp/pt-br/acesso-a-informacao/sistema-eletronico-de-informacoes-sei/00-cartilha_usuario_sei_out-23.pdf. Acesso em: 14 out. 2025.

BRASIL. Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome. PRINCÍPIOS DA LGPD. MDS, 2022. Disponível em: https://www.gov.br/mds/pt-br/acesso-a-informacao/lgpd/principios-da-lgpd. Acesso em: 14 out. 2025.

DONEDA, Danilo. DA PRIVACIDADE À PROTEÇÃO DE DADOS PESSOAIS: FUNDAMENTOS DA LEI GERAL DE PROTEÇÃO DE DADOS. 2. ed. São Paulo: Revista dos Tribunais, 2019.

GONZALES, Rafael L. L. OS DIREITOS AUTORAIS E A INTELIGÊNCIA ARTIFICIAL: UMA ANÁLISE DOS DIREITOS AUTORAIS DE CONTEÚDO PRODUZIDO POR INTELIGÊNCIAS ARTIFICIAIS E FORNECIDO A ELA. In: CIRNE, Mariana Barbosa; MARTINS, Amanda Ribeiro; ROSELLI, Igor Andrey. **Constituição, processo legislativo e Supremo Tribunal Federal: interagindo por mais direitos.** Brasília: CEUB, 2025.

MACIEL, Roberta A. C. CONSIDERAÇÕES SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LGPD, SUA APLICAÇÃO AO PODER PÚBLICO E O COMPARTILHAMENTO DE DADOS PESSOAIS PELOS ÓRGÃOS PÚBLICOS. *v. 3 (2023): Revista Judicial Brasileira - Edição Especial Direito Digital.* Disponível em: https://revistadaenfam.emnuvens.com.br/renfam/article/view/226/76. Acesso em: 19 nov. 2025.

OCDE. *OECD PRINCIPLES ON ARTIFICIAL INTELLIGENCE.* Paris: Organisation for Economic Co-operation and Development, 2019. Disponível em: https://oecd.ai/en/ai-principles. Acesso em: 10 out. 2025.

OCDE. *Recommendation of the Council on Artificial Intelligence*. Paris: OECD Publishing, 2019. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. Acesso em: 14 out. 2025.

PAULICHI, Jaqueline Silva; WOLOWSKI, Matheus RIBEIRO DE OLIVEIRA. O DILEMA JURÍDICO DA PROPRIEDADE INTELECTUAL NA INTELIGÊNCIA ARTIFICIAL: A MÁQUINA PODERÁ SER TITULAR DE DIREITO AUTORAL?. **Revista de Direito, Inovação, Propriedade Intelectual e Concorrência**, Florianopolis, Brasil, v. 7, n. 2, p. 1–16, 2022. DOI: 10.26668/IndexLawJournals/2526-0014/2021.v7i2.8086. Disponível em: https://www.indexlaw.org/index.php/revistadipic/article/view/8086. Acesso em: 19 nov. 2025.

PECK, Patrícia. *Direito Digital Aplicado 5.0.* São Paulo: Thomson Reuters Brasil, 2022.

PETRY, Gabriel Cemin; HUPFFER, Haide Maria. O PRINCÍPIO DA SEGURANÇA NA ERA DOS CIBERATAQUES: UMA ANÁLISE A PARTIR DO ESCOPO PROTETIVO DA LGPD. *Revista CNJ*, Brasília, v. 7, n. 1, p. 85–98, 2023. DOI: 10.54829/revistacnj.v7i1.445. Disponível em: https://www.cnj.jus.br/ojs/revista-cnj/article/view/445. Acesso em: 14 out. 2025.

PINHEIRO, Patrícia, P. *Proteção de dados pessoais: comentários à Lei nº 13.709/2018 (LGPD)*. 1. ed. São Paulo: Saraiva Educação, 2018.

SOUSA, Mariana L.; GOMES, Gabriela de F.; GOUVEIA, Geovanna I. A PROTEÇÃO DE DADOS APLICADA À INTELIGÊNCIA ARTIFICIAL: LIMITES, TRANSPARÊNCIA E RESPONSABILIDADES NA UTILIZAÇÃO DOS SISTEMAS DE IA. *Advances in Knowledge Representation*, [S. l.], v. 4, n. 2, p. 195–211, 2025. Disponível em: https://periodicos.ufmg.br/index.php/advances-kr/article/view/53484. Acesso em: 14 out. 2025.

VALIM, T. R. A. RESENHA DO LIVRO “DA PRIVACIDADE À PROTEÇÃO DE DADOS PESSOAIS: FUNDAMENTOS DA LEI GERAL DE PROTEÇÃO DE DADOS”, de Danilo Doneda. *Inova Jur*, Belo Horizonte, v. 1, n. 1, p. D1–D13, jan./jun. 2022.

COMO ESTÁ A REGULAÇÃO DE IA NO BRASIL?

Cláudio da Silva Souza
Heráclito Frederico Crisnamurth de Jesus Miranda
Júlio César Alves Lima
Rodrigo Moreira de Oliveira
Thiago Max Diego Xavier Silva

RESUMO

O objetivo deste texto é responder a pergunta-problema: como está a regulação de IA no Brasil? E como resposta foi elaborado quadro resumo com a tramitação do projeto de lei no Senado Federal nº 2.338/2023 e os termos de uso das empresas do Chat-Gpt e da Gemini. O que se evidencia é que o Estado ao normatizar e responsabilizar os conteúdos e ações da IA se dê de forma compartilhada com as empresas de tecnologia. Os termos de uso atribuem aos usuários a responsabilidade pelo uso e obtenção dos resultados. A conclusão não fixa em um modelo de regulação, contudo apresenta orientações a observar na definição das normas para os sistemas de IA.

Palavras-chave: Inteligência Artificial - IA, regulamentação, legislação.

Sumário: Introdução. 1. Método. 1.1 Contexto Histórico da Inteligência Artificial. 1.2 Era do Deep Learning e da IA Generativa (2010 até hoje). 2. Resultados. 3. Discussão. 4. Conclusão. Referências

1 INTRODUÇÃO

A Inteligência Artificial - IA[1] é o objeto de estudo do presente texto, que busca responder a pergunta-problema: *como está a regulação de IA no Brasil?*

[1] A inteligência artificial (IA) é um conjunto de tecnologias que permite que os computadores aprendam, raciocinem e realizem várias tarefas avançadas de maneiras que antes exigiam inteligência humana, como entender a linguagem, analisar dados e até mesmo fornecer sugestões úteis. É uma tecnologia transformadora que pode trazer mudanças significativas e positivas para as pessoas, as sociedades e o mundo.
Ela abrange muitas disciplinas diferentes, como ciência da computação, estatísticas e análises de dados, engenharia de hardware e software, linguística, neurociência e até mesmo filosofia e psicologia.
A IA ensina os computadores a fazerem coisas incríveis que nossos cérebros fazem, como entender o mundo ao redor, aprender coisas novas e até ter ideias inovadoras. Por exemplo, a IA é usada no reconhecimento óptico de caracteres (OCR) para extrair texto e dados de várias imagens e documentos.

Até pouco tempo a inteligência parecia ser reconhecida apenas em seres vivos e avançando a tecnologia nota-se que máquinas e sistemas de informática possuem também inteligência, podendo interagir com outras máquinas e seres vivos.

Acerca dessa novidade que surpreende, arrasta multidões de pessoas com suas inovações e também causa medo em razão da possibilidade de substituição e perda de posições de trabalho, a legislação é ponto a considerar relevante para entender o passado e presente, assim como tentar traçar normas para o futuro dos sistemas de IA.

O direito é compreendido, em parte relevante, para a definição de como deve ser a sociedade, a política, os poderes públicos e os direitos fundamentais. Nesse caminho de definição do dever-se está também a tecnologia, como será a IA, seu funcionamento, os limites e o espaço de possibilidades para expansão.

A IA como é um fenômeno novo e não inteiramente compreendido, produzir a norma é algo complexo e com maior grau de dificuldade. No entanto, existe proposta de regulação pelo Estado e por parte das empresas que avançam com os sistemas de IA, tais como protocolos e termos, nos quais expõe sua política de uso.

Para deixar evidente ao leitor, o objetivo deste texto é apresentar a regulação acerca de sistemas de IA, tanto do Estado (em vias de produção pelo Congresso Nacional) como das empresas que desenvolvem a tecnologia.

O presente texto está dividido em exposição de histórico da IA, método, resultados da leitura e das regulações estudadas, discussão e conclusão.

2 MÉTODO

Para levantamento das informações serão lidos termos de uso publicados pelas empresas de IA e proposta de legislação em trâmite no Congresso Nacional.

Esse processo transforma conteúdo não estruturado em dados estruturados e prontos para uso comercial, ajudando a descobrir insights valiosos. **GOOGLE CLOUD.** What is artificial intelligence? Disponível em: https://cloud.google.com/learn/what-is-artificial-intelligence?hl=pt-BR. Acesso em: 10 nov. 2025.

Listam-se as empresas de IA que estão dentro do conjunto a ser estudado aqui: Chat-GPT da empresa OpenAI Incorporated e Gemini do Google.

2.1 Contexto Histórico da Inteligência Artificial

O marco zero da inteligência artificial começou na década de 1940 com o surgimento dos primeiros computadores digitais, como ENIAC, primeiro computador elétrico, com isso a ideia de simular o raciocínio humano ganhou força. O marco da inteligência artificial foi amplamente creditado ao Workshop de Dartmouth, em 1956. Foi nesse evento que o cientista Jhon McCarthy cunhou o termo “inteligência Artificial” e reuniu pesquisadores para explorar a conjectura de que todo aspecto do aprendizado ou qualquer outra característica da inteligência pode, em princípio, ser tão precisamente descrito que uma máquina pode ser feita para simulá-lo (INSTITUTO DE ENGENHARIA, 2025).

Nas décadas de 1950 e 1960: foram criados os primeiros programas de IA, nos quais tinham a capacidade de resolver problemas de álgebra, provar teoremas lógicos e jogar damas. Nessa época havia uma crença generalizada de que uma IA com inteligência humana geral estava a apenas algumas décadas de distância. Nessa época Alan Turing propôs o famoso teste de turing para avaliar se uma máquina pode imitar o comportamento humano (INSTITUTO DE ENGENHARIA, 2025).

Entre as décadas 1970 e 1980: o progresso desacelerou devido às limitações do poder computacional e da complexidade de simular o conhecimento do mundo real levando a um período de ceticismo e cortes de financiamento (INSTITUTO DE ENGENHARIA, 2025).

Entre as décadas de 1990 e 2000: a IA mudou de foco. Em vez de tentar programar regras explícitas, pesquisadores se concentraram em criar sistemas que pudessem aprender a partir de dados (INSTITUTO DE ENGENHARIA, 2025). Esse foi o nascimento da era do Machine Learning (aprendizado de máquina). Um marco icônico quando o supercomputador Deep Blue da IBM derrotou o campeão mundial de xadrez Garry Kasparov.

2.2 Era do Deep Learning e da IA Generativa (2010 até hoje)

O grande salto da inteligência artificial contemporânea aconteceu com o avanço do Deep Learning, uma vertente do aprendizado de máquina que utiliza redes neurais profundas, compostas por várias camadas. Esse progresso foi impulsionado pela disponibilidade de grandes quantidades de dados (Big Data) e pelo uso intensivo de GPUs (unidades de processamento gráfico), resultando em conquistas impressionantes (INSTITUTO DE ENGENHARIA, 2025).

Em 2012, o algoritmo AlexNet marcou uma virada no campo da visão computacional, transformando o reconhecimento de imagens, por volta de 2017. A criação da arquitetura Transformer abriu caminho para os Modelos de Linguagem de Grande Escala (LLMs), como os da série GPT, capazes de compreender e produzir textos com uma naturalidade surpreendente (INSTITUTO DE ENGENHARIA, 2025). Hoje, a popularização da IA Generativa que consegue criar conteúdo originais como textos, imagens, músicas e códigos trouxe ferramentas como ChatGPT, Gemini, Midjourney e DALL-E para o cotidiano das pessoas, tornando a IA acessível e presente em diversas áreas (INSTITUTO DE ENGENHARIA, 2025).

O Chat GPT é um modelo para interagir com usuários em formato de conversa, recebendo perguntas do usuário e fornecendo resposta, é um modelo treinado para seguir instruções de um prompt e oferecer resposta (Chat CPT, 2025). A tecnologia em seu sítio informa acerca das limitações:

> Às vezes, o ChatGPT escreve respostas que têm um formato plausível, mas são incorretas ou não fazem sentido. É complicado corrigir esse problema, porque: (1) no momento, não existe uma fonte de verdade durante o treinamento de aprendizagem por reforço; (2) treinar o modelo para ser mais cauteloso faz com que ele recuse perguntas que sabe responder corretamente; e (3) o treinamento supervisionado desorienta o modelo, porque a resposta ideal depende daquilo que o modelo sabe (abre em uma nova janela) — e não do que o demonstrador humano sabe. (Chat GPT, 2025).

A interação do sistema com o usuário depende da pergunta, do modelo e do seu treinamento, assim como da base de dados. Tal questão se dá também com Gemini e a coleta de dados é algo que acompanha o uso pelos usuários para o aprendizado da máquina e correção de limitações.

Em consulta ao *Ajuda dos Apps do Gemini* pode ser observado o seguinte, relativo à limitação:

> Antes de usar os apps do Gemini
> Os Apps do Gemini podem cometer erros.
> Ao usar os apps do Gemini, sempre cheque as informações e as respostas não devem ser usadas para qualquer tipo de orientação profissional. (GOOGLE, 2025).

Em consulta aos Termos de Uso no Google da Gemini foi encontrada na seção "*Como o Google retém os dados que coletamos*" em que é exposto como o Google coletam os dados enquanto o usuário usa os serviços do Google, a explicação porque fazem isso e como você pode gerenciar suas informações e temas descritos na Política de Privacidade (GOOGLE, 2025). Tal política de retenção descreve por que mantém diferentes tipos de dados por diferentes períodos (GOOGLE, 2025).

Alguns dados podem ser excluídos a qualquer momento, alguns são excluídos automaticamente e outros são retidos por períodos mais longos, quando necessário (GOOGLE, 2025). Quando o usuário exclui dados, o Google segue uma política de exclusão para garantir que eles sejam removidos de forma segura e completa dos servidores ou retidos apenas de forma anônima (GOOGLE, 2025).

Cabe pontuar que os sistemas de IA para sua aprendizagem, treinamento e correção precisam de um conjunto de dados enorme, que pode ser alimentado pelos usuários e pela empresa.

Para finalizar esta seção sobre o método, cabe pontuar que a partir do levantamento das informações, será elaborado um quadro com a regulação sobre IA por parte do Estado e das empresas já mencionadas e marcação da data da consulta para tornar claro de qual momento diz respeito. Será discutido o que está posto de regulação pelas empresas de IA, a partir de seus termos de uso, como também do Estado, a partir de sua produção legislativa. Além disso, serão pontuadas as possibilidades e resistências para uma regulação vinda do Estado.

3 RESULTADOS

A partir do levantamento realizado, está apresentado, a seguir, na forma de quadro, os marcos regulatórios.

A análise das diferentes abordagens regulatórias revela um contraste entre a busca por uma legislação abrangente por parte do Estado e a implementação de regras mais focadas na utilização da tecnologia pelas empresas.

Latini e Fachinetti (2023) discutem três possibilidade de regulação de sistemas de IA: regulação estatal, autorregulação e corregulação. A regulação estatal é o modelo clássico realizado pelo Estado ou conjunto de Estados em que formula regras sobre a matéria com obrigatoriedade após a aprovação, sendo conhecida como regras rígidas (Latini e Fachinetti, 2023).

A autorregulação se dá pelos próprios atores que produzem e disponibilizam a tecnologia ao público, com pouca participação do Estado e maior liberdade para as empresas ((Latini e Fachinetti, 2023). O terceiro modelo é a corregulação com junção de esforços do Estado e das empresas, havendo uma definição dos papéis e do nível de participação para construção das normas, podendo haver maior ou menor liberdade para as empresas de sistema de IA podendo ocorrer também delegação de atribuição de um a outro ((Latini e Fachinetti, 2023).

Numa outra perspectiva mais aberta está a regulação por princípios, proposta por Engelmann (2024), em que a construção de princípios se dá interna e externamente ao ordenamento jurídico, forma de deixar espaço criativo para a regulação da IA pela perspectiva hermenêutica. Os princípios para orientação do intérprete estariam no texto constitucional, no direito natural, além disso podem haver princípios da economia, das ciências em geral, das áreas do conhecimento, numa maior pluralidade e flexibilidade regulatória (Engelmann, 2024).

A fonte para criação de princípios para regulação da IA pode estar na legislação, na jurisprudência, na ciência da computação, enfim, seria um espaço aberto para a criação de princípios para a regulação da IA.

Há ponderações e defesas de regulação num sentido ou no outro, desde se aguardar a maturidade, com finalidade de compreensão da tecnologia e depois disso

efetuar regulação, como em outra direção de que há necessidade e urgência para a regulação, não impedindo o aperfeiçoamento à medida da necessidade futura.

O quadro a seguir expõe os principais pontos para comparação:

QUADRO 1 - Comparação entre as regulações de IA

Tópico Regulatório	Projeto de Lei nº 2.338/2023 (Marco Legal da IA)	OpenAI (ChatGPT) – Políticas de Uso	Google (Gemini) – Política de Uso Proibido
Abordagem Principal	Baseada em riscos, classificando sistemas em: *risco excessivo*, *alto risco* e *demais categorias*.	Focada em proibições de usos específicos que possam gerar danos.	Centrada na proibição de usos que violem a lei, segurança ou gerem danos.
Direitos dos Indivíduos	Informação prévia, explicação sobre decisões automatizadas, não discriminação e intervenção humana.	Proteção da privacidade e proibição de uso para violação de direitos, difamação ou assédio.	Privacidade garantida e proibição de uso para desinformação, danos, ódio e violações legais.
Governança e Transparência	Exige Relatório de Impacto Algorítmico e supervisão humana para sistemas de alto risco.	Exige cumprimento das leis e transparência sobre o sistema de IA utilizado.	Proíbe conteúdos que possam enganar sobre sua origem e exige cumprimento da legislação.
Responsabilidade Civil	Responsabilização do fornecedor ou operador por danos causados por sistemas de IA.	Responsabilidade limitada: o usuário responde pelo uso e conteúdo gerado.	Mesma lógica: empresa isenta, usuário responde por uso indevido.
Sanções	Advertência, suspensão e multas até R$ 50 milhões ou 2% do faturamento.	Suspensão ou banimento da conta em caso de violação.	Restrição ou perda de acesso aos serviços.
Autoridade Fiscalizadora	Criação de autoridade competente para implementar e fiscalizar a lei.	Fiscalização interna via denúncias e monitoramento.	Empresa revisa conteúdos e aplica medidas diretamente.
Data da Consulta	26/09/2025	26/09/2025	26/09/2025

4 DISCUSSÃO

Observa-se que não há ainda uma legislação pelo Estado, somente o Projeto de Lei nº 2.338/2023 que foi aprovado no Senado Federal e encaminhado para a Câmara dos Deputados.

O Projeto de Lei 2.338 de 2023 é de autoria do Senador Federal Rodrigo Pacheco - PSD/MG - tendo a seguinte ementa: “Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana” (BRASIL, 2025). A situação atual do projeto de lei é estar aguardando Parecer do(a) Relator(a) na Comissão Especial destinada a proferir parecer ao Projeto de Lei nº 2338, de 2023, do Senado Federal, que "dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana" (PL233823) (BRASIL, 2025).

Relativo à tramitação do Projeto de Lei 2.338 de 2023, há requerimentos de apensamentos de outros projetos de lei, de realização de audiências públicas e seminário para debater a regulação da inteligência artificial com participação de estudiosos do tema, atores públicos e privados (BRASIL, 2025).

A redação constante para o último parecer do Senado Federal para o Projeto de Lei 2.338 de 2023 apresenta como fundamentos para o desenvolvimento, implementação e uso dos sistema de IA a centralidade da pessoa humana, o respeito e promoção aos direitos humanos e aos valores democráticos, livre desenvolvimento da personalidade e liberdade de expressão, proteção ao meio ambiente e ao desenvolvimento ecologicamente equilibrado, igualdade, não discriminação, pluralidade e diversidade, direitos sociais, em especial a valorização do trabalho humano, desenvolvimento socioeconômico, científico e tecnológico e inovação, defesa do consumidor, livre iniciativa e livre concorrência, privacidade, proteção de dados pessoais e autodeterminação informativa (BRASIL, 2024).

O Senado Federal na redação final do texto do Projeto de Lei 2.338 de 2023 deixou previsão de avaliação preliminar de riscos, antes da introdução e circulação no mercado ou utilização do sistema de IA (BRASIL, 2024).

Já as empresas de IA possuem seus termos de uso que dão o tom da regulação atualmente. Com a autorregulação, as empresas de IA possuem maior liberdade e como vantagens deste modelo estão o maior conhecimento da tecnologia quanto ao funcionamento e capacidade de resolução de problemas, evitam a elaboração de regras que dificultam a inovação e o desenvolvimento da IA, a adoção de padrões globais, certificações e regimes de validação (Latini e Fachinetti, 2023).

Latini e Fachinetti (2023) apontam, por outro lado, que com a autorregulação os principais *players* podem criar uma associação encarregada de elaboração de códigos de conduta, padrões e barreiras para entrada de novas empresas, como também dificuldades para atuação do Estado na fiscalização e aplicação de punição em caso de infração e ilícito.

Quanto à responsabilidade civil, as empresas de IA não se atribuem responsabilidade pelas operações, havendo relativa atribuição ao usuário da responsabilidade pelo conteúdo gerado e pelo uso (GEMINI e CHATGPT, 2025).

O que se evidencia é que sem legislação vinda do Estado não há responsabilização das empresas pelo conteúdo e ações da IA no modelo de autorregulação. Os termos de uso atribuem aos usuários a responsabilidade pelo uso e obtenção dos resultados. Em tal aspecto, a responsabilidade civil e criminal será abordada pelas regras gerais até a existência de regras específicas. A questão que se destaca aqui é a investigação para levantamento de provas, que poderá se dar por iniciativa daquele que entende sofrer violação de um direito ou o socorro de órgãos públicos, tal como Ministério Público, que vão precisar avançar no conhecimento da tecnologia para responsabilização, investigação, processamento e julgamento.

A discussão acerca da necessidade de regulação é sempre aberta, tendo posição em diferentes direções como exposto no seguinte trecho:

> As regulações não deveriam ser vistas apenas sob o prisma negativo, como se fossem sequências desnecessárias de proibições e deveres. Regulações bem desenhadas podem criar mercados, fomentar novas tecnologias, ampliar a gama de competidores, incrementar benefícios sociais e tornar interessantes investimentos privados. Adequações entre atividade produtiva, respeito a direitos fundamentais, meio ambiente e direitos dos consumidores não representam novidade, pois já assegurados na Constituição Federal (Art. 170-181). (ARIENTE, 2025, Page: RB-1.23)

A divisão quanto à regulação da IA é sentida nos discursos. Contrários à regulação estatal manifestam a favor da autorregulação pelas empresas de IA ou de legislação que lhe seja favorável. Manifestação de representantes das empresas de IA é comum no sentido de sua autorregulação:

> "Novas tecnologias frequentemente trazem novos desafios, e depende das empresas garantir que vamos desenvolver e

> lançar produtos de forma responsável" disse ao Senado dos EUA, em 2023, o CEO da Meta, Mark Zuckerberg, defendendo a autorregulação da IA. "Temos condições de criar proteções internas a esses sistemas." (INTERCEPT BRASIL, 2025)

A favor da regulação da IA vinda do poder público ganha conteúdo com regras relacionadas à proteção dos direitos autorais, dados pessoais e mercado de trabalho. Isto possui repercussão, contudo, o momento é de deslumbramento e a IA revela o mundo encantado a ser descoberto por todos. Para ter ciência de uma manifestação favorável à regulação, apresenta-se trecho da reportagem do Intercept:

> Do outro lado do debate, políticos, especialistas em tecnologia, representantes dos setores afetados pela IA, e representantes da sociedade civil defendem ferrenhamente uma regulamentação muito mais rígida. Eles querem a implementação antecipada de regras sobre direitos autorais, proteção de dados e boas práticas trabalhistas, além dos usos que afetam a segurança pública, com os *deepfakes* generativos, a criação de armas químicas e biológicas, e os ataques cibernéticos (INTERCEPT BRASIL, 2025).

Em regiões que houve avanço da regulação da IA pelo poder público, as empresas de IA, em reação, socorreu de lobby, manifestações nas redes sociais e ameaças de saídas de mercados como se vê:

> As gigantes da tecnologia também fizeram lobby agressivo contra o projeto da UE. A OpenAI teria obtido bons resultados na tentativa de reduzir o ônus regulatório da lei sobre a empresa, e Altman fez uma ameaça de que a OpenAI poderia deixar a Europa se ele considerar que a regulamentação está muito restrita (INTERCEPT BRASIL, 2025).

Em período recente, tentou-se regular matérias relacionadas a tecnologia e Internet, como se deu com o projeto de lei das *Fake News*:

> Em 2023, um abrangente projeto de "Lei das Fake News", como ficou conhecido, tentou obrigar as redes sociais a terem mais transparência e se responsabilizarem pela desinformação. O projeto de lei foi aprovado no Senado, mas acabou derrotado na Câmara, após intensa pressão pública do Google, da Meta, e do aplicativo de troca de mensagens Telegram (INTERCEPT BRASIL, 2025).

Relativo ao projeto de lei n. 2338 de 2023, houve sua aprovação no Senado Federal em 10 de dezembro de 2024 e na sequência foi remetido à Câmara do Deputados (BRASIL, 2025).

Um dos pontos de destaque na discussão está acerca da autoridade supervisora que o projeto de lei cria (BRASIL, 2025). Tal autoridade possui papel de fiscalização. Para as empresas de IA a autoridade é interna, empresa enquanto autoridade, podendo fiscalizar o uso, aplicar punições como exclusão de usuário mediante comunicações de violações e alteração da sua política de uso.

A competência de fiscalização e capacidade de punição será abordada em muitas instâncias além dos poderes judiciário e legislativo. A existência de autoridade pública com o papel de fiscalizar possivelmente não impede de as empresas de tecnologia também realizarem fiscalização, assim como no âmbito das punições, a competência será compartilhada ou dividida. As empresas de IA podem assumir papel preventivo para violações de direito e ilícitos, cabendo ao Estado atuar em caso de falha da prevenção.

Relativo à governança, a disponibilização de informações sobre riscos e segurança contribuem, além de afirmar que cumprem a legislação e os direitos individuais.

Quanto às sanções, o caminho da prevenção pelas empresas de IA pode surtir bastante efeito positivo, contudo a autoridade pública pode atuar quando houver falhas na prevenção, tendo um conjunto de instrumentos previstos na legislação para que possa lançar mão e aplicar, tendo o poder necessário para punir. O poder judiciário é também espaço para busca de punição em caso de violações de direitos e condutas que sejam ilícitas.

Como se apresenta em mundo novo a IA, as condutas podem não ser dadas em tipos para sua obsolescência aparecer em curto tempo e seja possível punição. A abertura para punição de condutas para além da tipificação colabora com esse momento de modernidade e inovação.

A utilização de dados a partir da interação dos usuários com os sistemas é um recurso importantíssimo para todos, para as empresas serve para treinamento do modelo, correção, aumento de capacidade, aumento da base de dados. Para os usuários são aprendizado para realizar o diálogo com o sistema, treinamento para fornecer melhores resposta, crença no sistema para fazer trabalhos com complexidades crescentes. Toda esta interação, envolve para todos, fornecimento de

informações que pode resvalar na Lei Geral de Proteção de Dados e demais normas que buscam preservar a personalidade e direitos individuais.

5 CONCLUSÃO

De forma conclusiva, não sendo realizada a regulação da IA pelo Estado fica, necessariamente, a regulação entregue às empresas de IA, que pela autorregulação promoverá os limites, possibilidades de expansão, responsabilização, permissão de conteúdos, proteção de direitos autorais, bem como as implicações da IA e seu funcionamento com o direito interno do Brasil.

Tal liberdade, diante da falta de regulação pelo Estado, é o cenário ideal e buscado pelas empresas de IA.

A regulação pelo Estado é a possibilidade de entregar à discussão pública acerca dos limites da IA para o Congresso Nacional e também para o Poder Executivo, ao criar a autoridade fiscalizadora e seu regulamento, podendo haver participação do cidadão nesse processo legislativo e das fiscalizações administrativas e cidadã.

O compartilhamento de competências na fiscalização e punição entre empresas e poder público evidencia-se como um caminho necessário, a colaboração das empresas de tecnologia para fornecimento de informações, indicação de autoria é tão importante que cabe deixar o papel de prevenção para as empresas. O poder público poderá atuar em caso de falha na prevenção.

Várias são as propostas de regulação, a partir do sujeito responsável, se pelo Estados ou pelas empresas, a adoção de alguma existente em outro país ou comunidade, ou a construção de regulação a partir de princípios. Cabe concluir que não se firmou em fixar aqui um modelo a ser adotado, em perspectiva democrática e do diálogo traz apenas algumas linhas a considerar para a regulação:

1. Participação do poder público e privado.
2. Compartilhamento de informações para evitar assimetria.

3. Definição de papéis e competências que não se esgotam, podendo haver sobreposição de atribuições para em falta de ação de um outro atuar.
4. Consideração da ética, filosofia e das ciências para definição das regras e da moral.
5. Preocupação com transparência (ou acesso de informações), segurança, riscos, processos de tomada de decisões.
6. Garantia que o ser humano é o ponto central.

REFERÊNCIAS

ARIENTE, Eduardo. Curso de Direito da Inovação.Ed. 2025. Publisher: Thomson Reuters Brasil, Page: RB-1.23, 2025. Disponível: https://next-proview.thomsonreuters.com/launchapp/title/rt/monografias/370092027/v2/page/RB-1.23%20.

BRASIL. Projeto de Lei nº 2.338, de 2023. Dispõe sobre o uso da Inteligência Artificial. Brasília, DF: Senado Federal, 2025.

BRASIL. Senado Federal. Projeto de Lei n° 2338, de 2023 - Tramitação. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233.

BRASIL. Senado Federal. Parecer nº 208, de 2024-PLEN/SF - Redação para o turno suplementar - Republicação. Parecer para o Projeto de Lei 2.338 de 2023. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9884955&ts=1742240908365&disposition=inline.

BRASIL. Câmara dos Deputados. PL 2338/2023 - Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2487262

CHAT GPT. Termo de uso. Disponível: https://chatgpt.com/.

CHAT GPT. Conheça o ChatGPT. Disponível em: https://openai.com/pt-BR/index/chatgpt/.

ENGELMANN, Wilson. INTELIGÊNCIA ARTIFICIAL A PARTIR DOS PRINCÍPIOS. In: PARENTONI, Leonardo; JÚNIOR, Wagner Meira [coordenadores]. Direito, Tecnologia e Inovação – v. VI: Ciência de Dados e Direito. Belo Horizonte: Centro DTIBR, 2024 (recurso eletrônico).

GEMINI. Termo de uso. Disponível: https://gemini.google.com/.

GOOGLE. Gemini - Como o Google retém os dados que coletamos. Disponível em: https://policies.google.com/technologies/retention Acesso em: 14 nov. 2025.

GOOGLE. Usar os apps do Gemini. Disponível em: https://support.google.com/gemini/answer/13275745?hl=ptBR&ref_topic=15280100&sjid=5372172187782535770-SA.

INTERCEPT BRASIL. 'Estão tentando eliminar todas as leis' - A luta global para regular inteligência artificial. Disponível: https://www.intercept.com.br/2025/01/21/luta-global-regulacao-inteligencia-artificial/?utm_source=google&utm_medium=cpc&utm_campaign=pmax_newsletter&gad_source=1&gad_campaignid=22545513018&gbraid=0AAAAA-GeiJdD6yQKzO26x7SZRg2K2mDwK&gclid=EAIaIQobChMI_4Pq4ceIkAMVeVlIAB1B-TBPEAAYASAAEgJg3vD_BwE.

INSTITUTO DE ENGENHARIA. A história da inteligência artificial. Disponível em: https://www.institutodeengenharia.org.br/site/2018/10/29/a-historia-da-inteligencia-artificial/

LATINI, LUCAS MALDONADO DIZ; FACHINETTI, ALINE FUKE. Caminhos para a regulação da inteligência artificial no Brasil. In: Marina Feferbaum (coordenação). Ética, governança e inteligência artificial. São Paulo: Almedina, 2023 (recurso eletrônico).

RESPONSABILIDADE CIVIL NAS VIOLAÇÕES AO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS: UMA ANÁLISE DA JURISPRUDÊNCIA BRASILEIRA

Alicia Alexandre de Sousa[1]
Ana Júlia Sarauza Castro [2]
Gabriel Machado Oliveira Fagundes[3]
Lucca de Sousa Ribeiro[4]

RESUMO

A Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), constitui marco essencial na consolidação do direito à privacidade e à proteção de dados no Brasil. Seu objetivo é regulamentar o tratamento de informações pessoais por pessoas físicas e jurídicas, assegurando transparência, segurança e respeito à dignidade humana. A lei adota, em seu artigo 42, o regime de responsabilidade civil objetiva dos agentes de tratamento, bastando a comprovação do dano e do nexo causal, sem necessidade de demonstração de culpa. No setor privado, a LGPD impõe deveres de governança, consentimento e medidas preventivas, exigindo das empresas uma postura ética e responsável na gestão de dados. Apesar dos desafios técnicos e financeiros, a adequação à legislação fortalece a confiança do consumidor e a credibilidade institucional. A jurisprudência recente, como a condenação da empresa Meta pelo Tribunal de Justiça de Minas Gerais, reforça a aplicação efetiva da norma e o compromisso com a proteção integral dos titulares, consolidando a privacidade como valor fundamental no cenário jurídico e digital brasileiro.

Palavras-chave: Lei Geral de Proteção de Dados; Responsabilidade civil; Privacidade; Setor privado; Proteção de dados.

[1] Graduando em Direito no UniCEUB - Centro Universitário de Brasília. E-mail: alicia.asousa@sempreceub.com
[2] Graduando em Direito no UniCEUB - Centro Universitário de Brasília. E-mail: ana.scastro@sempreceub.com
[3] Graduando em Direito no UniCEUB - Centro Universitário de Brasília. E-mail: gabriel.fagundes@sempreceub.com
[4] Graduando em Direito no UniCEUB - Centro Universitário de Brasília. E-mail: lucca.ribeiro@sempreceub.com

SUMÁRIO: Introdução; 1. A responsabilidade civil no direito brasileiro; 1.1 Fundamentos Jurídicos da Responsabilidade civil na LGPD; 1.2 Elementos da Responsabilidade Civil no Tratamento de Dados; 1.3 Natureza da Responsabilidade: Objetiva ou Subjetiva?; 1.4 Solidariedade entre controlador e operador; 1.5 Desafios e Perspectivas da Responsabilidade Civil na LGPD; 2. A LGPD no Âmbito Privado: Desafios e Oportunidades para a Proteção de Dados Pessoais; 2.1 O que é a LGPD; 2.2 A proteção de Dados Pessoais no Setor Privado; 2.3 Desafios para o Setor Privado; 2.4 As oportunidades para o Setor Privado; 2.5 Um grande potencial de INTERNACIONALIZAÇÃO; 3. Desafios para a Aplicação da LGPD no Âmbito Privado; 3.1 O Desafio da Cultura de Proteção de Dados; 3.2 O peso no bolso e as barreiras tecnológicas; 3.3 As dúvidas da lei: Incerteza Jurídica na Prática; 3.4 O dilema da Inovacao: Proteger a Privacidade; 3.5 Olhando para o Futuro: A proteção de dados como valor; 4. A jurisprudência acerca da responsabilidade civil em casos de violação da LGPD; Conclusão; Referências.

1 INTRODUÇÃO

A aplicação da LGPD, trouxe novos deveres às empresas e instituições públicas, exigindo, sobretudo, boas práticas de governança, transparência e responsabilidade no tratamento dos dados pessoais. Além disso, abriu caminho para a evolução de entendimentos jurisprudenciais que reforçam a responsabilização de agentes que violarem direitos dos titulares. Assim, a responsabilidade civil ganha importante lugar na legislação brasileira, seja para reparar danos, seja para prevenir condutas ilícitas.

Com efeito, este artigo analisa os fundamentos da responsabilidade civil previstos na LGPD, a responsabilidade objetiva do causador do dano, a evolução da jurisprudência, os desafios no setor privado para sua implementação em face dos casos de vazamento e violação de dados. Objetiva também o artigo, mostrar como o Judiciário vem interpretando a LGPD frente à dignidade da pessoa humana, a proteção de dados como elemento indispensável para a preservação da intimidade de todo cidadão na era digital.

2 A RESPONSABILIDADE CIVIL NO CONTEXTO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), representa um marco normativo na tutela dos direitos fundamentais à privacidade e à

proteção de dados. Entre seus pilares, destaca-se a responsabilização dos agentes de tratamento, que confere efetividade à norma e assegura a reparação dos danos decorrentes de eventuais violações. A responsabilidade civil, nesse contexto, atua como instrumento de garantia e prevenção, visando não apenas à compensação dos prejuízos sofridos, mas também à indução de condutas diligentes no tratamento de dados.

2.1 Fundamentos jurídicos da responsabilidade civil na LGPD

A LGPD adota, em seu artigo 42, um modelo de responsabilidade civil objetiva dos agentes de tratamento, controladores e operadores, quando demonstrado o dano decorrente de tratamento irregular de dados pessoais. Assim, dispensa-se a prova da culpa, bastando a comprovação do dano e do nexo causal entre este e a conduta ilícita.

O caput do artigo 42 dispõe que "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo".

Dessa forma, a norma consagra a proteção integral do titular, abrangendo tanto danos materiais quanto extrapatrimoniais, inclusive os de caráter coletivo, reforçando o caráter difuso e metaindividual do direito à privacidade.

2.2 Elementos da responsabilidade civil no tratamento de dados

A ilicitude na LGPD decorre da **violação de princípios e deveres legais** impostos aos agentes de tratamento, como os da finalidade, necessidade, transparência e segurança. A ausência de base legal para o tratamento, a coleta excessiva de dados ou a ausência de consentimento são exemplos de condutas que configuram ilícitos aptos a gerar responsabilidade.

O **dano**, para fins de responsabilização, pode ser **patrimonial** (como o uso indevido de informações para fins econômicos) ou **moral** (como a exposição indevida de dados sensíveis, violando a intimidade e a honra do titular). O **nexo**

causal liga a conduta do agente à ocorrência do prejuízo, sendo requisito indispensável para a configuração do dever de indenizar.

O §3º do art. 42 da LGPD prevê hipóteses de **exclusão de responsabilidade**, como a demonstração de que o agente:

- não realizou o tratamento que gerou o dano;
- não houve violação à legislação de proteção de dados;
- ou que o dano decorreu de culpa exclusiva do titular ou de terceiros.

Essas excludentes revelam a busca do legislador por equilibrar a proteção do titular com a segurança jurídica dos agentes econômicos.

2.3 Natureza da responsabilidade: objetiva ou subjetiva?

Embora o texto legal estabeleça a responsabilidade objetiva, parte da doutrina discute se, em certos casos, o regime não poderia ser subjetivo, especialmente quanto ao operador de dados.

Segundo Danilo Doneda (2020), a responsabilidade objetiva justifica-se pela assimetria entre os agentes e os titulares, que normalmente não possuem condições técnicas de compreender o tratamento de seus dados. Assim, a imputação objetiva visa "garantir a efetividade do direito à proteção de dados, diante da vulnerabilidade do titular frente às organizações que tratam suas informações".

Por outro lado, Caio Mário da Silva Pereira (2018), ao discorrer sobre a teoria geral da responsabilidade civil, ensina que esta se funda na ideia de reparação do dano injusto, sendo indiferente, em muitos casos, a presença de culpa quando o risco decorre da própria atividade. Transpondo seu ensinamento à LGPD, observa-se que o tratamento de dados é uma atividade de risco inerente, o que reforça a adequação do regime objetivo de responsabilidade.

2.4 Solidariedade entre controlador e operador

O §1º do art. 42 estabelece que o controlador e o operador responderão solidariamente pelos danos, quando ambos participarem do mesmo tratamento que deu causa ao prejuízo. Essa solidariedade é essencial para assegurar a reparação integral ao titular, conferindo-lhe maior facilidade na busca de indenização.

Contudo, o agente que reparar o dano poderá exercer o direito de regresso contra os demais responsáveis, na medida de sua participação na infração. Esse mecanismo harmoniza a justiça reparatória com a proporcionalidade na distribuição da responsabilidade.

2.5 Desafios e perspectivas da responsabilidade civil na LGPD

A responsabilidade civil na LGPD cumpre papel central na efetivação dos direitos fundamentais à privacidade e à proteção de dados pessoais. O regime objetivo adotado reflete a natureza de risco da atividade de tratamento e a vulnerabilidade dos titulares.

Como ensina Caio Mário da Silva Pereira (2018), o dever de indenizar constitui uma exigência de justiça e equilíbrio social, de modo que quem causa dano injusto deve repará-lo. A LGPD, ao incorporar essa diretriz, confere concretude à proteção de dados como verdadeiro direito da personalidade, reafirmando o compromisso do ordenamento jurídico brasileiro com a dignidade da pessoa humana e com o uso ético das tecnologias da informação.

3 A LGPD NO ÂMBITO PRIVADO: DESAFIOS E OPORTUNIDADES PARA A PROTEÇÃO DE DADOS PESSOAIS

Inicialmente é necessário entender o que é e como se aplica a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil. Instituída pela Lei nº 13.709/2018, essa lei chegou em nosso país com o objetivo de regulamentar o tratamento de dados pessoais, alinhando o Brasil às principais legislações internacionais de proteção de dados. A sua implementação no setor privado, com as respectivas implicações jurídicas, econômicas e sociais, é um desafio constante, especialmente levando em

consideração o vasto volume de dados pessoais tratados por empresas brasileiras de diferentes portes e setores.

Portanto, esse capítulo do livro irá observar e analisar a LGPD no âmbito do setor privado, abordando sobre a legislação específica, as implicações para que ocorra a proteção de dados pessoais de forma efetiva, as obrigações das empresas diante desse cenário, bem como os desafios que as organizações enfrentam para se adaptar à nova realidade jurídica.

3.1 O que é a LGPD (Lei Geral de Proteção de Dados Pessoais)?

A Lei Geral de Proteção de Dados Pessoais (LGPD) tem como principal objetivo garantir a privacidade e a segurança dos dados pessoais, criando regras para o seu armazenamento, tratamento, compartilhamento e eliminação. Dados pessoais são, conforme disposto no artigo 5º I da LGPD, a informação relacionada a pessoa natural identificada ou identificável.

Importante destacar que a referida lei se aplica a qualquer operação de tratamento de dados pessoais, seja por pessoa natural ou pessoa jurídica, de direito público ou privado, do país de sede ou da nacionalidade dos titulares dos dados, de acordo com o artigo 3º da LGPD. Fato esse que é possível entender que qualquer empresa que realize o tratamento de dados pessoais de indivíduos localizados no Brasil deve cumprir com as exigências da lei, independentemente de sua sede ou nacionalidade.

Além disso, a lei define algumas bases legais para que se realize o tratamento de dados pessoais, dentre elas está o consentimento do titular, o cumprimento de obrigação legal ou regulatória e o interesse legítimo do controlador. A questão do consentimento do titular é uma das bases mais comumente usadas no setor privado, especialmente para empresas que coletam dados em grande escala, como empresas de marketing e e-commerce.

3.2 A proteção de dados pessoais no setor privado

Diante do exposto acima sobre a LGPD, é preciso entender que no setor privado, essa lei exige que as próprias empresas adotem medidas rigorosas de governança de dados, promovendo a transparência destes e garantindo que sejam tratados de acordo com os princípios estabelecidos pela lei, tais como a finalidade, a necessidade e a segurança.

Nesse sentido, as principais obrigações das empresas privadas em relação à LGPD incluem a obtenção de consentimento explícito dos titulares, quando necessário, para o tratamento de dados, o estabelecimento de políticas de privacidade claras informando como os dados pessoais são tratados, a garantia dos direitos aos titulares dos dados, dentre outras.

É imperioso ressaltar ainda que as empresas devem estar preparadas, portanto, para incidentes de segurança que envolvem dados pessoais e adotar, de forma preventiva e corretiva, medidas em conformidade com a LGPD.

3.3 Desafios para o setor privado

Como visto anteriormente, percebemos que a implementação da LGPD representa um grande desafio para muitas das empresas no Brasil, especialmente para aquelas que não estavam previamente preparadas para lidar com o tratamento correto dos dados pessoais. Entre os desafios, podemos destacar a adaptação relacionada às exigências regulatórias, os custos, o treinamento dos funcionários e da empresa como um todo, além do monitoramento e auditoria dessa regulamentação.

3.4 As oportunidades para o setor privado

Apesar de a LGPD estabelecer alguns desafios significativos, também oferece inúmeras oportunidades para as empresas privadas que adotam a proteção dos dados como parte de seu plano estratégico empresarial. A conformidade com a LGPD pode ser vista como um diferencial para a empresa, pois pode proporcionar benefícios, seja a curto ou a longo prazo.

Portanto, as empresas que demonstram um certo compromisso com a proteção de dados pessoais podem conquistar maior confiança por parte dos

consumidores, o que, por sua vez, pode resultar em uma fidelização entre cliente e empresa.

3.5 Um grande potencial de internacionalização

Um ponto que recebe atenção dentro do tema abordado, é que a conformidade com a LGPD pode abrir portas para que as empresas brasileiras expandam suas operações para mercados internacionais.

Muitos países, especialmente na União Europeia, exigem conformidade com regulamentações semelhantes à LGPD para que as empresas possam negociar e processar dados de cidadãos estrangeiros. Nesse contexto, a adoção antecipada e preventiva da LGPD pode facilitar a internacionalização de empresas brasileiras.

Como podemos perceber, a LGPD representa um marco muito importante na proteção dos dados pessoais no Brasil. No entanto, ao adotar práticas adequadas de governança de dados e demonstrar compromisso com a privacidade dos titulares, as empresas não apenas cumprem a legislação, mas também podem se beneficiar de um aumento da confiança do consumidor e melhores práticas de gestão de dados.

À luz disso, a adequação à LGPD exige uma mudança cultural e organizacional, onde a proteção de dados deve ser vista não apenas como uma obrigação vinda de uma lei, mas como uma oportunidade de inovação e crescimento no mercado.

4 DESAFIOS PARA A APLICAÇÃO DA LGPD NO ÂMBITO PRIVADO

A chegada da Lei Geral de Proteção de Dados Pessoais (LGPD), em 2018, foi um marco importantíssimo para garantir que os brasileiros tivessem mais controle sobre seus dados e mais privacidade. No entanto, colocar essa lei em prática no dia a dia das empresas não é uma tarefa fácil. Existem diversos desafios técnicos, jurídicos e até mesmo de mentalidade que precisam ser superados para que os princípios da LGPD saiam do papel.

4.1 O desafio da cultura de proteção de dados

Um dos maiores "tropeços" que as empresas enfrentam é a falta de uma mentalidade focada na proteção de dados. Embora a LGPD exija boas práticas e programas de governança, muitas organizações ainda veem a adequação como um mero carimbo burocrático, um requisito formal.

O problema é que a lei não é só sobre papelada. Para que a LGPD funcione de verdade, é preciso uma mudança de comportamento que vai além da técnica: gestores e colaboradores precisam entender, de fato, a importância de proteger os dados das pessoas. Tratar dados deve ser visto não só como uma obrigação legal, mas como um pilar ético é essencial para construir a confiança do cliente na marca.

4.2 O peso no bolso e as barreiras tecnológicas

Outro desafio que pesa é a questão dos custos e das dificuldades técnicas. As pequenas e médias empresas, em particular, sentem o aperto. Elas costumam ter menos recursos financeiros e estruturais para investir em sistemas robustos de segurança, fazer auditorias internas complexas ou contratar um Encarregado de Dados altamente especializado.

Quando a infraestrutura de tecnologia falha, as empresas ficam vulneráveis a vazamentos, acessos indevidos e incidentes de segurança. Isso prejudica tanto a integridade dos dados quanto a reputação do negócio. Por isso, a aplicação da LGPD precisa de incentivos e políticas públicas que ajudem até mesmo as empresas menores a adotarem práticas seguras e acessíveis.

4.3 As dúvidas da lei: incerteza jurídica na prática

Apesar da atuação cada vez mais presente da Autoridade Nacional de Proteção de Dados (ANPD), ainda existe uma névoa de insegurança jurídica pairando sobre a interpretação de muitos pontos da LGPD. Questões como a base legal correta para tratar um dado, como deve ser o consentimento ideal, a

responsabilidade em caso de danos e a forma como as multas serão aplicadas ainda estão em aberto.

A falta de um conjunto de decisões e orientações uniformes (a chamada jurisprudência consolidada) acaba gerando uma aplicação desigual da lei no mercado, o que causa incerteza nas relações comerciais. A atuação clara e orientadora da ANPD é crucial para "desanuviar" o cenário e garantir que a lei seja aplicada de forma justa e eficaz.

4.4 O dilema da inovação: proteger a privacidade sem frear o progresso

O ritmo acelerado das tecnologias digitais impõe um desafio extra: como ser inovador e competitivo no mercado sem desrespeitar a privacidade? Empresas que trabalham com marketing digital, análise de dados e inteligência artificial estão constantemente buscando um equilíbrio entre suas estratégias de informação e o dever de proteger os direitos dos cidadãos.

Usar dados para personalizar produtos e serviços, se não for feito com transparência e consentimento claro, pode facilmente ferir os princípios da LGPD, como o da finalidade (usar o dado para o que foi coletado) e o da minimização (coletar apenas o estritamente necessário). Por isso, é fundamental que as empresas criem políticas de governança que garantam que a inovação seja ética e compatível com os valores de dignidade e liberdade.

4.5 Olhando para o futuro: a proteção de dados como valor

A aplicação da LGPD nas empresas ainda está em uma fase de amadurecimento. Para avançar, são necessários esforços conjuntos do governo, das empresas e da sociedade. A construção de uma verdadeira cultura de proteção de dados exige educação digital, a formação de profissionais capacitados e a continuidade do trabalho orientador e fiscalizador da ANPD.

No fim das contas, a proteção de dados vai além de uma obrigação legal; ela é uma prática de responsabilidade social corporativa. É o caminho para fortalecer a

confiança dos consumidores e garantir o desenvolvimento saudável e sustentável das relações econômicas no nosso mundo digital.

5 A JURISPRUDÊNCIA ACERCA DA RESPONSABILIDADE CIVIL EM CASOS DE VIOLAÇÃO DA LGPD

No âmbito jurisprudencial, o Tribunal de Justiça de Minas Gerais condenou a empresa Meta a indenizar diretamente usuários afetados por vazamentos de dados. O caso, que envolveu falhas de segurança nas plataformas da empresa entre 2018 e 2019, demonstra que o dever de cuidado imposto aos agentes de tratamento de dados não se limita à adoção de medidas formais de segurança, mas abrange a efetiva prevenção de incidentes que possam comprometer a privacidade dos usuários, em respeito a lei geral de proteção de dados. Veja-se na ementa:

> EMENTA: PROCESSUAL CIVIL. PRELIMINARES DE NÃO CONHECIMENTO DA SEGUNDA APELAÇÃO POR VIOLAÇÃO AO PRINCÍPIO DA UNIRRECORRIBILIDADE REJEITADA. ACOLHIDA A PRELIMINAR DE NÃO CONHECIMENTO DE PARTE DA SEGUNDA APELAÇÃO POR VIOLAÇÃO AO PRINCÍPIO DA DIALETICIDADE. REJEITAR A PRELIMINAR DE ILEGITIMIDADE PASSIVA. REJEITAR A PRELIMINAR DE ILEGITIMIDADE ATIVA. MÉRITO. AÇÕES CIVIS PÚBLICAS CONEXAS. SENTENÇA ÚNICA. INTERPOSIÇÃO DO MESMO RECURSO NOS DOIS PROCESSOS. PRINCÍPIO DA UNIRRECORRIBILIDADE. APELAÇÕES INTERPOSTAS EM CADA PROCESSO. IMPROPRIEDADE. JULGAMENTO DAS MATÉRIAS VERSADAS EM TODOS OS RECURSOS NA PRIMEIRA APELAÇÃO. PREJUDICADOS OS RECURSOS INTERPOSTOS NO SEGUNDO PROCESSO. PRELIMINAR DE ILEGITIMIDADE ATIVA REJEITADA. MÉRITO. INDENIZAÇÃO DE DANOS MORAIS COLETIVO – MAJORAÇÃO E DESTINAÇÃO. INAPLICABILIDADE DO PRINCÍPIO DA SIMETRIA – CONDENAÇÃO EM HONORÁRIOS DE SUCUMBÊNCIA. As associações instituídas na forma do art. 82, IV, do CDC estão legitimadas para propositura de ação civil pública em defesa de interesses individuais homogêneos, não necessitando para tanto de autorização dos associados. Por se tratar do regime de substituição processual, a autorização para a defesa do interesse coletivo em sentido amplo é estabelecida na definição dos objetivos institucionais, no próprio ato de criação da associação, não sendo necessária nova autorização ou deliberação assemblear. Constatada a vulnerabilidade do consumidor e a hipossuficiência em relação a empresa de

> poderio econômico importante deverão os pagamentos das indenizações serem realizados de forma direta aos consumidores, nos exatos termos pedidos na letra "E" da exordial. O Instituto do Dano Moral veio justamente para inibir a reiteração de prática de atos ilícitos para aquele que sofreu o dano devendo a indenização ser proporcional e razoável e principalmente para que aquele que pratica tal ato tenha mais zelo e cuidado para que não proceda de forma irresponsável e negligente em prejuízo do consumidor. Torna-se lógico que não se apresenta com razoabilidade sob o enfoque ético e político, equiparar ou tratar como simétricos grandes grupos econômicos/instituição do Estado com organizações não governamentais (de moradores, de consumidores, de pessoas com necessidades ambientais, de idosos, ambientais, entre outras), devendo haver condenação de honorários de sucumbência na forma do artigo 85,§2º, do Código de Processo Civil.

Observe-se que a condenação, estabelecendo-se o valor de R$ 10.000,00 a título de indenização por danos morais individuais a cada usuário lesado e R$ 40 milhões a título de dano moral coletivo ao Fundo Estadual de Defesa do Consumidor, se encontra fundamentada na existência de defeito na prestação do serviço. Como se vê, todos os vazamentos noticiados não decorreram apenas de violações externas inevitáveis, incidindo também em deficiências estruturais de segurança dos próprios sistemas. Em suma, houve falha de segurança dos próprios produtos oferecidos pela empresa, o que constitui defeito do serviço nos termos do artigo 14 do Código de Defesa do Consumidor.

Ademais, verifica-se que o acórdão reconhece também a violação ao direito fundamental à proteção de dados pessoais, protegido pela LGPD e pelo artigo 5°, inciso LXXIX, da Constituição Federal. A Lei Geral de Proteção de Dados exige que os controladores e os operadores adotem medidas técnicas e administrativas razoáveis contra acessos, perdas e furtos ou outras formas ilegais de tratamento dos dados pessoais. Portanto, a falha na fiscalização e proteção dos dados dos usuários viola o dever de cuidado e leva a responsabilidade civil.

No contexto jurídico, a responsabilidade da Meta assume natureza objetiva, uma vez que a relação entre usuários e plataforma é de consumo, dispensando a prova de culpa. Basta a demonstração do dano e do nexo causal para que surja o dever de indenizar. Essa compreensão é reforçada pela LGPD, que impõe aos controladores e operadores o dever de adotar medidas técnicas e administrativas

aptas a proteger os dados pessoais contra acessos não autorizados e situações ilícitas. Quando esse dever é violado, presume-se a falha na segurança e, consequentemente, a responsabilidade civil da empresa.

O entendimento também se destaca por dispensar a necessidade de comprovação individual do dano moral, reconhecendo que a violação da privacidade e da segurança informacional já constitui, por si só, lesão a um direito da personalidade. Tal presunção assevera que a violação de privacidade ou segurança informacional já constitui lesão a um direito de personalidade, sugerindo que a vítima não precisa demonstrar cada elemento de responsabilidade. A argumentação está ligada à jurisprudência que cada vez mais aceita dano moral ”in re ipsa”, ou seja, presumido, em casos de exposição indevida de dados, considerando que o sentimento de vulnerabilidade e o abalo à confiança do usuário são consequências naturais do vazamento, o qual é a parte hipossuficiente na lide. Além disso, o Tribunal buscou assegurar a efetividade da tutela coletiva ao determinar o pagamento direto das indenizações, evitando que milhões de consumidores tivessem de ingressar individualmente com ações judiciais para obter reparação.

Ao se analisar essa condenação, reforça-se o entendimento de que o tratamento de dados pessoais é uma atividade de risco, o que justifica a adoção da responsabilidade objetiva com base na teoria do risco da atividade. Empresas que exploram economicamente informações pessoais assumem o dever de zelar pela integridade e segurança desses dados, devendo responder pelos danos decorrentes de falhas em seus sistemas. Assim, a decisão do TJMG cumpre não apenas uma função reparatória, mas também pedagógica, ao firmar a responsabilidade do controlador de zelar pelo não vazamento dos dados.

Em síntese, a decisão contra a Meta evidencia uma evolução do direito civil e do direito do consumidor diante dos desafios da era digital. Ao responsabilizar uma das maiores empresas de tecnologia do mundo por falhas de segurança em seus sistemas, o Judiciário brasileiro afirma a centralidade do direito fundamental à proteção de dados e da privacidade. Mais do que uma condenação financeira, trata-se de um precedente que reforça a importância da transparência, da segurança e da

responsabilidade social das plataformas digitais no tratamento das informações pessoais de seus usuários.

Ademais, o Superior Tribunal de Justiça reconheceu a responsabilidade objetiva de uma seguradora pelo vazamento de dados sensíveis de um cliente. A decisão foi relatada pela ministra Nancy Andrighi. Veja-se na ementa:

> CIVIL. RECURSO ESPECIAL. CONTRATO DE SEGURO DE VIDA. RELAÇÃO DE CONSUMO. CÓDIGO DE DEFESA DO CONSUMIDOR. LEI GERAL DE PROTEÇÃO DE DADOS. VAZAMENTO DE DADOS SENSÍVEIS. RESPONSABILIDADE OBJETIVA. DANO MORAL PRESUMIDO. RECURSO CONHECIDO EM PARTE.DESPROVIMENTO. 1. Ação de obrigação de fazer c/c indenização por danos morais e materiais,da qual foi extraído o presente recurso especial, interposto em 28/6/2023 e concluso ao gabinete em 22/2/2024. 2. O propósito recursal é definir se, em contrato de seguro de vida, o vazamento de dados sensíveis do segurado gera: (a) dano moral presumido e (b) responsabilização objetiva da empresa seguradora. 3. Inexistência de negativa de prestação jurisdicional. Acórdão do Tribunal de origem devidamente fundamentado para solucionar integralmente a controvérsia submetida à sua apreciação. 4. Não há cerceamento de defesa nas hipóteses em que o julgador resolve a questão controvertida, de forma fundamentada, sem a produção da prova requerida pela parte, em virtude de considerar suficientes os elementos que integram os autos. 5. A matéria que não foi objeto de debate no acórdão recorrido, mesmo após a interposição de embargos declaratórios, não pode ser conhecida por meio de recurso especial. Súmula nº 211/STJ. 6. Cabe ao fornecedor o ônus de comprovar que cumpriu com seu dever de proteger dados pessoais do consumidor, sobretudo quando se tratam de dados sensíveis, nos termos do CDC (arts. 6º, VIII e 14, caput e §3º) e da LGPD (arts. 6º, X, 8º, §2º, 42, §2º e 48, §3º). 7. Há especial proteção legal aos chamados dados pessoais sensíveis: aqueles que, quando revelados, podem gerar algum tipo de discriminação, sobretudo os que incidem sobre "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico" (art. 5º, II, da LGPD). 8. O tratamento de dados pessoais sensíveis observa requisitos significativamente mais rigorosos, sobretudo com a exigência, em regra, do consentimento específico e destacado do titular (art. 11 da LGPD). 9. Em contrato de seguro de vida, deve-se empreender um rigoroso esforço para a proteção dos dados pessoais, já que, para sua celebração, a seguradora, para a avaliação dos riscos, recebe dados sensíveis sobre aspectos pessoais, familiares, financeiros e de saúde do segurado. 10. O vazamento de dados pessoais sensíveis fornecidos para a

> contratação de seguro de vida, por si só, submete o consumidor a riscos em diversos aspectos de sua vida, como em sua honra, imagem, intimidade, patrimônio, integridade física e segurança pessoal. 11. Por isso, em seguro de vida, na hipótese de vazamento de dados sensíveis do segurado, verifica-se a responsabilização objetiva da seguradora e a caracterização de dano moral presumido. 12. Conforme entendimento desta Corte, a revisão da compensação por danos morais só é viável em recurso especial quando o valor fixado for exorbitante ou ínfimo, o que não se constata no recurso sob julgamento. 13. Hipótese em que o acórdão recorrido, ao manter a responsabilização da seguradora, reconheceu que: i) houve vazamento de dados pessoais do consumidor; ii) tais dados são classificados como sensíveis, de modo a abranger informações fiscais, bancárias e sobre a saúde do consumidor; iii) há nexo de causalidade entre o vazamento de dados sensíveis do consumidor e falhas na prestação do serviço pela recorrente, que não atendeu a seu dever de garantir a proteção dos dados sensíveis do consumidor. 14. Recurso especial parcialmente conhecido e, nessa extensão, desprovido.

No caso analisado, um segurado ajuizou ação após ter sido informado de que seus dados, incluindo informações patrimoniais, bancárias e relativas à saúde, haviam sido expostos em decorrência de um incidente de segurança nos sistemas da seguradora. O Tribunal de Justiça de São Paulo havia reconhecido o dano moral e fixado indenização de R$15 mil, decisão que foi mantida pelo STJ. A Corte entendeu que, ainda que o vazamento tenha decorrido de ação de terceiros, como hackers, subsiste a responsabilidade objetiva da seguradora, uma vez que ela é a controladora dos dados e, portanto, detém o dever de implementar medidas eficazes de proteção e prevenção.

A ministra Nancy Andrighi destacou que, no contexto da LGPD, o tratamento de dados sensíveis demanda um nível reforçado de cuidado, pois o risco de violação à intimidade, à honra e à imagem é mais acentuado. Assim, a simples ocorrência de um incidente que exponha tais informações já configura potencial lesão à esfera moral do titular, sendo desnecessária a prova de dano concreto. A decisão reafirma a interpretação de que o dano moral, em casos de vazamento de dados sensíveis, é presumido, em razão da gravidade da violação e da vulnerabilidade do titular.

O fundamento jurídico adotado pelo STJ apoia-se diretamente no artigo 42 da LGPD, que prevê a responsabilidade civil objetiva dos agentes de tratamento controladores e operadores, especificamente pelos danos causados em decorrência

de violação à legislação de proteção de dados. Tal dispositivo consagra a teoria do risco, impondo às empresas o ônus de demonstrar que o dano não decorreu de falha em sua estrutura de segurança. No caso, a seguradora não conseguiu comprovar a existência de culpa exclusiva de terceiro ou de caso fortuito externo que rompesse o nexo causal. A Corte reforçou, ainda, que o risco da atividade é inerente ao modelo de negócio das seguradoras, o que atrai a aplicação do artigo 14 do Código de Defesa do Consumidor, o qual mais uma vez (assim como o caso mostrado anteriormente) consagra a responsabilidade objetiva pelos defeitos na prestação de serviços.

O acórdão reflete uma tendência consolidada do STJ em reconhecer a vulnerabilidade informacional do consumidor em interpretar a LGPD em consonância com o sistema protetivo do direito do consumidor. Essa leitura ampliada permite compreender que a proteção de dados não é apenas uma questão de segurança digital, mas um desdobramento direto do direito fundamental à privacidade e à autodeterminação informativa, previstos na Constituição Federal. Assim, a decisão transcende o caso concreto e assume papel pedagógico, advertindo o mercado securitário sobre a necessidade de adoção de medidas robustas de governança e compliance em proteção de dados.

Do ponto de vista prático, o julgamento impõe às seguradoras o dever de repensar suas estruturas internas de segurança da informação. O princípio do privacy by design, expressamente previsto na LGPD, exige que a proteção de dados esteja incorporada desde a concepção de qualquer produto, contrato ou sistema. Isso inclui a implementação de tecnologias de criptografia, controle de acesso, autenticação reforçada e monitoramento contínuo de vulnerabilidades. Além disso, a decisão estimula a criação de políticas de resposta a incidentes e de comunicação transparente com os titulares, em consonância com o artigo 48 da LGPD, que trata da notificação à Autoridade Nacional de Proteção de Dados (ANPD) e aos usuários em caso de incidentes de segurança.

Para o consumidor, o entendimento do STJ representa um avanço significativo na efetividade dos direitos garantidos pela LGPD. O reconhecimento da responsabilidade objetiva e do dano moral presumido reduz os obstáculos

probatórios enfrentados por titulares de dados, que, em geral, não possuem meios técnicos para demonstrar de que forma o vazamento ocorreu. A decisão também reforça a importância da transparência e da prestação de contas, estimulando uma cultura de confiança digital e respeito à privacidade.

Do ponto de vista teórico, o acórdão contribui para a consolidação de uma nova categoria de responsabilidade civil informacional, baseada não apenas na ocorrência de um ato ilícito, mas na falha em prevenir riscos decorrentes da manipulação de dados pessoais. Essa evolução normativa e jurisprudencial evidencia o deslocamento do eixo clássico da responsabilidade civil, centrado na culpa, para uma lógica de risco e do dever de segurança, mais compatível com a realidade tecnológica atual.

Em síntese, a decisão do STJ sobre a responsabilidade da seguradora pelo vazamento de dados sensíveis reafirma a centralidade da LGPD como instrumento de tutela da privacidade e da confiança nas relações jurídicas contemporâneas. O tribunal estabelece que o dever de proteger dados não é apenas técnico, mas jurídico, ético e contratual. A mensagem é inequívoca: quem se beneficia economicamente do tratamento de dados deve também suportar os riscos inerentes a essa atividade. Logo, é um precedente de grande importância para o fortalecimento da cultura de proteção de dados no Brasil e para a consolidação da responsabilidade civil informacional como um novo paradigma de tutela da dignidade humana na era digital.

6 CONCLUSÃO

A consolidação da jurisprudência brasileira sobre violação de dados, evidencia um movimento firme no sentido de fortalecer a tutela dos direitos fundamentais diante dos novos desafios impostos pela sociedade da informação. Com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD), os tribunais passaram a incorporar de maneira mais estruturada o entendimento de que a proteção de dados pessoais não é apenas um aspecto técnico, mas um elemento essencial para a preservação da privacidade, da dignidade da pessoa humana e da autodeterminação informativa. As decisões mais recentes demonstram que as instituições, sejam

privadas ou públicas, têm o dever jurídico de adotar medidas de segurança robustas, adequadas e proporcionais para evitar acessos indevidos, vazamentos e usos irregulares das informações sob sua guarda.

A jurisprudência tem evoluído no reconhecimento de que a violação de dados representa, por si só, uma afronta aos direitos da personalidade, ampliando a compreensão de dano moral para além dos prejuízos economicamente quantificáveis. Em diversos precedentes, os tribunais brasileiros afirmam que o dano moral pode ser presumido quando ocorre o vazamento de dados sensíveis, dado que essa exposição coloca o indivíduo em situação de vulnerabilidade, com riscos concretos de fraudes, golpes, discriminações ou estigmatizações. Essa orientação reforça o caráter protetivo da LGPD e torna mais eficaz o sistema de responsabilização, uma vez que impõe aos agentes de tratamento a obrigação de comprovar que adotaram todas as medidas possíveis para evitar o incidente.

Outro ponto relevante observado na jurisprudência é a diferenciação entre falhas sistêmicas inevitáveis e condutas negligentes. Ainda que os vazamentos possam decorrer de ações criminosas de terceiros, os tribunais têm entendido que isso não afasta, por si só, o dever de segurança das instituições. Muitas decisões apontam que a ausência de protocolos atualizados de proteção, a falta de criptografia, o armazenamento inseguro e a inexistência de respostas rápidas ao incidente configura falha no dever de cuidado. Assim, mesmo que o ataque seja externo, a responsabilidade permanece quando demonstrada deficiência ou omissão na gestão da segurança da informação.

Além disso, os julgados reforçam a importância da transparência no tratamento de dados. A omissão na comunicação do incidente ao titular e à Autoridade Nacional de Proteção de Dados (ANPD) constitui violação autônoma à LGPD e tem sido reconhecida pelos tribunais como agravante no momento da fixação da indenização. Essa postura jurisprudencial demonstra que a proteção de dados deve ser encarada como processo contínuo, que exige não apenas a implementação de recursos tecnológicos, mas também o compromisso ético e jurídico de informar adequadamente os titulares de dados sempre que houver risco relevante ao seu patrimônio moral ou material.

Diante desse cenário, conclui-se que a jurisprudência brasileira tem desempenhado papel fundamental na efetivação da LGPD, fortalecendo a responsabilização dos agentes de tratamento e incentivando práticas mais rigorosas de governança, prevenção e resposta a incidentes de segurança. O conjunto de decisões analisadas demonstra uma crescente maturidade jurídica no enfrentamento das violações de dados, alinhando o ordenamento nacional às tendências internacionais de proteção da privacidade. Assim, o Poder Judiciário contribui diretamente para a construção de um ambiente digital mais seguro, transparente e comprometido com os direitos fundamentais dos cidadãos, reafirmando que a proteção de dados pessoais é um pilar indispensável para a preservação da cidadania e da dignidade humana na era digital.

REFERÊNCIAS

A INTEROPERABILIDADE de dados na saúde e os desafios da privacidade: uma análise sob a perspectiva da LGPD. A proteção de dados no mundo digital e os desafios dos dados em saúde, [S. l.], p. 3-22, 29 maio 2025. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/8733. Acesso em: 20 set. 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 2.121.904 – SP (2024/0031292-7)**. Relatora: Ministra Nancy Andrighi. Voto sobre indenização de seguradora por vazamento de dados sensíveis do segurado. Brasília, DF, 2025. Disponível em: https://www.conjur.com.br/wp-content/uploads/2025/02/voto-Nancy-STJ-indenizacao-seguradora-vazamento-dados-sensiveis-segurado.pdf. Acesso em: 12 out. 2025.

DESAFIOS da implementação da Lei Geral de Proteção de Dados em serviços de saúde que fazem uso da telemedicina: uma revisão integrativa. [S. l.], p. 1-10, 26 mar. 2025. Disponível em: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/1238. Acesso em: 20 set. 2025.

DATA PRIVACY BRASIL. **A ação civil pública do Instituto Defesa Coletiva contra a Meta**: entrevista com Lilian Salgado. 2025. Disponível em: https://www.dataprivacybr.org/a-acao-civil-publica-do-instituto-defesa-coletiva-contra-a-meta-entrevista-com-lilian-salgado/. Acesso em: 12 out. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 15 ago. 2018. Disponível

em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 out. 2025.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Código Civil. **Diário Oficial da União**, Brasília, DF, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 15 out. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. **Diário Oficial da União**, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 out. 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da autoridade e da regulamentação. 2. ed. Rio de Janeiro: Forense, 2020.

PEREIRA, Caio Mário da Silva. **Responsabilidade Civil**. 12. ed. Rio de Janeiro: Forense, 2018.

PARTE II – PROTEÇÃO DE DADOS PESSOAIS, PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

SEÇÃO 2.1 - FUNDAMENTOS E DESAFIOS ESTRUTURANTES DA LGPD

A IMPORTÂNCIA DA PROTEÇÃO DE DADOS PESSOAIS PARA O EXERCÍCIO DA CIDADANIA DIGITAL NO ESTADO DEMOCRÁTICO DE DIREITO: ANÁLISE DO CENÁRIO CONTEMPORÂNEO

Allana Almeida de Oliveira[1]

RESUMO

O presente artigo tem como objeto de análise o cenário contemporâneo brasileiro e a crescente disputa judicial entre o direito e o surgimento de novas tecnologias no espaço digital, destacando-se o embate entre a inovação tecnológica e a proteção de direitos fundamentais. Observa-se, de modo mais profundo, a relevância da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), enquanto marco regulatório que estabelece parâmetros para o tratamento de informações pessoais, e da Lei de Acesso à Informação (Lei nº 12.527/2011) na proteção de dados pessoais, as quais garante a transparência administrativa, o controle social sobre os atos do poder público e contribuem para o fortalecimento da cidadania digital no Estado Democrático de Direito. Nesse sentido, a reflexão aqui proposta busca analisar a garantia do direito fundamental estabelecido pela Constituição Federal de 1988, a cidadania, entendida não apenas como participação política formal, mas também como exercício da autonomia intelectual individual no ambiente digital, onde o uso de dados pessoais influencia diretamente a liberdade de expressão, o acesso à informação e a formação do senso crítico. A pesquisa se justifica pelas inovações tecnológicas e em como sucedem os impactos causados no sistema de justiça, resultantes do desafio de adaptar normas jurídicas tradicionais às novas formas de interação social mediadas por tecnologias digitais. Por meio de uma revisão histórica em paralelo às transformações atuais, busca-se demonstrar como a evolução normativa impacta diretamente a vida pessoal e coletiva, ressaltando que a efetividade digital depende da harmonização entre inovação, proteção de dados e preservação da dignidade humana.

Palavras-chaves: Lei geral de proteção de dados; lei de acesso à informação; proteção de dados pessoais; cidadania digital.

SUMÁRIO: 1. Introdução; 2. Contexto histórico das tecnologias; 3. Proteção de dados como direito fundamental e dificuldades enfrentadas pela violação de direitos;

[1] Graduanda em Direito do Centro Universitário de Brasília - UniCEUB. Aluna da disciplina de Direito, Tecnologia e Inovação. Email: allana.oliveira1@icloud.com

4. Perspectivas e Caminhos para o Fortalecimento da Cidadania Digital; 5. Caso concreto exemplificativo 6. Considerações finais; 7. Referências bibliográficas.

1 INTRODUÇÃO

Ao longo dos séculos, os avanços tecnológicos transformaram profundamente as formas de interação social, econômica e política, instaurando um contexto em que essas "novidades" constroem-se a cada dia como um meio essencial para o funcionamento da sociedade como um todo. Dessa forma, a proteção de dados deixa de ser apenas uma questão de privacidade e passa a assumir papel essencial na manutenção harmoniosa da sociedade e também na consolidação da cidadania digital, entre outros direitos fundamentais que foram diretamente impactados pelo cenário virtual.

A cidadania digital é pautada na ideia de que os indivíduos podem exercer plenamente seus direitos e deveres no âmbito digital. No Brasil, dois momentos foram primordiais para efetivar a proteção de dados pessoais e informações, a promulgação da Lei Geral de Proteção de Dados Pessoais (Lei nº **13.709/2018**) e a Lei de Acesso à Informação (Lei n° **12.527/2011**). Além disso, a propagação de informações em massa trouxe à tona uma preocupação nova, a divulgação de notícias "fakes", as quais impactam diretamente no cenário político brasileiro.

A incidência recorrente de notícias de cunho modificado, impacta na percepção dos indivíduos acerca do estado democrático brasileiro e também influencia diretamente no exercício da cidadania digital. Ainda, aqueles que não possuem conhecimento acerca dos próprios direitos e deveres como cidadão, da importância de buscar fontes seguras para se informar, acabam tendo o senso crítico individual prejudicado.

2 CONTEXTO HISTÓRICO DAS TECNOLOGIAS

O renomado geógrafo brasileiro, Milton Santos, apresenta em sua obra uma nova visão sobre a globalização. Ele explicita que não é um processo homogêneo, mas sim multifacetado, com ênfase em uma dimensão socioeconômica central, onde

as disparidades entre países e dentro deles se acentuam e também como um fenômeno que reconfigura as identidades culturais e territoriais.

Ademais, versou sobre como a globalização se manifesta como uma perversidade, em que com a intensificação do fluxo de informações, capitais, bens e serviços, o mercado decorrente desse cenário propicia uma dificuldade em construir laços de solidariedade coletiva. Entretanto, apesar de apresentar tal fenômeno desta forma, vislumbra também uma oportunidade, uma globalização mais humana e participativa, visando reduzir as desigualdades dela decorrentes.

A partir das inovações tecnológicas surgidas a partir do fenômeno da globalização e outros marcos, como a Terceira Revolução Industrial, o cenário da sociedade moderna tem passado por inúmeros desafios e transformações desde então, entre elas o desenvolvimento da Inteligência Artificial como ferramentas cotidianas. Entretanto, é preciso que haja uma análise detalhada em relação a forma com que essas ferramentas são utilizadas e também na coletânea de dados. Nos anos 1990, a popularização da internet deu início à sociedade da informação, marcada pela crescente digitalização de dados. Por conseguinte, o conceito de cidadania digital emergiu.

Nos anos 2000, as redes sociais ganharam espaço, assim como os smartphones e serviços em nuvem, e novamente, o compartilhamento de dados pessoais se intensificou. Surgem as plataformas digitais (como Google, Facebook, Amazon), cuja lógica de funcionamento se baseia na coleta massiva de dados dos usuários para fins de personalização de conteúdo, direcionamento de publicidade e, muitas vezes, manipulação comportamental.

A coleta de dados refere-se ao processo de reunir informações sobre um tópico específico através de fontes. Ela é responsável por uma etapa importante da análise de dados que serve para embasar decisões estratégicas de uma organização. Dessa forma, uma empresa consegue identificar tendências no mercado, compreender melhor acerca de padrões de consumo e de comportamento da sociedade, formas para manter-se competitivo no mercado, entre outras informações. Portanto, é válido ressaltar que a coleta de dados é crucial para a eficiência empresarial como um todo.

Segundo dados apresentados pela Associação de Defesa de Dados Pessoais e do Consumidor (ADDP), o número de crimes digitais cresceu 45% em relação ao ano de 2024, somando cerca de 5 milhões de fraudes. A crescente dos números tem sido objeto de preocupação da proteção de dados e motivo por uma busca assertiva em relação à garantia de direitos.

Diante disso, a Lei Geral de Proteção de Dados, promulgada em 2018 e vigorando desde 2020, estabeleceu novas exigências e responsabilidades para as empresas que lidam com dados pessoais no Brasil. Entretanto, diversos empreendimentos ainda encontram desafios na adequação completa aos requisitos presentes na LGPD, principalmente em relação a adaptação de sistemas e processos para lidar de forma segura com os dados coletados. A LGPD é uma forma de compromisso com a segurança tanto da empresa quanto dos clientes, especialmente em setores que lidam com volumes significativos de informações sensíveis.

3 PROTEÇÃO DE DADOS COMO DIREITO FUNDAMENTAL E DIFICULDADES ENFRENTADAS PELA VIOLAÇÃO DE DIREITOS

Assim como diversos ordenamentos jurídicos, a proteção de dados passou a ser reconhecida como um direito fundamental autônomo - aquele que possui existência própria, não sendo uma mera extensão de outro direito fundamental e portanto estrutura normativa independente, ainda que possa dialogar com outros direitos, como por exemplo a vinculação com os preceitos da dignidade humana, à privacidade e também à liberdade de expressão - a partir da Emenda Constitucional nº 115/2022, que instituiu na Constituição Federal: a proteção de dados pessoais entre os direitos e garantias fundamentais e também a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Em citações doutrinárias de grande relevância no tópico em questão, a doutrinadora Laura Schertel Mendes aborda o caráter estruturante do direito à proteção de dados alegando que esse direito fundamental representa também um verdadeiro poder de controle sobre as informações pessoais, necessário para garantir a liberdade e a igualdade em ambientes digitais. Em paralelo a essa afirmação, o

renomado filósofo alemão Immanuel Kant, em sua obra "O que é o esclarecimento?" expõe a importância e necessidade de cada indivíduo sair do que é denominado como menoridade, que seria a incapacidade de fazer uso de seu entendimento sem a direção de outro e adentrar o período da maioridade, através da busca por conhecimento próprio e formação de senso crítico individual.

A ideia apresentada por Kant está intimamente ligada ao ideal de autonomia, tanto intelectual quanto moral. Ainda, explicita que um indivíduo só se torna verdadeiramente livre a partir do momento em que é capaz de pensar por si mesmo e agir conforme sua própria convicção e sua razão, não apenas seguindo ideias ou opiniões externas. Portanto, é possível associar diretamente com a obtenção de dados no cenário digital.

No mundo digital contemporâneo, os indivíduos estão sujeitos e expostos à manipulação de dados, algoritmos implícitos e vigilância invisível, muitas vezes sendo induzidos a uma opinião pré estabelecida pelas empresas para direcionar de forma intencional porém inapropriada, o indivíduo. Nesse sentido, ao longo da utilização desses dados, as plataformas digitais, empresas e até mesmo os governos podem fazer com que o cidadão perca o controle sobre sua identidade, opiniões e decisões, que de acordo com os preceitos do pensamento kantiano, representa uma nova forma de "menoridade" moderna - uma submissão à lógica tecnológica que o impede de agir livremente.

Diante das situações abordadas acerca da capacidade de manipulação dos dados de forma inapropriada por diversos agentes, outros pontos de suma relevância no tocante às problemáticas enfrentadas atualmente, é possível citar os casos de vazamento massivos de dados, como o ocorrido em 2021 que expôs mais de 220 milhões de brasileiros, a imposição de contratos de adesão com termos abusivos e que violam a transparência no uso de dados, além de abordar tais contratos com termos extremamente completos e de difícil compreensão rápida por parte dos usuários, a dificuldade estrutural da ANPD para fiscalizar e aplicar sanções de forma efetiva e também o desconhecimento generalizado pela população sobre os próprios direitos.

Nesse sentido, a proteção de dados é considerada a peça-chave do constitucionalismo digital por estar relacionado diretamente com o exercício de outros direitos fundamentais e o próprio Estado Democrático de Direito em contextos atuais de hiperconectividade, conforme ressalta o fundador do Data Privacy Brasil, Bruno Bioni. Assim, além das barreiras técnicas enfrentadas pelas empresas em realizar a adaptação de políticas internas e externas para proteção dos usuários, há também questões políticas e estruturais que acabam por fragilizar a democracia e os direitos coletivos. É necessário que haja ações estatais, da sociedade civil e do setor privado, conjuntamente, para garantir a efetividade a esse direito, com foco primordial na transparência e responsabilização.

A cidadania digital é condição essencial para que o cidadão participe ativamente e livremente do debate público e também da vida política sem que haja receio da vigilância excessiva, censura ou manipulação algorítmica. A proteção de dados garante que os pilares da democracia perpetuem, com base na liberdade, na igualdade e autonomia individual.

4 PERSPECTIVAS E CAMINHOS PARA O FORTALECIMENTO DA CIDADANIA DIGITAL

O exercício da cidadania, a partir da evolução dos meios de comunicação, se estende hoje em dia ao ambiente virtual, não se limitando apenas à dimensão jurídica. O virtual se consolida como um dos principais recursos de manifestação da vontade do povo, de expressão, de consumo de informações e diversas outras interações proporcionadas. Deste modo, é imprescindível repensar os instrumentos jurídicos e institucionais que garantam que a tecnologia esteja em função da liberdade e igualdade, e não da manipulação e controle social.

Como medida promissora para o exercício da cidadania digital e medida de fortalecimento, a consolidação da cultura de proteção de dados como princípio ético e social é de suma pertinência. Todavia, para alcançar esse marco, depende da ampla conscientização social sobre os riscos, os direitos dos cidadãos e as responsabilidades inerentes ao uso de dados, bem como os benefícios de sair do que é chamado de “esclarecimento’’ por Immanuel Kant. Além do mais, programas

educacionais e linguagem facilitada são medidas simplistas porém essenciais para que o cidadão compreenda o impacto na vida própria e as consequências negativas da exploração indevida de seus dados.

Outro aspecto importante é o fortalecimento institucional da Autoridade Nacional de Proteção dos Dados (ANPD), órgão responsável por fiscalizar e desempenhar papel fundamental da regulação e cumprimento da LGPD por parte das empresas. É necessário que o Estado garanta a independência administrativa e técnica, além de fornecer os recursos adequados para que a mesma consiga realizar seu objetivo com êxito, seja financeiramente ou tecnicamente.

Em relação ao âmbito político, área que experimenta grande controle de dados sensíveis, como campanhas eleitorais e serviços públicos digitais, o uso indevido de dados para manipulação do comportamento dos usuários e direcionamento de desinformação representa uma ameaça direta à cidadania e à soberania popular. Como forma de lidar com esses episódios, as políticas de governança de dados devem ser aprimoradas, garantindo que os algoritmos responsáveis pela manipulação de dados pessoais seja dotado de imparcialidade, para que não cause prejuízos à opinião individual e dificulte o acesso às informações verídicas.

Além disso, o fortalecimento da cidadania digital transcende domínios, entre elas, a redução das desigualdades de acesso às tecnologias da informação. Como mencionado anteriormente, o direito à proteção de dados pessoais é um direito fundamental autônomo que interage, ainda, com outros direitos, como por exemplo o direito à inclusão digital, que é uma extensão do direito à cidadania, pois sem acesso à internet e aos meios digitais, uma parcela significativa da população permanece excluída dos debates públicos, tendo em vista que se tornou um meio primordial para expressar opiniões. Nesse sentido, a universalização do acesso à internet constitui condição essencial para o exercício pleno da cidadania digital.

Por fim, nota-se a necessidade de fomentar uma espécie de ética pública digital, pautada na responsabilidade coletiva sobre o uso das tecnologias. Ainda, a criação de políticas que busquem conscientizar os cidadãos sobre sites que estão em consonância com a LGPD e a LAI, respeitando os direitos dos indivíduos e

garantindo a participação ativa, crítica e consciente na esfera pública digital, indo de encontro a práticas antidemocráticas e que possam propiciar desinformação em massa.

5 CASO CONCRETO EXEMPLIFICATIVO

No ano eleitoral de 2022, o Brasil vivenciava um período intenso de polarização política, nunca visto anteriormente na história do país na dimensão em que ocorreu. Apesar de ter sido a primeira eleição com a LGPD, em vigor desde 2020, e com regras estabelecidas para aplicativos, a preocupação com a temática ocorria desde 2018, quando ocorreu contestações ao Whatsapp devido a denúncias baseadas no envio em massa de mensagens, por exemplo. Ainda, foi noticiado posteriormente que empresas contratadas por empresários ligados à campanha do antigo presidente Jair Bolsonaro (PL) foram usadas com o objetivo de atacar opositores e divulgar informações falsas.

Diante desse contexto, nota-se a utilização de tratamento de dados com finalidade diversa da originária. Tendo em vista o potencial de influência e a escalabilidade de lucros não somente dentro de uma empresa mas também em diversas áreas capazes de alterar fluxos democráticos, a partir da utilização dos dados e podendo se tornar insidioso, amplificou a necessidade de parâmetros que pudessem adequar as bases gerais da LGPD para o contexto eleitoral da época.

Portanto, em novembro de 2021 a Agência Nacional de Proteção de Dados (ANPD) e o Tribunal Superior Eleitoral (TSE) firmaram acordo de cooperação técnica com o intuito de criar uma estrutura jurídica para aplicação nas eleições do ano seguinte. Como resultado, foi apresentado um Guia Orientativo baseado nas principais bases legais para coleta e utilização desses dados, sendo: consentimento, legítimo interesse e cumprimento da obrigação legal.

A utilização desses preceitos estabelece ferramentas que auxiliam a formação de pensamento próprio, alcançando o esclarecimento, conforme a ideia kantiana, preza pelas bases democráticas do país, buscando a propagação de informações

verídicas e sem o intuito de influenciar as preferências e ideologia política dos usuários, entre outros benefícios, resguardando as propensões de cada indivíduo.

6 CONSIDERAÇÕES FINAIS

O estudo realizado permitiu compreender as dimensões envolvidas na cidadania digital no Brasil e a dependência direta da efetivação da proteção de dados pessoais como direito fundamental e como instrumento inerente à dignidade humana e à privacidade. Tendo em vista o Estado Democrático de Direito, o uso responsável acerca das informações coletadas e o uso dos dados pessoais, são essenciais para garantir a liberdade individual, a capacidade de autonomia informacional e a participação dos cidadãos em debates públicos.

A análise demonstrou que a Lei Geral de Proteção de Dados Pessoais e a Lei de Acesso à Informação representam um marco regulatório primordial para a estruturação de uma cultura de proteção e segurança no tratamento de dados. Ambas proporcionam um cenário de confiança entre o cidadão e os agentes responsáveis pela proteção e manipulação adequada dos dados, entretanto, devem ser fortalecidas e munidas dos recursos necessários e disponíveis para que a instituição da ANPD efetive com excelência o serviço a ela atribuído.

Observou-se, ainda, que os avanços tecnológicos trouxeram desafios inéditos ao cenário contemporâneo, exigindo uma flexibilidade das normas jurídicas. A manipulação de dados tem sido alvo frequente de debates políticos a fim de resguardar a capacidade de desenvolvimento intelectual próprio, buscando não ser munido de influência externas e outras manipulações.

Assim, conclui-se que a efetiva proteção de dados está intrinsecamente ligada à efetividade do Estado Democrático de Direito no século XXI. Através de uma construção sólida de proteção informacional, visando valorizar a dignidade da pessoa humana, a liberdade e a igualdade, será possível assegurar aos cidadãos que o processo tecnológico seja um ambiente seguro para manifestação de opiniões e liberdade de expressão, servindo como um instrumento de emancipação humana, conforme a ideia apresentada por Kant, e não como um meio de dominação, além de

compreender-se que a proteção de dados pessoais é uma exigência ética ligada à autonomia do sujeito.

Em síntese, as perspectivas em relação à importância da proteção de dados pessoais para o exercício da cidadania no Estado Democrático de Direito a partir de uma análise do cenário contemporâneo necessitam da integração entre a área da educação, regulação e inclusão. A proteção de dados pessoais, enquanto direito fundamental, constitui eixo estruturante dessa transformação pois assegura ao cidadão o controle sobre sua autonomia informacional e a liberdade de agir no âmbito virtual sem coerções. O desafio principal está em garantir que o avanço tecnológico esteja em consonância com a norma da LGPD a fim de garantir um ambiente seguro para os cidadãos efetivarem a sua cidadania digital.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 03 out. 2025.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto na Constituição Federal. Brasília, DF: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 04 out. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014 (Marco Civil da Internet).** Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 05 out. 2025.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Inclui a proteção de dados pessoais entre os direitos e garantias fundamentais. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 06 out. 2025.

PUCRS Online. *Milton Santos e a outra globalização: sua perspectiva*. Brasília, DF: PUCRS Online, s.d. Disponível em: https://online.pucrs.br/blog/milton-santos-globalizacao. Acesso em: 02 out. 2025.

PUCRS Online. *Globalização, competitividade e mercado global*. Brasília, DF: PUCRS Online, s.d. Disponível em: https://online.pucrs.br/blog/globalizacao-competitividade-mercado-global. Acesso em: 03 out. 2025.

IMPRESSÕES DE MARIA. *Por uma outra globalização: Milton Santos contra a perversidade do capitalismo*. Brasília, DF: Impressões de Maria, s.d. Disponível em: https://impressoesdemaria.com.br/por-uma-outra-globalizacao-milton-santos-contra-a-perversidade-do-capitalismo/. Acesso em: 04 out. 2025.

FERNANDES, Paulo Irineu B. *Milton Santos e as três faces da globalização*. Brasília, DF: Dal Mediterraneo Aglio Ceani, 24 set. 2020. Disponível em: https://dalmediterraneoaglioceani.wordpress.com/2020/09/24/paulo-irineu-b-fernandes-milton-santos-e-as-tres-faces-da-globalizacao/. Acesso em: 05 out. 2025.

JUSBRASIL. *O impacto das novas tecnologias no ordenamento jurídico*. Brasília, DF: JusBrasil, 7 nov. 2023. Disponível em: https://www.jusbrasil.com.br/artigos/o-impacto-das-novas-tecnologias-no-ordenamento-juridico/2036414339. Acesso em: 06 out. 2025.

PM3. *Coleta de dados*. Brasília, DF: PM3, s.d. Disponível em: https://pm3.com.br/blog/coleta-de-dados/. Acesso em: 07 out. 2025.

ASSOCIAÇÃO DE DEFESA DE DADOS PESSOAIS E DO CONSUMIDOR (ADDP). Relatório anual sobre crimes digitais no Brasil. São Paulo, 2024. Disponível em: https://www.addp.org.br/relatorios/2024. Acesso em: 07 out. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Relatório de atividades de 2023. Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/relatorios. Acesso em: 08 out. 2025.

PLEXI. *Coleta de dados e LGPD: como utilizar dados em acordo com a legislação*. Brasília, DF: Plexi, s.d. Disponível em: https://plexi.com.br/blog/coleta-de-dados-e-lgpd-como-utilizar-dados-em-acordo-com-a-legislacao/. Acesso em: 08 out. 2025.

MIGALHAS. *Proteção de dados pessoais como direito fundamental autônomo e competência legiferante privativa da União*. Brasília, DF: Migalhas, s.d. Disponível em: https://www.migalhas.com.br/depeso/314538/protecao-de-dados-pessoais-como-direito-fundamental-autonomo-e-competencia-legiferante-privativa-da-uniao. Acesso em: 09 out. 2025.

CERQUEIRA, Carolina. Eleição de 2022 é a 1ª com a Lei de Proteção de Dados e novas regras para aplicativos. CNN Brasil, São Paulo, 14 set. 2022. Disponível em: https://www.cnnbrasil.com.br/politica/eleicao-de-2022-e-a-1a-com-a-lei-de-protecao-de-dados-e-novas-regras-para-aplicativos/. Acesso em: 20 nov. 2025.

DE ALMEIDA, Renato Ribeiro). Direito eleitoral, LGPD e eleições gerais 2022. ConJur, 23 mai. 2022. Disponível em: https://www.conjur.com.br/2022-mai-23/direito-eleitoral-lgpd-eleicoes-gerais-2022/. Acesso em: 20 nov. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD); Tribunal Superior Eleitoral (TSE). *Guia orientativo: aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral* [recurso eletrônico]. Brasília: TSE, 2021. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_lgpd_final.pdf. Acesso em: 20 nov. 2025.

A COLETA DE DADOS PESSOAIS E OS DESAFIOS ENVOLVENDO PRIVACIDADE E SEGURANÇA

Lucas Krisney Lima de Oliveira[1]

RESUMO

O presente material analisa a coleta e o tratamento de dados pessoais no contexto da economia digital, evidenciando os riscos à privacidade, segurança da informação e à liberdade individual decorrentes da atuação das plataformas digitais. A pesquisa destaca a Lei Geral de Proteção de Dados (LGPD) como marco regulatório essencial na consolidação de direitos e deveres relacionados à proteção de dados no Brasil, estabelecendo princípios, mecanismos de fiscalização e regime sancionatório. A partir da análise de casos concretos, como os vazamentos envolvendo a Meta Platforms, a Cambridge Analytica e a Serasa Experian, o material evidencia as fragilidades estruturais do sistema de governança informacional e a necessidade de fortalecimento institucional da Autoridade Nacional de Proteção de Dados (ANPD). Observa-se que a aplicação prática das sanções pela ANPD, Procons e Ministério Público reflete avanços relevantes, embora ainda limitados por desafios técnicos, transnacionais e de conformidade empresarial. O que resta demonstrado é que a efetividade da LGPD depende da conjugação entre regulação robusta, fiscalização eficiente e conscientização social, exigindo a adoção de práticas empresariais transparentes e o aprimoramento contínuo das políticas públicas voltadas à proteção de dados pessoais no Brasil.

Palavras-chave: Proteção de dados; Privacidade; LGPD; ANPD; Responsabilização.

1 INTRODUÇÃO

O cenário contemporâneo é marcado pela centralidade dos dados pessoais como insumo essencial na economia digital e interações sociais. Verifica-se que em plataformas digitais, redes sociais e serviços online passaram a estruturar seus modelos de negócio baseado na coleta e análise massiva de informações de seus usuários, prática que, embora possibilite a personalização de serviços e o

[1] Bacharelando em Direito no Centro Universitário de Brasília (UniCEUB). Estagiário no Conselho Federal da OAB (CFOAB).

desenvolvimento de novos produtos, expõe os indivíduos a riscos significativos, como violações de privacidade, manipulação comportamental e discriminação.

A proteção de dados pessoais, diante desse contexto, consolidou-se como um dos principais desafios da atualidade, sendo reconhecida como direito fundamental tanto em instrumentos normativos internacionais, como a Declaração Universal dos Direitos Humanos de 1948 e a Convenção Europeia de Direitos Humanos de 1950, quanto na própria Constituição da República Federativa do Brasil de 1988. O avanço das tecnologias de informação e comunicação, aliado à crescente vulnerabilidade decorrente de vazamentos em larga escala, reforçou a necessidade de criação de um marco regulatório específico para disciplinar o tratamento de dados no Brasil.

A promulgação da Lei nº 13.709/2018, a chamada Lei Geral de Proteção de Dados Pessoais (LGPD), representou um marco nesse processo, estabelecendo princípios, direitos e deveres aplicáveis ao tratamento de dados pessoais, bem como instituindo mecanismos de responsabilização e sanção para hipóteses de descumprimento. A criação da Autoridade Nacional de Proteção de Dados (ANPD) consolidou a estrutura fiscalizatória da legislação, atribuindo-lhe competência para instaurar procedimentos administrativos, aplicar medidas cautelares e impor sanções proporcionais e fundamentadas.

A relevância do tema é evidenciada pela ocorrência de incidentes emblemáticos, como os vazamentos de dados envolvendo a Meta Platforms, o escândalo da Cambridge Analytica e episódios registrados em território nacional, a exemplo da divulgação de milhões de CPFs e falhas de segurança. Esses casos demonstram a amplitude dos riscos associados ao tratamento de dados e a necessidade de aperfeiçoamento constante das práticas regulatórias e empresariais.

Portanto, diante de todo esse cenário, o presente material tem como objetivo examinar os mecanismos de responsabilização previstos na LGPD, destacando o papel da ANPD e de outros órgãos de defesa do consumidor e do Ministério Público, além de analisar casos concretos de aplicação de sanções no Brasil e, consequentemente, avaliar a efetividade do regime sancionatório da legislação e identificar seus limites práticos, especialmente em face da complexidade dos fluxos informacionais transnacionais e da assimetria entre usuários e plataformas digitais.

2 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE:

O avanço tecnológico e a consolidação da sociedade dentro da internet transformaram profundamente a dinâmica das relações sociais e econômicas. A informação passou a ser um ativo estratégico, capaz de induzir decisões políticas, mercadológicas e até pessoais. O tratamento de dados pessoais tornou-se elemento central da economia contemporânea.

A proteção da privacidade, entendida como um dos direitos fundamentais, tem sido objeto de reflexão desde o século XIX, sendo consagrada em diversos instrumentos normativos internacionais, como a Declaração Universal dos Direitos Humanos de 1948 e a Convenção Europeia de Direitos Humanos de 1950. O tema encontrou respaldo na Constituição da República Federativa do Brasil de 1988, que assegura a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas.

O avanço e acesso de tecnologias e privacidade, no entanto, ganhou novas dimensões. A noção de autodeterminação informativa, formulada inicialmente pela jurisprudência alemã na década de 1980, passou a constituir referência teórica para o debate contemporâneo. Esse conceito traduz a ideia de que o indivíduo deve deter controle sobre os seus próprios dados, decidindo de maneira livre e informada acerca de sua coleta, utilização e compartilhamento.

2.1 A coleta de dados pessoais pelas plataformas digitais:

As plataformas digitais, como redes sociais, serviços de *streaming*[2], aplicativos de mobilidade e *marketplaces*[3], possuem em seus modelos de negócio a extração massiva de dados de seus usuários, através de mecanismos como *cookies*[4], rastreadores, geolocalização, dados de navegação e análise preditiva de comportamento. O que se percebe é que conseguem formar perfis detalhados,

[2] *Streaming* é a transmissão de conteúdo multimídia pela internet em tempo real, permitindo assistir a vídeos, ouvir músicas ou ver eventos ao vivo sem a necessidade de baixar os arquivos completos para o dispositivo.

[3] *Marketplace* é uma plataforma online que reúne vendedores de diversos segmentos para oferecer seus produtos e serviços em um único lugar, funcionando como um "shopping virtual".

[4] *Cookies* funcionam como uma memória, permitindo que o *site* se lembre das suas preferências, detalhes de login e atividades de navegação para melhorar sua experiência *online*.

capazes de revelar preferências, hábitos, posicionamentos políticos e até aspectos sensíveis da vida privada.

A coleta, embora muitas vezes apresentada com uma roupagem da "personalização da experiência do usuário", muitas vezes converte-se em coleta abusiva, sobretudo quando realizada sem consentimento válido ou de maneira desproporcional à finalidade declarada. A assimetria informacional existente entre usuários e plataformas digitais acentua essa problemática, considerando que os termos de uso e políticas de privacidade são, em regra, extensos, técnicos e de difícil compreensão, dificultando o exercício efetivo da autonomia informativa.

Portanto, a exploração econômica dos dados, por meio da publicidade direcionada e venda de informações para interessados, potencializa riscos à privacidade e segurança, especialmente quando aliada à ausência de transparência no tratamento desses dados. O resultado é a crescente exposição dos indivíduos a práticas de manipulação comportamental, fraudes e discriminações algorítmicas.

3 CASOS DE VAZAMENTOS DE DADOS PESSOAIS:

3.1 Facebook, Instagram e Whatsapp

Entre os episódios mais significativos acerca da proteção de dados pessoais, cabe pontuar a empresa Meta Platforms, controladora do Facebook, Instagram e do aplicativo de mensagens WhatsApp. Em 2021, foi revelado o vazamento de informações de aproximadamente 533 milhões de usuários em mais de 100 países, incluindo cerca de 8 milhões de brasileiros. Dentre as informações expostas, haviam nomes completos**,** números de telefone, endereços de e-mail**,** dados de localização**,** informações de relacionamento e, em alguns casos, imagens de perfil dos usuários.

Esse incidente evidenciou falhas dentro de mecanismos de segurança da própria empresa, bem como a ausência de medidas preventivas adequadas no tratamento de dados pessoais, em desacordo com princípios basilares previstos tanto no Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia quanto na Lei Geral de Proteção de Dados Pessoais no Brasil. A falha decorreu de uma vulnerabilidade no recurso de sincronização de contatos, que permitia a

extração massiva de informações públicas por meio de técnicas automatizadas de raspagem, conhecida como *scraping*[5].

A amplitude do vazamento gerou impactos significativos à privacidade e segurança dos usuários, ocasionando aumento expressivo nas tentativas de fraudes, golpes de engenharia social, extorsões e perseguições virtuais, reacendendo o debate acerca da responsabilidade civil e administrativa das plataformas digitais, considerando que a Meta Platforms foi questionada quanto à sua transparência na comunicação do incidente e à adoção de medidas corretivas eficazes.

O caso ganhou ainda mais relevância ao demonstrar a necessidade de atuação mais efetiva da Autoridade Nacional de Proteção de Dados (ANPD), especialmente no que tange à fiscalização de grandes empresas transnacionais que tratam dados de cidadãos brasileiros. O episódio consolidou-se como marco de alerta sobre os riscos associados à concentração de informações pessoais em ecossistemas digitais e à importância da governança de dados pessoais como instrumento de tutela da privacidade.

3.2 Cambridge Analytica

O escândalo envolvendo a empresa Cambridge Analytica é outro marco emblemático, pois demonstrou a utilização de dados pessoais para fins de manipulação política, revelando, ainda, fragilidades estruturais no ecossistema digital e impulsionando a criação de marcos regulatórios internacionais, como o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil.

O ponto fulcral deste escândalo consistiu na obtenção indevida de dados pessoais de aproximadamente 80 milhões de usuários do Facebook pela empresa Cambridge Analytica. A prática teve origem em um método aparentemente inofensivo, baseado na aplicação de um quiz de personalidade na plataforma, similar a testes populares como “Qual princesa da Disney você seria?” ou “A qual casa de Hogwarts você pertence?”, desenvolvido por um pesquisador vinculado à empresa.

[5] *Scraping* é usar programas automatizados, como *bots*, para extrair dados e conteúdo de *sites* na internet.

A gravidade do caso, contudo, decorreu de uma falha de autorização no sistema do Facebook, que permitiu a coleta não apenas dos dados dos usuários que participaram do quiz, mas também das informações de toda a sua rede de contatos. Esse procedimento configurou uma violação direta ao princípio do consentimento informado, uma vez que a maior parte dos titulares de dados não tinha ciência ou não havia autorizado o compartilhamento de suas informações com terceiros, tampouco sua utilização para fins de perfilização comportamental e direcionamento de propaganda eleitoral.

Essa conduta trouxe à tona a problemática envolvendo a utilização secundária de dados pessoais, ou seja, o aproveitamento para finalidades distintas daquelas inicialmente informadas ao usuário. Dentre os principais aspectos observados, destacam-se:

a. Manipulação política e disseminação de desinformação.

A Cambridge Analytica utilizou técnicas de análise massiva de dados e modelagem psicométrica para identificar eleitores indecisos e, posteriormente, direcionar a eles campanhas personalizadas e conteúdos falsos. Essa estratégia, amplamente empregada nas eleições presidenciais dos Estados Unidos em 2016, demonstrou a capacidade de influenciar decisões políticas por meio da exploração de perfis psicológicos e comportamentais.

b. Responsabilidade corporativa e segurança da Informação.

O modelo de negócios do Facebook permitia, antes do escândalo, a concessão de acesso a dados pessoais de usuários sem transparência adequada ou mecanismos de auditoria eficazes. O caso evidenciou a necessidade de corporações adotarem práticas éticas e mecanismos de governança de dados, assegurando medidas robustas de segurança e políticas claras de tratamento.

c. Transparência e controle pelo titular.

O escândalo revelou que o controle sobre as informações pessoais estava inteiramente nas mãos das plataformas digitais, não dos usuários. A partir desse caso, consolidou-se a exigência de fortalecer o poder decisório do titular dos dados,

mediante consentimento explícito, direito de acesso, retificação, portabilidade e eliminação de informações pessoais.

Diante de todo o exposto, cabe esclarecer que a repercussão culminou na convocação do presidente do Facebook, Mark Zuckerberg, para prestar depoimento perante o Congresso dos Estados Unidos, após delações que expuseram a extensão do esquema e sua influência sobre processos eleitorais, resultando em diversas medidas judiciais, aplicação de multas milionárias e audiências parlamentares que colocaram em xeque a transparência e ética das plataformas digitais.

3.3 Vazamentos no Brasil

O Brasil também é marcado por episódios de grande magnitude e relevância relacionados à violação de dados pessoais. Em 2021, surgiram denúncias de usuários da Serasa Experian, empresa de análise de crédito, voltadas ao vazamento de informações de mais de 200 milhões de pessoas, número próximo à quantidade da população nacional, indicando possível duplicidade e exposição de dados de pessoas falecidas. O conjunto de informações vazadas incluía números de CPF, nomes completos, endereços, telefones, faixas salariais e pontuações de crédito, supostamente obtidos a partir de bases de dados de órgãos públicos e instituições privadas.

O incidente colocou em risco não apenas a privacidade dos cidadãos, mas também a segurança nacional, considerando que possibilitou a comercialização dessas informações em fóruns na deep *web*[6], visando crimes como estelionato, abertura indevida de contas bancárias e obtenção de benefícios sociais de forma fraudulenta.

A propósito, tal incidente evidencia que a fragilidade na governança de dados pessoais não se restringe a empresas estrangeiras, alcançando também instituições sediadas no território nacional, reforçando a importância da LGPD e do papel da Autoridade Nacional de Proteção de Dados (ANPD), cuja atuação deve concentrar-

[6] *Deep web* é a parte da internet que não é indexada pelos mecanismos de busca comuns, como Google ou Bing, e inclui conteúdos acessíveis apenas com login, senhas ou links diretos, por exemplo, bancos de dados acadêmicos, sistemas internos, e-mails, ou sites restritos.

se na prevenção de incidentes, fiscalização de agentes de tratamento e aplicação de sanções administrativas adequadas.

Portanto, resta demonstrado que o ocorrido serve como marco de alerta para a sociedade brasileira, revelando que a efetividade da tutela da privacidade depende não apenas da existência de normas protetivas, mas também da maturidade institucional e da adoção de uma cultura de segurança da informação em todos os níveis, sendo público e privado.

4 A LEI Nº 13.709/2018 E OS MECANISMOS DE RESPONSABILIZAÇÃO:

4.1 Estrutura normativa e objetivos da Lei Nº 13.709/2018

A LGPD disciplina sobre o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade, estabelecendo um conjunto diversificado de medidas que podem ser aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD) em razão de infrações aos seus preceitos, incluindo sanções administrativas, pecuniárias e restritivas de atividades.

4.2 O papel da autoridade nacional de proteção de dados e instrumentos de fiscalização

A Autoridade Nacional de Proteção de Dados (ANPD) foi instituída como o órgão administrativo responsável pela fiscalização e pela aplicação da LGPD. Dentre suas atribuições, destacam-se a instauração de procedimentos de investigação, a adoção de medidas cautelares e a imposição de sanções administrativas, sempre observados os princípios do devido processo legal. A ANPD, com o intuito de conferir maior previsibilidade e proporcionalidade ao regime sancionatório, editou o Regulamento de Dosimetria e Aplicação de Sanções Administrativas (Resolução CD/ANPD nº 4/2023), que estabelece critérios e parâmetros objetivos para o cálculo e a gradação das penalidades.

4.3 Sanções previstas e critérios de dosimetria

A LGPD, conforme o art. 52, estabelece, de maneira expressa, as sanções administrativas passíveis de aplicação pela ANPD, conforme exposto a seguir:

1. Advertência, com prazo para adoção de medidas corretivas;

2. Multa simples, limitada a 2% do faturamento bruto da empresa no Brasil, limitada a R$ 50.000.000,00 por infração;

3. Multa diária;

4. Publicização da infração;

5. Bloqueio;

6. Eliminação dos dados pessoais envolvidos.

7.Suspensão parcial do funcionamento do banco de dados por até 6 meses, prorrogável.

8.Suspensão do exercício da atividade de tratamento de dados por até 6 meses, prorrogável.

9.Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

O Regulamento de Dosimetria da ANPD, por sua vez, disciplina a metodologia de cálculo das multas, prevendo taxa básica, valor-base e a aplicação de fatores atenuantes ou agravantes, determinando que a aplicação das sanções seja devidamente fundamentada e graduada, assegurando ao infrator o pleno exercício do contraditório e da ampla defesa.

A propósito, cabe salientar que os valores arrecadados a título de multa são destinados ao Fundo de Defesa dos Direitos Difusos (FDD), conferindo caráter coletivo à finalidade da sanção.

Portanto, o sistema sancionatório da Lei nº 13.709/2018, regulamentado pela ANPD, busca equilibrar a efetividade da proteção de dados pessoais com a garantia

de segurança, proporcionalidade e respeito às garantias fundamentais dos administrados.

4.4 Exemplos práticos de aplicação de sanções no Brasil

A jurisprudência, somada com a atuação conjunta de órgãos voltados à defesa do consumidor e do Ministério Público, evidencia que a responsabilização por incidentes de segurança e vazamentos de dados pessoais se desenvolve de diversas formas, abrangendo a esfera administrativa, civil e, em certos casos, penal. Esse cenário reforça a complexidade do sistema de responsabilização e o caráter multifacetado da tutela da proteção de dados no Brasil, que combina mecanismos sancionatórios, reparatórios e pedagógicos, com o objetivo de fomentar a cultura de proteção de dados pessoais e a responsabilização efetiva.

No âmbito da ANPD, destaca-se a decisão proferida em 2023 na ação administrativa instaurada contra a empresa Telekall Infoservice. A Coordenação-Geral de Fiscalização (CGF) concluiu que a empresa realizou tratamento de dados pessoais sem respaldo legal e deixou de indicar o encarregado pelo tratamento desses dados, em evidente afronta no rol de dispositivos legais da LGPD.

A ANPD aplicou, como resultado, advertência e multa pecuniária o que se consolidou como a primeira sanção administrativa, demonstrando a efetividade do regime sancionatório mesmo em relação a empresas de pequeno porte, reforçando, ainda, a isonomia no cumprimento das obrigações legais.

A propósito, cabe destacar que a ANPD não se limita à esfera privada. Em 2024, houve a aplicação de sanções a órgãos e entidades do setor público que deixaram de notificar incidentes de segurança ou falharam na implementação de medidas de governança e mitigação de riscos.

Paralelamente, órgãos de defesa do consumidor têm exercido papel relevante ao aplicar sanções administrativas decorrentes de incidentes que afetaram diretamente os consumidores, como, por exemplo, as autuações em face do iFood , motivadas por alterações indevidas em cadastros de usuários e ataques cibernéticos,

nas quais foram impostas sanções pelo Procon-RJ e por outros órgãos do Sistema Nacional de Defesa do Consumidor (SNDC).

Portanto, embora muitas ações ainda se encontrem em tramitação, sem decisões definitivas com condenações indenizatórias, os casos analisados ilustram a coexistência entre as esferas administrativa e judicial e a complementariedade dos instrumentos de responsabilização no sistema brasileiro de proteção de dados pessoais, demonstrando, inclusive, a evolução institucional do país no enfrentamento de incidentes de segurança, consolidando gradualmente um regime de responsabilização efetivo, coerente e preventivo.

4.5 Efeitos práticos e limites da responsabilização

A análise dos casos apresentados permite extrair observações práticas relevantes acerca da aplicação do regime sancionatório instituído pela Lei Geral de Proteção de Dados.

Em primeiro lugar, constata-se que a Autoridade Nacional de Proteção de Dados (ANPD) vem utilizando sanções tanto pecuniárias quanto não pecuniárias, em conformidade com a LGPD e com a Resolução CD/ANPD nº 4/2023, que regulamenta os critérios e parâmetros para aplicação de sanções. Dentre as medidas adotadas, destacam-se advertências, publicização das infrações, suspensão parcial ou total do tratamento de dados pessoais, bloqueio de bases de dados e a imposição de medidas corretivas acompanhadas de multa diária.

Essa diversidade de instrumentos sancionatórios revela a flexibilidade regulatória da ANPD, permitindo que a adequação à resposta estatal perante a natureza e gravidade da infração, bem como ao porte econômico do responsável pelo tratamento dos dados. Essa abordagem confirma o caráter pedagógico e preventivo das sanções, conforme enfatizado pela própria ANPD em seus comunicados oficiais, e alinha-se à prática internacional de autoridades de proteção de dados, como a *European Data Protection Board* (EDPB) no âmbito do GDPR.

Em segundo lugar, observa-se que a dosimetria das penalidades busca assegurar a proporcionalidade e razoabilidade das sanções, calibrando-as conforme a

gravidade do dano, o grau de cooperação, a boa-fé demonstrada e o benefício econômico obtido com a infração. Contudo, a efetividade punitiva, na prática, depende de fatores externos, que transcendem os dispositivos legais, como a capacidade técnica de investigação da ANPD, o intercâmbio de informações entre órgãos nacionais, a cooperação internacional em incidentes de caráter transfronteiriço, nos quais múltiplas jurisdições compartilham competência regulatória.

A propósito, é importante salientar outro aspecto relevante refere-se às empresas multinacionais, que enfrentam desafios específicos de execução e conformidade, especialmente quanto à execução prática das multas aplicadas no Brasil e ao alinhamento entre políticas globais de proteção de dados e exigências locais da LGPD. Essa realidade reforça a necessidade de estratégias de *compliance*[7] multinível, capazes de conciliar as diretrizes de diferentes ordenamentos.

A aplicação prática do regime sancionatório da LGPD revela um sistema em evolução contínua, que combina instrumentos administrativos, judiciais e educativos de responsabilização e demanda aprimoramento técnico, institucional e normativo constante. A consolidação de um modelo de governança de dados eficaz depende não apenas do rigor punitivo, mas também da capacidade estatal de fiscalização, cooperação internacional e engajamento do setor privado na construção de uma cultura de proteção em um ambiente cada vez mais complexo, digital e transnacional.

5 CONCLUSÃO

A análise realizada ao longo deste material evidencia que a coleta e o tratamento de dados pessoais por plataformas digitais representam desafios contemporâneos à tutela dos direitos fundamentais, em especial à privacidade, segurança da informação e à liberdade individual. A LGPD estabelece um marco normativo sólido, assentado em princípios estruturantes, como a finalidade,

[7] *Compliance* é o conjunto de práticas e procedimentos que uma empresa adota para garantir que suas atividades estejam em conformidade com leis, regulamentos, normas internas e padrões éticos.

necessidade, transparência e a responsabilização, e dotado de mecanismos de controle e sanção que visam assegurar a conformidade no tratamento de dados.

A aplicação prática desse regime sancionatório, ilustrada por casos nacionais e internacionais de grande repercussão, revela tanto a efetividade quanto os limites da atuação estatal. Percebe-se que a Autoridade Nacional de Proteção de Dados (ANPD) vem exercendo papel progressivamente relevante na consolidação de uma cultura de proteção de dados no país, utilizando instrumentos pecuniários e não pecuniários, como advertências, multas, suspensão de atividades e publicização de infrações, conforme previsto na LGPD. Contudo, a efetividade das sanções ainda depende de fatores institucionais e técnicos, como a capacidade investigativa da autoridade, a cooperação internacional e o nível de maturidade das políticas de governança corporativa de empresas.

Ademais, restou demonstrado que empresas multinacionais enfrentam obstáculos adicionais na execução de penalidades e na harmonização entre as exigências regulatórias locais e as políticas globais de *compliance*, o que reforça a necessidade de coordenação transnacional entre autoridades de proteção de dados e de aprimoramento dos mecanismos de *accountability*[8].

Logo, decorre de um equilíbrio entre regulação robusta, fiscalização eficiente e conscientização social. O fortalecimento da cultura de proteção de dados demanda educação digital dos usuários, transparência corporativa e cooperação institucional contínua.

Diante de todo o exposto, recomenda-se a ampliação de estudos empíricos sobre a percepção dos titulares quanto a seus direitos, bem como a avaliação dos impactos concretos das sanções aplicadas pela ANPD, de modo a subsidiar políticas públicas mais eficazes e promover um aperfeiçoamento constante do sistema brasileiro de proteção de dados pessoais.

REFERÊNCIAS

[8] *Accountability* é a responsabilidade para dar explicações e responder por suas ações, decisões e resultados, promovendo transparência e compromisso.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Perguntas frequentes: o que são dados pessoais sensíveis.* Brasília: ANPD, 2025. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 6 out. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *ANPD aplica primeira sanção administrativa com base na LGPD.* Brasília: ANPD, 6 jul. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-primeira-sancao-administrativa-com-base-na-lgpd. Acesso em: 6 out. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Critérios e parâmetros para aplicação de sanções administrativas.* Brasília: ANPD, 2023. Disponível em: https://www.gov.br/anpd. Acesso em: 6 out. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia orientativo sobre dosimetria e aplicação de sanções administrativas.* Brasília: ANPD, 2023. Disponível em: https://www.gov.br/anpd. Acesso em: 6 out. 2025.

BBC NEWS BRASIL. *Vazamento expõe dados de 533 milhões de usuários do Facebook.* Publicado em 4 abr. 2021. Disponível em: https://www.bbc.com/portuguese/geral-56630386. Acesso em: 6 out. 2025.

BBC NEWS BRASIL. *Vazamento expõe dados de 220 milhões de brasileiros e inclui até CPFs de pessoas mortas.* Publicado em 29 jan. 2021. Disponível em: https://www.bbc.com/portuguese/brasil-55857399. Acesso em: 6 out. 2025.

BRASIL. *Constituição da República Federativa do Brasil de 1988.* Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 6 out. 2025.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018.* Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 6 out. 2025.

BRASIL. *Resolução CD/ANPD nº 1, de 28 de outubro de 2021.* Dispõe sobre o processo de fiscalização e aplicação de sanções administrativas. Brasília: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/normativos/resolucoes. Acesso em: 6 out. 2025.

BRASIL. *Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023.* Estabelece metodologia para cálculo do valor-base das sanções de multa. Brasília: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/normativos/resolucoes/resolucao-cd-anpd-no-4-de-24-de-fevereiro-de-2023.pdf. Acesso em: 6 out. 2025.

CASTRO, Rodrigo Pironti Aguirre de; LIMA, Bruna Martins. A responsabilidade civil nas violações de dados pessoais: reflexões à luz da LGPD. *Revista de Direito, Estado e Telecomunicações*, v. 14, n. 2, 2022.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação da autoridade e da autodeterminação informativa.* Rio de Janeiro: Renovar, 2020.

EUROPEAN DATA PROTECTION BOARD (EDPB). *Guidelines 04/2022 on the calculation of administrative fines under the GDPR.* Brussels: EDPB, 2022. Disponível em: https://edpb.europa.eu. Acesso em: 6 out. 2025.

EUROPEAN UNION. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – GDPR).* Official Journal of the European Union, L 119, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 6 out. 2025.

FORBES. *Massive Facebook data leak: what happened and what to do next.* 4 abr. 2021. Disponível em: https://www.forbes.com/sites/kateoflahertyuk/2021/04/04/massive-facebook-data-leak-what-happened-and-what-to-do-next/. Acesso em: 6 out. 2025.

G1. *Vazamento de dados de 220 milhões de brasileiros inclui CPF, score e salário.* 26 jan. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/26/vazamento-de-dados-de-220-milhoes-de-brasileiros-inclui-cpf-score-e-salario.ghtml. Acesso em: 6 out. 2025.

INFOMONEY. *Caso Cambridge Analytica: vazamento de dados no Facebook.* Disponível em: https://www.infomoney.com.br. Acesso em: 6 out. 2025.

JUS NAVIGANDI. *Jurisprudência e doutrina sobre dados pessoais sensíveis.* Disponível em: https://www.jus.com.br. Acesso em: 6 out. 2025.

MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang. *Tratado de Proteção de Dados Pessoais.* São Paulo: Thomson Reuters Brasil, 2021.

OLIVEIRA, Rafael Zanatta; CAVALCANTE, Larissa. Governança de dados e proteção da privacidade no Brasil. *Revista de Direito, Estado e Telecomunicações*, v. 14, n. 2, 2022.

PROCON-RJ. *Procon-RJ multa iFood por falhas em segurança de dados e atendimento.* 2022. Disponível em: https://www.procon.rj.gov.br. Acesso em: 6 out. 2025.

RODRIGUES JÚNIOR, Otávio Luiz. Responsabilidade civil por vazamento de dados pessoais: panorama e desafios da LGPD. *Revista dos Tribunais*, v. 112, n. 1012, 2023.

SCHREIBER, Anderson. *Direito Civil e Internet: privacidade, proteção de dados e responsabilidade civil.* 3. ed. São Paulo: Atlas, 2021.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO). *Dados sensíveis — LGPD.* Brasília: SERPRO, 2025. Disponível em: https://www.portal.gov.br. Acesso em: 6 out. 2025.

THE HACK. *Serasa Experian é investigada após vazamento de dados de brasileiros.* 2021. Disponível em: https://thehack.com.br/serasa-experian-e-investigada-apos-vazamento-de-dados-de-brasileiros/. Acesso em: 6 out. 2025.

CONSENTIMENTO OU COERÇÃO? UMA LEITURA CRÍTICA DA LGPD: ENTRE AUTONOMIA, ARQUITETURA DE ESCOLHAS, PROPORCIONALIDADE E GOVERNANÇA

Felipe Martins Obliziner[1]
Larissa Maria de Figueiredo[2]

RESUMO

Este artigo analisa criticamente o papel do consentimento na Lei Geral de Proteção de Dados Pessoais (LGPD), questionando sua efetividade como instrumento de proteção da autodeterminação informacional dos indivíduos em um ecossistema digital cada vez mais complexo, automatizado e assimétrico. Embora o consentimento figure formalmente como uma das bases legais para o tratamento de dados pessoais, sua prática concreta frequentemente revela fragilidades estruturais, derivadas tanto do desenho das interfaces como de desequilíbrios de poder entre titulares e controladores. Com base em uma abordagem interdisciplinar, o presente trabalho articula fundamentos jurídicos, sociológicos e tecnológicos para propor uma leitura crítica do consentimento, examinando suas limitações, suas condições de legitimidade e os mecanismos que podem garantir sua efetividade. Parte-se da premissa de que o consentimento, quando reduzido a um clique automático, deixa de representar a liberdade do titular e passa a funcionar como mecanismo simbólico de legitimação de práticas invasivas. Defende-se, portanto, que o consentimento só é válido se inserido em um contexto de governança robusta, proporcionalidade, simetria decisória, e responsabilidade institucional. A análise se desenvolve por meio de uma estrutura em doze seções que discutem desde os fundamentos normativos até os desafios regulatórios contemporâneos, passando por tópicos como I.A, biometria, ambientes vulneráveis, padrões escuros e direito comparado.

Palavras-chave: LGPD; consentimento; privacidade; arquitetura de escolhas; governança; responsabilidade; autodeterminação informacional.

[1] Felipe Martins Obliziner – graduando do curso de Direito do UNICEUB – felipe.obliziner@sempreceub.com.
2 Larissa Maria de Figueiredo - graduanda do curso de Direito do UNICEUB - larissa.figueiredo@sempreceub.com.

1 INTRODUÇÃO

A sociedade contemporânea encontra-se profundamente imersa em um ambiente digital que transforma dados pessoais em ativos estratégicos. Cada interação online, seja ela uma pesquisa, um clique ou uma navegação passiva, resulta na geração de informações que são coletadas, armazenadas, cruzadas e monetizadas por agentes públicos e privados. Nesse contexto, o consentimento emerge como um dos pilares centrais do marco legal brasileiro de proteção de dados, a LGPD, refletindo uma tentativa normativa de resgatar a autonomia do titular frente ao crescente poder de controle dos dados por parte de grandes corporações e plataformas digitais.

Contudo, a promessa de autonomia informacional por meio do consentimento tem sido objeto de críticas crescentes. Em ambientes marcados por assimetrias técnicas, informacionais e econômicas, o consentimento perde sua característica deliberativa e se transforma em ato compulsório, automatizado e desprovido de significado jurídico ou ético. Interfaces manipulativas, padrões escuros, contratos de adesão e termos complexos constituem barreiras reais à compreensão e ao exercício efetivo da liberdade.

Este trabalho propõe-se a investigar criticamente essa problemática, partindo da hipótese de que o consentimento isolado, tal como praticado atualmente, é incapaz de garantir a autodeterminação informacional dos indivíduos. O estudo estrutura-se em torno de doze sessões temáticas, nas quais serão examinados: o sentido material do consentimento, as arquiteturas de escolhas, os limites da proporcionalidade, a governança de dados, os contextos de vulnerabilidade, a relação com outras bases legais, o impacto da inteligência artificial e a experiência comparada internacional.

2 O SENTIDO MATERIAL DO CONSENTIMENTO

A LGPD, em seu artigo 5º, inciso XII, define consentimento como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o

tratamento de seus dados pessoais para uma finalidade determinada". Essa definição, embora juridicamente precisa, esconde camadas mais profundas de complexidade. O conceito de "livre" nem sempre encontra respaldo nas práticas correntes. A liberdade decisória, em um contexto digital altamente dependente de serviços online, é frequentemente substituída pela aceitação compulsória de termos para acesso a plataformas, redes sociais, ferramentas educacionais e bancárias. Dessa forma, a pretensa autonomia é suprimida por uma coerção estrutural que transforma o consentimento em ato simbólico.

Do ponto de vista da teoria jurídica, o consentimento precisa ser analisado sob a lente da proporcionalidade e da finalidade legítima do tratamento. Não basta que o titular clique em "aceito"; é necessário que compreenda, com linguagem acessível, as reais consequências do uso de seus dados. Isso implica traduzir juridicamente o consentimento como um ato comunicativo, que se concretiza apenas quando há equilíbrio entre as partes e condições reais de recusa, revogação e renegociação.

Autores como Mendes (2019) e Doneda (2020) têm argumentado que o consentimento deve ser compreendido como parte de um regime de responsabilidade compartilhada. O titular não é o único responsável por proteger sua privacidade; cabe ao controlador criar condições materiais para que essa proteção ocorra. Isso inclui oferecer opções granulares, permitir revogações simples e garantir transparência nos fluxos de dados.

Essa perspectiva é reforçada pela Constituição Federal de 1988, que consagra a dignidade da pessoa humana como fundamento da República. O direito à privacidade e à autodeterminação informacional deriva diretamente desse princípio, e deve ser compreendido como um direito fundamental, indivisível e inalienável. Assim, o consentimento é válido apenas se for expressão dessa dignidade, e não instrumento de sua supressão.

3 ARQUITETURA DE ESCOLHAS, MANIPULAÇÃO DIGITAL E PADRÕES ESCUROS

No ambiente digital, a apresentação das opções ao usuário exerce papel decisivo no modo como decisões são tomadas. Essa estrutura de decisões, chamada "arquitetura de escolhas", é composta por elementos de design, linguagem e fluxo de interface que orientam comportamentos sem que os usuários percebam que estão sendo influenciados. Quando usada de maneira maliciosa, essa arquitetura passa a representar uma forma de coerção simbólica, comprometendo diretamente a validade do consentimento.

Estudos como o de Mathur et al. (2019) demonstram que as interfaces digitais são frequentemente estruturadas para induzir o consentimento ao tratamento de dados, utilizando técnicas conhecidas como "dark patterns" (padrões escuros). Exemplos comuns incluem botões de aceite mais visíveis que os de recusa, caixas pré-marcadas, linguagem ambígua ou confusa e jornadas de navegação que desestimulam a recusa ao tratamento.

Essa manipulação não é meramente estética ou funcional: trata-se de uma escolha deliberada que desequilibra a relação entre titulares e controladores. O consentimento obtido nessas condições não pode ser considerado "livre" nem "informado", já que resulta de induções muitas vezes imperceptíveis, mas eficazes. A LGPD, ao estabelecer a necessidade de transparência e facilidade de revogação do consentimento, busca mitigar esses efeitos. No entanto, a aplicação prática dessas exigências ainda encontra sérios problemas que impedem a sua total eficácia.

A Autoridade Nacional de Proteção de Dados (ANPD) já reconheceu, em suas diretrizes e notas técnicas, a existência dos padrões escuros como prática contrária aos princípios da LGPD. Contudo, ainda são escassas as sanções efetivas aplicadas com base nessa fundamentação. A ausência de jurisprudência consolidada sobre o tema contribui para a manutenção de práticas nocivas, que perpetuam o desequilíbrio entre agentes de tratamento e titulares de dados.

É necessário que a arquitetura de escolhas seja submetida a critérios éticos claros e auditáveis. O design de consentimento deve promover a autonomia do usuário e facilitar a compreensão. Isso implica na adoção de uma abordagem conhecida como "privacy by design" (privacidade desde o design), onde a proteção

de dados é incorporada desde a concepção dos sistemas, e não apenas como etapa posterior de conformidade.

4 PROPORCIONALIDADE, MINIMIZAÇÃO E AVALIAÇÕES DE IMPACTO

A aplicação do consentimento como base legal exige que o tratamento de dados observe, além dos requisitos formais, princípios materiais como o da proporcionalidade. Esse princípio, de matriz constitucional, exige que as medidas adotadas sejam adequadas, necessárias e proporcionais em sentido estrito. No âmbito da LGPD, isso significa que o controlador deve demonstrar que o tratamento proposto é essencial para atingir uma finalidade legítima, que não há meio menos invasivo e que os benefícios superam os riscos impostos aos direitos do titular.

Dois instrumentos previstos na LGPD operacionalizam essa análise: o Relatório de Impacto à Proteção de Dados Pessoais (DPIA) e o Relatório de Avaliação de Interesse Legítimo (LIA). O DPIA, nos termos do artigo 38 da LGPD, deve ser elaborado nos casos em que o tratamento de dados possa acarretar riscos elevados aos direitos fundamentais dos titulares. Já o LIA é um documento complementar que justifica o uso da base legal do legítimo interesse, analisando a necessidade, expectativa razoável e medidas mitigatórias.

A utilização do DPIA e do LIA ainda é incipiente no Brasil. Muitas organizações desconhecem sua existência ou interpretam esses instrumentos como exigências apenas formais. Esse equívoco compromete a função preventiva dessas ferramentas, que deveriam servir como mecanismos de auto regulação, controle e transparência. É necessário que a ANPD avance na padronização e exigência de tais documentos, especialmente em setores de risco elevado, como saúde, educação, tecnologia e finanças.

Outro princípio relevante é o da minimização de dados, previsto no artigo 6º, inciso III da LGPD. Ele estabelece que apenas os dados estritamente necessários para a realização de uma finalidade devem ser coletados e tratados. Essa regra visa reduzir o volume de dados expostos, limitar o risco de vazamentos e impedir abusos no uso de informações pessoais. Na prática, entretanto, a coleta excessiva de dados

continua sendo uma prática comum, muitas vezes justificada pela conveniência comercial.

A exigência de proporcionalidade deve também ser aplicada na definição da duração do tratamento e do armazenamento dos dados. O prazo de retenção precisa estar vinculado à finalidade informada no momento do consentimento, e deve ser limitado no tempo. A ausência de prazos definidos, ou a manutenção indefinida de informações, representa violação direta à LGPD e às boas práticas internacionais.

Em síntese, o consentimento legítimo é aquele que não apenas atende aos requisitos formais de clareza e liberdade, mas também se insere em um modelo de tratamento orientado por princípios como proporcionalidade, necessidade e responsabilidade. A adoção de avaliações de impacto e o compromisso com a minimização representam passos essenciais para transformar o consentimento de um ato simbólico em um instrumento real de proteção.

5 GOVERNANÇA, RESPONSABILIDADE E CULTURA DA CONFORMIDADE

A governança em proteção de dados ultrapassa o campo jurídico e adentra o território da cultura organizacional. A LGPD consagra, no artigo 6º, inciso X, o princípio da responsabilização e da prestação de contas, conhecido como accountability (responsabilidade). Isso implica não apenas cumprir a lei, mas demonstrar de forma transparente, proativa e contínua esse cumprimento. Assim, o consentimento precisa estar inserido em uma estrutura institucional que valorize a privacidade como eixo estratégico.

A accountability (responsabilidade) exige a adoção de mecanismos internos que permitam o mapeamento dos dados pessoais tratados, a revisão periódica de finalidades, a limitação de acesso, a educação continuada dos colaboradores e a resposta rápida a incidentes. Empresas maduras em proteção de dados possuem políticas internas detalhadas, comitês de privacidade, registros de atividades de tratamento e relatórios de impacto integrados aos processos decisórios.

A ANPD tem adotado uma abordagem de regulação responsiva, buscando orientar os agentes econômicos antes de aplicar sanções. Essa estratégia favorece a construção de uma cultura de conformidade, mas precisa ser acompanhada de medidas coercitivas eficazes para que os princípios da LGPD não se tornem letra morta.

Além disso, a cultura da conformidade depende de um processo educacional contínuo. O consentimento precisa ser compreendido por todos os atores envolvidos no tratamento de dados, não apenas por advogados ou encarregados de proteção. Desenvolvedores, analistas, gestores e até o atendimento ao cliente devem ser treinados sobre os fundamentos da LGPD e a importância de respeitar as escolhas do titular. A proteção de dados deve estar no DNA da organização, e não restrita ao departamento jurídico.

A governança também inclui mecanismos externos de controle social. Relatórios de transparência, canais de atendimento ao titular, painéis públicos e auditorias independentes fortalecem a confiança e reduzem a assimetria entre empresas e usuários. A sociedade civil tem papel fundamental na fiscalização das práticas digitais, por meio de ações coletivas, denúncias, observatórios e pesquisas empíricas. Sem participação ativa da sociedade, o consentimento continuará sendo um rito vazio.

6 CONSENTIMENTO EM CONTEXTOS VULNERÁVEIS: TRABALHO, INFÂNCIA, SAÚDE E BIOMETRIA

Um dos principais limites do consentimento como base legal é sua aplicação em contextos de vulnerabilidade, nos quais a liberdade decisória é comprometida por relações de dependência, desigualdade ou assimetria de poder. Nessas situações, o consentimento dificilmente pode ser considerado “livre”, ainda que formalmente expresso. A LGPD reconhece parcialmente esse problema, ao prever bases legais alternativas para determinados cenários, mas a prática ainda revela fragilidades significativas.

No ambiente laboral, por exemplo, a relação de subordinação entre empregador e empregado compromete a voluntariedade do consentimento. O

trabalhador pode sentir-se coagido a aceitar o tratamento de seus dados por receio de retaliações, demissões ou prejuízos profissionais. Por esse motivo, a doutrina e a ANPD têm recomendado que, sempre que possível, o tratamento de dados no contexto do trabalho se fundamente em outras bases legais, como cumprimento de obrigação legal ou execução de contrato.

A situação se agrava em setores que utilizam tecnologias sensíveis, como biometria facial para controle de ponto, vigilância por câmeras com reconhecimento de emoções ou rastreamento de produtividade. Tais práticas, além de invasivas, muitas vezes carecem de justificativa proporcional e violam direitos fundamentais à intimidade e à dignidade. O consentimento, nestes casos, não pode ser um álibi para legitimar práticas abusivas.

Em relação ao tratamento de dados de crianças e adolescentes, a LGPD impõe regras mais restritivas. O artigo 14 estabelece que o tratamento deve ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou responsável legal. Além disso, as informações devem ser fornecidas de maneira acessível, considerando a compreensão do público infantojuvenil. No entanto, o cumprimento efetivo dessas exigências ainda é limitado, especialmente em aplicativos e plataformas digitais.

Na área da saúde, o tratamento de dados sensíveis exige cuidados redobrados. Informações sobre doenças, exames, histórico clínico e uso de medicamentos dizem respeito à esfera íntima da pessoa humana. O consentimento para o tratamento desses dados deve ser informado, específico e restrito à finalidade informada. O uso indevido de dados de saúde, seja para fins comerciais ou discriminatórios, representa violação grave da LGPD e pode acarretar sanções administrativas e civis.

Por fim, a coleta e uso de dados biométricos — como impressões digitais, íris, voz ou reconhecimento facial — tem se expandido rapidamente no Brasil, sem a devida análise de proporcionalidade e segurança. Por se tratarem de dados sensíveis e de difícil reversão em caso de vazamento, o consentimento para seu uso deve ser tratado com máxima cautela. A ANPD já emitiu recomendações sobre o tema, mas a ausência de regulamentação específica deixa lacunas jurídicas e operacionais que precisam ser urgentemente preenchidas. É fundamental que sejam definidos critérios

técnicos e jurídicos para o uso legítimo da biometria, com exigência de proporcionalidade, avaliação de impacto e consentimento reforçado, especialmente nos contextos em que o titular não possui alternativas reais de escolha.

7 AUTODETERMINAÇÃO INFORMACIONAL COMO DIREITO FUNDAMENTAL

A autodeterminação informacional constitui um dos conceitos mais relevantes e sofisticados no debate contemporâneo sobre proteção de dados. Originado na jurisprudência do Tribunal Constitucional Alemão, particularmente na decisão de 1983 sobre o Censo Federal (Volkszählungsurteil), esse direito garante ao indivíduo o poder de decidir sobre a coleta, o uso e a circulação de suas informações pessoais. Trata-se, portanto, de um direito à gestão da própria identidade informacional, com impactos profundos na identidade informacional, com impactos profundos na vida privada e na esfera pública, da construção da personalidade e do exercício de liberdades e direitos fundamentais.

No contexto brasileiro, embora o termo "autodeterminação informacional" não conste expressamente na Constituição Federal de 1988, sua estrutura axiológica permite reconhecer esse direito como decorrência direta dos princípios da dignidade da pessoa humana, da privacidade e da liberdade. A LGPD, ao dispor sobre o controle dos titulares sobre seus dados, aproxima-se dessa concepção e contribui para consolidá-la no ordenamento jurídico nacional.

O consentimento, nesse cenário, representa um instrumento de concretização da autodeterminação. No entanto, como já discutido, sua eficácia depende de condições institucionais, sociais e técnicas que garantam liberdade real de escolha. Se o consentimento é obtido em ambientes de coerção, opacidade ou dependência econômica, ele perde seu valor como expressão de vontade e, portanto, não realiza o direito à autodeterminação informacional.

Mais do que proteger dados, a LGPD deve proteger os sujeitos de direito. A centralidade da pessoa humana implica que o tratamento de dados seja avaliado à luz de seus impactos existenciais, identitários e sociais. O uso de informações pessoais

para discriminação, manipulação comportamental ou vigilância ubíqua fere diretamente esse princípio e exige respostas jurídicas firmes.

A incorporação da autodeterminação informacional como direito fundamental explícito, nos moldes das constituições da Alemanha e da União Europeia, fortaleceria significativamente o arcabouço normativo brasileiro. Essa mudança permitiria um controle constitucional mais rigoroso sobre políticas públicas e práticas privadas que envolvam tratamento de dados, e elevaria o nível de proteção jurídica dos titulares.

8 CONSENTIMENTO VERSUS LEGÍTIMO INTERESSE: UMA ANÁLISE CRÍTICA

Entre as bases legais previstas na LGPD, o consentimento e o legítimo interesse do controlador ocupam posições de destaque. No entanto, ambos apresentam riscos e limites que precisam ser analisados com profundidade. O consentimento, como já discutido, pode ser fragilizado por estruturas de coerção simbólica. O legítimo interesse, por sua vez, é mais suscetível à interpretação abusiva, podendo justificar tratamentos invasivos sem a devida transparência ou possibilidade de oposição.

O artigo 7º, inciso IX, da LGPD, permite o tratamento de dados com base no legítimo interesse, desde que respeitados os direitos e liberdades fundamentais do titular e que haja a expectativa razoável quanto ao uso. Essa cláusula, inspirada no GDPR, exige uma avaliação de proporcionalidade, cujos critérios devem ser cuidadosamente documentados. O problema é que muitos controladores recorrem ao legítimo interesse como uma forma de escapar dos requisitos formais do consentimento, tratando dados sem o conhecimento ou a concordância explícita dos titulares. Essa prática compromete a transparência e enfraquece os direitos informacionais, transformando uma exceção legal em justificativa genérica para coleta massiva de dados.

A ANPD, em suas orientações preliminares, têm ressaltado que o legítimo interesse não pode ser utilizado para finalidades incompatíveis com os direitos do titular, especialmente em tratamentos que envolvam dados sensíveis, crianças,

grandes volumes ou perfis de vulnerabilidade. Nesses casos, recomenda-se o uso de outras bases legais ou a adoção de medidas mitigadoras robustas.A escolha entre consentimento e legítimo interesse não deve ser feita com base na conveniência operacional, mas sim em critérios objetivos de legalidade, necessidade e ética. É essencial que os controladores conduzam um LIA (Legitimate Interests Assessment), (Avaliação de interesses legítimos), antes de adotar essa base legal, e que o documento esteja disponível para auditoria da ANPD ou do próprio titular, caso solicitado.

Ainda permanecem situações em que se pode cogitar o uso combinado ou sequencial de bases legais. Por exemplo, um serviço pode tratar dados com base no contrato, mas oferecer funcionalidades adicionais com base no consentimento específico do usuário. Essa granularidade contribui para reforçar a transparência e o controle do titular, evitando o uso indevido de uma base legal genérica como justificativa para todos os tratamentos.

Em resumo, tanto o consentimento quanto o legítimo interesse têm papéis importantes na LGPD, mas precisam ser aplicados com rigor técnico e responsabilidade ética. A proteção de dados é um direito fundamental e, como tal, não pode ser relativizado por razões comerciais ou operacionais. O uso consciente das bases legais fortalece a credibilidade da LGPD e a confiança do cidadão na proteção de seus direitos digitais.

9 ALGORITMOS, INTELIGÊNCIA ARTIFICIAL E DECISÕES AUTOMATIZADAS

O avanço das tecnologias baseadas em inteligência artificial (IA) e aprendizado de máquina trouxe novos desafios para a proteção de dados pessoais. Na economia digital contemporânea, decisões relevantes sobre acesso a crédito, oportunidades de emprego, diagnósticos médicos e até investigações criminais estão sendo delegadas a sistemas automatizados, frequentemente sem transparência ou possibilidade de contestação pelos afetados.

A LGPD, em seu artigo 20, prevê que o titular dos dados tem direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento

automatizado de dados pessoais que afetem seus interesses. Esse dispositivo busca garantir uma espécie de "direito à explicação" e à revisão humana das decisões automatizadas, aproximando-se do que prevê o GDPR no contexto europeu. No entanto, a implementação prática desse direito enfrenta barreiras técnicas e institucionais significativas.

Muitos controladores alegam que seus algoritmos são protegidos por segredo comercial, dificultando a transparência sobre os critérios utilizados para tomada de decisão. Essa opacidade algorítmica coloca os titulares em situação de desvantagem, violando os princípios da equidade, da informação e da autodeterminação informacional. Em tais contextos, o consentimento, ainda que formalmente colhido, não é suficiente para proteger os direitos fundamentais, pois o titular sequer compreende como seus dados serão utilizados, tampouco tem condições reais de avaliar os impactos de decisões automatizadas sobre sua vida, seja no acesso a crédito, oportunidades de trabalho ou serviços essenciais.

O tratamento automatizado de dados sensíveis, como etnia, religião, saúde ou orientação sexual, agrava ainda mais a situação. Modelos treinados com dados enviesados podem reproduzir e amplificar desigualdades históricas, gerando discriminações automatizadas que escapam ao controle humano. O uso desses sistemas exige, portanto, avaliação prévia de impacto, medidas de mitigação de riscos e monitoramento contínuo da performance algorítmica.

Nesse cenário, o consentimento deve ser revisto à luz do risco algorítmico. É necessário que os controladores forneçam informações claras e compreensíveis sobre o funcionamento básico dos sistemas utilizados, sua finalidade, os critérios principais de decisão e os direitos do titular. Além disso, a revisão de decisões automatizadas deve ser conduzida por pessoas com formação técnica e sensibilidade ética, aptas a compreender as limitações dos modelos e a considerar as especificidades do caso concreto.

10 DIREITO COMPARADO: EUROPA, CANADÁ, COREIA DO SUL E ESTADOS UNIDOS

A análise comparada das legislações internacionais em proteção de dados permite compreender diferentes abordagens sobre o consentimento e suas limitações. Na União Europeia, o GDPR estabelece critérios rigorosos para a validade do consentimento, exigindo que seja dado de forma livre, específica, informada e inequívoca. O regulamento também proíbe práticas coercitivas, como o bloqueio de funcionalidades em caso de recusa. Diversas decisões dos órgãos reguladores europeus têm reforçado essa perspectiva, determinando que o consentimento só é válido quando o titular tem liberdade real para recusá-lo, sem sofrer prejuízos ou limitações de acesso a serviços essenciais.

No Canadá, a legislação federal (PIPEDA) adota um modelo baseado no consentimento significativo, ou seja, aquele que ocorre em condições de real compreensão e liberdade. A abordagem canadense valoriza a clareza na linguagem, a facilidade de revogação e o controle granular sobre as finalidades. Recentes reformas legislativas têm buscado fortalecer os poderes do Privacy Commissioner (comissário de privacidade), além de aumentar as sanções para condutas ilegais.

A Coreia do Sul, por sua vez, possui uma das legislações mais robustas da Ásia em matéria de proteção de dados, com destaque para a Personal Information Protection Act (PIPA) (Lei de Proteção de Informações Pessoais). O país impõe limites rigorosos à coleta de dados sensíveis, exige consentimento separado para finalidades distintas e proíbe o uso compulsório do consentimento como condição para acesso a serviços essenciais. A atuação proativa da Personal Information Protection Commission (PIPC) (Comissão de Proteção de Informações), tem sido elogiada internacionalmente.

Nos Estados Unidos, a ausência de uma legislação federal única gera um cenário fragmentado e assimétrico. Algumas leis estaduais, como a California Consumer Privacy Act (CCPA) (Lei de Privacidade do Consumidor) e sua evolução, a California Privacy Rights Act (CPRA), (Lei de Direitos de Privacidade da Califórnia), aproximam-se dos padrões internacionais, mas a maioria dos estados ainda carece de proteção efetiva. O modelo estadunidense valoriza o controle pelo mercado e a autorregulação, mas tem sido criticado por permitir práticas abusivas, especialmente por grandes plataformas digitais.

No Brasil, a LGPD inspirou-se no GDPR, mas ainda enfrenta desafios para alcançar sua plena efetividade. A comparação com os modelos internacionais revela que o consentimento só é eficaz quando combinado com mecanismos de fiscalização robustos, autoridades independentes e cultura organizacional comprometida com a ética digital. A simples formalização do consentimento, sem ambiente institucional que o sustente, resulta em sua banalização.

11 CASOS PARADIGMÁTICOS E DECISÕES DA ANPD

A atuação da Autoridade Nacional de Proteção de Dados (ANPD) tem sido fundamental para a construção da jurisprudência administrativa sobre consentimento e proteção de dados no Brasil. Embora recente, a autoridade já publicou diversas orientações, notas técnicas e iniciou processos sancionatórios que elucidam o entendimento prático da LGPD.

Um dos casos emblemáticos envolveu uma empresa de tecnologia que exigia o aceite de termos genéricos como condição para uso de seu aplicativo. A ANPD apontou que a ausência de granularidade nas opções de consentimento violava os princípios da necessidade e da transparência, pois os titulares não podiam escolher quais dados fornecer nem compreender claramente para quais finalidades seriam utilizados.

Outro caso relevante foi a coleta de dados biométricos de crianças para controle de frequência escolar em redes públicas de ensino. A ANPD alertou que o tratamento de dados sensíveis de menores exige não apenas consentimento parental específico, mas também fundamentação na estrita necessidade. A autoridade considerou que havia desproporcionalidade entre o objetivo pretendido e a tecnologia adotada, recomendando a suspensão da prática.

Em decisões sobre o setor financeiro, a ANPD também identificou abusos na utilização da base legal do legítimo interesse. Algumas instituições usavam essa justificativa para marketing direto e compartilhamento de dados com terceiros sem informar adequadamente os titulares. A autoridade reforçou que o legítimo interesse

exige avaliação prévia de impacto e expectativa razoável por parte do usuário, elementos que estavam ausentes nos casos analisados.

Esses precedentes indicam que a ANPD tem se posicionado de forma técnica e orientadora, mas com potencial sancionador crescente. A consolidação da jurisprudência administrativa contribuirá para uniformizar interpretações, ampliar a segurança jurídica e inibir práticas abusivas. O consentimento, inserido nesse ecossistema regulatório, poderá recuperar seu valor como instrumento de autonomia e não apenas como expediente formal.

12 CONCLUSÃO

Ao longo deste artigo, examinamos criticamente o papel do consentimento na LGPD, questionando sua efetividade em garantir a autodeterminação informacional dos titulares de dados. Embora previsto como base legal central, o consentimento frequentemente se mostra insuficiente diante de práticas digitais que envolvem manipulação de escolhas, coleta excessiva de informações e uso de tecnologias opacas.

Demonstrou-se que o consentimento autêntico exige um conjunto de condições materiais: transparência, linguagem acessível, revogabilidade, granularidade e simetria decisória. Além disso, deve estar inserido em uma estrutura de governança ética, com mecanismos de responsabilidade, avaliação de impacto e controle social. Apenas nesse contexto o consentimento pode cumprir sua função protetiva.

A análise também evidenciou os desafios específicos do consentimento em contextos vulneráveis, como relações laborais, dados de crianças, saúde e biometria. A utilização dessas informações sensíveis requer maior rigor jurídico, cautela institucional e acompanhamento pela ANPD. O uso indevido do consentimento nestes casos contribui para ampliar desigualdades e violar direitos fundamentais.

Por fim, refletiu-se sobre o cenário internacional e a importância da atuação da ANPD para consolidar um modelo brasileiro eficaz de proteção de dados. A experiência comparada demonstra que o consentimento, por si só, não basta. Ele

precisa ser parte de um ecossistema normativo que inclua fiscalização ativa, cultura institucional, educação digital e responsabilidade compartilhada.

Proteger dados é proteger pessoas. O consentimento, enquanto manifestação da vontade informada, só terá valor se for expressão legítima da liberdade, e não sua negação velada. A LGPD representa uma conquista civilizatória, mas seu sucesso dependerá de nossa capacidade coletiva de construir uma ética pública da privacidade.

REFERÊNCIAS

ANPD – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guias orientativos e notas técnicas. Brasília, DF: ANPD, [2021-2023].

BAUMAN, Zygmunt; LYON, David. Vigilância líquida. Rio de Janeiro: Zahar, 2013.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*, Brasília, DF, 15 ago. 2018.

CASTELLS, Manuel. The rise of the network society. 2. ed. Oxford: Wiley-Blackwell, 2009.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 2. ed. Rio de Janeiro: Forense, 2020.

HAN, Byung-Chul. Sociedade do cansaço. Petrópolis: Vozes, 2017.

MATHUR, Arunesh et al. Dark patterns at scale: findings from a crawl of 11,000 shopping websites. *Proceedings of the ACM on Human-Computer Interaction*, v. 3, n. CSCW, p. 1-32, 2019.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor. São Paulo: Revista dos Tribunais, 2019.

THALER, Richard; SUNSTEIN, Cass. Nudge: improving decisions about health, wealth, and happiness. New Haven: Yale University Press, 2008.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. *Jornal Oficial da União Europeia*, L 119, p. 1-88, 4 maio 2016.

ZUBOFF, Shoshana. The age of surveillance capitalism. New York: PublicAffairs, 2019.

DATA BROKERS E PROTEÇÃO DE DADOS PESSOAIS: UMA ANÁLISE PRINCIPIOLÓGICA

Melissa Braga[1]
Rafael Tadeu Simões Barreto[2]

RESUMO

A centralidade dos dados pessoais na economia digital favoreceu a expansão de mercados especializados na coleta, agregação e comercialização de informações, especialmente pelos data brokers. Essas empresas operam de modo amplamente opaco, reunindo dados de múltiplas fontes e realizando enriquecimento e perfilização para fins comerciais, preditivos e securitários. Tal dinâmica, fundada no uso secundário e na geração de inferências, desafia princípios basilares da proteção de dados, como finalidade, necessidade, transparência e não discriminação.

No Brasil, a consagração da proteção de dados como direito fundamental e a positivação da autodeterminação informativa pela Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais - LGPD (BRASIL, 2018), impõem limites relevantes às práticas dos data brokers. Contudo, a assimetria informacional e a crise do consentimento evidenciam a insuficiência de um modelo centrado exclusivamente na manifestação individual de vontade, sobretudo diante do tratamento massivo e automatizado típico desse setor. A ausência de regulamentação específica na LGPD acentua lacunas e incertezas quanto aos limites jurídicos aplicáveis.

O artigo analisa a compatibilidade do modelo de negócios dos data brokers com a principiologia da LGPD, identificando riscos, tensões regulatórias e desafios para a proteção efetiva dos titulares. Sustenta-se a necessidade de uma abordagem que articule tutela principiológica, accountability, regulação de risco e fortalecimento da atuação da ANPD, de modo a enfrentar a opacidade estrutural desse mercado e assegurar a proteção adequada dos direitos fundamentais.

Palavras-chave: Data Brokers; Proteção de Dados Pessoais; LGPD; Autodeterminação Informativa; Big Data.

1 INTRODUÇÃO

1 Graduanda em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: melissabrg@sempreceub.com.
2 Graduando em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: rafael.barreto@sempreceub.com.

Os dados pessoais se tornaram um ativo estratégico na economia digital, pois permitem compreender comportamentos, prever demandas, otimizar processos e criar novos modelos de negócios. Para alguns, integram os fatores primários da produção — ao lado da terra, do capital e da mão de obra —, sendo frequentemente comparados ao petróleo pelo seu elevado valor econômico (CARRIERE-SWALLOW, HAKSAR, 2019).

A Revolução Digital transformou profundamente a lógica econômica ao instituir os dados como principal vetor de funcionamento dos mercados. Empresas como Facebook, Google, Netflix e Spotify são exemplos desse novo modelo, em que os ganhos ocorrem por meio da monetização de suas enormes bases de usuários, com publicidade direcionada para usuários que podem ser potenciais consumidores, de acordo com o seu perfil e preferências manifestadas online.

Nesse aspecto, acrescenta-se a lógica Internet das Coisas (Internet of Things - IoT) e a coleta massiva de dados por meio de dispositivos físicos, tais como carros, eletrodomésticos e outros equipamentos que ao coletarem e trocarem dados na rede de computadores, permite não apenas conhecer, mas também antecipar demandas dos seus usuários. Assim, os mercados passam a operar com base em informações contínuas, moldando ofertas personalizadas e deslocando a concorrência do preço para a precisão em atender desejos individuais, reinventando a dinâmica capitalista contemporânea (ABRAMOVAY, 2019).

Nesse novo modelo de negócios, a competitividade das empresas está fortemente relacionada à qualidade, contemporaneidade e volume da sua base de dados, bem como à capacidade de utilizar esse recurso de forma estratégica a fim de entregar produtos ou serviços capazes de satisfazer as necessidades dos clientes com mais eficiência.

Naturalmente, esse mercado gera demanda por um modelo de negócios voltado à agregação, coleta, armazenamento e enriquecimento de dados, cujo propósito é fornecer, a quem estiver disposto a adquiri-los, uma relação selecionada de consumidores em potencial, mais diretamente relacionados ou interessados no produto ou serviço ofertado. Em outras palavras, nesse arranjo, o fornecedor situado na ponta final da cadeia não precisa realizar todo o processo de tratamento

informacional — da coleta ao processamento automatizado dos dados —, pois pode simplesmente contratar esse serviço, limitando-se a indicar os critérios de seleção ou o público-alvo desejado.

A fonte primária dos dados pessoais têm origens diversas, desde cadastros realizados pelos próprios titulares com o propósito de ter acesso a bens, serviços, benefícios, brindes, até mesmo por meio de cookies, preferências, interações e comportamento em páginas acessadas pelo usuário.

O interesse de ter acesso a um público seleto, resultado de um perfil traçado por hábitos ou histórico de consumo, e da abundância de dados digitalizados oriundos de fontes diversas, desenvolveu um mercado muito lucrativo de venda de dados. Com o advento e aprimoramento de ferramentas de captura e tratamento de dados, na lógica do Big Data, em que um volume descomunal de dados é estruturado e analisado para uma gama indeterminada de finalidades. Como bem exposto por Bioni (2021), milhares de bases de dados são criadas e agregadas a outras para identificar uma série de comportamentos e inferir a sua recorrência no futuro. O autor acrescenta que a mesma base de dados pode ser reutilizada, bastando que o algoritmo seja redefinido, tornando-se assim flexível para as mais diversas finalidades. Há também a possibilidade de agregação de outros dados e informações à base de modo a traçar um perfil melhor definido do potencial consumidor ("enriquecimento de dados"), com o propósito de atingir indivíduos por meio de anúncios ou posicionamento de produto ou serviço específico ("profiling" ou "perfilização").

Diante da realidade em que dados e informações pessoais passaram a ser tratados como verdadeiras commodities, este artigo aborda os principais atores desse mercado: os data brokers, ou corretoras de dados. Busca-se estabelecer uma correlação entre esse modelo de negócio e o marco regulatório vigente, destacando os aspectos jurídicos envolvidos no tratamento de tais informações à luz da LGPD.

2 OS *DATA BROKERS*

Os data brokers, também denominados corretores de dados ou information brokers, são empresas com finalidade lucrativa que agregam, coletam, armazenam, licenciam e vendem dados pessoais, incluindo seus derivados e inferências (ZANATTA; SECAF; MENDONÇA, 2021). Atuam como intermediários, revendendo ou cedendo os dados a outras empresas (VERBICARO; VIEIRA, 2021).

Historicamente operam de forma discreta e, na maioria das vezes, o titular/consumidor desconhece a sua existência e suas práticas. De fato, não têm interesse no uso final do dado, pois seu modelo de negócio acaba com a venda do dado para o maior preço ao maior número de consumidores possíveis (RUSCHEMEIER, 2023). As fontes de dados são variadas: do próprio titular ("fonte primária"), de agentes de tratamento que obtiveram o dado diretamente do titular ("fontes secundárias") ou por meio de ferramentas para captura desses dados na rede ("web crawlers"). As fontes secundárias podem ou não se beneficiar economicamente pelo repasse dos dados, mas assume-se que, a depender do volume de dados que detêm em sua base, a venda da base de dados pode ser economicamente atrativa.

Os dados e informações oriundas de diferentes fontes são processados pelos data brokers, no processo de "enriquecimento" mencionado anteriormente e são vendidos, sob demanda, às empresas consumidoras da informação que, por sua vez, identificam o consumidor, cujo perfil está mais proximamente vinculado ao produto ou serviço ofertado ("perfilização"), conforme exposto por Ruschemeier (2023).

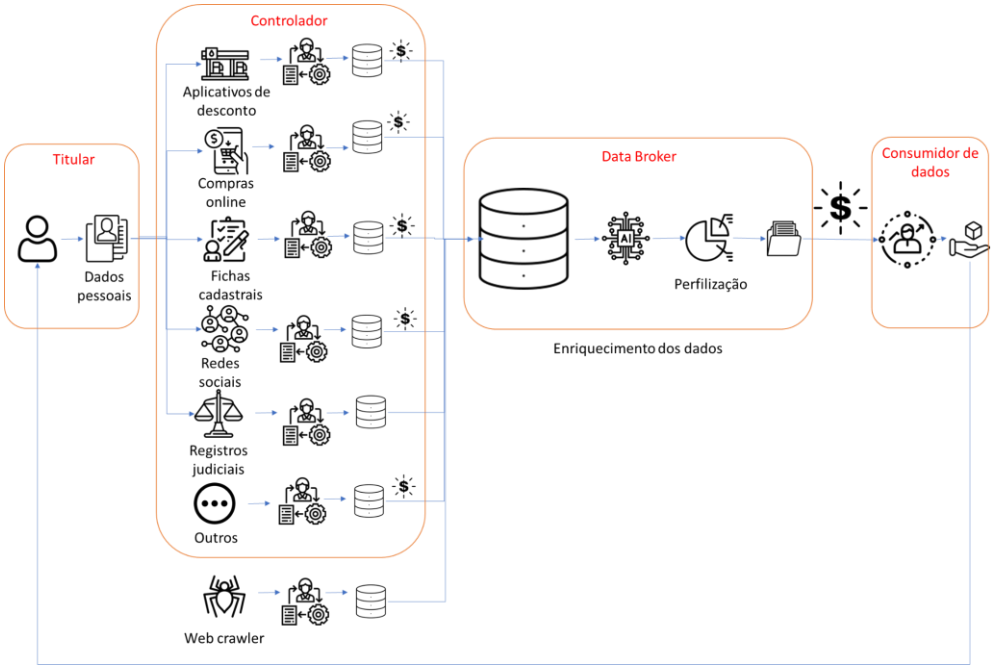


Figura 1: Ilustração do processo de tratamento de dados realizado pelos data brokers.

A atuação dos data brokers movimenta um negócio bilionário de enriquecimento e perfilização de consumidores (ZANATTA; SECAF; MENDONÇA, 2021) e opera um mercado complexo com muitas camadas de corretores que oferecem e trocam dados entre si (FEDERAL TRADE COMMISSION, 2014).kapers

Segundo as principais empresas de segurança na internet (KASPERSKY, s.d.; NORTON, s.d.; MCAFEE, s.d.) as maiores corretoras de dados em atuação são Experian, Equifax, Acxiom e Epsilon que secretamente captam dados de milhões de pessoas e distribuem aos seus clientes. A Axion e Experian, por exemplo, atuam no setor de marketing digital e em relatórios de crédito (CRAIN, 2016). A Grand View Research estimou o tamanho do mercado global de corretores de dados em US$ 277,97 bilhões em 2024 e prevê que deverá atingir US$ 512,45 bilhões até 2033, crescendo a um CAGR de 7,3% de 2025 a 2033 (GVR, 2024).

3 DIREITOS FUNDAMENTAIS IMPACTADOS PELO TRATAMENTO DE DADOS PELOS *DATA BROKERS*

3.1 A natureza constitucional da proteção de dados

A proteção de dados pessoais transcende a noção tradicional de privacidade, sendo considerada um direito fundamental autônomo no ordenamento jurídico brasileiro (SARLET, 2021). O Supremo Tribunal Federal (STF) reconheceu este status em 2020, consolidando que a proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos (BRASIL, 2020). Tal entendimento foi posteriormente positivado pela Emenda Constitucional nº 115, em fevereiro de 2022 (BRASIL, 2022).

Historicamente, a proteção de dados é vista como um desdobramento do direito à privacidade (DONEDA, 2011). O conceito de privacidade evoluiu do simples "direito de estar só" (BRANDEIS; WARREN, 1890) para abarcar o direito de manter o controle das próprias informações (RODOTÀ, 2008).

Os dados pessoais e a privacidade relacionam-se por uma equação onde o maior grau de privacidade está associado à menor difusão de dados pessoais, e vice-versa (DONEDA, 2011). No contexto do Direito, a proteção de dados está predominantemente ligada à dimensão informacional da privacidade, que busca o resguardo de dados e informações dos indivíduos contra o mau uso e os abusos da sua utilização (ARTESE, 2017; PEIXOTO; EHRHARDT JÚNIOR, 2018).

Desses direitos fundamentais decorre o fundamento da autodeterminação informativa, consagrado na LGPD como um de seus fundamentos (BRASIL, 2018, art. 2º, II). Esse direito ou poder garante ao titular a autonomia para deliberar sobre o acesso, uso e difusão de seus dados pessoais, sendo o consentimento livre e informado considerado uma "exigência constitucional estrita" para seu exercício (SARLET, 2021).

Contudo, no cenário de datificação apresentado acima, no qual o cotidiano dos indivíduos é transformado em dados (SILVA, 2019), a discussão sobre a qualificação jurídica dos dados pessoais é crucial. Nesse aspecto, traz-se em pauta as duas principais visões sobre a natureza jurídica dos dados: a Teoria Personalista e a Teoria Realista ou Patrimonial.

Na Teoria Personalista, tem-se o entendimento de que os dados pessoais são um componente da identidade e personalidade das pessoas (ROCHEFELD, 2018). A tutela dos dados é, em essência, a tutela do seu titular, pois os dados são um atributo da personalidade humana. Essa visão busca salvaguardar a pessoa humana em qualquer momento da atividade econômica, sendo um valor máximo do ordenamento (TEPEDINO, 2004). Na Teoria Realista, por sua vez, os dados são um elemento de valor, passível de ser apropriado, coletado e comercializado (ROCHEFELD, 2018).

Facilmente traça-se uma correlação entre a autodeterminação informativa e a Teoria Personalista. Contudo, para Rochefeld (2018), a adoção de uma visão puramente personalista pode ser considerada drástica para o funcionamento da economia. Bioni (2021) acrescenta que a "trava" do consentimento estaria a todo momento bloqueando o fluxo dos dados pessoais e os cidadãos seriam sobrecarregados com tal estratégia normativa, gerando a "fadiga do consentimento" e, consequentemente prejudicando a inovação. Portanto, alguns autores sugerem a patrimonialização gradativa dos dados, estabelecendo que quanto mais ligações os dados tiverem com a pessoa e mais ajudarem a revelar sua identidade, mais devem ser tratados na órbita da proteção jurídica da pessoa singular (ROCHEFELD, 2018).

Duas soluções têm sido adotadas para enfrentar esse impasse. A primeira é a hipótese de legítimo interesse do controlador ou de terceiro, prevista na LGPD. A segunda consiste nas autorizações genéricas incluídas em políticas de privacidade, que os usuários prontamente (ou apressadamente) aceitam para acessar determinado serviço. No entanto, amparados de forma frágil nessas bases legais, muitos agentes de tratamento acabam negligenciando outros dispositivos essenciais da lei, especialmente aqueles relacionados aos direitos e liberdades dos titulares, conforme será tratado mais adiante.

Outro aspecto relevante a ser considerado é que o modelo de negócios predominante, o zero-price advertisement business model, pressupõe que os usuários "pagam" pelos serviços com seus próprios dados pessoais (STRANDBURG, 2020). Sem essa contrapartida oferecida pelo usuário/titular, tais serviços se tornariam pagos, o que poderia inviabilizar o acesso por parte da

população de baixa renda e, consequentemente, reduzir suas oportunidades de participação no mercado (MENDES, 2014).

3.2 A crise autodeterminação e a busca por uma proteção coletiva

Embora o direito à autodeterminação informativa seja reconhecido como fundamental, a crescente complexidade do mercado de dados impulsionou o surgimento da chamada "crise do consentimento". O modelo de autodeterminação informacional, centrado no controle individual sobre os dados pessoais (BIONI, 2016), enfrenta diversos desafios estruturais e cognitivos na sociedade contemporânea.

Do ponto de vista cognitivo, o modelo parte da premissa de um indivíduo plenamente racional e informado; contudo, pesquisas demonstram que as pessoas raramente leem ou compreendem as políticas de privacidade às quais consentem (SOLOVE, 2013).

Além disso, há uma marcante assimetria de poder e de alternativas. Em muitos casos, o consentimento assume caráter meramente formal, pois a recusa em fornecer dados implica, na prática, a impossibilidade de acesso a bens ou serviços, dada a profunda desigualdade entre controlador e titular (BIONI, 2016).

O chamado efeito agregacional evidencia que, embora o consentimento seja prestado em contextos específicos, dados aparentemente inofensivos podem ser combinados e processados de forma a revelar novas informações ou perfis antes desconhecidos, contrariando as expectativas legítimas do titular (SOLOVE, 2006).

Diante desses problemas, o quadro regulatório baseado estritamente na autodeterminação informacional demonstra-se insuficiente para lidar com o contexto dos dados como ativos econômicos (BIONI, 2016).

Para complementar o modelo individual, surge a dimensão coletiva da proteção de dados. A privacidade possui um valor coletivo (codependência), pois o nível de proteção de um indivíduo não depende apenas de suas escolhas isoladas, mas também das decisões de outros agentes sociais (BARUH; POPESCU, 2017).

A proteção coletiva implica a necessidade de retirada de encargos do indivíduo na salvaguarda de suas informações (SCARONI, 2020). Isso se concretiza na abordagem da regulação de risco, que busca identificar e mitigar preventivamente os riscos a direitos e liberdades fundamentais (ZANATTA, 2017).

A LGPD, ao ser interpretada em conjunto com o Código de Defesa do Consumidor (CDC) e os precedentes do Superior Tribunal de Justiça (STJ), reforça a importância da tutela coletiva contra práticas como a discriminação algorítmica, que ofende princípios constitucionais como a dignidade da pessoa humana e a não discriminação (SILVA; CRUZ, 2022). A Lei Geral de Proteção de Dados visa zelar pela proteção dos direitos fundamentais, sendo que a sua verdadeira eficácia advém da integração da legislação (LGPD), do Código Civil e do Código de Defesa do Consumidor (ZANATTA; SECAF; MENDONÇA, 2021).

4 REGULAÇÃO BRASILEIRA DE DADOS PESSOAIS E A ATUAÇÃO DOS DATA BROKERS

4.1 Análise do caso face aos princípios da LGPD

A LGPD exerce impacto direto sobre as operações dos data brokers que tratam informações de cidadãos brasileiros ou que atuam no território nacional (ZANATTA; SECAF; MENDONÇA, 2021). Com sua entrada em vigor, a Lei instaurou um novo paradigma regulatório, impondo uma reconfiguração na lógica do tratamento de dados pessoais. Além disso, ao enunciar, no art. 6º, os princípios que orientam toda a disciplina, a LGPD contribui para suprir lacunas normativas e oferece diretrizes interpretativas para os demais dispositivos legais.

A atuação dos data brokers desafia de maneira transversal os princípios fundamentais da LGPD, revelando um modelo de negócios cuja lógica se distancia significativamente das garantias estruturantes do regime de proteção de dados no Brasil.

A atividade dos data brokers suscita diversos questionamentos quanto à sua compatibilidade com o regime jurídico da proteção de dados pessoais, sobretudo no que diz respeito ao impacto sobre os direitos dos titulares. A começar pelos

princípios da finalidade, adequação e necessidade (LGPD, art. 6, inc. I-III), que formam o núcleo de orientação do tratamento de dados na LGPD, observa-se que tais parâmetros são sistematicamente tensionados por esse modelo de negócio.

Uma vez que os dados são repassados às corretoras de dados, perde-se por completo a cadeia de custódia e, com ela, a capacidade de assegurar que o tratamento permaneça vinculado à finalidade original informada ao titular. Essa ruptura também compromete o princípio da adequação, pois, desconhecido o contexto em que os dados serão utilizados por agentes subsequentes, não há garantias de que o uso mantido pelo data broker ou por seus clientes seja compatível com as expectativas legítimas do titular. Na prática, a própria natureza do negócio pressupõe que o agente intermediário, muitas vezes, desconheça o tratamento específico que será dado aos dados até o surgimento da demanda comercial.

Soma-se a isso o fato de que a lógica intrínseca ao Big Data se mostra profundamente antagônica ao princípio da necessidade e à consequente obrigação de minimização, uma vez que incentiva a acumulação de quantidades exponenciais de dados sem uma finalidade clara e específica.

A esses problemas somam-se desafios igualmente relevantes relacionados aos princípios da transparência, segurança, prevenção , não discriminação e responsabilização e prestação de contas (LGPD, art. 6, inc. VI-X). A histórica opacidade que caracteriza o mercado de data brokers compromete o princípio da transparência (LGPD, art. 6, inc. VI), já que o titular não dispõe de informações claras sobre quem trata seus dados, para quais propósitos, com quais critérios e por quanto tempo. A falta de visibilidade sobre os fluxos de tratamento também dificulta a avaliação das medidas de segurança adotadas ao longo da cadeia, bem como a identificação de riscos e a implementação de medidas preventivas proporcionais. Diante das ramificações e proporção que o negócio pode atingir, não se vislumbra o controle do titular sobre a cadeia de custódia de seus dados pessoais e, portanto, não há que se falar da prerrogativa do titular sobre a possibilidade de ter livre acesso a seus dados ou da possibilidade de exatidão e clareza deles, o que constitui uma clara afronta aos princípios do livre acesso, qualidade dos dados e transparência (LGPD, art. 6, inc. IV-VI).

Além disso, o uso de dados agregados e enriquecidos para fins de segmentação comportamental pode potencializar práticas discriminatórias, ainda que não intencionais, atingindo grupos vulneráveis ou reforçando vieses existentes nos mercados de saúde, crédito e emprego. A própria estrutura fragmentada da atividade, marcada por múltiplos agentes, revendas sucessivas e ausência de contato direto com o titular, fragiliza a responsabilização e dificulta a prestação de contas, tornando incerto quem, em última instância, deve responder pelas violações à LGPD ou pelos danos experimentados pelos titulares.

4.2 Outras potenciais interfaces da LGPD com o *Data Brokers*

Tanto a LGPD quanto a legislação internacional não possuem disposições específicas para lidar com os data brokers (ZANATTA; SECAF; MENDONÇA, 2021), embora especialistas apontem a necessidade premente da regulação dessa matéria.

Embora os princípios da LGPD, examinados anteriormente, atuem como importantes vetores interpretativos, sua natureza ampla e abstrata impõe limites concretos à sua aplicação, especialmente diante de práticas de tratamento altamente dinâmicas e tecnologicamente sofisticadas.

Passemos assim para outros dispositivos da LGPD que podem fornecer subsídios à análise do caso. Para tanto, tomemos como ponto de partida a ilustração da cadeia de custódia da Figura 1. Tudo começa pelo titular dos dados, que fornece suas informações para serem tratadas sob a gestão ou coordenação de um controlador, ou disponibilizam na rede mundial de computadores, tornando-a suscetível de serem capturadas pelos web crawlers. Até esse momento, a hipótese que ampara o tratamento pode ser qualquer uma das elencadas no art. 7º da LGPD.

Descartando as hipóteses de tratamento direcionadas para aspectos de obrigação legal, execução de políticas públicas, pesquisa, exercício regular de direitos, proteção da vida e da saúde — dispostas nos incisos II a VIII do art. 7º da LGPD — passemos a uma análise mais minuciosa sobre a aplicabilidade do

consentimento (art. 7º, I) e do interesse legítimo (art. 7º, IX) para o caso dos data brokers.

No que se refere ao consentimento, a LGPD estabelece que ele precisa ser livre, informado, inequívoco e específico para uma finalidade determinada (art. 5º, XII). Assim, o consentimento não é uma "carta branca" que, uma vez concedido, autoriza qualquer tratamento para os mais diversos propósitos. Na lógica da cadeia de custódia ilustrada na Figura 1, ainda que o tratamento pelo primeiro controlador seja feito com base no consentimento, esse consentimento não se estende a tratamentos distintos do originalmente contratado. No caso de outros tratamentos — sejam eles pelo mesmo controlador ou por terceiros —, um novo consentimento deveria ser obtido de cada titular. Na lógica do modelo de negócios dos data brokers, isso é praticamente inviável, considerando o volume de dados tratados, o que inviabiliza o próprio tratamento.

Como bem coloca Bruno Bioni (2021), o Big Data é incompatível com a dinâmica normativa da autodeterminação informacional, na medida em que permite que um volume descomunal de dados seja estruturado e analisado para uma gama indeterminada de finalidades.

A posição dos titulares de dados no ambiente digital é fragilizada pela assimetria de poder inerente à relação com os agentes de tratamento. Consequentemente, o consentimento frequentemente se configura como uma ficção jurídica, dado que a adesão aos termos se torna condição sine qua non para acessar serviços e produtos que são, muitas vezes, essenciais. Somado a isso, o advento de novas tecnologias dificulta que o indivíduo consiga antever ou controlar, no ato da coleta, os riscos futuros decorrentes do uso e da agregação desses dados, conforme argumentam Mendes e Fonseca (2020).

A complexidade e a opacidade inerentes ao mercado de data brokers, somadas à lógica do Big Data de coletar volumes exponenciais de dados tratados acima, demonstram que o modelo da autodeterminação informacional baseado primariamente no consentimento individual é insuficiente para garantir a proteção efetiva dos direitos fundamentais.

Descartando-se a hipótese do consentimento para o modelo de negócio dos data brokers, seguimos à análise da segunda possível base legal de tratamento: o interesse legítimo.

Para muitos, o legítimo interesse é visto como um "coringa", estrategicamente posicionado, como a última hipótese legal do art. 7º, para os casos em que o controlador não consiga se enquadrar em nenhuma das hipóteses anteriores. Indiscutivelmente, trata-se de uma base mais flexível.

Segundo Frazão (2022), trata-se da hipótese mais controversa, especialmente no que diz respeito às métricas ou parâmetros que possam justificar o tratamento de dados por interesse (comercial) do agente de tratamento, diante de potenciais prejuízos aos direitos e liberdades fundamentais do titular. Nesse aspecto, o legislador, a fim de evitar abusos do legítimo interesse, trouxe no art. 10 certa delimitação para o uso dessa hipótese de tratamento de dados, nos seguintes termos:

> **Art. 10.** O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> I - apoio e promoção de atividades do controlador; e
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
> § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu legítimo interesse, observados os segredos comercial e industrial.

Os dispositivos dos incisos I e II são extremamente vagos e amplos. De fato, o inciso I pouco acrescenta à hipótese legal do art. 7º. No entanto, quando combinado com o inciso II, reforça as premissas da LGPD, trazendo para o centro da discussão o objetivo da lei: proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural (LGPD, art. 1º). Além disso, os parágrafos subsequentes reforçam a necessidade de

limitação do tratamento aos dados estritamente necessários para a finalidade pretendida e a obrigação de transparência sobre esse tratamento.

Contudo, nesse mercado, o valor econômico dos dados reside primariamente em seu uso secundário, ou seja, na reutilização de informações geradas para um propósito posterior, muitas vezes indefinido. Ou seja, se o cliente do *data broker* for uma empresa do ramo do comércio, os dados serão tratados de modo a extrair o perfil de consumo do titular; se for da área da saúde, serão analisados hábitos alimentares, práticas esportivas e assim por diante. Na medida em que esses dados são repassados para terceiros, neste caso os data brokers, não há garantias de que o tratamento será fiel à especificidade inicialmente informada, sequer haverá um controle da cadeia de custódia.

Além disso, os dados tornam-se exponencialmente mais valiosos quando submetidos ao armazenamento e processamento automatizado. Essa dinâmica, que é a essência do *Big Data*, coloca-se em antagonismo direto com a lógica da proteção de dados, especialmente no que tange ao disposto no art. 20 da Lei (grifo nosso):

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas **unicamente com base em tratamento automatizado de dados** pessoais que **afetem seus interesses**, incluídas as decisões destinadas a definir o seu **perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.**

5 PERSPECTIVAS FUTURAS: UM LONGO CAMINHO A SER PERCORRIDO

5.1 O papel da ANPD

A responsabilidade por colocar em prática a LGPD recai sobre a Autoridade Nacional de Proteção de Dados (ANPD), conforme disposto no art. 55-J da lei. Trata-se de uma instituição ainda jovem no cenário regulatório brasileiro, cuja atuação vem sendo gradualmente estruturada por meio da edição de regulamentos, guias orientativos e publicações técnicas que buscam estabelecer as bases operacionais para a adequada implementação da LGPD. Embora a Lei possua natureza autoaplicável, a ANPD é a instituição capaz de estabelecer critérios

objetivos para atividades de tratamento de alto risco, muitas das quais envolvem diretamente data brokers, sobretudo quando seus bancos de dados são utilizados para fins de segmentação comportamental, enriquecimento de perfis, marketing direcionado ou como insumo para sistemas de inteligência artificial. A autoridade também pode fomentar instrumentos específicos, tais como códigos de conduta, selos de conformidade, guias de boas práticas e modelos de due diligence, que permitam trazer maior previsibilidade e responsabilidade a um mercado historicamente marcado pela ausência de controle.

Não se descarta, nessa lógica, a necessidade de interpretar a LGPD em conjunto com outros diplomas normativos que compõem o arcabouço jurídico brasileiro de proteção ao titular de dados, em especial A Lei nº 8.078/1990 - Código de Defesa do Consumidor, (BRASIL, 1990) e a Lei nº 12.965/2014 - Marco Civil da Internet (BRASIL, 2014).

5.2 Regulação de risco e tutela coletiva

O paradigma da proteção de dados deve ser complementado pela regulação de risco, que representa uma guinada teórica (ZANATTA, 2017) em relação à proteção individual. A regulação de risco implica:

- **Identificação de Riscos *Ex Ante*:** O tratamento de dados pessoais traz riscos aos direitos fundamentais que devem ser identificados e mitigados por mecanismos preventivos. A ANPD pode exigir o Relatório de Impacto à Proteção de Dados Pessoais (LGPD, art. 38) quando o tratamento implicar alto risco (LGPD, art. 55-J, XIII).
- **Gestão e Mitigação:** A regulação de risco pressupõe a disseminação de métodos de gestão de riscos (ZANATTA, 2017) e a adoção de medidas que busquem a remoção do ilícito (ZANATTA; SECAF; MENDONÇA, 2021).

5.3 *Accountability*

Para lidar com a crise do consentimento, é crucial a implementação de obrigações e instrumentos regulatórios que fortaleçam a responsabilidade demonstrável (accountability) das empresas, o que está intimamente ligado ao modelo de regulação de risco.

O accountability corresponde à adoção de políticas de privacidade compatíveis com a lei e princípios, mecanismos de desempenho, transparência e avaliação de risco (CENTER FOR INFORMATION POLICY LEADERSHIP, 2015). É um dever do controlador e operador que implica na capacidade de comprovar a observância e o cumprimento das normas (LGPD, art. 6º, IX). Quanto mais sensível ou derivado for o dado, maior é a necessidade de accountability.

Já o privacy by design é uma abordagem preventiva (LGPD, art. 46, § 1º) que propõe a integração da proteção de dados no design e arquitetura de produtos e serviços (HUSTINX, 2010; ZANATTA; SECAF; MENDONÇA, 2021). Embora enfrente desafios como a relutância das organizações em implementá-la, ela é fundamental para a proteção dos dados pessoais.

5.4 O papel estratégico da educação digital e da autorregulação

A proteção de dados pessoais não depende apenas da legislação, mas de uma abordagem preventiva que incorpore mecanismos de proteção pelos próprios agentes econômicos.

A educação digital e a conscientização são cruciais para que a população possa exercer um controle mais profundo sobre o funcionamento das tecnologias e os reais impactos que elas apresentam.

O desconhecimento dos consumidores sobre a existência e as práticas dos data brokers (VERBICARO; VIEIRA, 2021) reforça a assimetria informacional (FRAZÃO, 2020). Portanto, é necessário conscientizar as pessoas sobre o valor dos seus dados, visto que muitos não refletem que, ao aceitar termos de uso de privacidade, estão consentindo com a coleta de dados que serão inseridos no mercado.

A própria Autoridade Nacional de Proteção de Dados (ANPD) reconhece a necessidade de Ações Educativas (ANPD, 2023), pois a qualidade dos requerimentos recebidos (denúncias e petições) em 2022 foi prejudicada pela falta de cumprimento dos requisitos pelos titulares.

A implementação de mecanismos de autorregulação e responsabilidade demonstrável por parte das empresas é fundamental para a proteção dos dados pessoais.

A LGPD prevê a importância da adoção de política de boas práticas e governança (art. 52, § 1º, IX) e de mecanismos capazes de minimizar o dano (art. 52, § 1º, VIII). O uso de privacy by design e a documentação de riscos (accountability) são formas de cumprir com esses princípios.

Em dados mais próximos do derivado ou inferido (como os gerados por data brokers), a consciência do titular e, consequentemente, o consentimento, perdem significado, tornando a responsabilidade demonstrável da empresa mais necessária (ARTESE, 2017).

Dessa forma, o papel da ANPD é essencial para guiar a autorregulação e a conformidade, atuando como instância regulatória que emite opiniões técnicas específicas para a proteção de dados. A Autoridade também pode editar normas, orientações e procedimentos simplificados para startups e microempresas, conforme disposto no Decreto n° 10.474/2020, art. 2°, XVIII (BRASIL, 2020).

O mais importante é entender que a força normativa do direito aplicado aos data brokers é proveniente da leitura integrada da LGPD com o Código Civil e a Lei n° 8.078/90, interpretando-se os bons precedentes construídos pelo Superior Tribunal de Justiça (STJ) (ZANATTA; SECAF; MENDONÇA, 2021).

A perspectiva futura exige, portanto, a implementação de modelos teóricos complementares (SILVA, 2019), focados na tutela coletiva e em deveres impostos aos agentes de tratamento.

6 CONCLUSÃO

A sociedade da informação, impulsionada pelo fenômeno dos data brokers, consolidou os dados pessoais como o ativo econômico mais valioso, intensificando a coleta e a comercialização em volumes exponenciais (SILVA, 2019).

Esse funcionamento, que é marcado pela opacidade, expõe os titulares dos dados a graves riscos, tais como perfilização ilícita e a violação da privacidade (ZANATTA; SECAF; MENDONÇA, 2021). O desafio central reside no controle sobre a forma de utilização dos dados, e não em que são utilizados.

Em que pese a Lei Geral de Proteção de Dados (LGPD) represente um avanço elementar no ordenamento jurídico brasileiro, tornando a proteção de dados pessoais um direito fundamental autônomo (SARLET, 2021; SILVA; CRUZ, 2022), o modelo de negócios dos data brokers apresenta incompatibilidades com seus princípios. Destacando-se a prática de uso secundário de dados como expressamente vedada pelo princípio da finalidade (LGPD, art. 6°, I).

A adoção do modelo da autodeterminação informativa, embora louvável (SILVA, 2019), se demonstra insuficiente para resolver os problemas estruturais e cognitivos da sociedade da informação. A dita "fadiga do consentimento" é consequência direta disso. Aliado à isso, ocorre uma falsa sensação de controle (SILVA, 2019). Dessa forma, torna-se imperioso retirar o ônus de proteção do titular.

Neste diapasão, a proteção efetiva dos direitos fundamentais exige que o modelo individual de proteção de dados seja complementado pela dimensão coletiva, adotando-se uma regulação de risco e um fortalecimento da responsabilidade demonstrável (accountability) dos agentes de tratamento (SILVA, 2019).

A materialização da estratégia preventiva, sempre balizada pelo comando constitucional de equilíbrio entre a promoção da inovação e a tutela dos direitos (conforme o Art. 2º da LGPD), evidencia-se na adoção de três vetores prioritários:

1. **Promoção de Inovação Responsável:** Essa regulação tem como objetivo gerar segurança jurídica e diretrizes éticas para inovação, de forma a proporcionar compatibilidade entre tratamento de dados com os direitos fundamentais e a não discriminação.

2. **Superação da Crise de Consentimento:** Modelos complementares devem ser os responsáveis por implementar a proteção, como o *Privacy by Design* (SILVA,2019), e, independentemente de prova de dano individual, uma regulação que coíba o ilícito estrutural (ZANATTA; SECAF; MENDONÇA, 2021)

3. **Segurança Jurídica para o Mercado:** A legislação e o diálogo das fontes fornecem a base para que os agentes de tratamento cumpram suas obrigações, exigindo uma interpretação das normas pautada em seus princípios e fundamentos, e não apenas em checklists de conformidade.

Em suma, a difícil missão de proteger os dados pessoais exige a integração entre a lei, técnicas preventivas e a promoção de transparência e confiança, sob a óptica de preocupação coletiva (SILVA, 2019). Havendo esse arcabouço teórico-pragmático, guiado por uma ANPD independente, será possível conciliar a tutela de dados pessoais e o desenvolvimento econômico, podendo-se haver benéfices da reutilização de dados sem haver detrimento dos direitos fundamentais.

REFERÊNCIAS

ABRAMOVAY, Ricardo. Commodities na era da economia de dados. **Valor Econômico**, n. 110, p. 27, 2019. Disponível em: https://valor.globo.com/mundo/blog-do-fmi/post/2019/09/a-economia-dos-dados.ghtml. Acesso em: 14 out. 2025.

ARTESE, Gustavo. Privacidade e proteção de dados pessoais: a diluição do consentimento e a responsabilidade demonstrável (accountability). **Revista Fórum de Direito na Economia Digital: RFDED**, Belo Horizonte, ano 1, n. 1, p. 141-162, jul./dez. 2017.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Relatório de Atividades Realizadas - 2022**. Publicação digital, Brasília: ANPD, ago. 2023.

BARUH, Lemi; POPESCU, Mihaela. Big data analytics and the limits of privacy self-management. **New Media & Society**, v. 19, n. 4, p. 579-596, 2017.

BIONI, Bruno R. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: **Forense**, 2020.

BIONI, Bruno Ricardo. Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. 2016. Dissertação (Mestrado em Direito) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2016.

BRANDEIS, Louis D.; WARREN, Samuel D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, dez. 1890.

BRASIL. [Decreto]. Decreto nº 10.474, de 26 de agosto de 2020. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados (ANPD)... **Diário Oficial da União**, Brasília, DF.

BRASIL. [Emenda Constitucional]. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e o rol de competências privativas da União. Diário Oficial da União, Brasília, DF.

BRASIL. [Lei]. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências (Código de Defesa do Consumidor - CDC). **Diário Oficial da União**, Brasília, DF.

BRASIL. [Lei]. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). **Diário Oficial da União**, Brasília, DF.

BRASIL. [Lei]. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF.

BRASIL. Supremo Tribunal Federal. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387. Relatora: Min. Rosa Weber. Julgamento em: 07 mai. 2020. Publicado em: 12 nov. 2020.

CARRIÈRE-SWALLOW, Yan; HAKSAR, Vikram. A economia dos dados. Blog do FMI – **Valor Econômico**, 24 set. 2019. Disponível em: https://valor.globo.com/mundo/blog-do-fmi/post/2019/09/a-economia-dos-dados.ghtml. Acesso em: 15 out. 2025.

CENTER FOR INFORMATION POLICY LEADERSHIP (CIPL). **The CIPL Accountability Framework**. 2015.

CRAIN, Matthew. The limits of transparency: Data brokers and commodification. **New Media & Society**, v. 20, n. 1, 2016. Disponível em: https://doi.org/10.1177/1461444816657096. Acesso em: 15 out. 2025.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, n. 2, p. 91-108, jul./dez. 2011.

FEDERAL TRADE COMMISSION (FTC). **Data Brokers: A call for Transparency and Accountability**. Washington, D.C.: FTC, 2014. Disponível em: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf. Acesso em: 14 out. 2025.

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 (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. p. 23-52.

FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. **Curso de Proteção de Dados - Fundamentos da LGPD**. Rio de Janeiro: Forense, 2022.

GRAND VIEW RESEARCH. **Data broker market report**. Disponível em: https://www.grandviewresearch.com/industry-analysis/data-broker-market-report. Acesso em: 15 out. 2025.

HUSTINX, Peter. Privacy by design: delivering the promises. **Identity in the Information Society**, v. 3, n. 2, p. 253-255, 2010. Disponível em: https://link.springer.com/content/pdf/10.1007/s12394-010-0061-z.pdf.

KASPERSKY. How to stop data brokers from selling your personal information. Disponível em: https://www.kaspersky.com/resource-center/preemptive-safety/how-to-stop-data-brokers-from-selling-your-personal-information. Acesso em: 15 out. 2025.

MCAFEE. What is a data broker?. Disponível em: https://www.mcafee.com/blogs/tips-tricks/what-is-a-data-broker/. Acesso em: 15 out. 2025.

MENDES, Laura Schertel. Privacidade, proteção de dados pessoais e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: **Saraiva**, 2014.

MENDES, Laura Schertel; FONSECA, Luísa Ferreira Leite. O direito à proteção de dados e a crise do consentimento. **Revista Brasileira de Direito Civil**, v. 23, n. 1, p. 101-125, 2020.

NORTON. Data brokers. Disponível em: https://us.norton.com/blog/privacy/data-brokers. Acesso em: 15 out. 2025.

PEIXOTO, Fabrício B.; EHRHARDT JÚNIOR, Marcos. A proteção de dados pessoais e o consumidor na sociedade da informação. In: PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. São Paulo: Saraiva Educação, 2018. p. 43-63.

ROCHEFELD, Judith. Como qualificar os dados pessoais? Uma perspectiva técnica e normativa da União Europeia em face dos gigantes da Internet. **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 10, n. 1, p. 61-84, maio 2018.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RUSCHEMEIER, Hannah. Data Brokers and European Digital Legislation. **EDPL European Data Protection Law Review**, v. 9, p. 27-38, 2023. Disponível em: https://ssrn.com/abstract=4521470. DOI: 10.21552/edpl/2023/1/7. Acesso em: 15 out. 2025.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: MENDES, Laura Schertel et al. (Coords.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

SCARONI, Rafael Garcia. **A mercadoria é você: o uso secundário dos dados pessoais**. Trabalho de Conclusão de Curso (Graduação em Ciências Jurídicas e Sociais) - Faculdade de Direito, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2020.

SILVA, Michael César; CRUZ, Rayenne dos Santos Lima. Responsabilidade civil e novas tecnologias: discriminação algorítmica, proteção ao consumidor e Lei Geral de Proteção de Dados. **Revista Jurídica Luso Brasileira**, Lisboa, Ano 8, n. 6, p. 1645-1683, 2022.

SILVA, Mayara Rocumback Vieira da. A proteção de dados pessoais e seus desafios regulatórios. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, v. 114, p. 791-815, jan./dez. 2019.

SOLOVE, Daniel J. A taxonomy of privacy. **University of Pennsylvania Law Review**, v. 154, p. 477-560, jan. 2006.

SOLOVE, Daniel J. The myth of privacy consent. **George Washington Law Review**, v. 81, p. 1883-1913, 2013.

STRANDBURG, Katherine J. Free Fall: The Online Market's Consumer Preference Disconnect. 2020. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2323961. Acesso em: 14 out. 2025.

TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil-constitucional brasileiro. In: TEPEDINO, Gustavo. **Temas de direito civil**. 3. ed. Rio de Janeiro: Renovar, 2004.

VERBICARO, Dennis; VIEIRA, Janaína. A nova dimensão da proteção do consumidor digital diante do acesso a dados pessoais no ciberespaço. **Revista de Direito do Consumidor**, São Paulo, v. 134, n. 30, p. 195-226, mar./abr. 2021.

ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação do risco: uma nova moldura teórica? In: **I Encontro da Rede de Pesquisa em Governança da Internet**, 14 nov. 2017.

ZANATTA, Rafael A. F.; SECAF, Helena; MENDONÇA, Julia. A aplicabilidade da Lei Geral de Proteção de Dados Pessoais aos corretores de dados. In: VILLAS BOAS CUEVA, Ricardo; FRAZÃO, Ana. **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters, 2021, p. 957-988.

ENGENHARIA SOCIAL E VULNERABILIDADES HUMANAS: COM A LEI GERAL DE PROTEÇÃO DE DADOS CONTRIBUI PARA A CIBERSEGURANÇA

Nicolle de Castro Oliveira[1]
Victor Matias Andrade Monteiro[2]

RESUMO

Este trabalho visa apresentar a Lei nº 13.709/2019, Lei Geral de Proteção de Dados (LGPD) e o conceito de engenharia social, destacando como a LGPD pode ser aplicada para combater o crimes cibernéticos, que utilizam da engenharia social, em suas diversas modalidades, além de traçar o perfil da vítima procurada pelos criminosos e como essas pessoas podem se proteger de forma preventiva, buscando amparo legal na aludida legislação. Com esse intuito, este artigo apresenta um acórdão do Tribunal de Justiça do Distrito Federal e Territórios (TJDFT) que utiliza da legislação supracitada como arcabouço jurídico para combater ativamente a prática da atividade criminosa, bem como garantir o direito à reparação civil da vítima e a responsabilização das plataformas digitais por negligenciar procedimentos de segurança, atentando contra a proteção dos usuários.

Palavras-chave: Lei Geral de Proteção de Dados (LGPD); Cibersegurança; Engenharia social; Phishing; Proteção de dados pessoais; Crimes cibernéticos.

SUMÁRIO: Introdução. 1. Função e aplicação da LGPD; 1.1. Desenvolvimento; 1.2. Aplicação em casos concretos; 2. Engenharia social; 2.1. Aplicação; 3. Phishing; 3.1. Aplicação; 3.2. Meios de Proteção; 3.3. Grupos vulneráveis; 3.4. Realidade socioeconômica das vítimas; 3.5. Discussão; Conclusões; Referências.

1 INTRODUÇÃO

O avanço das tecnologias digitais e a expansão do acesso à internet transformaram as relações sociais e profissionais, mas também aumentaram a exposição dos usuários a riscos cibernéticos. Entre as práticas mais recorrentes está a

[1] Graduando em Direito do UniCEUB - Centro Universitário de Brasília.
[2] Graduando em Direito do UniCEUB - Centro Universitário de Brasília.

engenharia social, que explora a vulnerabilidade humana e o desconhecimento sobre os meios digitais para obter dados e informações das potenciais vítimas.

Nesse contexto, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), surge como instrumento essencial para a proteção da privacidade e da segurança das informações, estabelecendo diretrizes para o tratamento de dados por pessoas físicas e jurídicas e ressaltando a responsabilização e a necessidade de reparação em casos de atividade ilícita.

Este artigo tem como objetivo analisar de que forma a LGPD contribui para o fortalecimento da cibersegurança, especialmente no combate a crimes baseados na engenharia social. Conjuntamente, busca-se compreender o perfil social e econômico das vítimas e como essa espécie de crime cibernético opera, promovendo maior conscientização sobre a importância da proteção de dados no ambiente digital.

1 FUNÇÃO E APLICAÇÃO DA LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD), N° 13.709, vigorada no segundo semestre de 2018, tem sua disposição prevista no Artigo 1°: "sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

1.1 Desenvolvimento

Seu desenvolvimento tem como inspiração o avanço do contexto global de digitalização e demandas nacionais por maior proteção da privacidade dos indivíduos, criando um marco jurídico no país de regulamentação e tratamento de dados pessoais. Com o crescimento exponencial do volume de dados coletados virtualmente, vazamento de dados bancários, de saúde e cadastros públicos, os usuários demandaram mais que apenas leis sensoriais. A União Europeia com o Regulamento Geral de Proteção de Dados (GDPR) foi a referência direta para o nascimento da LGPD. Seus objetivos estão concentrados em garantir o direito

fundamental à privacidade e proteção de dados pessoais, estabelecendo regras claras para coleta, armazenamento e compartilhamento de dados, responsabilizando empresas e órgãos públicos no tratamento dessas informações, harmonizando a legislação brasileira com os padrões internacionais, permitindo mais competitividade e confiança em negócios globais.

1.2 Aplicação em casos concretos

O Banco Central (BC), no âmbito das suas competências, trabalha com dados pessoais de diversos tipos e naturezas para desenvolver suas atividades. O BC recebe os dados pessoais do cliente por três tipos de vias: quando os usuários acessam os serviços digitais, quando as instituições financeiras enviam, ou quando os órgãos públicos compartilham. O Banco Central trata os dados pessoais para cumprir leis ou políticas públicas, identificar problemas em serviços, melhorar a navegação ou até dar proteção ao crédito. As medidas de segurança adotadas pelo BC consistem em cumprir a LGPD e normas correlatas, compartilhar dados com outros órgãos em observância à lei, por determinação judicial, ou em contratos, convênios ou instrumentos similares, determinando que as empresas contratadas sigam a Política de Privacidade, enviando email somente em resposta a contato prévio ou para cumprir lei ou política pública, permitindo tratamento de dados apenas por profissionais especializados e treinados e guardando os dados em locais seguros e privados. Acessando o Relatório de Impacto à Proteção de Dados Pessoais, disponibilizado pelo Banco Central, os clientes podem saber quais ações estão sendo adotadas para fortalecer os controles e sistemas de proteção de dados.

2 ENGENHARIA SOCIAL

A engenharia social é um gênero de manipulação onde o agente usufrui da inocência e fragilidade de usuários virtuais para acessarem contas, dados, senhas e endereços sigilosos. É cometido majoritariamente no meio virtual, mas pode alcançar a vítima por outros meios de comunicação, como por ligações ou abordagens psicológicas. Seus alvos incluem pessoas vulneráveis tecnologicamente, que creem estar contribuindo para pesquisas, confirmação de informações ou resgate

de acesso digital. Sua influência é arquitetada com base no comportamento do usuário, permissão de cookies (pequenos arquivos de texto que um site salva no dispositivo do usuário para armazenar informações sobre a navegação) e gostos particulares, alinhado com suas possíveis respostas ao ataque, focando em difícil reconhecimento de ameaças.

2.1 Aplicação

Digitalmente, os executores premeditam cenários onde os lesados devem aceitar ou ceder suas informações particulares, gozando dos direitos e capacidades resguardadas. Alguns casos apontam propagação de malwares, programas desenvolvidos para danificar, interromper ou obter acesso não autorizado a sistemas de computador, como vírus, para conduzir, coletar ou criptografar maliciosamente os dados dos afetados. Um famoso caso de malware foi o "Cavalo de Troia Zeus" ou "Zbot", focado no sistema operacional Microsoft Windows, onde cria-se um botnet (rede de computadores ou dispositivos infectados, controlados remotamente por um criminoso cibernético para realizar ataques e aplicar golpes) que dá permissão ao proprietário para coletar grande quantidade de informações, moderado por um servidor de comando e controle administrativo secreto a uma rede de computadores corrompidos. Seus redirecionamentos de serviços financeiros, roubando credenciais bancárias das máquinas infectadas, são feitos monitorando sites e registrando pressionamentos de teclas, reconhecendo o login do usuário. Seus métodos de infecção consistem em envios de mensagens de spam (mensagem eletrônica não solicitada e em massa, enganosos ou maliciosos, enviada por email, SMS, redes sociais ou outras plataformas) por email e execuções de downloads, processo de transferir dados de um sistema remoto para um dispositivo local. A autenticação de dois fatores é uma das formas de impedimento de invasão desse malware, visto que versões atuais podem ser encontradas em diversos dispositivos móveis, como Android e Apple (sistemas operacionais).

3 PHISHING

É uma prática da engenharia social baseada no ganho da confiança da vítima pelo golpista, que aprende seus hábitos e ambientes virtuais frequentados. Criando uma confusão de acesso, por link (elemento clicável em uma página da web, que direciona você para outro local online quando clicado) de site ou email, que aparenta ser legal, o agente influencia o usuário a disponibilizar seus dados pessoais e financeiros. A fraude é consumada quando a vítima fornece o dado necessário, muitas vezes ligado à contas financeiras, configurando o crime de estelionato.

3.1 Aplicação

Por meio de envio de emails falsos ou links com direcionamento suspeito, o agente conduz a vítima para um ambiente virtual simulado, como sites (endereço eletrônico) governamentais ou bancários, fazendo-o preencher dados pessoais e armazenando-os para utilizá-los nos sites oficiais. Ressalta-se a semelhança entre os sites autênticos das entidades governamentais e os criados com intuito fraudulento, esse utilizando de imagens oficiais e URL (forma padronizada de representação de diferentes documentos, mídia e serviços de rede na internet, capaz de fornecer a cada documento um endereço único) semelhante, sendo diferenciado do oficial apenas por uma letra ou um ponto, dificultando a percepção do golpe, principalmente para as vítimas mais vulneráveis. Corroborando com as ferramentas visuais utilizadas para mascarar o link ou email falsos, os criminosos se fazem valer do senso de urgência do destinatário para diminuir o senso de atenção, como por exemplo, com o uso de mensagens sobre a necessidade de envio de dados pessoais para autenticar o proprietário da conta bancária, devido uma tentativa de invasão.

3.2 Meios de proteção

Endereços de email com nomes aleatórios, erros ortográficos ou sites não autênticos são sinais de tentativa de invasão por embustes. Para prevenção e combate, os próprios softwares, conjunto de instruções, dados ou programas que dizem a um computador ou outro dispositivo como executar tarefas específicas, oferecem proteção conforme suas atualizações e antivírus próprios, além de sites fornecerem logotipos, informações para contato e captcha, verificação em duas

etapas, para login. A autenticação de dois fatores, que funciona como um segundo passo para acesso à uma conta, tem como opções geradores de senhas aleatórias eficientes e fornecimento de tokens de hardware (dispositivos de segurança externos que são conectados ao computador) de uma empresa para funcionários, muitas vezes como forma de chaveiro, que produz códigos a cada intervalo de tempo, sendo uma das formas mais antigas de autenticação. Ademais, companhias utilizam de emails corporativos, tais como Microsoft 365 ou Google Workspace, que garantem proteções avançadas. Empresas legítimas sempre alertam e esclarecem não solicitarem informações pessoais por meios de comunicação informais.

3.3 Grupo de vulneráveis

Conforme consulta realizada pelo Instituto de Pesquisa DataSenado em 2025, que entrevistou mais de 22 mil pessoas, os mais afetados por golpes virtuais são jovens entre 16 e 29 anos, 27% das vítimas. Esse dado contraria o senso comum, de que os mais vulneráveis, os idosos, seriam os mais afetados, porém estes correspondem a 16% das vítimas. Essa informação encontra embasamento no nível de exposição à internet dos entrevistados, apontando que o público jovem sofre mais golpes digitais por estarem conectados por períodos maiores em comparação aos idosos, dado comprovado segundo pesquisa realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic), ligado a Unesco, que aponta que 99% do público entre 16 e 24 anos declararam utilizar a internet todos os dias ou quase todos os dias, enquanto essa porcentagem reduz para 88% quando se trata dos idosos.

3.4 Realidade socioeconômica das vítimas

Outro importante dado da consulta revela uma maior incidência de golpes virtuais em pessoas que recebem até 2 salários mínimos, 51% dos entrevistados, possuindo as vítimas, em 35% dos casos, apenas o ensino médio completo, revelando o público alvo procurado pelos criminosos virtuais. Outro perfil buscado pelos cibercriminosos são indivíduos em situação de endividamento, devido às tentativas de regularização da situação financeira, momento esse que os golpistas

aproveitam para enviar boletos, chaves PIX e links falsos com a promessa e quitação ou renegociação da dívida, conforme relata o presidente da Associação Brasileira de Defesa dos Clientes e Consumidores de Operações Financeiras Bancárias, Raimundo Nonato Filho.

3.5 Discussão

A Lei Geral de Proteção de Dados está servindo de base jurídica para decisões que combatem ativamente os cibercrimes, como o apresentado no Acórdão 2023743, 0704490-21.2025.8.07.0020, do relator juiz MARCO ANTONIO DO AMARAL, da Terceira Turma Recursal dos Juizados Especiais do Tribunal de Justiça do Distrito Federal e Territórios (TJDFT).

O recurso consiste na tentativa da parte ré de afastar a responsabilidade pelo pagamento indevido de boleto bancário pela parte autora, uma vez que, segundo a defesa, a fraude foi perpetuada por terceiro em favor próprio, não havendo participação da empresa ou de seus colaboradores na ação ilícita. Porém o tribunal decidiu por manter a responsabilidade objetiva da parte devido ao vazamento de dados da vítima e das informações sobre o contrato de prestação de serviço necessários para a confecção do boleto falso. Outro fato destacado no acórdão foi a forma de acesso à forma de pagamento da mensalidade do serviço prestado pelo réu, pois estava na plataforma oficial, sendo inclusive necessário uso de login e senha para obter o boleto, tornando o aparente mais digno de confiança, justificando o pagamento. Não obstante, também foi apontada a situação de vulnerabilidade da autora, por se tratar de uma idosa de 72 anos de idade, o que presume um desconhecimento relativo sobre o uso de plataformas digitais e acerca da identificação da prática de cibercrimes como o phishing.

O tribunal decidiu, com base nos Artigos 42, 43 e 44 da LGPD, que tratam sobre a responsabilidade e do ressarcimento de danos quando as normas expressas na legislação pertinente não são seguidas e quando não for oferecida a segurança que o titular pode esperar, rejeitar o recurso, mantendo a responsabilidade da prestadora de serviço pelo golpe realizado por terceiro.

4 CONCLUSÃO

A crescente sofisticação dos crimes cibernéticos, especialmente aqueles baseados na engenharia social, evidencia a vulnerabilidade humana como ponto central da segurança digital. Diante desse cenário, a Lei Geral de Proteção de Dados desempenha papel fundamental não apenas na prevenção, mas também na proteção e reparação das vítimas após a ocorrência do delito.

A LGPD estabelece responsabilidades objetivas para os agentes de tratamento de dados, impondo-lhes o dever de adotar medidas técnicas e administrativas capazes de assegurar a integridade e o sigilo das informações pessoais. Quando ocorre o vazamento ou uso indevido de dados, a legislação garante ao titular o direito à reparação civil, conforme os Artigos 42 a 44, da Lei Geral de Proteção de Dados, reforçando o amparo jurídico das vítimas e promovendo a responsabilização das instituições envolvidas.

Assim, a LGPD representa também um instrumento de proteção após a violação, que ampara o cidadão lesado, assegurando transparência, prestação de contas e justiça. Além disso, incentiva organizações a investirem em políticas de segurança da informação e educação digital, reduzindo a reincidência de ataques e fortalecendo a confiança nas relações virtuais. Evidencia-se, portanto, que a efetividade da aludida legislação, aliada à conscientização dos usuários por meio do acesso à informação, constituem um pilar essencial para o fortalecimento da cibersegurança e da proteção no ambiente virtual, no contexto brasileiro.

REFERÊNCIAS

FORNASIER, Mateus de Oliveira. KNEBEL, Norberto Milton Paiva. SILVA, Fernanda Viero da. Phishing e engenharia social: entre a criminalização e a utilização de meios sociais de proteção. **Revista Meritum**, Belo Horizonte, vol. 15, n. 1, p. 116-129, jan./abr. 2020. DOI: https://doi.org/10.46560/meritum.v15i1.7771

FALLA, Diego Augusto Aparecido; PINTO, Giuliano Scombatti. Engenharia social e a importância da cibersegurança na atualidade. **Interface Tecnológica**, v. 20, n. 2, 2023. DOI: https://doi.org/10.31510/infa.v20i2.1759

RIBEIRO, Bárbara Ianca Zanaqui; CASATI, Lucia Helena de Oliveira. **Uma análise da LGPD com foco em Engenharia Social**. Americana: Faculdade de Tecnologia

de Americana “Ministro Ralph Biasi”, 2021. Disponível em: https://ric.cps.sp.gov.br/bitstream/123456789/12791/1/20212S_B%c3%a1rbara%20Ianca%20Zanaqui%20Ribeiro_OD1440.pdf

BANCO CENTRAL DO BRASIL. **LGPD**. s.d. Disponível em: https://www.bcb.gov.br/acessoinformacao/lgpd

HOUSTON CHRISTIAN UNIVERSITY. **What is Cybersecurity Engineering?**. s.d. Disponível em: https://hc-edu.translate.goog/articles/what-is-cybersecurity-engineering/?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt&_x_tr_pto=rq

INTERNATIONAL BUSINESS MACHINES CORPORATION. **O que é engenharia social?**. s.d. Disponível em: https://www.ibm.com/br-pt/think/topics/social-engineering

CAMÊLO, Maria Adriana. **Engenharia Social**: como aspectos psicológicos podem se relacionar com golpes e fraudes. Portal do Investidor, gov.br. Publicado em 25 jun. 2024. Disponível através do seguinte link: https://www.gov.br/investidor/pt-br/penso-logo-invisto/engenharia-social-como-aspectos-psicologicos-podem-se-relacionar-com-golpes-e-fraudes-1

PUC-RIO. **Engenharia Social**. Especialização CCEC PUC-Rio. Disponível em: https://especializacao.ccec.puc-rio.br/blog/engenharia-social

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tânia Aparecida. Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital. **Perspectivas em Ciência da Informação**, v. 27, n. 3, p. 26-45, set./dez. 2022. Disponível em: https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/

https://www.scielo.br/j/tl/a/fjTggfMzKDbCDTQrS4MBGFg/?format=html&lang=pt

CORTEZ, Igor Siqueira; KUBOTA, Luís Cláudio. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. **Revista de Administração – RAUSP**, São Paulo, v. 48, n. 4, p. 757-769, out./nov./dez. 2013. Disponível através do seguinte link: https://www.scielo.br/j/rausp/a/tH7hv6Jh3YcdjBNgsgzfXSM/?format=html&lang=pt

BRASIL. Senado Federal. **Golpes virtuais aumentam e não fazem distinção de idade**. 11 abr 2025. Disponível em: https://www12.senado.leg.br/noticias/infomaterias/2025/04/golpes-virtuais-aumentam-e-nao-fazem-distincao-de-idade.

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. **Acórdão nº 2.035.455, Proc. nº 0725415-98.2025.8.07.0000**. Relator(a): Sandra Reves. 7ª Turma Cível. Julg. 20 ago. 2025. Publicado no DJe em 02 set 2025.

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. **Acórdão nº 2.029.381, Proc. nº 0712129-45.2024.8.07.0014**. Relator(a): Luís Eduardo Yatsuda Arima. 1ª Turma Recursal. Julg. 07 ago 2025. Publicado no DJe em 18 ago 2025.

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. **Acórdão nº 2.023.743, Proc. nº 0704490-21.2025.8.07.0020**. Relator(a): Marco Antonio do Amaral. 3ª Turma Recursal. Julg. 21 jul 2025. Publicado no DJe em 30 jul 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado. **Diário Oficial da União**, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

MICROSOFT. **What is two-factor authentication (2FA)?**, s.d. Disponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-is-two-factor-authentication-2fa.

FLOWTI Tecnologia Ltda. **Como a segurança da informação é afetada pela nova Lei Geral de Proteção de Dados**, 16 jul. 2021. Disponível em: https://flowti.com.br/blog/como-a-seguranca-da-informacao-e-afetada-pela-nova-lei-geral-de-protecao-de-dados.

IT Protect. **Impactos da Engenharia Social na Segurança da Informação**. 14 abr 2025. Disponível em: https://www.itprotect.com.br/tecnologia/impactos-da-engenharia-social-na-seguranca-da-informacao/.

Pedra, David. **O que é uma ameaça em segurança da informação? Como calcular o seu impacto?**. 03 ago 2022. Disponível em: https://www.siteware.com.br/blog/seguranca/o-que-e-uma-ameaca-em-seguranca-da-informacao/.

Claranet. **Engenharia social**: o que é e como se proteger. s.d. Disponível em: https://www.claranet.com/br/blog/engenharia-social-o-que-e-e-como-se-proteger.

IB Cybersecurity. **Engenharia social** – segurança cibernética, s.d. Disponível em: https://ibcybersecurity.com.br/blog/engenharia-social-seguranca-cibernetica.

SEÇÃO 2.2 - LGPD EM SETORES ESPECÍFICOS

A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NO SETOR DA SAÚDE BRASILEIRA: DESAFIOS E IMPLICAÇÕES

Gabriela França da Costa[1]
Gabriela Teixeira Honorato[2]
Isabela Saraiva Faria[3]
Matheus Caiado Tosta[4]

RESUMO

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, representa um marco regulatório na proteção de dados no Brasil, alinhando o país com legislações internacionais, como o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, e estabelecendo diretrizes claras para a coleta, uso, armazenamento e compartilhamento de dados pessoais. Promulgada com o objetivo de proteger os direitos fundamentais de liberdade e privacidade dos indivíduos, a LGPD abrange o tratamento de dados em meios físicos e digitais, realizado por pessoas físicas ou jurídicas, tanto de direito público quanto privado [1]. O tratamento de dados, conforme definido pela lei, engloba qualquer operação que utilize um dado pessoal, desde a coleta até a eliminação. No contexto do setor da saúde, que lida com informações de natureza altamente sensível, a aplicação da LGPD apresenta desafios e implicações significativas, especialmente diante do crescente processo de digitalização de dados e do risco de vazamentos.

SUMÁRIO: 1. Introdução; 2. Saúde público e privada no Brasil e o aumento da digitalização de dados; 3. Como a LGPD se aplica no setor da saúde atualmente; 4. Diferenças entre Dados pessoais e dados sensíveis e como a LGPD trata deles; 5. Consequências dos vazamentos de dados sensíveis; 5.1. Como os pacientes podem exercer seus direitos? 6. Problemáticas no Setor de saúde e dados sensíveis; 6.1. Farmácias e o consumo indevido de dados; 6.2. Dados de Gestantes e Vazamentos; 6.3. Caso Jornalista Marília Gabriela; 7. Conclusão; 8. Referências.

1 INTRODUÇÃO

[1] Gabriela França da Costa, graduanda em Direito pelo Centro Educacional Universitário de Brasília – CEUB e graduanda em biologia pela Universidade de Brasília- UnB. E-mail: gabifranca1835@gmail.com
[2] Gabriela Teixeira Honorato, graduanda em Direito pelo Centro Educacional Universitário de Brasília - CEUB. E-mail: gabi.t.honorato@gmail.com
[3] Isabela Saraiva Faria, graduanda em Direito pelo Centro Educacional Universitário de Brasília – CEUB
[4] Matheus Caiado Tosta, graduando em Direito pelo Centro Educacional Universitário de Brasília – CEUB. E-mail: matheus.caiado@sempreceub.com

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, foi instituída para salvaguardar os direitos de liberdade, privacidade e a livre formação da personalidade de cada indivíduo. Ela regulamenta o tratamento de dados pessoais, que pode ocorrer tanto em formatos físicos quanto digitais, por qualquer pessoa física ou jurídica, seja de direito público ou privado [1]. O conceito de tratamento de dados é amplo, abrangendo atividades como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração [1].

Ademais, a LGPD também estabelece os direitos dos titulares, que incluem o acesso às informações, a correção, a exclusão, a portabilidade e o direito à revogação do consentimento. Além disso, a lei cria a Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar, orientar e aplicar sanções em caso de descumprimento da legislação [12].

No âmbito da LGPD, existem figuras chave responsáveis pelo tratamento dos dados: o Controlador, que toma as decisões sobre o tratamento; o Operador, que realiza o tratamento em nome do Controlador; e o Encarregado (DPO), que atua como canal de comunicação entre as partes e a ANPD [1]. A finalidade do tratamento deve ser sempre clara e explícita, e no setor público, está frequentemente ligada à execução de políticas públicas [1].

2 SAÚDE PÚBLICA E PRIVADA NO BRASIL E O AUMENTO DA DIGITALIZAÇÃO DE DADOS

"Saúde" é um termo que está tão em pauta hodiernamente que a conceituar não é a tarefa mais fácil, principalmente sob diferentes perspectivas do direito como a civilista e a constitucional. A OMS (Organização Mundial da Saúde) define o termo da seguinte forma: "A saúde é um estado de completo bem-estar físico, mental e social, e não consiste apenas na ausência de doença ou de enfermidade". (Constituição Da Organização Mundial Da Saúde, 1946). Diante desse conceito, percebe-se que foge do senso comum a ideia de que saúde é apenas a falta de doença, mas envolve abordagens sociais, individuais, políticas e jurídicas

O setor da saúde no Brasil tem passado por um intenso processo de digitalização, tanto na esfera pública quanto na privada. O uso de sistemas informatizados para armazenamento, compartilhamento e análise de dados clínicos, como prontuários eletrônicos, plataformas de telemedicina, aplicativos de saúde e sistemas de gestão hospitalar, tem se tornado cada vez mais comum [13].

A Rede Nacional de Dados em Saúde (RNDS), plataforma oficial de interoperabilidade do Ministério da Saúde, exemplifica essa transformação.Criada para conectar diversos sistemas de saúde, a RNDS permite o compartilhamento seguro e padronizado de dados, visando maior eficiência na gestão da informação e aprimoramento dos serviços de saúde [2]. A RNDS opera em conformidade com a LGPD, garantindo a segurança e privacidade das informações, com acesso restrito para fins assistenciais e de gestão [2].

Profissionais de saúde, por meio do SUS Digital Profissional, podem acessar o histórico clínico dos pacientes, otimizando o atendimento e evitando exames desnecessários. Os cidadãos, por sua vez, podem consultar seus próprios dados de saúde, como atendimentos, vacinas e medicamentos, através do aplicativo “Meu SUS Digital” [2]. Essa integração entre instituições públicas e privadas, facilitada pela RNDS, fortalece a gestão da saúde pública e promove um cuidado contínuo e eficiente [2].

Segundo o Ministério da Saúde, mais de 87% das Unidades Básicas de Saúde (UBS) utilizam prontuários eletrônicos para registrar e acompanhar o atendimento dos pacientes [14]. O governo federal, por meio da Estratégia de Saúde Digital 2020–2028, busca ampliar a integração entre os sistemas públicos e privados, facilitando o acesso a informações clínicas e melhorando a eficiência na gestão da saúde [13].

No entanto, esse avanço traz desafios importantes relacionados à privacidade e à segurança da informação. A centralização de grandes volumes de dados sensíveis aumenta o risco de incidentes, como vazamentos, acessos indevidos e uso comercial não autorizado, exigindo políticas rigorosas de governança e conformidade com a LGPD [12].

3 COMO A LGPD SE APLICA NO SETOR DA SAÚDE ATUALMENTE

A aplicação da LGPD no setor da saúde é de suma importância, dada a natureza sensível dos dados tratados. Clínicas, hospitais, consultórios e demais estabelecimentos de saúde, tanto públicos quanto privados, devem se adequar à lei [3]. O Ministério da Saúde, por exemplo, atua como Controlador de uma vasta quantidade de dados pessoais, incluindo dados de saúde, e adota medidas técnicas e administrativas para garantir a segurança da informação, além de possuir políticas internas que orientam o uso e compartilhamento de dados [3].

A lei determina que o tratamento de dados relativos à saúde só pode ocorrer em hipóteses específicas, como para o cumprimento de obrigação legal, proteção da vida, tutela da saúde por profissionais ou instituições de saúde, ou mediante consentimento explícito do titular [16].

A proteção de dados pessoais é uma diretriz fundamental para a transformação digital do Sistema Único de Saúde (SUS) e é uma premissa do Programa SUS Digital [3]. A LGPD exige que as instituições de saúde informem os pacientes sobre o uso de seus dados, esclarecendo quais dados são coletados e para qual finalidade [4]. Além disso, a lei estabelece direitos para os titulares dos dados, como a confirmação da existência de tratamento, acesso aos dados, correção de informações incompletas ou desatualizadas, anonimização, bloqueio ou eliminação de dados desnecessários, e a revogação do consentimento [3].

A ANPD, em conjunto com o Ministério da Saúde, tem publicado orientações e notas técnicas voltadas para a implementação da LGPD no setor, esclarecendo boas práticas e interpretando os dispositivos legais à luz das peculiaridades das atividades de saúde [12]. Ainda assim, muitos estabelecimentos enfrentam dificuldades para adequar processos e infraestrutura, especialmente em regiões com menor investimento em tecnologia [14].

4 DIFERENÇAS ENTRE DADOS PESSOAIS E DADOS SENSÍVEIS E COMO A LGPD TRATA DELES

A LGPD estabelece uma distinção crucial entre dados pessoais e dados pessoais sensíveis, conferindo a estes últimos um nível de proteção mais elevado devido ao seu potencial discriminatório [5]. Enquanto os Dados Pessoais são informações que permitem identificar ou tornar identificável uma pessoa natural. Exemplos incluem nome, CPF, endereço, e-mail, telefone, entre outros. Os Dados Pessoais Sensíveis são dados que, se revelados, podem gerar discriminação.

A LGPD os define como dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos [5]. No setor da saúde, a maioria das informações tratadas se enquadra na categoria de dados sensíveis, exigindo, portanto, cuidados adicionais e bases legais mais restritas para seu tratamento.

Os dados pessoais sensíveis podem ser classificados em quatro categorias: Dados pessoais sensíveis de origem, que se referem à origem racial ou étnica; dados pessoais sensíveis de crenças, relativos às informações sobre as convicções religiosas, opiniões políticas e a filiação a sindicatos ou a organizações de caráter religioso; dados pessoais sensíveis corporais, que são dados referentes à saúde, dados genéticos e dados biométricos e dados pessoais sensíveis sexuais: relativos à vida sexual das pessoas [20].

O tratamento de dados sensíveis é permitido apenas em situações específicas, com o consentimento explícito do titular (que deve ter forma específica e destacada e deve ser direcionado para finalidades específicas), o cumprimento de obrigação legal ou regulatória, execução de políticas públicas, estudos por órgãos de pesquisa, exercício regular de direitos, proteção da vida ou incolumidade física do titular ou de terceiros, tutela da saúde (exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária), ou garantia da prevenção à fraude e à segurança do titular [1].

No caso dos dados de saúde, a LGPD impõe regras mais restritivas de tratamento. O consentimento deve ser específico e destacado, e o uso das informações deve respeitar os princípios da finalidade, necessidade, adequação e

segurança [16]. Qualquer uso para fins comerciais ou de marketing, por exemplo, sem base legal adequada, é considerado infração [12]. Além disso, a lei determina que o compartilhamento de dados sensíveis só pode ocorrer em condições seguras, com garantias de anonimização quando possível e supervisão de medidas de proteção pela ANPD [12].

As medidas de segurança a serem adotadas para o tratamento de dados devem ser, de acordo com o art.6, VII da LGPD, medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Sendo as medidas técnicas de responsabilidade da TI, utilizando recursos informáticos para garantir a segurança dos dados e as medidas administrativas são as atividades desenvolvidas pelos agentes de tratamento [21].

5 CONSEQUÊNCIAS DOS VAZAMENTOS DE DADOS SENSÍVEIS

O vazamento de dados sensíveis, especialmente no setor da saúde, pode acarretar consequências graves para os indivíduos e para as instituições envolvidas. Para os titulares, há risco de exposição de informações íntimas, constrangimento, discriminação e até chantagem [18]. Dados sobre doenças, tratamentos, histórico médico, gravidez ou condições genéticas, se divulgados indevidamente, podem afetar a reputação e a vida social ou profissional da pessoa envolvida. Para as instituições, as consequências também são significativas.

A LGPD prevê sanções rigorosas para violações, que incluem: Riscos Legais e Litígios, indivíduos afetados podem mover ações judiciais buscando compensação por danos financeiros, emocionais e à reputação. As empresas podem enfrentar custos substanciais com litígios; impacto na Confiança e Reputação, a perda de confiança pública e o dano à reputação da instituição são significativos, podendo levar à perda de clientes e pacientes; impacto Operacional e Financeiro: Vazamentos geram custos adicionais com investigações internas, auditorias de segurança, atualizações de sistemas e melhorias na infraestrutura de TI [7].

A LGPD estabelece advertências, multas de até 2% do faturamento da empresa (limitadas a R$ 50 milhões por infração) e, em casos extremos, a proibição de processar dados pessoais. A gravidade da violação e o esforço da empresa em proteger os dados influenciam a determinação das penalidades [7], além disso a sanção deve ser aplicada levando em consideração os seguintes parâmetros e critérios [22]:

a. Gravidade e a natureza das infrações e dos direitos pessoais violados;
b. Boa fé do infrator;
c. Vantagem auferida ou pretendida pelo infrator;
d. Condução econômica do infrator;
e. Reincidência;
f. Grau do dano;
g. Cooperação do infrator;
h. Adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano;
i. Adoção de política de boas práticas corretivas;
j. Proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Nos últimos anos, a ANPD conduziu investigações envolvendo grandes redes de farmácias e laboratórios por coleta e uso inadequado de dados de clientes em programas de fidelidade [12][15]. Esses casos exemplificam a importância de práticas transparentes e seguras no manuseio de dados de saúde [17].

Para mitigar esses riscos, as instituições devem implementar medidas preventivas robustas, como criptografia, controles de acesso e autenticação, treinamentos de conscientização para colaboradores e planos de resposta a incidentes [7].

5.1 Como os pacientes podem exercer seus direitos?

Se caso aconteça de dados sensíveis vazarem, os pacientes têm a possibilidade de exercer seus direitos por meio de canais como: (i) Gov.br (Fala.BR), (ii) Ouvidoria-Geral do SUS (OuvidorSUS), (iii) telefone 136 (Disque Saúde) [6].

Esses canais são de extrema importância no que se refere a facilitação do acesso dos cidadãos aos seus direitos, uma vez que os sites ou linguagem utilizada por esses serviços dificultam seu entendimento, principalmente aos cidadãos mais vulneráveis quando se trata de tecnologia e educação. Diante disso, esses canais permitem que o cidadão exerça a transparência ativa, podendo então ter acesso às informações, resolvendo seus problemas sem a necessidade de entrar com requerimentos ou processos judiciais, o que ajuda a destravar ou a não sobrecarregar o sistema judiciário.

Outrossim, o direito à saúde pode ser abordado em um contexto multifacetado, e é possível ser analisado em diferentes áreas do direito, podendo ser responsabilidade do direito civil ou do direito constitucional, sendo geridos pelo estado, município, UNIÃO etc. As autoras Taisa Maria Macena de Lima e Maria de Fátima Freire de Sá explicam esse contexto da seguinte forma:

> Em síntese, qualquer investigação quanto à saúde como objeto de direito, não deve perder de vista as seguintes dimensões: i) direito fundamental individual, porquanto assegurado a todos na Constituição da República, com reconhecida eficácia horizontal; ii) direito social, voltado para o Estado que deve atuar na criação de políticas públicas; iii) direito de personalidade, como construção individual. (LIMA; SÁ, 2015, p. 71).

Pode-se dizer, também, que as garantias fundamentais da vida estão correlacionadas com a responsabilidade civil, podendo ser encontrado no art.5º da Constituição Federal, fora o Código Civil no que diz respeito, por exemplo, à personalidade da pessoa humana; exposto do art.11 ao 21 do CC.

Os direitos de personalidade tutelam sobre à vida, liberdade, vida privada, honra, imagem, identificação, integridade física e psíquica. E, é primordial analisar em como o atendimento à saúde, e a gestão do hospital pode influenciar a implicar

nesses requisitos. As políticas de saúde interagem com diferentes interesses no contexto político, que envolve uma atitude em prol da sociedade de forma organizada e institucionalizada. Miranda afirma que o propósito primário da gestão em saúde é a produção de decisões, "que desencadeiam o processo de intermediação das políticas" (MIRANDA apud CARVALHO et al,2012, pp2) [23].

6 PROBLEMÁTICAS NO SETOR DE SAÚDE E DADOS SENSÍVEIS

O setor de saúde enfrenta problemáticas específicas em relação à LGPD e ao tratamento de dados sensíveis. A grande quantidade e a natureza íntima das informações tornam o setor um alvo frequente para incidentes de segurança e uso indevido de dados.

Uma pesquisa feita pelo professor Zulmar Fachin e Anabela Cristina Hirata ao buscar entender melhor como os dados sensíveis, mais especificamente a saúde, é protegida pela LGPD chegou à conclusão de que a Lei Geral de Proteção de Dados protege adequadamente os dados pessoais sensíveis, porém é necessário que os agentes de tratamento, bem como empresas, instituições e governos, estejam comprometidos com a efetivação das normas e isso tem sido o maior desafio.

Além disso, a integração entre sistemas públicos e privados de saúde ainda apresenta falhas em termos de segurança e anonimização. Embora a Estratégia de Saúde Digital do Ministério da Saúde preveja interoperabilidade entre bases de dados, a anonimização insuficiente pode permitir a reidentificação de pacientes, comprometendo a privacidade [13][14]. Outros desafios incluem ataques cibernéticos a hospitais e laboratórios, que têm se tornado frequentes no país [18], e a falta de clareza para o usuário sobre como seus dados são utilizados. Pesquisas do Procon-SP mostram que a maioria dos consumidores não sabe de que forma seus dados são coletados e compartilhados, o que reduz a efetividade do consentimento informado [17].

Assim, embora a LGPD forneça um arcabouço jurídico robusto, sua implementação efetiva depende da conscientização das instituições, da adoção de

tecnologias seguras e da atuação contínua da ANPD para fiscalizar e educar o setor [12].

Algumas situações ilustram essas dificuldades:

6.1 Farmácias e o consumo indevido de dados

As farmácias, ao lidarem com dados pessoais e sensíveis (como histórico de compras de medicamentos, que pode revelar condições de saúde), são particularmente vulneráveis. A prática de exigir o CPF dos clientes para conceder descontos, por exemplo, tem sido questionada e, em alguns casos, multada, como ocorreu com a Raia Drogasil pelo Procon/MG [8]. Essa prática expõe os consumidores a riscos de privacidade, pois os dados coletados podem ser utilizados para fins não informados ou compartilhados indevidamente [8].

Os impactos para os consumidores incluem fraudes financeiras, roubo de identidade, exposição de informações de saúde (que pode levar à discriminação) e prejuízos emocionais. Para as empresas, as consequências vão desde sanções financeiras e legais até danos à reputação e perda de mercado [8]. As farmácias devem aderir aos princípios da LGPD, como finalidade, necessidade, transparência, segurança e consentimento explícito para o tratamento de dados [8].

6.2 Dados de gestantes e vazamentos

Casos de vazamento de dados de gestantes evidenciam a fragilidade na proteção de informações sensíveis. Aplicativos e clínicas especializadas frequentemente coletam dados sobre ciclos menstruais, exames e planos de parto, que podem ser compartilhados com terceiros sem o devido consentimento. Esse tipo de dado, por seu caráter extremamente íntimo, pode ser utilizado para fins discriminatórios, violando direitos fundamentais.

Um laboratório foi condenado por utilizar indevidamente dados de uma gestante que havia sofrido um aborto espontâneo. Dias após o ocorrido, a mulher recebeu ofertas de serviços relacionados à gravidez, sem ter fornecido consentimento para o compartilhamento de suas informações [9].

O Tribunal de Justiça de São Paulo (TJ-SP) reconheceu a gravidez como um dado sensível, conforme o artigo 5º, inciso II, da LGPD. O compartilhamento dessas informações sem o consentimento da titular, especialmente em um momento tão delicado, configura uma violação dos princípios da LGPD. Este caso destaca a responsabilidade solidária entre controlador e operador de dados e a necessidade de as empresas investirem em cibersegurança para evitar o compartilhamento indevido de dados sensíveis [9].

6.3 Caso jornalista Marília Gabriela

A jornalista Marília Gabriela revelou recentemente ter vivido uma situação de violação de privacidade. Segundo ela, foi surpreendida ao ser abordada por uma colunista, que afirmou ter acesso a todos os exames realizados por Marília em um laboratório e buscava confirmar os resultados antes de publicar uma matéria sobre o assunto.

A apresentadora relatou ter ficado espantada com a abordagem, já que nem ela própria, como paciente, havia recebido os resultados dos exames até aquele momento. Ao questionar a colunista sobre a origem das informações, descobriu que os dados haviam sido repassados diretamente pelo laboratório.

Diante da gravidade da situação, Marília Gabriela entrou em contato com o laboratório para relatar o ocorrido e comunicou que pretendia acionar judicialmente a empresa, uma vez que não autorizou o compartilhamento de suas informações médicas, configurando um vazamento indevido de dados pessoais e sensíveis. Para que não aconteça o que foi relatado no caso acima, é preciso que laboratórios e hospitais mantenham o sigilo de dados sensíveis coletados e que realizem treinamentos eficientes com a equipe [10].

7 CONCLUSÃO

A LGPD impõe um novo paradigma para o tratamento de dados no Brasil, com especial relevância para o setor da saúde. A digitalização crescente, embora traga benefícios como a otimização do atendimento e a integração de sistemas,

também amplifica os riscos de vazamentos e o uso indevido de dados sensíveis. A distinção entre dados pessoais e sensíveis, e as rigorosas exigências para o tratamento destes últimos, são cruciais para garantir a privacidade e a segurança dos pacientes.

As consequências de um vazamento de dados são severas, abrangendo desde multas financeiras e litígios até danos irreparáveis à reputação das instituições. Casos como a coleta indevida de CPF em farmácias e o vazamento de dados de gestantes demonstram a necessidade urgente de adequação e de uma cultura de proteção de dados robusta em todo o setor de saúde. A conformidade com a LGPD não é apenas uma obrigação legal, mas uma responsabilidade ética e um diferencial estratégico para as organizações que buscam construir e manter a confiança de seus usuários.

REFERÊNCIAS

[1] BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd. Acesso em: 7 nov. 2025.

[2] BRASIL. Ministério da Saúde. **Rede Nacional de Dados em Saúde**. Disponível em: https://www.gov.br/saude/pt-br/composicao/seidigi/rnds. Acesso em: 7 nov. 2025.

[3] BRASIL. Ministério da Saúde. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd. Acesso em: 7 nov. 2025.

[4] SABIN. **LGPD na proteção de dados de saúde**. Disponível em: https://blog.sabin.com.br/saude/lgpd-na-protecao-de-dados-de-saude/. Acesso em: 7 nov. 2025.

[5] BRASIL. **Qual a diferença entre dados pessoais e dados sensíveis?** Disponível em: https://www.gov.br/lncc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/campanha-lgpd/2024/qual-a-diferenca-entre-dados-pessoais-e-dados-sensiveis. Acesso em: 8 nov. 2025.

[6] BRASIL. Ministério da Saúde. **Como o paciente pode exercer seus direitos?** Disponível em: https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd#:~:text=Para%20exercer%20seus%20direitos%2C%20o,@saude.gov.br. Acesso em: 8 nov. 2025.

[7] JUNQUEIRA, C. **Consequências do vazamento de dados de saúde sob a ótica da LGPD**. Disponível em: https://jcm.adv.br/artigo/consequencias-do-vazamento-de-dados-de-saude-sob-a-otica-da-lgpd/. Acesso em: 8 nov. 2025.

[8] MIGALHAS. **A LGPD e seus desafios: proteção de dados nas redes farmacêuticas**. Disponível em: https://www.migalhas.com.br/depeso/423530/a-lgpd-e-seus-desafios--protecao-de-dados-nas-redes-farmaceuticas. Acesso em: 9 nov. 2025.

[9] APDADOS. **Condenação por vazamento de dados sobre gravidez evidencia impacto da LGPD**. Disponível em: https://apdados.org/noticia/condenacao-por-vazamento-de-dados-sobre-gravidez-evidencia-impacto-da-lgpd-23-07-2022. Acesso em: 9 nov. 2025.

[10] CARDOSO FREIRE ADVOCACIA. **Caso da jornalista Marília Gabriela**. Disponível em: https://cardosofreire.adv.br/jornalista-marilia-gabriela-denuncia-laboratorio-por-vazamento-de-dados/. Acesso em: 7 nov. 2025.

[11] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Dispõe sobre o tratamento de dados pessoais e altera a Lei nº 12.965/2014**. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 nov. 2025.

[12] ANPD – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Nota técnica e inquérito sobre o tratamento de dados pessoais por redes de drogarias**. Brasília, 2025. Disponível em: https://www.gov.br/anpd/. Acesso em: 11 nov. 2025.

[13] BRASIL. Ministério da Saúde. **Estratégia de Saúde Digital para o Brasil 2020–2028**. Brasília: Ministério da Saúde, 2020. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf. Acesso em: 11 nov. 2025.

[14] BRASIL. Ministério da Saúde. **Mais de 87% das UBS utilizam prontuário eletrônico**. Brasília, 18 jun. 2025. Disponível em: https://www.gov.br/saude/. Acesso em: 11 nov. 2025.

[15] CNN BRASIL. **ANPD notifica Drogasil por uso indevido de dados de clientes**. São Paulo, 11 fev. 2025. Disponível em: https://www.cnnbrasil.com.br. Acesso em: 8 nov. 2025.

[16] MINISTÉRIO PÚBLICO FEDERAL (MPF). **O que é a LGPD**. Brasília, 2024. Disponível em: https://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd. Acesso em: 7 nov. 2025.

[17] PROCON-SP. **Alerta: pesquisa sobre uso de dados por farmácias e desinformação**. São Paulo, 26 jun. 2025. Disponível em: https://www.procon.sp.gov.br. Acesso em: 7 nov. 2025.

[18] JUSBRASIL. **Vazamento de dados pessoais sensíveis na área da saúde – retrospectiva 2020–2021**. 2024. Disponível em: https://www.jusbrasil.com.br. Acesso em: 7 nov. 2025.

[19] APDADOS. **Alerta: coleta abusiva de dados em farmácias**. São Paulo, 8 jul. 2024. Disponível em: https://apdados.org. Acesso em: 11 nov. 2025.

[20] TEFFÉ, Chiara Spadaccini de. **Dados pessoais sensíveis: qualificação, tratamento e boas práticas**. 1. ed. São Paulo: Foco, 2022.

[21] JIMENE, Camilla do Vale. **Da segurança do sigilo dos dados**. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (org.). *LGPD: Lei Geral de Proteção de Dados – Comentada*. São Paulo: Thomson Reuters Brasil, 2019.

[22] HIRATA, A. C.; FACHIN, Z. A. **Direito fundamental à saúde na sociedade da informação e da tecnologia**. *Revista do Instituto de Direito Constitucional e Cidadania*, v. 6, n. 1, e028, 2021. DOI: https://doi.org/10.48159/revistadoidcc.v6n1.e028.

[23] CARVALHO, et al. **A gestão do SUS e as práticas de monitoramento e avaliação**: possibilidades e desafios para a construção de uma agenda estratégica. 2012.

PROTEÇÃO DE DADOS SENSÍVEIS NA SAÚDE SUPLEMENTAR SOB A ÓTICA DA LGPD: OS LIMITES DO TRATAMENTO DE INFORMAÇÕES PELOS PLANOS DE SAÚDE DIANTE DA FINALIDADE CONTRATUAL E DA VEDAÇÃO À PRÁTICAS ABUSIVAS E DISCRIMINATÓRIAS

Kemille Christine Araújo de Sousa[1]
Luciana Geralda Silva Duarte[2]
Sofia Fortes Soares Dutra Moraes[3]
Stephanie da Fonseca Soares[4]

RESUMO

O presente artigo tem por objetivo analisar os limites do tratamento de dados sensíveis pelos planos de saúde à luz da Lei Geral de Proteção de Dados (Lei nº 13.709/2018). Considerando que o direito à saúde, sobretudo no âmbito da saúde suplementar, demanda o manuseio de informações pessoais e vulneráveis, discute-se até que ponto as operadoras podem utilizá-las sem extrapolar a finalidade legítima do contrato. Para tanto, examina-se a natureza jurídica dos dados sensíveis, os requisitos legais para seu tratamento e a aplicação de princípios constitucionais relacionados à dignidade da pessoa humana e à vedação de práticas abusivas e discriminatórias. Analisa-se, ainda, a interface entre a LGPD e as normas regulatórias da Agência Nacional de Saúde Suplementar (ANS), com destaque para os riscos decorrentes da utilização indevida de informações, como seleção de risco, reajustes injustificados ou exclusão de beneficiários. Busca-se, assim, refletir sobre a necessidade de conciliar a proteção da privacidade dos titulares de dados com a efetividade da prestação de serviços de saúde, de modo a garantir um equilíbrio entre a atividade econômica das operadoras e a preservação dos direitos fundamentais dos beneficiários.

[1] Graduanda em Direito do UniCEUB – Centro Universitário de Brasília. Email: kemille.christine@sempreceub.com
[2] Graduanda em Direito do UniCEUB – Centro Universitário de Brasília. Email: luciana.duarte@sempreceub.com
[3] Graduanda em Direito do UniCEUB – Centro Universitário de Brasília. Email: sofia.fortes@sempreceub.com
[4] Graduanda em Direito do UniCEUB – Centro Universitário de Brasília. Email: stephanie.soares@sempreceub.com

Palavras-chave: LGPD; dados sensíveis; saúde suplementar; planos de saúde; tratamento de dados pessoais; práticas abusivas; dignidade da pessoa humana.

SUMÁRIO: Introdução. 1. Conceito e Relevância dos Dados Sensíveis na Saúde. 1.1 Conceito e Natureza dos Dados Sensíveis. 1.2 Relevância no Setor da Saúde. 2. O Regime de Tratamento de Dados e o Limite da Finalidade Contratual. 2.1 A Execução do Contrato de Plano de Saúde como Base Legal e seus Requisitos. 2.2 A Vedação de Práticas Discriminatórias pelo art. 11, §5º da LGPD. 3. Análise do Diálogo Regulatório entre a LGPD e a regulação da saúde suplementar. 3.1 Compatibilidade entre a LGPD e as Normas da ANS. 3.2 Práticas Abusivas no Tratamento de Dados de Saúde. 4. Impacto do Tratamento Indevido e Mecanismos de Tutela. 4.1 Dignidade da Pessoa Humana e Direito à Saúde. 4.2 Mecanismos de Fiscalização e Responsabilização. Conclusão. Referências.

1 INTRODUÇÃO

Inicialmente, convém retratar a disciplina de tratamento de dados pessoais dentro da esfera da sociedade digital. Na mesma proporção que as informações e os dados pessoais assumem papéis de importância e oportunidades, representam, também, ameaças aos direitos de privacidade, intimidade, autodeterminação informativa e à própria dignidade humana. Nessa toada, a denominada Lei Geral de Proteção de Dados, passa a vigorar em nosso ordenamento jurídico com vistas a disciplinar e a proteger o tratamento de dados pessoais. Nessa perspectiva, em alinhamento ao lecionado pelo artigo 1º da LGPD, constata-se que sua principal função é de trazer proteção aos direitos fundamentais à liberdade e à privacidade, além do livre desenvolvimento da personalidade da pessoa natural. Contudo, para além do seu objetivo protetivo quanto ao tratamento de dados pessoais, a LGPD foi além. Ela faz alusão a uma categoria específica de dados pessoais, os dados sensíveis. Sua definição é abarcada pelo inciso II do artigo 5º:

> Art. 5º Para os fins desta Lei, considera-se: [...] II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Assim, dada a natureza e conteúdo dos dados pessoais sensíveis, revela-se imperativa a adoção de medidas de proteção extraordinárias. Isso se justifica pelo fato de que o tratamento inadequado desses dados pode conduzir, com maior facilidade, a situações de discriminação ou uso excessivo, especialmente no âmbito

do direito social à saúde, em que tais informações possuem caráter extremamente vulnerável e estratégico para a garantia de direitos fundamentais.

Nesse viés, considerando que o direito à saúde envolve, necessariamente, a coleta e o tratamento de dados pessoais sensíveis, mostra-se imprescindível a adoção de mecanismos de proteção mais rigorosos e específicos, tendo em vista que tais informações se encontram diretamente relacionadas à tutela da dignidade da pessoa humana e à preservação de direitos fundamentais. Nessa perspectiva, por se tratar de dados sensíveis, o tratamento somente poderá ocorrer mediante o consentimento expresso do titular ou de seu responsável legal, devendo ainda estar vinculado a finalidades determinadas e explícitas, em estrita conformidade com o disposto no art. 11 da LGPD. Com isso, empreende-se dizer que frente ao disposto pela alínea ´´f´´, do art 11, para que os profissionais ou serviços de saúde consigam realizar suas funções, com vistas, acima de tudo, a promover a devida e apropriada tutela do direito essencial da saúde, se mostra fulcral o tratamento de dados sensíveis para tais atividades.

Dessa forma, e com maior especificidade, o presente artigo tem por objetivo central analisar a problemática da gestão e proteção dos dados sensíveis de saúde no âmbito da saúde suplementar. Para tanto, propõe-se a examinar os limites do tratamento desses dados por parte das operadoras de planos de saúde, considerando-se, especialmente, a finalidade contratual que justifica tal tratamento. Nesse contexto, também se destaca o papel da Agência Nacional de Saúde Suplementar (ANS) como órgão regulador e fiscalizador, incumbido de assegurar o cumprimento das disposições legais e contratuais relativas à proteção de dados pessoais sensíveis.

A LGPD introduziu uma nova perspectiva sobre a proteção de dados no ordenamento jurídico brasileiro. No caso dos dados de saúde, classificados como sensíveis nos termos da legislação, impõe-se um regime jurídico especial, voltado à proteção da privacidade e da dignidade da pessoa humana. Assim, à luz dos princípios da finalidade, necessidade e adequação, o tratamento de dados sensíveis da saúde deve observar limites estritos. Em regra, essas informações somente podem ser tratadas por profissionais da saúde ou por instituições legalmente autorizadas, e sempre com finalidades legítimas, explícitas e previamente determinadas.

Nesse sentido, no que se refere aos contratos firmados entre usuários e operadoras de planos de saúde, destaca-se a necessidade de compatibilizar a autonomia privada com as normas de ordem pública da LGPD. Cláusulas contratuais que autorizem o tratamento amplo ou genérico de dados sensíveis, sem base legal específica ou finalidade legítima, devem ser consideradas nulas. Como observa Diniz (2007), os contratos devem observar os princípios da boa-fé, da probidade e da lealdade, sendo inválidas as disposições que afrontem os direitos da personalidade.

Nesse diapasão, é cristalino dizer que:

> Com a entrada em vigor da LGPD, profissionais da saúde, clínicas médicas, hospitais e centros de saúde, entre outros, que realizarem tratamento de dados pessoais sensíveis relacionados à saúde, entre outros, que realizarem tratamento de dados pessoais sensíveis relacionados à saúde deverão adotar medidas para adaptar suas atividades às normas previstas na LGPD, sob pena de estarem em desconformidade e sujeitos às sanções previstas na norma, que podem ir desde a aplicação de multas pecuniárias até a proibição do uso de dados pessoais sensíveis.(Botelho e Paleari do Amaral Camargo, 2021, p. 20.)

Nesse sentido, no que se refere aos contratos firmados entre usuários e operadoras de planos de saúde, destaca-se a necessidade de compatibilizar a autonomia privada com as normas de ordem pública da LGPD. Cláusulas contratuais que autorizem o tratamento amplo ou genérico de dados sensíveis, sem base legal específica ou finalidade legítima, devem ser considerados.

Nessa perspectiva, diante do elevado interesse público envolvido, impõe-se destacar que o tratamento de dados pessoais sensíveis relacionados à tutela da saúde demanda um cuidado ainda mais rigoroso. Tal exigência decorre da necessidade de estrita observância aos fundamentos e princípios estabelecidos na Lei Geral de Proteção de Dados Pessoais, notadamente os princípios da finalidade, necessidade, adequação, segurança e da prevenção, além dos preceitos constitucionais que tutelam a dignidade da pessoa humana, a intimidade e os direitos fundamentais da personalidade, conforme previsto nos artigos 1º, III, e 5º, X e XII, da Constituição Federal. A esse respeito, Doneda (2020) destaca que “a exposição de dados sensíveis no setor da saúde pode produzir impactos concretos e irreversíveis sobre a vida

privada dos indivíduos, exigindo uma abordagem normativa mais rigorosa e protetiva."

Assim, revela-se imprescindível o estabelecimento de balizas normativas claras e adequações legais específicas para orientar e legitimar os procedimentos de tratamento de tais dados, sobretudo no contexto da saúde suplementar, cujas operações envolvem o

compartilhamento constante de informações entre operadoras, prestadores de serviços, laboratórios, clínicas e até mesmo plataformas digitais de atendimento remoto.

Porquanto, cumpre ratificar o papel fiscalizatório e regulador da Agência Nacional de Saúde Suplementar (ANS), autarquia federal vinculada ao Ministério da Saúde, dotada de competências regulatórias, preventivas e repressivas. A dizer: em alinhamento ao artigo 4º da Lei nº 9.961/2000, compete à ANS, entre outras atribuições, "promover a defesa do interesse público na assistência suplementar à saúde, regulando as operadoras setoriais, inclusive quanto às suas relações com prestadores e consumidores, contribuindo para o desenvolvimento das ações de saúde no País" (BRASIL, 2003). Reforçando-se, por conseguinte, a importância da atuação da agência na conformação de um ambiente regulatório que assegure não apenas a proteção dos usuários dos planos de saúde, mas também a observância dos direitos fundamentais no tratamento de dados sensíveis.

Diante do exposto, a LGPD se revela como marco essencial na proteção de dados pessoais, alinhando-se aos princípios da democracia brasileira e à dignidade da pessoa humana. A lei prevê procedimentos específicos para o tratamento de dados sensíveis, reconhecendo sua maior vulnerabilidade, especialmente no contexto da saúde, em que apenas autoridades sanitárias podem realizar o tratamento, independentemente do consentimento do titular, em razão do interesse público.

Nesse diapasão, o presente artigo visa abordar, em suma, a seguinte problemática: até que ponto os planos de saúde podem tratar dados sensíveis sem extrapolar os limites da finalidade legítima, evitando práticas abusivas, excessivas ou discriminatórias? A problemática se acentua diante do risco de utilização das informações para seleção de risco, reajustes injustificados ou exclusão de

beneficiários com condições de saúde mais custosas, o que poderia violar não apenas a LGPD, mas também normas setoriais, como a Lei nº 9.656/1998 e regras da ANS, bem como princípios constitucionais da dignidade humana e da função social da saúde.

2 CONCEITO E RELEVÂNCIA DOS DADOS SENSÍVEIS NA SAÚDE

2.1 Conceito e natureza jurídica dos dados sensíveis

A Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD) — representou um marco fundamental na regulamentação do uso de informações pessoais no Brasil, estabelecendo regras claras para a coleta, tratamento, armazenamento e compartilhamento de dados. A promulgação da norma decorre do avanço tecnológico e da consequente intensificação da circulação de informações em meios digitais, o que potencializou riscos à intimidade, à privacidade e aos direitos fundamentais dos indivíduos (BOTELHO; CAMARGO, 2021, p. 3-4).

A LGPD, em seu art. 5º, I, define dado pessoal como "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018). Dentro desse universo, a lei prevê uma categoria especial denominada de dados pessoais sensíveis, que recebem tutela jurídica reforçada em razão do potencial discriminatório e do caráter profundamente íntimo dessas informações. Nos termos do art. 5º, II, são considerados sensíveis aqueles que dizem respeito, dentre outros, ao "dado referente à saúde ou à vida sexual, dado genético ou biométrico" (BRASIL, 2018).

O tratamento diferenciado conferido a essas informações decorre do elevado risco de violação de direitos fundamentais e de práticas discriminatórias quando utilizadas de forma inadequada. Como observam Botelho e Camargo (2021, p. 3-4), os dados sensíveis revelam aspectos centrais da personalidade e da identidade do titular, de modo que sua proteção mais rigorosa é indispensável à preservação da dignidade humana. A doutrina ressalta que a natureza jurídica dessa categoria impõe a observância de um regime jurídico especial, com hipóteses legais mais restritas e

exigência de fundamentação específica para o tratamento (GONÇALO et al., 2021, p. 8).

No setor da saúde, essa preocupação se acentua. Informações como diagnósticos, resultados de exames, histórico clínico e dados genéticos pertencem ao núcleo mais íntimo da vida privada e, se manipuladas indevidamente, podem ser utilizadas de maneira discriminatória, afetando o acesso a serviços ou a inclusão social. Lisboa (2021, p. 73) explica que a proteção dessas informações está diretamente ligada ao respeito à autonomia e à integridade do indivíduo, além de representar uma garantia de que o tratamento ocorrerá dentro dos limites constitucionais.

A LGPD, ao conferir tratamento diferenciado aos dados sensíveis, reforça o princípio da autodeterminação informacional, que assegura ao titular o poder de decidir sobre o uso e a circulação de seus dados. Segundo Matheus (2025, p. 132), essa abordagem reflete uma mudança paradigmática na proteção de direitos, deslocando o foco do simples sigilo para o controle ativo e informado sobre a informação pessoal. Isso significa reconhecer os dados como extensão da própria personalidade, merecendo tutela jurídica equivalente à dos demais direitos da personalidade.

2.2 Relevância no setor da saúde

No contexto da saúde suplementar, o tratamento de dados sensíveis é ao mesmo tempo indispensável e delicado. As operadoras de planos de saúde precisam acessar e processar informações clínicas de seus beneficiários para autorizar procedimentos, realizar auditorias, elaborar estatísticas e cumprir obrigações regulatórias. A disponibilização dessas informações constitui condição indispensável tanto para a execução do contrato quanto para a garantia da assistência.

Contudo, a legislação veda que essa necessidade operacional se traduza em uso irrestrito. A utilização dessas informações deve permanecer vinculada às finalidades contratuais e observar estritamente as bases legais e princípios previstos

na LGPD (LISBOA, 2021, p. 73). O princípio da finalidade exige que o tratamento tenha propósitos legítimos, específicos e informados ao titular, ao passo que o princípio da necessidade impõe a limitação do tratamento ao mínimo indispensável (BRASIL, 2018).

Quando o tratamento extrapola os limites legais, abre-se espaço para práticas abusivas e discriminatórias. É vedado, portanto, o uso de dados sensíveis com finalidades puramente econômicas — como a elaboração de perfis de risco (seleção de risco), reajustes desproporcionais com base em condições de saúde ou o compartilhamento com terceiros para fins comerciais. O tratamento será considerado legítimo apenas quando diretamente vinculado à assistência em saúde ou à tutela da vida e da integridade física (LISBOA, 2021, p. 74).

Botelho e Camargo (2021, p. 4) alertam que tais condutas não apenas violam a LGPD, mas também afrontam princípios do Código de Defesa do Consumidor (CDC) e normas da Agência Nacional de Saúde Suplementar (ANS), que vedam discriminação no acesso aos serviços. Nesse contexto, a conformidade com a LGPD exige políticas robustas de governança e transparência, sobretudo diante do uso de tecnologias como Big Data e inteligência artificial (GONÇALO et al., 2021, p. 19).

3 O REGIME DE TRATAMENTO DE DADOS E O LIMITE DA FINALIDADE CONTRATUAL

3.1 A execução do contrato de plano de saúde como base legal e seus requisitos

No âmbito da saúde suplementar, a execução do contrato constitui uma das bases legais que autorizam o tratamento de dados. A LGPD estabelece no art. 7º, inciso V, a permissão para o tratamento de dados pessoais “quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular” (BRASIL, 2018). Com relação aos dados sensíveis, o art. 11, inciso II, alínea “f”, da LGPD, autoriza o tratamento “para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária” (BRASIL, 2018).

Essa dupla legitimação impõe que o tratamento, ainda que fundamentado na execução contratual, tenha sua finalidade ligada à assistência e à proteção da vida. Assim, o princípio da necessidade (LGPD, art. 6º, III) atua como parâmetro essencial, restringindo o tratamento ao mínimo indispensável para atingir sua finalidade legítima. Como observa Lisboa (2021, p. 73), a execução contratual deve ser compreendida como um instrumento de viabilização da assistência à saúde, e não como autorização genérica para a coleta e manipulação de dados para fins comerciais.

Gonçalo et al. (2021, p. 19) ressaltam que a execução contratual, embora legítima, deve sempre ser acompanhada de medidas de transparência e governança, incluindo políticas internas claras, controle de acesso às informações e registro das operações de tratamento. O desvio dessa finalidade compromete a autodeterminação informacional e pode configurar violação à legislação.

3.2 A vedação de práticas discriminatórias pelo art. 11, §5º da LGPD

A proteção dos dados sensíveis na saúde não se limita à definição de bases legais para o tratamento. A LGPD também impõe restrições substantivas quanto ao uso dessas informações, destacando-se a vedação expressa de práticas discriminatórias. O art. 11, §5º,da lei dispõe que "é vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários" (BRASIL, 2018).

Essa proibição reflete a preocupação do legislador com os riscos de exclusão social e econômica que podem decorrer do uso indevido de informações médicas. A utilização de dados clínicos para negar cobertura, segmentar beneficiários ou impor reajustes com base em condições pré-existentes caracteriza discriminação ilícita e afronta a função social do contrato, instrumento essencial à efetivação do direito fundamental à saúde (CF, art. 6º e art. 196).

No mesmo sentido, a vedação ao tratamento discriminatório de dados sensíveis decorre da aplicação dos princípios do Código de Defesa do Consumidor

(CDC). O CDC, em seu art. 6º, inciso IV, assegura a proteção contra práticas abusivas e discriminatórias no fornecimento de serviços, garantindo que o consumidor, parte vulnerável na relação, não seja onerado de forma desproporcional. Como advertem Botelho e Camargo (2021), tais práticas podem ocorrer de forma sutil, mas comprometem a essência do contrato.

Lisboa (2021, p. 74) observa que a vedação de discriminação se conecta diretamente ao princípio constitucional da dignidade da pessoa humana, reforçando que a proteção de dados sensíveis, nesse contexto, transcende a dimensão técnica e se insere como instrumento de justiça social, garantindo que a informação não seja utilizada como mecanismo de exclusão no acesso à saúde. A ausência de programas estruturados de compliance digital nas operadoras, segundo Matheus (2025, p. 134), figura como um dos principais fatores que perpetuam tais violações.

4 ANÁLISE DO DIÁLOGO REGULATÓRIO ENTRE A LGPD E A REGULAÇÃO DA SAÚDE SUPLEMENTAR

A relação entre a Lei Geral de Proteção de Dados Pessoais (LGPD) e a regulação da saúde suplementar, sob responsabilidade da Agência Nacional de Saúde Suplementar (ANS), apresenta um campo fértil para a análise jurídica. A LGPD estabelece princípios rígidos sobre o tratamento de dados sensíveis, como os de saúde, enquanto a ANS impõe obrigações regulatórias às operadoras de planos de saúde, muitas das quais exigem tratamento intenso de informações pessoais. Nesta seção, busca-se verificar a compatibilidade entre esses dois regimes normativos, além de identificar práticas potencialmente abusivas que emergem da assimetria entre teoria e prática regulatória.

4.1 Compatibilidade entre a LGPD e as normas da ANS

A princípio, o tratamento de dados pessoais sensíveis por operadoras de saúde possui base legal legítima. A ANS exige a coleta e o compartilhamento de dados para fins de fiscalização, auditoria, formação de base estatística e intercâmbio de informações, como ocorre no uso do Padrão TISS (Troca de Informação em

Saúde Suplementar). Nesse contexto, a base legal do "cumprimento de obrigação legal ou regulatória pelo controlador", prevista no artigo 11, inciso II, alínea "a" da LGPD, é frequentemente invocada.

No entanto, o mero enquadramento formal em uma base legal não exime o agente de observar os princípios fundamentais da lei, especialmente o princípio da necessidade, estabelecido no artigo 6º, inciso III. Este princípio impõe que o tratamento de dados deve se restringir ao mínimo necessário para a realização da finalidade pretendida. Surge, então, o questionamento: a ANS exige apenas o mínimo necessário de dados? Ou sua regulamentação, ainda que bem-intencionada, promove um tratamento excessivo e desproporcional de dados sensíveis?

A resposta a essa questão exige uma análise crítica do escopo das exigências da ANS e da conduta das operadoras. Se a coleta de dados extrapola o que é necessário para atender às finalidades regulatórias, ela deixa de ser legítima sob a LGPD. Há indícios de que, na prática, as operadoras aproveitam-se das exigências da ANS para coletar e armazenar grandes volumes de informações, muitas vezes utilizadas para finalidades não informadas ou não compatíveis com aquelas autorizadas.

Diante dessa tensão normativa, impõe-se a necessidade de um diálogo institucional mais estruturado entre a ANPD (Autoridade Nacional de Proteção de Dados) e a ANS. Embora a ANS detenha competência regulatória sobre o setor de saúde suplementar, é a ANPD que possui a autoridade central para interpretação e fiscalização da LGPD. Assim, caberia à ANPD emitir diretrizes específicas para o setor de saúde suplementar, promovendo a harmonização entre os interesses regulatórios e a proteção da privacidade dos usuários.

Em conclusão, o equilíbrio entre a regulação setorial e a proteção de dados só será possível com a articulação eficaz entre ANS e ANPD. A ausência dessa coordenação abre espaço para insegurança jurídica e para o uso indevido de dados sensíveis sob o pretexto do cumprimento regulatório.

4.2 Práticas abusivas no tratamento de dados de saúde

A LGPD, em seu artigo 11, §5º, proíbe expressamente o tratamento de dados sensíveis para fins discriminatórios, ilícitos ou abusivos. Apesar disso, observa-se que diversas operadoras de planos de saúde praticam condutas que, embora revestidas de aparente legalidade, resultam em discriminação indireta e em violação de direitos fundamentais dos titulares.

Uma dessas práticas é a chamada seleção de risco, ou cherry picking, que consiste em filtrar, restringir ou encarecer o acesso ao plano com base em dados de saúde do consumidor. Operadoras que acessam o histórico médico de potenciais clientes conseguem prever a sinistralidade futura e, com isso, recusam propostas ou oferecem planos com mensalidades proibitivas. Embora o acesso aos dados possa ter ocorrido em contexto legítimo (como durante uma cotação), sua utilização para excluir beneficiários vulneráveis representa clara violação à LGPD e aos princípios da boa-fé e da não discriminação.

Outro exemplo é o uso de dados sensíveis para aplicar reajustes abusivos com base na sinistralidade individual. Um caso concreto é ilustrado pela decisão da 2ª Vara Cível do Foro Regional XI – Pinheiros, em São Paulo (processo nº 1008981-31.2024.8.26.0011), em que a consumidora teve aumentos expressivos em sua mensalidade, passando de R$ 856,10 em 2019 para R$ 2.224,07 em 2024, com base em cláusula de reajuste por sinistralidade. O juízo declarou a cláusula abusiva, determinando sua substituição pelos índices oficiais da ANS e a devolução dos valores pagos a maior. A sentença ressaltou a ausência de comprovação técnica da sinistralidade e a falta de transparência, elementos que violam tanto o CDC quanto os princípios da LGPD, especialmente o da necessidade e da boa-fé.

Além disso, dados de saúde vêm sendo utilizados para fins não autorizados, como marketing direcionado, propostas comerciais para planos mais caros ou mesmo a negativa de cobertura com base em informações sensíveis previamente coletadas. Há relatos também de rescisão unilateral de contratos por parte de operadoras, com base em supostas omissões de informações médicas, muitas vezes sem o devido contraditório. Um exemplo ilustrativo ocorreu em decisão da 7ª Turma Cível do TJDFT (2024), onde uma operadora foi condenada por negar cobertura de internação de urgência alegando carência contratual. O plano foi obrigado a arcar

com os custos e indenizar o beneficiário por danos morais. A Corte reconheceu que a negativa baseada em cláusula genérica, sem análise do contexto clínico, configura abuso e desrespeito ao direito à saúde, podendo também ser entendida como uso indevido de informação sensível.

Essas práticas configuram extrapolações de finalidade e ferem frontalmente os princípios estruturantes da LGPD. O dado sensível, que deveria ser protegido com o mais alto grau de segurança e proporcionalidade, é transformado em ativo econômico, com consequências nefastas à dignidade dos usuários.

5 IMPACTOS DO TRATAMENTO INDEVIDO E MECANISMOS DE TUTELA

O tratamento indevido de dados pessoais sensíveis no setor da saúde suplementar, especialmente quando utilizado de forma abusiva pelas operadoras de planos de saúde, extrapola os limites da legalidade e afeta diretamente a dignidade da pessoa humana. A violação da LGPD, neste contexto, não é apenas uma infração formal, mas implica em efeitos materiais sobre os direitos fundamentais dos titulares. Este tópico aborda as consequências dessas violações e os instrumentos disponíveis no ordenamento jurídico brasileiro para a proteção efetiva dos usuários de planos de saúde.

5.1 Dignidade da pessoa humana e direito à saúde

O primeiro e mais evidente impacto do tratamento ilícito de dados de saúde recai sobre o direito constitucional à saúde (art. 196 da Constituição Federal). Quando o acesso a serviços de saúde suplementar é restringido em razão de dados sensíveis, seja por meio de reajustes abusivos, negativas de cobertura ou exclusões contratuais baseadas em histórico médico, o titular deixa de usufruir plenamente de um direito social garantido pela Constituição. A discriminação indireta promovida pelas operadoras, ao tratar desigualmente aqueles que mais necessitam de atenção médica, compromete o princípio da igualdade material e desvirtua a própria lógica da proteção da saúde.

Além disso, há o dano existencial e a estigmatização do titular. O indivíduo que é classificado como "de alto risco" ou "oneroso" por seu histórico de saúde carrega uma marca que afeta sua relação com o mercado e com o próprio sistema de saúde. Tal estigma compromete sua autonomia, autoestima e até mesmo sua inserção social, especialmente quando leva à exclusão de planos de saúde, recusa de coberturas ou imposição de valores inacessíveis. Nesses casos, a dignidade da pessoa humana, valor-fonte de todo o ordenamento jurídico, é frontalmente violada.

A jurisprudência brasileira já reconheceu que práticas abusivas no setor, como reajustes com base em sinistralidade sem transparência ou negativas de cobertura indevidas, configuram violação de direitos fundamentais e enseja reparação por danos morais. Com a entrada em vigor da LGPD, esses entendimentos ganham ainda mais força, pois a legislação fornece fundamentos específicos para coibir o tratamento discriminatório de dados sensíveis, reforçando a proteção da integridade física e psíquica dos indivíduos.

5.2 Mecanismos de fiscalização e responsabilização

A proteção do titular de dados sensíveis contra o uso indevido por operadoras de saúde se dá tanto na esfera administrativa quanto judicial.

No âmbito administrativo, destaca-se o papel da Autoridade Nacional de Proteção de Dados (ANPD), responsável pela fiscalização e aplicação de sanções previstas na LGPD. Dentre elas, incluem-se advertências, multas e até a proibição de tratamento de dados. Dado o caráter sensível e essencial da saúde, é razoável defender que a ANPD dê prioridade à fiscalização do setor de saúde suplementar, elaborando guias específicas em conjunto com a ANS para garantir uma atuação regulatória harmônica, proporcional e eficaz.

Na esfera judicial, o consumidor pode valer-se da tutela jurisdicional individual ou coletiva, especialmente por meio das regras do Código de Defesa do Consumidor (CDC), que se aplica subsidiariamente à LGPD. A convergência entre o CDC e a LGPD permite combater cláusulas abusivas, garantir o direito à informação clara e adequada e pleitear indenização por danos morais e materiais em caso de

violação aos direitos de proteção de dados. Casos como o julgado pela 2ª Vara Cível de Pinheiros (SP) e pela 7ª Turma Cível do TJDFT demonstram que o Judiciário está atento a essas condutas e reconhece os danos sofridos pelos titulares.

Além disso, uma das formas mais eficazes de prevenir abusos é o fortalecimento de políticas de governança de dados dentro das operadoras. A adoção de mecanismos internos de transparência, controle e segurança da informação, além de programas de compliance voltados à LGPD, contribui para reduzir os riscos de tratamento indevido e restabelece a confiança do usuário no sistema. A governança de dados, nesse sentido, deve ser vista não como mera formalidade, mas como estratégia de proteção da dignidade humana e de valorização do próprio serviço prestado.

O tratamento inadequado de dados pessoais sensíveis pelas operadoras de saúde suplementar representa uma violação multifacetada: infringe a legislação de proteção de dados, os direitos do consumidor, normas contratuais e, sobretudo, princípios constitucionais. Os impactos não são meramente teóricos, são reais, profundos e afetam diretamente o acesso à saúde, à privacidade e à dignidade do ser humano. O ordenamento jurídico brasileiro, por meio da LGPD, da atuação da ANPD e do poder judiciário, oferece instrumentos concretos para a reparação desses danos. No entanto, a solução definitiva depende da integração entre regulação setorial e proteção de dados, além de uma mudança de postura por parte dos agentes do setor.

6 CONCLUSÃO

Diante do exposto, destaca-se a importância da Lei Geral de Proteção de Dados Pessoais (LGPD) como marco normativo essencial na defesa dos direitos fundamentais à privacidade, à autodeterminação informativa e à dignidade da pessoa humana. As presentes práticas abusivas identificadas como a seleção de risco (cherry picking), os reajustes desproporcionais e abusivos com base na sinistralidade individual e o uso indevido de informações médicas para fins não autorizados, como marketing direcionado, evidenciam o descompasso existente entre a teoria protetiva da LGPD e a realidade do mercado de saúde suplementar. Tais condutas, ao

transformar dados sensíveis em instrumentos de exclusão econômica e social, afrontam não apenas a legislação de proteção de dados, mas também os direitos do consumidor e os princípios constitucionais que regem os direitos da igualdade e da dignidade humana.

Devido à natureza e a vulnerabilidade dos dados pessoais sensíveis, é imprescindível a adoção de medidas de proteção extraordinárias e o estabelecimento de leis claras e adequações legais específicas que orientam e legitimam os procedimentos de tratamento desses dados, sobretudo no contexto da saúde suplementar, cujas operações envolvem diretamente o compartilhamento de informações entre operadoras, prestadores de serviços, laboratórios, clínicas e plataformas digitais de atendimento remoto. Somado a isso, a atuação das operadoras de planos de saúde deve ser norteada de acordo com os parâmetros legais de tratamento e à vedação de discriminação previstos no art. 11, §5º, da LGPD. A implementação de políticas internas de governança de dados, programas de compliance e mecanismos de transparência representam não somente exigências legais, como também, um compromisso ético com a tutela da dignidade humana e com o fortalecimento da confiança no sistema de saúde suplementar.

Ademais, é importante salientar a necessidade de uma articulação e coordenação eficaz entre a ANS (Agência Nacional de Saúde Suplementar) e ANPD (Autoridade Nacional de Proteção de Dados) que conversa, busca e contribui para a diminuição da insegurança jurídica, como também do uso indevido de dados sensíveis em cumprimento regulatório. Apesar da competência regulatória em relação ao setor de saúde suplementar, a ANPD é a responsável pela autoridade central que interpreta e fiscaliza a atuação da LGPD, cabendo a ela a emissão de diretrizes específicas ao setor de saúde suplementar, visando promover a harmonia entre os interesses regulatórios e a proteção da privacidade dos usuários. Logo, é indispensável o diálogo estrutural e institucional entre os entes reguladores, os profissionais e as instituições de saúde. A proteção dos dados sensíveis deve ser compreendida como extensão da própria proteção da vida e da integridade do ser humano, reafirmando que a informação, no Estado Democrático de Direito, deve servir à promoção da cidadania e não à sua restrição.

Portanto, no que tange a proteção de dados na saúde suplementar, faz-se necessário a consolidação de uma cultura que enxergue a Lei Geral de Proteção de Dados Pessoais (LGPD) além de um instrumento normativo, mas como uma entrada que caminhe para a efetivação dos direitos fundamentais à saúde, à dignidade, à privacidade e à integridade da pessoa humana, em consonância com os princípios constitucionais e com o ordenamento jurídico, além dos princípios estabelecidos na Lei Geral de Proteção de Dados Pessoais: os princípios da finalidade, necessidade, adequação, segurança e da prevenção, de forma a promover a conjugação entre a ética, a transparência e a responsabilidade institucional.

REFERÊNCIAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia orientativo sobre tratamento de dados pessoais para fins acadêmicos.** 2021. Disponível em: https://www.gov.br/anpd/. Acesso em: 05 out. 2025.

AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR (ANS). **Padrão TISS – Troca de Informação em Saúde Suplementar**. Disponível em: https://www.gov.br/ans/pt-br. Acesso em: 05 out. 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014** (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor.** Diário Oficial da União: seção 1, Brasília, DF, 12 set. 1990.

FIESP; SESI; OBSERVATÓRIO NACIONAL DA INDÚSTRIA. **41% das indústrias não adotam estratégias para reduzir sinistralidade em planos de saúde, mostra pesquisa**. Saúde Digital News, 13 dez. 2024. Disponível em: https://saudedigitalnews.com.br/13/12/2024/plano-de-saude-41-das-industrias-nao-adotam-es trategias-para-reduzir-sinistralidade-mostra-pesquisa/. Acesso em: 06 out. 2025.

G1. **Justiça declara abusiva cláusula de reajuste por sinistralidade em plano de saúde. Ponto Jurídico**, 28 maio de 2024. Disponível em: https://pontojuridico.com.br/justica-declara-abusiva-clausula-de-reajuste-por-sinistralidade-e m-plano-de-saude/. Acesso em: 06 out. 2025.

JURINEWS. **TJ-SP proíbe reajustes em plano de saúde sem comprovação de sinistralidade**. 18 set. 2025. Disponível em: https://jurinews.com.br/destaque-nacional/tj-sp-proibe-reajustes-em-plano-de-saude-sem-com provacao-de-sinistralidade/. Acesso em: 06 out. 2025.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS (TJDFT). **Plano de saúde é condenado por negativa de internação com base em carência contratual.** 18 jan. 2024. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/noticias/2024/janeiro/periodo-de-carencia-plan o-de-saude-e-condenado-por-negativa-de-cobertura. Acesso em: 06 out. 2025.

SANTOS, Gabriel Fernandes dos. **O tratamento de dados sensíveis na saúde suplementar e a LGPD: a competência da ANS e os diálogos com a ANPD**. Jus.com.br, 23 jan. 2023. Disponível em: https://jus.com.br/artigos/102147/o-tratamento-de-dados-sensiveis-na-saude-suplementar-e-algpd-a-competencia-da-ans-e-os-dialogos-com-a-anpd?utm_source Acesso em: 08 de outubro de 2025

PINHEIRO, Weider Silva; JANKOWITSCH, Jhonata; ARAÚJO, Cássia Roberta Silva de; SILVA, Ana Carolinne da. **A proteção de dados pessoais nas relações contratuais privadas: limites e possibilidades da LGPD**. Revista DCS, v. 22, n. 80, p. 8–9, maio 2025. DOI: 10.54899/dcs.v22i80.2875. Disponível em: https://ojs.revistadcs.com/index.php/revista/article/view/2875/2337. Acesso em: 8 out. 2025.

BOTELHO, Marcos César; CAMARGO, Elimei Paleari do Amaral. **A aplicação da Lei Geral de Proteção de Dados na saúde.** Revista de Direito Sanitário, São Paulo, v. 21, n. [sem número], p. 13–15, out. 2021. Disponível em: https://revistas.usp.br/rdisan/article/view/168023 178494. Acesso em: 8 out. 2025.

GONÇALO, Wemerson; SOUZA, Maria Clara de; SANTOS, Wellington Pinheiro dos; OLIVEIRA, Fábio Henrique Cavalcanti de. **Abordagens regulatórias na proteção de dados em saúde: uma revisão integrativa de 2018 a 2023.** Physis: Revista de Saúde Coletiva, Rio de Janeiro, v. 35, n. 1, e350113, 2025. Disponível em: https://www.scielo.br/j/physis/a/56MHDpw9hrMKXYzCWyB77Cp/. Acesso em: 12 out. 2025.

LISBOA, Adriana Marconato. **Tratamento de dados sensíveis no setor da saúde brasileira e o impacto provocado pela Lei Geral de Proteção de Dados.** Itajaí, p. 29–36, nov. 2021. Disponível em: https://biblioteca.univali.br/pergamumweb/vinculos/pdf/Adriana%20Marconato%20Lisboa.p df. Acesso em: 12 out. 2025.

MATHEUS, Ana Carolina Couto. **Privacidade e proteção de dados na saúde suplementar: uma análise crítica do caso Klara Castanho à luz do ordenamento jurídico brasileiro e do compliance.** Virtuajus, Belo Horizonte, v. 10, n. 18, p. 125–140, 2025. Disponível em:

https://periodicos.pucminas.br/virtuajus/article/view/35769. Acesso em: 12 out. 2025. Periódicos PUC Minas

MATTOS, Fábio; JUNGES, Ivone. **Tratamento de dados pessoais sensíveis e o roadmap de adequação à LGPD dos laboratórios de análises clínicas**. p. 14–18. Disponível em: file:///C:/Users/sofia/Downloads/milena-oliveira,+23640-1192624857-1-CE.pdf. Acesso em: 8 out. 2025.

A OPACIDADE NOS PLANOS DE SAÚDE PRIVADOS: DESAFIOS AO ACESSO DO BENEFICIÁRIO À INFORMAÇÃO À LUZ DA LGPD E DA LAI.

Luísa Helena Pereira dos Santos[1]

RESUMO

Trata-se, sobre dinâmica aplicada pelos planos de saúde privados no Brasil, que revelam um cenário em que as estruturas complexas de gestão e intermediação acabam dificultando o acesso dos beneficiários a informações fundamentais e que são de direito indiscutível do usuário. A articulação entre operadoras, administradoras e prestadores credenciados cria um ambiente propício para a retenção de dados e a circulação fragmentada de informações, especialmente quando envolvem registros contratuais. Embora a LGPD estabeleça parâmetros rigoroso para conter os avanços destas práticas, a opacidade da saúde suplementar persiste, transformando isso em um instrumento de vantagem econômica. Somam-se a isso a fragilidade de fiscalização e baixa difusão de orientações acessíveis, os únicos prejudicados são os clientes que enfrentam uma série de práticas abusivas, tendo muitas vezes que se socorrer do poder judiciário. Neste contexto, o estudo reflete os desafios que ultrapassam a mera regularidade administrativa, envolvendo a necessidade de fortalecer mecanismos de transparência, responsabilidade e de acesso efetivo a informação, com o objetivo prático de relações mais equilibradas e éticas, de forma a reforçar a dignidade e direitos do consumidor.

Palavras-chave: Planos de saúde, saúde suplementar, informações, práticas abusivas, usuário, LGPD.

SUMÁRIO: 1. Introdução. 2. Responsabilidades das Operadoras e a violação ao direito do consumidor. 3. Tratamentos das informações e impactos da opacidade. 4. Fiscalização 5. conclusão.

1 INTRODUÇÃO

[1] Graduanda de Direito, cursando o 6º semestre no UniCEUB - Centro Universitário de Brasília. E-mail: luisahelena.psantos@gmail.com

O setor de saúde suplementar no Brasil constitui uma das áreas mais complexas e economicamente relevantes do país, abrangendo milhões de beneficiários, diversas operadoras privadas, administradoras de planos e órgãos credenciados responsáveis pela prestação de serviços de atendimento médico-hospitalares. Esta área é tão vasta que abrange cerca de 25% da população do país, ou seja, 51 milhões de brasileiros, que buscam nestes projetos atendimento especializado de saúde.

Apesar da centralidade desse setor na provisão de cuidados à população, é possível observar que a atuação dessas instituições quase nunca sempre se alinha aos princípios de transparência e proteção de dados, principalmente no que diz respeito às informações que deveriam ser disponibilizadas aos beneficiários. A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, estabelece normas rigorosas para o tratamento de dados pessoais, incluindo as sensíveis, como informações sobre saúde. Nos artigos desta lei, é nítida a obrigação das operadoras em informar quais dados são coletados, a finalidade do uso, como serão armazenados e com quem serão compartilhados, e inclusive, o compartilhamento com o proprietário destas informações.

No entanto, muitas operadoras de planos de saúde, suas administradoras e os órgãos credenciados encontram formas de burlar esses requisitos legais, valendo-se da opacidade e da complexidade para obter vantagens financeiras ou reduzir responsabilidades, em detrimento do consumidor, gerando uma consequente lesão aos beneficiários, e promovendo práticas abusivas que geram constrangimento aos usuários.

2 DA RESPONSABILIDADE DAS OPERADORAS E A VIOLAÇÃO DO DIREITO DO CONSUMIDOR

As operadoras de planos de saúde privados têm a responsabilidade de fornecer cobertura adequada aos beneficiários e de tratar seus dados pessoais de forma transparente, segura e dentro dos limites legais. Isso inclui disponibilizar informações sobre contratos, reajustes, negativas de cobertura, procedimentos realizados e relatórios médicos. As administradoras, por sua vez, atuam na

intermediação entre os beneficiários e os prestadores de serviços credenciados, muitas vezes assumindo o papel de filtro, decidindo quais informações chegam ao consumidor e de que forma. Já os órgãos credenciados, que prestam efetivamente os serviços de saúde, também fazem parte da cadeia de tratamento de dados sensíveis, uma vez que lidam diretamente com registros médicos, exames, diagnósticos e tratamentos. A falha na integração e a falta de transparência nesse sistema complexo favorecem práticas que podem prejudicar o beneficiário, criando barreiras artificiais ao acesso de informações que deveriam ser facilmente disponíveis.

A LGPD, Lei Geral de Proteção de Dados, (Lei nº 13.709/2018), estabelece princípios fundamentais que deveriam proteger o beneficiário de tais práticas. Entre eles estão a finalidade, que determina que os dados só podem ser utilizados para propósitos legítimos e específicos; a necessidade, que limita o tratamento ao mínimo necessário para atingir os objetivos; e a transparência, que garante ao titular o direito de acessar informações claras sobre como seus dados são utilizados. No entanto, muitas operadoras se aproveitam da complexidade regulatória e da estrutura de prestadores credenciados para criar lacunas que permitam a retenção ou omissão de dados. Um exemplo recorrente é a prática de cancelamentos indevidos, onde o plano cancela a adesão, está muitas vezes antiga e obriga o usuário a contratar uma nova modalidade, atual e revigorada, consequentemente mais cara. Ao não disponibilizar relatórios detalhados sobre auditorias internas, utilização de serviços ou critérios de reajuste, a operadora consegue reduzir custos ou evitar responsabilidades, enquanto o consumidor permanece desinformado.

Imagine, outro exemplo, de vida ou morte, onde um procedimento cirúrgico solicitado pelo usuário ao plano de saúde é indevidamente negado, sem justificativas plausíveis. Ao solicitar a proposta de adesão, o contrato ou a justificativa, o titular não recebe o documento, ou lhe são entregues papéis genéricos ou desconexos. Nessas circunstâncias, o usuário encontra-se em posição de vulnerabilidade, muitas vezes sendo compelido a aceitar como definitiva a decisão unilateral da operadora. Tal prática revela-se vantajosa apenas para o plano de saúde, que, ao omitir-se ou agir de forma obscura, evita o cumprimento de obrigações contratuais, isentando-se do custeio de procedimentos previstos.

A omissão das operadoras, compromete intimamente à autodeterminação informativa, fragiliza beneficiário e conduz a quebra da boa-fé objetiva, demonstrando que essas irregularidades afrontam um fundamento constitucional destinado a resguardar a dignidade e a segurança jurídica do consumidor.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> XXXII - o Estado promoverá, na forma da lei, a defesa do consumidor;

3 TRATAMENTO DAS INFORMAÇÕES E IMPACTO DA OPACIDADE

As leis de tratamento de dados desempenham um papel essencial na proteção da privacidade e na promoção da segurança das informações pessoais em uma sociedade cada vez mais digitalizada. Sua principal função é estabelecer regras claras sobre como os dados podem ser coletados, utilizados, armazenados e compartilhados, garantindo que o titular tenha controle sobre suas próprias informações. Além disso, essas normas visam assegurar a transparência nas relações entre cidadãos, empresas e o poder público, prevenindo abusos e usos indevidos dos dados. Ao mesmo tempo, buscam equilibrar a proteção da intimidade com o desenvolvimento tecnológico e econômico, estimulando práticas responsáveis e éticas no tratamento das informações. Nesse sentido, legislações como a Lei Geral de Proteção de Dados (LGPD) no Brasil representam um marco de cidadania digital, reforçando o respeito aos direitos fundamentais e à dignidade da pessoa humana no ambiente virtual e físico.

Além disso, práticas como atrasos na entrega de documentos, respostas parciais a solicitações de informações, procedimentos burocráticos excessivos e a centralização do controle de dados das administradoras dificultam o exercício dos direitos do beneficiário previstos na LGPD. Essa opacidade não apenas prejudica financeiramente o usuário, que pode ter cobranças indevidas ou sofrer reajustes abusivos, mas também gera impactos psicológicos, como insegurança e estresse,

principalmente quando há tratamentos contínuos ou de alta complexidade envolvidos. Os órgãos credenciados, por sua vez, muitas vezes fornecem informações incompletas ou inconsistentes sobre procedimentos e resultados, ampliando ainda mais a dificuldade de acesso a dados precisos.

Nesse contexto, é fundamental entender os limites que a Lei de proteção de dados impõe sobre qualquer entidade que seja responsável por tratar e armazenar quaisquer informações pessoal de outrem. Os controladores, ou seja, os responsáveis por tratar essas informações são submetidos a normas rígidas, voltadas para compatibilizar o tratamento e trazer medidas de segurança para estes dados e seus usuários. Dessa forma, a lei é clara ao dizer que é obrigatório a implantação dessas medidas, e em caso contrário serão submetidos a responsabilização pelos danos causados. Neste panorama, as operadoras de planos de saúde devem se debruçar e tratar suas informações de acordo com lei, de forma que garanta a segurança dignidade dos beneficiários.

Apesar de transmitir uma ideia de controle e sugerir uma expectativa de adequação das práticas e do tratamento dessas informações, a realidade demonstra um cenário muito distante desse ideal.

4 FISCALIZAÇÃO E ATUAÇÃO REAL

A atuação da Agência Nacional de Saúde Suplementar (ANS) é crucial nesse cenário, pois cabe a ela fiscalizar as operadoras e garantir que as normas de transparência e proteção de dados sejam respeitadas. No entanto, a fiscalização enfrenta limitações, especialmente diante da complexidade operacional do setor e da multiplicidade de prestadores e intermediários. Embora a LAI (Lei nº 12.527/2011) se aplique principalmente ao setor público, seus princípios de acesso à informação e transparência influenciam a atuação da ANS, que deveria atuar para assegurar que as operadoras disponibilizem informações claras e completas aos beneficiários. A dificuldade de fiscalização permite que muitas operadoras continuem utilizando estratégias de opacidade como forma de reduzir responsabilidades, aumentar lucros e dificultar o exercício de direitos por parte dos consumidores.

Casos práticos ilustram a gravidade da situação. É comum que beneficiários solicitando relatórios detalhados sobre procedimentos realizados ou negativas de cobertura recebam respostas genéricas, com linguagem técnica complexa ou informações incompletas. Em situações de reajustes contratuais, os critérios utilizados muitas vezes não são claramente explicados, e a documentação necessária para contestar decisões pode ser difícil de acessar. Em casos mais graves, o tratamento de dados pessoais sensíveis como histórico médico, exames e diagnósticos é realizado sem informar claramente ao titular como essas informações estão sendo utilizadas, violando diretamente os princípios da LGPD e permitindo que operadoras se beneficiem da retenção ou manipulação de dados.

Além disso, a falta de informação para os usuários é fator determinante para o fortalecimento das práticas dessas instituições. Pouco se fala da atuação da Agência Nacional de Saúde perante as operadoras de planos de saúde e como ela assegura o atendimento adequado e dentro das normas de acesso e tratamento de dados. Diante disso, não há publicidade de como agir em face de situações de abusividade e como identificá-las. Não basta existir formas de segurança ao beneficiário se elas não chegam até eles.

É importante destacar que a opacidade não é apenas uma questão de burocracia, mas uma estratégia que permite ganhos econômicos e redução de responsabilidades legais. Ao dificultar o acesso à informação, as operadoras podem negar procedimentos sem contestação, aplicar reajustes com menor risco de questionamento e evitar eventuais responsabilidades por falhas de prestação de serviços. Essa dinâmica demonstra um uso estratégico da falta de transparência para maximizar lucros à custa do consumidor, mostrando que a proteção de dados e o direito à informação não são apenas conceitos teóricos, mas instrumentos essenciais para a defesa dos direitos dos beneficiários.

Essa problemática ganhou tanta força, que as ações judiciais contra planos de saúde aumentaram 31,5% em 9 meses, chegando a 36 mil casos em 2024, em uma breve pesquisa no GOV. Os beneficiários estão se socorrendo do poder judiciário para garantirem documentos básicos e de direito; eles não enxergam saída e muitas vezes se veem obrigados a deixar sua adesão. Tudo isso pelo constrangimento e

pressão imposto pelo plano de saúde, ou então a instituição de práticas que não são cabíveis como aumentos arrazoados nas suas mensalidades.

Para mitigar esses problemas, é fundamental que as operadoras adotem políticas internas de transparência efetiva, garantindo acesso rápido e completo a informações relevantes. Ferramentas digitais, canais de comunicação claros e procedimentos simplificados são medidas que podem facilitar o cumprimento da LGPD e reduzir a opacidade. Além disso, os beneficiários precisam ser educados sobre seus direitos, para que possam exercer o acesso a dados, questionar decisões e corrigir informações incorretas. A ANS deve reforçar sua fiscalização, exigindo que as operadoras e os órgãos credenciados cumpram integralmente os requisitos legais e imponha sanções quando constatadas falhas.

5 CONCLUSÃO

Em conclusão, a opacidade nas operadoras de planos de saúde privados, suas administradoras e órgãos credenciados representa um obstáculo significativo ao pleno exercício dos direitos dos beneficiários, permitindo que práticas abusivas prosperem. O descumprimento da LGPD, aliado à complexidade burocrática e à falta de fiscalização eficiente, favorece a apropriação de benefícios pelas operadoras em detrimento do consumidor. Garantir transparência, acesso à informação e proteção de dados não é apenas uma obrigação legal, mas uma necessidade ética para criar um sistema de saúde suplementar mais justo, eficiente e confiável, no qual os direitos dos beneficiários sejam efetivamente respeitados e protegidos.

REFERÊNCIAS

BIONE, Bruno. Proteção de dados pessoais: principais desafios na sociedade digital. Disponível em: https://share.google/x4lDOWLnrBWdX3pA2.

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

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: — *editora não informada*, 2019. Disponível em: https://share.google/grdyyxNciTPCWERcC.

SANTOS, Diego Costa Barbosa; MOURA, Gabriel Aparecido Salvador de; SILVA, Jordão Horácio da. E-saúde e os desafios à proteção da privacidade no Brasil: uma análise da gestão de dados pessoais de pacientes no âmbito da Lei nº 13.709/2018. *Revista Raízes no Direito*, v. 13, n. 2, p. 95–119, 2025. DOI: 10.37951/2318-2288.2024v13i2.p95-119. Disponível em: https://periodicos.unievangelica.edu.br/index.php/raizesnodireito/article/view/8050/5661.

ANÁLISE DA COLETA DE FOTOS EM CADASTRO PARA ACESSO A LOCAIS PÚBLICOS SEGUNDO OS FUNDAMENTOS E PRINCÍPIOS DA LGPD

Éryn Sousa Aguiar[1]
Filipe Moura da Silva[2]
Giovana Gomes Barros[3]
Melissa Braga[4]

RESUMO

A Lei Geral de Proteção de Dados (LGPD) dispõe sobre os princípios que regem a proteção de dados, bem como sobre os direitos dos titulares e a responsabilidade dos agentes de tratamento. Este artigo tem como objetivo analisar a aplicabilidade dos princípios da LGPD à coleta de fotografias e ao uso dessas imagens para o acesso a locais públicos por meio do reconhecimento facial. A partir do estudo da LGPD e de pesquisas acerca da utilização de dados biométricos em ambientes de uso comum, o presente trabalho busca elucidar as principais implicações decorrentes do fornecimento desses dados pelos titulares, a falta de transparência das instituições coletoras e a necessidade de uma proteção mais rigorosa, tendo em vista que tais informações são de natureza pessoal e sensível.

Palavras-chave: Dados pessoais sensíveis; Reconhecimento facial; LPGD.

SUMÁRIO: 1. Introdução; 2. Reconhecimento facial; 2.1 Como é feito o reconhecimento facial?; 2.2 A coleta de fotografias para cadastro de acesso; 3. Aspectos legais; 3.1 Fundamentos, hipóteses e princípios legais; 3.2 A coleta de fotografias sob a perspectiva dos princípios e fundamentos da LGPD; 4. Casos recentes; 5. Boas práticas e recomendações; 6. Conclusões; 7. Referências.

1 INTRODUÇÃO

[1] Graduanda em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: erynaguiiar@sempreceub.com.
[2] Graduando em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: filipe.mouras@sempreceub.com.
[3] Graduanda em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: giovana.barros@sempreceub.com.
[4] Graduanda em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: melissabrg@sempreceub.com.

O uso de parâmetros e padrões biométricos no reconhecimento de pessoas remonta a muitas décadas e até mesmo séculos. Embora a origem do estudo da biometria seja incerta, sabe-se que, por volta do século XIX, alguns sistemas já vinham sendo desenvolvidos, principalmente na área criminalística. Inicialmente, as características físicas eram o único recurso de identificação, depois surgiram as classificações de impressões digitais e, atualmente, as técnicas mais avançadas já exploram o estudo da íris e o reconhecimento facial.[5]

É essencial adotar um olhar amplo sobre as características biométricas, que não se restringem às impressões digitais e faciais, mas abrangem o conjunto de traços que permitem identificar a unicidade de um indivíduo. Assim, também incluem aspectos comportamentais, como a assinatura, a voz, entre outros.[6]

No Brasil, as técnicas biométricas vêm sendo aplicadas em diversos contextos. No controle de fronteiras e aeroportos, por exemplo, é possível identificar a saída de indivíduos com restrições judiciais e conferir maior celeridade aos procedimentos de autorização de entrada no país. De modo semelhante, muitas instituições financeiras adotam a biometria facial e digital como fatores de segunda autenticação em transações e pagamentos. Essa medida garante maior segurança aos usuários contra golpes e fraudes.[7]

Entretanto, o uso mais comum da biometria encontra-se no cotidiano. Cada vez mais, prédios, condomínios, academias e universidades vêm substituindo chaves e cartões de acesso por sistemas mais modernos de credenciais. Aos dados já usualmente coletados nesses ambientes (nome, idade, data de nascimento e número do CPF), acrescentam-se os dados biométricos (fotografias faciais e impressões digitais).

---

[5] BIOCONNECT. ***Biometric History: From Ancient Methods to AI-Powered Identity***. Blog BioConnect, 20 fev. 2024. Disponível em: https://bioconnect.com/blog/2024/02/20/from-ancients-to-ai-tracing-our-digital-identities-throughout-biometric-history. Acesso em: 07 out. 2025.

[6] SERASA EXPERIAN. **Tipos de biometria: qual deles é o mais seguro do mercado?**. *Serasa Experian*, 14 jun. 2023. Disponível em: https://www.serasaexperian.com.br/conteudos/tipos-de-biometria-qual-deles-e-o-mais-seguro-do-mercado/. Acesso em: 07 out. 2025.

[7] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS – ANPD. ***Radar Tecnológico: biometria e reconhecimento facial – estudos preliminares*.** Brasília: ANPD, 2024. p. 14-15. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-biometria-anpd.pdf. Acesso em 07 out. 2025.

Percebe-se, portanto, que, por trás da busca por praticidade e segurança institucional, forma-se um banco de dados pessoais sensíveis sob a guarda de instituições que, em sua maioria, desconhecem os dispositivos da Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709/2018)[8] acerca do tratamento desse tipo de dado. Como consequência, não há transparência para o titular, acerca dos demais tratamentos, para além da coleta, tais como processamento, armazenamento e, principalmente, eliminação desses dados.

Este artigo tem como objetivo avaliar a questão da coleta de dados biométricos para fins de segurança e ponderar sobre essa coleta tomando por base princípios estabelecidos pela LGPD. Para tanto, será feita uma extensa análise sobre os potenciais riscos assumidos pelo titular ao fornecer esses dados e possíveis alternativas, tanto para o titular quanto para o agente de tratamento, para preservar tanto a segurança institucional quanto os direitos fundamentais de liberdade e de privacidade do titular.

2 RECONHECIMENTO FACIAL

2.1 Como é feito o reconhecimento facial?

A tecnologia de reconhecimento facial funciona por meio da comparação de características faciais selecionadas de uma determinada imagem com rostos presentes em um banco de dados[9]. Trata-se, portanto, de um processo empírico, a partir da comparação de características já conhecidas em outro momento, ou seja, busca confirmar se aquele rosto corresponde a alguém previamente registrado. Esse método de identificação biométrica utiliza traços relevantes do rosto humano para fins de identificação, oferecendo um processo sem contato que geralmente é altamente eficaz. A identificação facial, por sua vez, é considerada um método científico, pois se apoia em critérios técnicos e biológicos como a unicidade, a

[8] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 out. 2025.

[9] LI, Qinjun et al. Facial Recognition Technology: A Comprehensive Overview. **Academic Journal of Computing & Information Science**, [S. l.], v. 6, n. 7, p. 15-26, 2023. DOI: 10.25236/AJCIS.2023.060703.

imutabilidade e a perenidade das características, garantindo maior precisão e confiabilidade. Na prática, o reconhecimento serve para reconhecer novamente quem já foi visto, enquanto a identificação busca comprovar a identidade de forma estruturada e sistemática[10].

Diante do elevado potencial das fotografias como fonte de dados pessoais, seja quando disponibilizadas voluntariamente pelo usuário na internet, seja quando obtidas por meio de vazamentos de bancos de dados, elas têm sido amplamente utilizadas na execução de golpes digitais. As fotos podem ser usadas pelos criminosos para criar contas bancárias falsas e solicitações fraudulentas de crédito, como também facilitar fraudes avançadas com criação de deep fakes[11,12,13].

2.2 A coleta de fotografias para cadastro de acesso

Com o advento de sistemas informatizados, tornou-se comum o uso de sistemas de câmeras e leitores de impressões digitais, para acessos a lugares públicos e condomínios. O principal argumento dessa coleta é a praticidade e incremento na segurança patrimonial e do indivíduo. Por outro lado, essa tecnologia enfrenta desafios em relação aos dados pessoais coletados, em especial o biométricos e, mais especificamente, às fotografias tratadas nesses cadastros.

No ambiente digital e em sistemas de monitoramento, fotografias são capturadas, processadas e cruzadas com outras bases de dados, permitindo que algoritmos identifiquem e classifiquem indivíduos com grande precisão. De acordo

[10] DUARTE, Renata; BALDASSO, Rosane Pérez; BEUX, Luciano; ALBERT, Ana Carolina Fafreldines; CORTELLETTI DOS SANTOS, Nicole; FERNANDES, Mário Marques. Aplicação dos sistemas biométricos de reconhecimento facial na segurança pública. *Brazilian Journal of Forensic Sciences, Medical Law and Bioethics*, [S. l.], v. 11, n. 1, p. 1–21, 2021. DOI: 10.17063/bjfs11(1)y20211-21. Disponível em: https://www.bjfs.org/bjfs/bjfs/article/view/848. Acesso em: 26 set. 2025.

[11] MATO GROSSO (Estado). Ministério Público. Hackers publicam 'mega vazamento' de fotos de brasileiros na dark web. **Ministério Público do Estado de Mato Grosso**, Cuiabá, [2024]. Disponível em: https://www.mpmt.mp.br/conteudo/1217/149818/hackers-publicam-megavazamento-de-fotos-de-brasileiros-na-dark-web. Acesso em: 14 out. 2025.

[12] G1. Entenda se golpistas conseguem usar suas fotos nas redes para burlar o reconhecimento facial. **G1**, Rio de Janeiro, 26 jul. 2025. Disponível em: https://g1.globo.com/tecnologia/noticia/2025/07/26/entenda-se-golpistas-conseguem-usar-suas-fotos-nas-redes-para-burlar-o-reconhecimento-facial.ghtml. Acesso em: 14 out. 2025.

[13] O GLOBO. Golpe da 'selfie': criminosos utilizam foto das vítimas para roubar dados pessoais. **O Globo**, Rio de Janeiro, 22 jan. 2025. Disponível em: https://oglobo.globo.com/economia/noticia/2025/01/22/golpe-da-selfie-criminosos-utilizam-foto-das-vitimas-para-roubar-dados-pessoais.ghtml. Acesso em: 14 out. 2025.

com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), essas imagens podem ser consideradas dados pessoais sensíveis, pois permitem a identificação do titular. Assim, devem ser tratadas de maneira diferenciada, observando os princípios de proteção e segurança da informação[14].

Uma imagem vale mais do que mil palavras. Esse ditado, amplamente conhecido, ilustra a força comunicativa de uma fotografia, mas, no contexto atual de coleta e tratamento de dados pessoais, também revela um aspecto preocupante: a quantidade de informações sensíveis que pode ser extraída de uma simples imagem. Uma fotografia pode revelar uma variedade de informações pessoais, tanto visíveis diretamente em seu conteúdo — como identidade, raça, religião, orientação sexual ou estado de saúde — quanto inferidas por meio de tecnologias avançadas de reconhecimento facial e análise de padrões de comportamento[15].

Por meio de tratamento automatizado outras inferências socioculturais podem ser extraídas, a partir do ambiente capturado ou até mesmo preferências pessoais podem ser deduzidas pela análise de vestimentas, adereços ou símbolos presentes na foto. Esse potencial informativo pode não só aumentar o risco de inferências falseadores[16], mas também amplia o risco de discriminação[17].

Portanto, embora o ditado ressalta o poder expressivo de uma imagem, ele também alerta, no cenário contemporâneo, para a necessidade de cautela e responsabilidade ao capturar, compartilhar e armazenar fotografias. No contexto de acessos a locais públicos e privados, onde o fornecimento de imagens se tornou

[14] **BRASIL.** Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

[15] CEBRIAN, F. S. P.; PRUDENTE, G. A.; GUEDES, M. S.; SILVA, M. C. F.; SÁ, M. L. D.; MORAES, T. G. *Radar Tecnológico nº 2 da ANPD: Biometria e Reconhecimento Facial*. Brasília, DF: **Autoridade Nacional de Proteção de Dados**, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-biometria-anpd-1.pdf. Acesso em: 14 out. 2025.

[16] **FLORES, Pablo Jamilk.** Inferências falseadoras como base para a pós-verdade. *Revista Línguas & Letras*, v. 18, n. 41, p. 20–32, 2017. e-ISSN: 1981-4755. DOI: 10.5935/1981-4755.20170022. Disponível em: https://www.academia.edu/45352711/Infer%C3%AAncias_Falseadoras_Como_Base_Para_a_P%C3%B3s_Verdade. Acesso em: 14 out. 2025.

[17] **TEIXEIRA, Michelli Christine de Jesus.** O reconhecimento fotográfico de pessoas motivado por preconceito: o limite entre a legalidade e a ilegalidade. *Revista de Artigos Científicos dos Alunos da EMERJ*, v. 15, n. 12, p. 816–831, jul./dez. 2023. Disponível em: https://emerj.tjrj.jus.br/files/pages/paginas/trabalhos_conclusao/1e2semestre2023/pdf/Tomo_II/Michelli_Christine_de_Jesus_Teixeira_816-831.pdf. Acesso em: 14 out. 2025.

prática comum, é fundamental equilibrar segurança e praticidade com o respeito aos direitos fundamentais de privacidade e proteção de dados.

A situação é agravada na medida em que, muitas vezes, a coleta da fotografia é posta como condição para acesso ao serviço, sem dar ao titular dos dados outra opção para o acesso. Também não é raro que o atendente responsável pela interlocução com o titular não saiba justificar a razão da coleta nem o tipo de tratamento que será realizado após ela. Assim, o titular de dados encontra-se diante de um dilema: fornecer os dados correndo o risco de ter um tratamento inadequado ou o vazamento de seus dados em razão da fragilidade do sistema de armazenamento ou não acessar o serviço. Diante dessa situação, geralmente cede, tornando-se refém do tratamento que será feito pelo controlador.

Feita a contextualização do problema, é possível avançar para sua análise à luz da LGPD, em especial sobre a compatibilidade das práticas de tratamento de dados com os princípios da lei, como a finalidade, a adequação, a necessidade e a segurança, a fim de elaborar uma compreensão aprofundada das implicações jurídicas e práticas do caso.

3 ASPECTOS LEGAIS

3.1 Fundamentos, hipóteses e princípios legais

Desde que entrou em vigor, a LGPD instituiu uma nova maneira para o tratamento de dados pessoais. Organizações públicas e privadas que tratam dados pessoais, sejam elas controladoras ou operadoras, passaram a repensar e adequar seus sistemas e processos para se adequarem à lei.

Se por um lado traz o titular como elemento central da lei, por meio do respeito à privacidade (art. 2º, I), a autodeterminação informativa (art. 2º, II), a liberdade de expressão, de informação, de comunicação e de opinião (art. 2º, III), a inviolabilidade da intimidade (art. 2º, IV), da honra e da imagem e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (art. 2º, VII), por outro lado, incentiva o desenvolvimento econômico e tecnológico e a inovação (art. 2º, V), assim como a

livre iniciativa, livre concorrência e a defesa do consumidor (art. 2º, VI). Dessa forma, seus fundamentos não têm por objetivo obstruir o avanço tecnológico, tampouco impedir o tratamento de dados pessoais, mas sim conciliar proteção aos titulares com o progresso econômico e social.

Para tanto**,** a Lei Geral de Proteção de Dados (LGPD) estabelece que qualquer dado pessoal só pode ser coletado se estiver amparado por uma hipótese legal do art. 7º. Contudo, o mero enquadramento em uma hipótese legal não autoriza o agente de tratamento a tratar os dados da maneira como mais lhe for conveniente. Ao contrário, além de observar a boa-fé, devem ser observados os princípios elencados no art. 6º da Lei, em especial o tratamento tem que ser limitado ao mínimo necessário para a consecução de suas finalidades, em observância do princípio da necessidade.

Além disso, em atendimento ao princípio da transparência (LGPD, art. 6º-III), o titular tem direito de saber exatamente o que está sendo feito com seus dados. Isso inclui entender por que essas informações estão sendo solicitadas, como elas serão usadas, por quanto tempo ficarão armazenadas e com quem poderão ser compartilhadas[18].

Superado o entendimento de que a coleta de imagens para acesso a locais trata da coleta de um dado biométrico e, logo, um dado pessoal sensível, a LGPD oferece garantias ampliadas, reconhecendo esta categoria especial de informações, cujo tratamento pode ensejar discriminações ilícitas ou abusivas de seu titular, devendo, portanto, ser protegidos de forma ampliada. Por esse motivo, o tratamento torna-se ainda mais restritivo, baseado em duas hipóteses dispostas no art. 11: o consentimento ou o atendimento a uma das finalidades específicas do inciso II do referido artigo. Desse artigo, extrai-se que o consentimento do titular é a regra e, para além disso e a título de exceção, são apresentadas as hipóteses em que o tratamento pode ser realizado sem o consentimento do titular.

[18] TRIBUNAL REGIONAL ELEITORAL DO Piauí – TRE-PI. *LGPD: Qual a finalidade da coleta dos seus dados?* 24 nov. 2021. (Atualizado em 23 ago. 2022). Disponível em: https://www.tre-pi.jus.br/comunicacao/noticias/2021/Novembro/lgpd-qual-a-finalidade-da-coleta-dos-seus-dados. Acesso em: 14 out. 2025.

3.2 A coleta de fotografias sob a perspectiva dos princípios e fundamentos da LGPD

O tratamento de imagens do titular para fins de cadastro fundamenta-se, principalmente, nos aspectos de segurança institucional e patrimonial e, em segundo plano, na conveniência oferecida ao titular, que pode acessar uma instituição ou condomínio sem a necessidade de apresentar documentos comprobatórios de sua identidade, economizando tempo e simplificando o procedimento de acesso.

Em se tratando de questões de segurança, é indiscutível a necessidade de identificação e de cadastro para acesso a locais públicos ou em condomínios. Sem o controle de entrada e saída de pessoas, esses locais e as pessoas que nele circulam ficam suscetíveis a infrações.

A uma análise inicial da lei, o legítimo interesse se apresenta como a hipótese legal que melhor se aplica a esse tratamento, na medida em que respalda e promove as atividades do controlador, ao mesmo tempo em que protege o titular no contexto da prestação de serviços que lhe são destinados (LGPD, art. 10, II).

No entanto, em se tratando de dados sensíveis, a hipótese do legítimo interesse não se aplica, restando, portanto, a hipótese do art. 11, inc. II-g, que trata da garantia da prevenção à fraude e à segurança do titular. Para Chiara Teffé, essa hipótese legal "substitui" a hipótese do legítimo interesse. Contudo, a autora alerta que a aplicação desta hipótese mostra-se equivocada quando for possível identificar a pessoa natural com outros dados pessoais (não sensíveis) e que os dados que serão tratados sejam realmente indispensáveis para se alcançar a prevenção de fraudes e proteção do titular[19].

Após identificar o fio da meada, procede-se à análise do dispositivo à luz do caso concreto. Para uma exposição mais clara e organizada, o tema será abordado em duas situações distintas, permitindo uma avaliação sistemática de cada aspecto envolvido e facilitando a compreensão das implicações jurídicas de cada cenário:

[19] **TEFFÉ, Chiara Spadaccini.** Do tratamento de dados pessoais sensíveis. In: MAGALHÃES MARTINS, Guilherme; LONGHI, João Vitor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (Coordenadores). *Comentários à Lei Geral de Proteção de Dados Pessoais*. Indaiatuba, SP: Foco, 2024.

a) Com consentimento:

Nos termos do inciso XII do art. 5º da Lei Geral de Proteção de Dados (LGPD), o consentimento deve ser **livre**, **informado**, **inequívoco** e **específico** para uma finalidade determinada. À luz desse dispositivo, é pertinente questionar em que medida, na prática cotidiana, as operações de coleta de dados realmente observam esses requisitos legais.

Quando a coleta de imagens é imposta como condição para o acesso a determinado local, verifica-se, na realidade, a inexistência de liberdade de escolha por parte do titular, configurando vício de consentimento, conforme dispõe o art. 8º, § 3º, da LGPD. Soma-se a isso o fato de que, em grande parte dos casos, o titular não recebe informações claras e adequadas sobre o tratamento de seus dados, pois os profissionais encarregados dessa etapa — normalmente recepcionistas, porteiros ou agentes de segurança — não possuem capacitação técnica para cumprir as exigências legais de informação e transparência.

Essa lacuna informacional compromete a própria validade do consentimento, na medida em que a autorização do titular não pode ser considerada inequívoca quando o controlador não dispõe de elementos para comprovar que a manifestação de vontade foi efetiva e consciente. Como bem adverte Maldonado, "na ausência de certeza, certamente se estará em momento de insegurança para o controlador, o que pode ensejar o entendimento de ilicitude do tratamento dos dados pessoais, com as consequências negativas daí decorrentes".

Outro aspecto relevante é o requisito da **especificidade**, característica central do consentimento. É por meio dela que se definem, de forma precisa, os dados estritamente necessários à consecução das finalidades legítimas do controlador. Essa delimitação não é um ato meramente formal, mas um exercício de responsabilidade e conformidade, que exige do controlador a identificação objetiva das razões que justificam o tratamento, bem como a demonstração de sua adequação aos princípios da LGPD, especialmente os da necessidade, finalidade e proporcionalidade.

b) Sem consentimento:

Neste caso, o controlador deve se enquadrar em alguma das hipóteses do art. 11-II. O mero enquadramento em algumas dessas hipóteses não isenta o controlador de se atentar para os demais dispositivos legais, em especial sobre a necessidade e proporcionalidade da coleta de dados sensíveis para essa finalidade.

Com ou sem consentimento, o tratamento de dados sensíveis, aqui compreendido pelo sentido do inciso X do art. 5º da LGPD, eleva o tratamento de dados em um outro nível, em que um número maior de salvaguardas demandadas ao controlador e operador, se houver.

Essa complexidade aumenta se há mais de um agente de tratamento e, neste caso, o titular dificilmente tem controle ou sequer conhecimento sobre como essas informações serão usadas.

Um dos principais aspectos é que o tratamento de dados pessoais sensíveis é uma das situações em que a ANPD pode exigir a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), conforme disposto no art. 38 da LGPD[20]. Embora nada impeça que o controlador elabore o RIPD se demandando, a ANPD recomenda que o relatório seja feito antes do tratamento dos dados, pois trata-se de um instrumento de planejamento, em que diante dos riscos identificados, o controlador poderá propor e executar salvaguardas para seu processo. As medidas cabíveis para isso não raramente envolvem tempo e recursos financeiros, assim como equipe especializada para sua implementação.

Nessa mesma lógica de riscos para o tratamento dos dados, outro aspecto que deve ser considerado em se tratando de dados pessoais sensíveis, é o aspecto de segurança e sigilo dos dados. A Lei prevê no art. 46, parágrafo 1º que a ANPD pode dispor sobre padrões técnicos mínimos a serem adotados pelos agentes de tratamento. Ou seja, o agente de tratamento que trata dados sensíveis deverá investir em um sistema adequado para preservar a qualidade e a segurança dos dados.

Nas palavras de Viviane Maldonado, “a segurança e a prevenção são pilares essenciais na proteção de dados”. A autora argumenta que, embora a legislação

[20] **AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD).** Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Brasília: ANPD, 06 abr. 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 14 out. 2025.

estabeleça regras detalhadas para o tratamento correto dos dados, o mero cumprimento dessas normas não é suficiente se não houver uma segurança efetiva no manuseio das informações. A lei, portanto, só é efetivamente atendida quando a segurança dos dados é garantida na prática.

4 CASOS RECENTES

Com o avanço do reconhecimento facial há uma crescente banalização da coleta de imagens. Casos de lojas como a Hering, que monitoram a reação dos clientes a roupas para adequarem sua publicidade, evidenciam que os dados biométricos não são mais tratados apenas para fins de segurança[21]. Especificamente, neste caso, Secretária Nacional do Consumidor (SENACON) aplicou multa à empresa, sob a alegação de que ofendeu vários direitos básicos previstos no Código de Defesa do Consumidor, além de configurar prática abusiva[22].

Em fevereiro deste ano, a ANPD determinou a instauração de um processo de fiscalização sobre 23 clubes de futebol em razão do cadastramento biométrico e identificação biométrica de torcedores. O sistema de cadastramento foi implementado por força da Lei Geral do Esporte[23] (Lei nº 14.597/2023) que determina o uso desses sistemas em locais com capacidade superior a vinte mil pessoas. Por força da Lei do Esporte, o torcedor que deseja comparecer aos jogos deve realizar o cadastro biométrico prévio na plataforma de venda de ingressos e, a partir do cadastro biométrico, a entrada do torcedor fica condicionada a verificação de sua identidade nas catracas.

[21] **GASPARINI, Luciana Casemiro.** Hering terá que explicar o que faz com dados de reconhecimento facial de clientes. *O Globo*, 26 fev. 2019. Disponível em: https://oglobo.globo.com/economia/defesa-do-consumidor/hering-tera-que-explicar-que-faz-com-dados-de-reconhecimento-facial-de-clientes-23482114. Acesso em: 14 out. 2025.

[22] SECRETARIA NACIONAL DO CONSUMIDOR (SENACON). Secretaria Nacional do Consumidor aplica multa a empresa por reconhecimento facial. *Ministério da Justiça e Segurança Pública*, 14 ago. 2020. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/secretaria-nacional-do-consumidor-aplica-multa-a-empresa-por-reconhecimento-facial. Acesso em: 14 out. 2025.

[23] BRASIL. Lei nº 14.597, de 14 de junho de 2023. Institui a Lei Geral do Esporte. Diário Oficial da União: seção 1, Brasília, DF, p. 6, 15 jun. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14597.htm. Acesso em: 14 out. 2025.

Após analisar o caso e a manifestação dos times, embora a Agência tenha reconhecido que não havia proibição do tratamento de dados biométricos para verificação da identidade, exigiu dos clubes a apresentação do RIPD[24].

No contexto de saúde suplementar, o IDEC publicou em 2023 uma nota técnica alertando para os riscos do uso de biometria facial. Além de reforçar os princípios da LGPD, a nota reforça a responsabilidade objetiva dos controladores em caso de incidentes e destaca a importância de medidas como anonimização, exclusão segura e comunicação rápida em caso de vazamentos. Como conclusão o Instituto conclui que a biometria facial é além de ser desnecessário, considerando que o uso da biometria facial é dispensável, já que a identificação pode se dar por meios alternativos e já disponíveis para uso do mercado[25].

5 BOAS PRÁTICAS E RECOMENDAÇÕES

Ao nosso ver, o tratamento biométrico adequado — em especial no que diz respeito à coleta de fotografias faciais — depende da atuação coordenada de três atores centrais: o titular dos dados, o controlador e as autoridades governamentais.

Em primeiro lugar, o titular dos dados deve ser colocado no centro do processo, com informações claras, acessíveis e completas sobre a finalidade, os riscos e os direitos relacionados ao tratamento de sua imagem. Deve tomar consciência de que seus dados pessoais têm valor e que o mau uso deles pode comprometer a sua segurança, sua privacidade e seu patrimônio. Nesse aspecto, o Titular deve sempre questionar a razão pela qual a coleta está sendo feita e para que esses dados serão utilizados. O questionamento crítico sobre a razão e o destino dos dados fazem com que os agentes de tratamento revejam a forma como tratam os dados e capacitem sua equipe para responder aos questionamentos do titular.

[24] **AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD).** ANPD fiscaliza uso de sistema de reconhecimento facial na venda de ingressos e na entrada de estádios por 23 clubes de futebol. Brasília: ANPD, 18 fev. 2025. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-fiscaliza-uso-de-sistema-de-reconhecimento-facial-na-venda-de-ingressos-e-na-entrada-de-estadios-por-23-clubes-de-futebol. Acesso em: 14 out. 2025.

[25] IDEC – Instituto Brasileiro de Defesa do Consumidor. ***Biometria facial, acesso à saúde é direito fundamental à proteção de dados pessoais: nota técnica sobre o uso de dados biométricos em estabelecimentos de saúde suplementar*.** São Paulo: IDEC, jul. 2023. Disponível em: https://idec.org.br/sites/default/files/nt_biometria_facial_no_setor_de_saude_-_idec.pdf. Acesso em: 14 out. 2025.

Em segundo lugar, o controlador tem a responsabilidade de adotar práticas transparentes e seguras, assegurando que a coleta ocorra de forma proporcional e limitada à hipótese legal aplicável.

Nesse contexto, o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) constitui o instrumento mais valioso para o agente de tratamento de boa-fé. Mais do que um simples documento que descreve os processos de tratamento de dados pessoais passíveis de gerar alto risco à observância dos princípios gerais de proteção de dados, às liberdades civis e aos direitos fundamentais do titular, o RIPD funciona como uma ferramenta de planejamento. Ele permite ao controlador antecipar e implementar medidas, salvaguardas e mecanismos de mitigação de risco, assegurando o cumprimento da legislação e a proteção efetiva dos direitos dos titulares. Assim, independentemente do tipo de dado tratado, mas em especial no tratamento de dados pessoais sensíveis, deve ser considerado um instrumento de planejamento.

Para além do RIPD, dois são os fatores para o tratamento de dados com sucesso - a primeira delas é a infraestrutura e a segunda a equipe. Entre esses dois fatores, a primeira é mais onerosa pois envolve investimento em equipamentos e softwares para permitir o tratamento, em especial o armazenamento, de maneira segura. Nem sempre o agente de tratamento de pequeno porte tem condições para arcar com esse investimento, o que leva à reavaliação pelo controlador sobre a necessidade do tratamento de dados sensíveis, e das alternativas de tratamento de outros dados.

Ainda que o agente de tratamento tenha uma boa infraestrutura de hardware e software, se sua equipe não for capacitada, o risco de vazamentos, perda ou alteração dos dados é grande. Especial atenção deve ser dada à equipe de atendimento ao público, que deve ter conhecimento sobre as bases da LGPD e o motivo pelo qual o tratamento está sendo realizado. A nomeação de um encarregado, nos termos do artigo 41 da LGPD é imprescindível para a definição de um ponto focal dentro da instituição para sanar dúvidas e coordenar ações com a equipe e fazer a interlocução com o titular, a alta gestão e, se necessário, com a ANPD.

Por fim, **as autoridades governamentais**, especialmente as de proteção de dados e defesa do consumidor, desempenham um papel essencial de fiscalização e regulação. Compete a elas estabelecer parâmetros normativos, fiscalizar o cumprimento da legislação e impor sanções quando necessário, garantindo um ambiente de confiança e segurança jurídica.

Para além da atuação da Autoridade Nacional de Proteção de Dados, cujas atribuições estão claramente definidas em lei, é necessário identificar outras autoridades estratégicas. Essas autoridades estão vinculadas a setores nos quais há tratamento massivo de dados pessoais sensíveis para fins de cadastro, como o setor de saúde, as plataformas de tecnologia e o próprio poder público.

Na esfera governamental, alguns embriões de alternativas, para conciliar a segurança institucional e patrimonial à segurança dos dados pessoais, destaca-se a nova carteira de identidade nacional com QR Code. Oferece um sistema de identificação baseado em dados biométricos e tecnologias criptográficas, dificultando fraudes e falsificações. Ademais, sua integração com serviços públicos e privados reduz a necessidade de múltiplos cadastros e a exposição de dados pessoais, além de permitir autenticação em tempo real[26].

6 CONCLUSÕES

A tecnologia tem avançado a passos largos, criando dispositivos que, à primeira vista, facilitam e simplificam a vida do titular de dados. No entanto, cadastros que prometem praticidade ao usuário ou asseguram a segurança institucional e patrimonial para as organizações têm sido realizados, muitas vezes, sem uma análise criteriosa dos riscos associados aos direitos fundamentais e aos princípios assegurados pela Constituição Federal e pela Lei nº 13.709/2018 (LGPD).

Essa banalização do tratamento de dados pode gerar danos irreversíveis ao titular, sobretudo diante de práticas inadequadas, como a coleta excessiva de informações.

[26] GOVERNO DIGITAL. Identificação do cidadão e Carteira de Identidade Nacional. Disponível em: https://www.gov.br/governodigital/pt-br/identidade/identificacao-do-cidadao-e-carteira-de-identidade-nacional. Acesso em: 14 out. 2025.

Todo esse processo requer uma revisão profunda e articulada entre os atores envolvidos: desde a conscientização dos titulares, passando pelo planejamento adequado dos agentes de tratamento, até a implementação de mecanismos legais e tecnológicos pelas autoridades governamentais, capazes de reduzir a multiplicidade de tratamentos e garantir que as finalidades institucionais sejam cumpridas com responsabilidade e segurança.

REFERÊNCIAS

BIOCONNECT. ***Biometric History: From Ancient Methods to AI-Powered Identity***. Blog BioConnect, 20 fev. 2024. Disponível em: https://bioconnect.com/blog/2024/02/20/from-ancients-to-ai-tracing-our-digital-identities-throughout-biometric-history. Acesso em: 07 out. 2025.

SERASA EXPERIAN. **Tipos de biometria: qual deles é o mais seguro do mercado?**. *Serasa Experian*, 14 jun. 2023. Disponível em: https://www.serasaexperian.com.br/conteudos/tipos-de-biometria-qual-deles-e-o-mais-seguro-do-mercado/. Acesso em: 07 out. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS – ANPD. ***Radar Tecnológico: biometria e reconhecimento facial – estudos preliminares*.** Brasília: ANPD, 2024. p. 14-15. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-biometria-anpd.pdf. Acesso em 07 out. 2025.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 out. 2025.

LI, Qinjun et al. Facial Recognition Technology: A Comprehensive Overview. **Academic Journal of Computing & Information Science**, [S. l.], v. 6, n. 7, p. 15-26, 2023. DOI: 10.25236/AJCIS.2023.060703.

MATO GROSSO (Estado). Ministério Público. Hackers publicam 'mega vazamento' de fotos de brasileiros na dark web. **Ministério Público do Estado de Mato Grosso**, Cuiabá, [2024]. Disponível em: https://www.mpmt.mp.br/conteudo/1217/149818/hackers-publicam-megavazamento-de-fotos-de-brasileiros-na-dark-web. Acesso em: 14 out. 2025.

G1. Entenda se golpistas conseguem usar suas fotos nas redes para burlar o reconhecimento facial. **G1**, Rio de Janeiro, 26 jul. 2025. Disponível em: https://g1.globo.com/tecnologia/noticia/2025/07/26/entenda-se-golpistas-conseguem-usar-suas-fotos-nas-redes-para-burlar-o-reconhecimento-facial.ghtml. Acesso em: 14 out. 2025.

O GLOBO. Golpe da 'selfie': criminosos utilizam foto das vítimas para roubar dados pessoais. **O Globo**, Rio de Janeiro, 22 jan. 2025. Disponível em: https://oglobo.globo.com/economia/noticia/2025/01/22/golpe-da-selfie-criminosos-utilizam-foto-das-vitimas-para-roubar-dados-pessoais.ghtml. Acesso em: 14 out. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

CEBRIAN, F. S. P.; PRUDENTE, G. A.; GUEDES, M. S.; SILVA, M. C. F.; SÁ, M. L. D.; MORAES, T. G. *Radar Tecnológico nº 2 da ANPD: Biometria e Reconhecimento Facial*. Brasília, DF: **Autoridade Nacional de Proteção de Dados**, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-biometria-anpd-1.pdf. Acesso em: 14 out. 2025.

TEIXEIRA, Michelli Christine de Jesus. O reconhecimento fotográfico de pessoas motivado por preconceito: o limite entre a legalidade e a ilegalidade. *Revista de Artigos Científicos dos Alunos da EMERJ*, v. 15, n. 12, p. 816–831, jul./dez. 2023. Disponível em: https://emerj.tjrj.jus.br/files/pages/paginas/trabalhos_conclusao/1e2semestre2023/pdf/Tomo_II/Michelli_Christine_de_Jesus_Teixeira_816-831.pdf. Acesso em: 14 out. 2025.

TRIBUNAL REGIONAL ELEITORAL DO Piauí – TRE-PI. *LGPD: Qual a finalidade da coleta dos seus dados?* 24 nov. 2021. (Atualizado em 23 ago. 2022). Disponível em: https://www.tre-pi.jus.br/comunicacao/noticias/2021/Novembro/lgpd-qual-a-finalidade-da-coleta-dos-seus-dado.Acesso em: 14 out. 2025.

TEFFÉ, Chiara Spadaccini. Do tratamento de dados pessoais sensíveis. In: MAGALHÃES MARTINS, Guilherme; LONGHI, João Vitor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (Coordenadores). *Comentários à Lei Geral de Proteção de Dados Pessoais*. Indaiatuba, SP: Foco, 2024.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Brasília: ANPD, 06 abr. 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 14 out. 2025.

GASPARINI, Luciana Casemiro. Hering terá que explicar o que faz com dados de reconhecimento facial de clientes. *O Globo*, 26 fev. 2019. Disponível em: https://oglobo.globo.com/economia/defesa-do-consumidor/hering-tera-que-explicar-que-faz-com-dados-de-reconhecimento-facial-de-clientes-23482114. Acesso em: 14 out. 2025.

SECRETARIA NACIONAL DO CONSUMIDOR (SENACON). Secretaria Nacional do Consumidor aplica multa a empresa por reconhecimento facial. *Ministério da Justiça e Segurança Pública*, 14 ago. 2020. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/secretaria-nacional-do-consumidor-aplica-multa-a-empresa-por-reconhecimento-facial. Acesso em: 14 out. 2025.

BRASIL. Lei nº 14.597, de 14 de junho de 2023. Institui a Lei Geral do Esporte. Diário Oficial da União: seção 1, Brasília, DF, p. 6, 15 jun. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14597.htm. Acesso em: 14 out. 2025.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). ANPD fiscaliza uso de sistema de reconhecimento facial na venda de ingressos e na entrada de estádios por 23 clubes de futebol. Brasília: ANPD, 18 fev. 2025. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-fiscaliza-uso-de-sistema-de-reconhecimento-facial-na-venda-de-ingressos-e-na-entrada-de-estadios-por-23-clubes-de-futebol. Acesso em: 14 out. 2025.

IDEC – Instituto Brasileiro de Defesa do Consumidor. ***Biometria facial, acesso à saúde é direito fundamental à proteção de dados pessoais: nota técnica sobre o uso de dados biométricos em estabelecimentos de saúde suplementar*.** São Paulo: IDEC, jul. 2023. Disponível em: https://idec.org.br/sites/default/files/nt_biometria_facial_no_setor_de_saude_-_idec.pdf. Acesso em: 14 out. 2025.

GOVERNO DIGITAL. Identificação do cidadão e Carteira de Identidade Nacional. Disponível em: https://www.gov.br/governodigital/pt-br/identidade/identificacao-do-cidadao-e-carteira-de-identidade-nacional. Acesso em: 14 out. 2025.

DUARTE, Renata; BALDASSO, Rosane Pérez; BEUX, Luciano; ALBERT, Ana Carolina Fafreldines; CORTELLETTI DOS SANTOS, Nicole; FERNANDES, Mário Marques. Aplicação dos sistemas biométricos de reconhecimento facial na segurança pública. *Brazilian Journal of Forensic Sciences, Medical Law and Bioethics*, [S. l.], v. 11, n. 1, p. 1–21, 2021. DOI: https://doi.org/10.17063/bjfs11(1)y20211-21. Disponível em: https://www.bjfs.org/bjfs/bjfs/article/view/848. Acesso em: 26 set. 2025.

FACHIN, Z.; HIRATA, A. C. A proteção jurídica dos dados pessoais sensíveis relativos à saúde. *Revista Jurídica*, [S. l.], v. 3, n. 70, p. 1–23, 2022. Disponível em: https://research.ebsco.com/linkprocessor/plink?id=62a7f1f5-57eb-3931-99f2-ce9bd378b5e1. Acesso em: 26 set. 2025.

MENDES, L. S.; FONSECA, G. C. S. da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. *Revista Estudos Institucionais*, [S. l.], v. 6, n. 2, p. 507–533, 2020. DOI: https://doi.org/10.21783/rei.v6i2.521. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/521. Acesso em: 15 set. 2025.

NETO, Gabriel de Oliveira Cavalcanti. *LGPD, cidades inteligentes e privacidade. Revista Sociedade Científica*, v. 6, n. 1, Pernambuco, 2023. Disponível em: https://revista.scientificsociety.net/wp-content/uploads/2023/06/Art00083-2023.pdf. Acesso em: 15 set. 2025.

RECONHECIMENTO FACIAL EM CONDOMÍNIOS: LIMITES E RISCOS À LUZ DA LGPD

Enrico Rizotto Senedese[1]

RESUMO

O artigo analisa a adoção de sistemas de reconhecimento facial em condomínios sob a perspectiva da Lei Geral de Proteção de Dados Pessoais (LGPD), destacando os limites jurídicos, os riscos decorrentes do tratamento de dados biométricos e as alternativas menos invasivas disponíveis. Parte-se da premissa de que a imagem facial, quando utilizada para identificação automatizada, constitui dado pessoal sensível, o que exige bases legais estritas, consentimento livre e informado e robustas medidas de segurança. Examina-se, ainda, a problemática do consentimento obtido de forma coercitiva nos condomínios, em que os moradores e visitantes não dispõem de meios alternativos de acesso, bem como os riscos de vazamento, comercialização indevida e usos secundários desses dados. A partir da LGPD, de manifestações de entidades como o IDEC e de decisões e casos práticos sobre biometria, conclui-se que a imposição do reconhecimento facial como condição exclusiva para ingresso em edifícios residenciais e comerciais tende a ser desproporcional e incompatível com a proteção de dados como direito fundamental, impondo a necessidade de soluções híbridas, realização de Relatório de Impacto à Proteção de Dados e fortalecimento da governança em privacidade.

Palavras-chave: reconhecimento facial; LGPD; dados biométricos; condomínios; privacidade.

SUMÁRIO: Introdução; 1. Marco Legal Aplicável; 2. A Coercitividade do Consentimento; 3. Comercialização e Uso Indevido; 4. Perspectiva Jurisprudencial; 5. Alternativas e Boas Práticas; 6. Conclusão; 7. Referências.

1 INTRODUÇÃO

A disseminação de sistemas de reconhecimento facial em condomínios residenciais e comerciais no Brasil atingiu cerca de um milhão de unidades, conforme estimativa da Associação Brasileira de Síndicos de Condomínio - Abrascond em parceria com o Instituto Brasileiro de Geografia e Estatística - IBGE,

[1] Graduando em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: enrico.senedese@sempreceub.com.

(G1, 2025). Essa tecnologia integra um contexto mais amplo de digitalização da segurança e do crescente uso de vigilância tecnológica em espaços privados de uso coletivo. A identificação de moradores, visitantes e prestadores de serviço por meio da captura e processamento automatizado da imagem facial é frequentemente apresentada como uma solução moderna, eficiente e potencialmente mais segura, capaz de substituir meios tradicionais como chaves, cartões ou senhas.

Entretanto, essa narrativa tecnológica convive com preocupações legítimas relacionadas à privacidade, à proteção de dados pessoais e à liberdade dos titulares, sobretudo quando a coleta de dado biométrico se torna condição para o exercício de direitos fundamentais, como o acesso à própria unidade condominial. Conforme a Lei Geral de Proteção de Dados Pessoais — LGPD (Lei nº 13.709/2018), a biometria facial é classificada como dado pessoal sensível e, por isso, seu tratamento exige requisitos rigorosos e cautela em sua exigência compulsória em ambientes condominiais.

O problema central que se coloca é até que ponto condomínios podem condicionar o ingresso de moradores e visitantes ao cadastramento em sistemas de reconhecimento facial, sem incorrer em violação à LGPD, à Constituição Federal e aos direitos fundamentais à privacidade, autodeterminação informativa e desenvolvimento livre da personalidade. Diante disso, este estudo objetiva analisar juridicamente o uso do reconhecimento facial em condomínios, focalizando a coercitividade do consentimento, os riscos relacionados ao armazenamento e uso indevido dos dados, bem como possíveis alternativas técnicas e organizacionais compatíveis com a legislação vigente.

Metodologicamente, a pesquisa é de natureza teórica e documental, embasada na análise da LGPD, jurisprudência, doutrina especializada e orientações institucionais, além de posicionamentos de entidades como o Instituto Brasileiro de Defesa do Consumidor (IDEC) acerca do uso do reconhecimento facial em condomínios. Ao término, espera-se oferecer recomendações práticas para a adoção responsável dessa tecnologia, enfatizando a necessidade de equilíbrio entre segurança e privacidade.

2 MARCO LEGAL APLICÁVEL

O reconhecimento facial, quando utilizado como método de autenticação para ingresso em condomínios por meio de dispositivos específicos, caracteriza-se inequívoca e juridicamente como coleta e tratamento de dado biométrico sensível, diferente do simples registro de imagens por câmeras tradicionais de segurança, que apenas captam imagens de entrada e saída para fins de controle interno. Esse dado biométrico é gerado após processamento técnico capaz de identificar, medir e analisar atributos fisiológicos do titular, como explica Teffé, ressaltando que somente o tratamento especializado (por exemplo, algoritmos de reconhecimento facial) transforma uma imagem de registro em dado biométrico, sujeito à Lei Geral de Proteção de Dados Pessoais (TEFFÉ, 2022, p. 110). Dados biométricos englobam a análise e mensuração de impressões digitais, íris, retina, comportamentos característicos e, como no caso do reconhecimento facial, traços distintivos do rosto do indivíduo (TEFFÉ, 2022, p. 108). Portanto, câmeras de segurança comuns não produzem dados biométricos, mas apenas registros visuais; já os dispositivos de reconhecimento facial realizam coleta estruturada e processada, incorrendo em todas as obrigações da legislação específica.

A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) estrutura o regime jurídico do tratamento de dados no Brasil, fixando fundamentos, princípios e regras aplicáveis também aos condomínios enquanto controladores de dados de moradores, visitantes e trabalhadores. O artigo 1º da LGPD define como objetivo central a proteção dos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade, vinculando o tratamento de dados à tutela desses direitos e não meramente à eficiência operacional.

Entre os princípios gerais do artigo 6º da LGPD (Lei 13.709/2018) estão finalidade, adequação, necessidade, segurança, prevenção, transparência e responsabilização, todos imprescindíveis ao avaliar a implementação de reconhecimento facial. O princípio da necessidade exige limitar o tratamento ao mínimo indispensável para cumprir a finalidade, demandando justificativa concreta para uso da biometria em vez de meios menos invasivos, conforme recomendações doutrinárias e regulamentares.

A LGPD distingue dados pessoais comuns e sensíveis: dados sensíveis, segundo o art. 5º, II, incluem biometria vinculada à pessoa natural. A imagem processada por sistemas de reconhecimento facial constitui dado biométrico sensível, sujeitando-se a hipóteses mais restritivas do artigo 11, exigindo proteção reforçada, base legal específica e mecanismos de segurança avançados. Isso diferencia esses sistemas dos registros audiovisuais convencionais, tornando essencial a observância das exigências da LGPD (TEFFÉ, 2022, p. 108-110).

Constitucionalmente, a proteção à privacidade, intimidade, vida privada e imagem está no artigo 5º, X, da CF e reforçada pelo reconhecimento da proteção de dados pessoais como direito fundamental autônomo, por meio de emenda constitucional, nº 115/2022, promulgada em fevereiro de 2022. Tal contexto aumenta o rigor da análise de medidas que condicionem o exercício de direitos essenciais – como acesso à moradia – ao fornecimento de dados sensíveis, determinando interpretação protetiva e restritiva quanto à coleta, guarda e uso desses dados em condomínios.(BRASIL, 1988; BRASIL, 2022)

3 A COERCITIVIDADE DO CONSENTIMENTO

No modelo predominante de implantação do reconhecimento facial em condomínios, o fundamento jurídico usualmente invocado é o consentimento do titular, apresentado nas portarias como parte do "protocolo de segurança" e operacionalizado por meio de cadastros de identificação que funcionam, na prática, como termos de autorização implícitos. Contudo, a LGPD exige que o consentimento seja "manifestação livre, informada e inequívoca" do titular, para finalidades determinadas, vedando expressamente o tratamento de dados pessoais mediante vício de consentimento (arts. 5º, XII, e 8º, §§ 3º e 4º, LGPD (Brasil, 2018)).

Em muitos casos, o morador é comunicado de que, para ter acesso às áreas comuns, à garagem ou mesmo à sua unidade, deverá necessariamente registrar sua biometria facial, sem que lhe seja oferecido meio alternativo de ingresso, como chave, cartão ou senha. A situação necessita maior cautela ainda se tratando de visitantes, que não possuem qualquer relação de vínculo formal frente ao

condomínio, adentrando o condomínio eventualmente com um único propósito pontual, como visitar familiares ou para exercer a prestação de serviços, tais como entregas ou consertos, sendo coagidos a realizar o cadastro facial, sob pena de não terem a entrada liberada pela portaria. Nessa hipótese, o "consentimento" não é verdadeiramente livre, pois representa condição para exercício de direito essencial, o que revela uma forma de coação indireta incompatível com a LGPD e com a lógica da autodeterminação informativa, conforme previsto no artigo 8º, § 4º, e no artigo 6º da Lei nº 13.709/2018 (Brasil, 2018).

O IDEC - Instituto de Defesa do Consumidor, ao analisar o uso de reconhecimento facial em condomínios, sustenta que a implementação da tecnologia jamais pode ser imposta unilateralmente e que é desproporcional exigí-la como única forma de acesso, devendo o condomínio oferecer pelo menos uma alternativa não biométrica (IDEC, 2023). Posição semelhante é adotada por autores e por decisões e pareceres que indicam a necessidade de disponibilização de outro meio de entrada, sob pena de violação de princípios como a liberdade do titular, a necessidade, a proporcionalidade e a não discriminação.

Ao se comparar o reconhecimento facial com métodos menos invasivos, como cartões magnéticos, etiquetas RFID, QR Codes ou senhas, observa-se que estes também permitem controle de acesso e registro de entradas sem exigir a coleta permanente de dados biométricos irrecuperáveis, o que enfraquece o argumento da indispensabilidade da biometria. Essa constatação reforça que, em regra, a imposição do reconhecimento facial como condição de acesso tende a configurar consentimento viciado, nulo nos termos da Lei nº 13.709/2018, artigos 5º, XII, e 8º, §§ 3º e 4º (Brasil, 2018).

A adoção de sistemas de reconhecimento facial em condomínios envolve, via de regra, a constituição de bancos de dados com registros de imagens, templates biométricos, identificadores de moradores, visitantes e prestadores de serviços, bem como informações complementares como CPF, RG, unidade e horários de entrada e saída. Esses bancos, muitas vezes gerenciados por empresas terceirizadas, ampliam significativamente a superfície de risco, sobretudo quando não há estrutura técnica e organizacional robusta para sua proteção.

Relatos de incidentes e análises setoriais mostram que muitos condomínios não contam com políticas formais de segurança da informação, gestão de acessos, criptografia adequada ou procedimentos de resposta a incidentes, o que os torna particularmente vulneráveis a vazamentos, sequestro de dados e acessos indevidos. A LGPD, por sua vez, impõe o dever de adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais, bem como a obrigação de comunicação de incidentes relevantes à ANPD e aos titulares afetados, nos termos do art. 48 da Lei nº 13.709/2018 (Brasil, 2018).

O risco é agravado pelo caráter irrecuperável dos dados biométricos: enquanto senhas e cartões podem ser substituídos em caso de comprometimento, o rosto do titular não pode ser "trocado", de modo que a exposição desses dados pode gerar consequências permanentes em termos de fraude, vigilância e usurpação de identidade. A eventual utilização de imagens ou templates biométricos vazados em outros sistemas de autenticação, como contas digitais (em bancos ou redes sociais) ou serviços públicos, amplia o potencial dano e a responsabilidade civil e administrativa dos controladores e operadores.

Nessas circunstâncias, a avaliação de proporcionalidade deve considerar não apenas a promessa de aumento de segurança patrimonial, mas também a gravidade dos danos possíveis aos titulares em caso de falhas, o que sugere a adoção de medidas de minimização de dados, segregação de bases, criptografia forte e políticas estritas de retenção e descarte. O condomínio que não demonstra capacidade de armazenar corretamente imagens e dados biométricos pode ser responsabilizado e sancionado pela Autoridade Nacional de Proteção de Dados (ANPD), inclusive com multas e bloqueio ou eliminação dos dados, conforme arts. 52 e seguintes da Lei nº 13.709/2018 (Brasil, 2018).

Um exemplo recente deste eminente risco materializou-se na região de Jundiaí (SP), onde dados de moradores de condomínios — incluindo documentos pessoais, fotos de autenticação facial, e informações de veículos — passaram a ser comercializados na dark web após um suposto vazamento em sistemas de reconhecimento facial administrados por empresa terceirizada. O caso levou à investigação policial e evidenciou não só a exposição de dados pessoais à venda

ilegal, mas também a ineficácia de medidas preventivas e a vulnerabilidade diante do acesso de funcionários ou de falhas nos controles técnicos. Essa situação ilustra, na prática, o potencial dano, a importância da responsabilidade dos agentes de tratamento e a necessidade de rigor absoluto na segurança e gestão dos dados biométricos sensíveis, conforme determina a LGPD (SINDICONET, 2024).

4 COMERCIALIZAÇÃO E USO INDEVIDO

Além dos riscos de incidentes de segurança, a existência de grandes bases biométricas privadas suscita preocupações quanto à possibilidade de uso secundário e comercialização de dados sem conhecimento ou anuência dos titulares. A Lei nº 13.709/2018 (Brasil, 2018) veda o uso compartilhado de dados pessoais sensíveis com fins econômicos sem observância estrita das hipóteses legais (arts. 7º, 10, 11 e 46). Cabe à Autoridade Nacional de Proteção de Dados (ANPD) disciplinar ou proibir esse tipo de prática, conforme prevêem os arts. 48, 52 e 55-D da mesma lei.

Na perspectiva de defesa do consumidor, o Instituto Brasileiro de Defesa do Consumidor (IDEC) adverte que a utilização de reconhecimento facial em condomínios para finalidades diversas da segurança de acesso, como marketing, perfilhamento ou venda de informações para terceiros, seria manifestamente ilícita, violando a finalidade informada e a confiança legítima dos titulares (IDEC, 2023). Em cenários extremos, o uso indevido de dados biométricos pode servir para monitoramento abusivo, discriminação, seleção de pessoas ou outras práticas contrárias à dignidade humana e à igualdade, princípios resguardados no artigo 1º, inciso III, e no artigo 5º da Constituição Federal de 1988 (Brasil, 1988), bem como no artigo 6º, inciso III da Lei nº 13.709/2018 (Brasil, 2018).

O debate conecta-se diretamente aos direitos fundamentais à privacidade, à intimidade, à imagem e à proteção de dados, reconhecidos pela Constituição e reforçados pela LGPD como fundamentos do regime de tratamento de dados. A exploração econômica de dados sensíveis sem base legal e transparência não apenas configura infração administrativa, mas pode ensejar responsabilidade civil por danos morais coletivos e individuais, além de repercussões em esferas penais e consumeristas.

Assim, projetos de reconhecimento facial em condomínios devem deixar explicitadas, em instrumentos formais, as finalidades estritas do tratamento, vedando o compartilhamento com terceiros para qualquer uso não diretamente relacionado à segurança do edifício, sob pena de nulidade do consentimento e sanções pela autoridade reguladora. A ausência de cláusulas claras e de mecanismos de supervisão reforça o risco de desvio de finalidade, o que recomenda forte cautela por parte de síndicos, administradoras e empresas fornecedoras de tecnologia.

5 PERSPECTIVAS JURISPRUDENCIAIS E DOUTRINÁRIAS

O debate sobre o uso do reconhecimento facial em condomínios, embora ainda recente, já evidencia na jurisprudência e na doutrina uma postura cautelosa e de proteção em relação ao tratamento de dados biométricos para controle de acesso e vigilância. Casos que envolvem biometria em contextos como consumo, trabalho e serviços públicos têm sido utilizados como parâmetros para reconhecer a sensibilidade desses dados, a necessidade de consentimento livre e informado, e a recomendação da adoção de medidas menos invasivas.

A jurisprudência ressalta que o reconhecimento dos dados pessoais sensíveis como direito fundamental autônomo impõe uma interpretação rigorosa às hipóteses de seu tratamento, especialmente em situações de desequilíbrio entre controlador e titular, como ocorre entre condomínios e moradores.

Entidades de defesa do consumidor, como o IDEC, reforçam uma leitura restritiva da exceção da LGPD que permite o tratamento de dados biométricos para prevenção à fraude e segurança, alegando que tal justificativa dificilmente se sustenta em condomínios diante de alternativas tecnológicas menos invasivas. Esse entendimento encontra consonância em decisões judiciais e orientações da Autoridade Nacional de Proteção de Dados (ANPD), que afastam a aplicação genérica do legítimo interesse ou da segurança para justificar o tratamento indiscriminado de dados sensíveis.

Nesse contexto, a doutrina majoritária advoga pela aplicação rigorosa dos princípios da razoabilidade e da proporcionalidade. Exige-se que condomínios

demonstrem que o reconhecimento facial é indispensável, eficaz e implementado com salvaguardas robustas, o que é raramente comprovado na prática. A ausência de regulamentação específica para o uso do reconhecimento facial em ambientes privados eleva o grau de prudência necessário, prevenindo a consolidação de práticas que possam ser inconstitucionais ou incompatíveis com a LGPD.

Exemplo jurisprudencial relevante é o julgamento do Tribunal de Justiça de São Paulo no processo nº 1012430-21.2024.8.26.0003, em que o condomínio demandante buscava obrigar a moradora a realizar o cadastro biométrico facial para acesso às dependências. A decisão reconheceu a legitimidade da implantação da biometria facial para segurança condominial, mas firmou que a adesão não pode ser compulsória, devendo ficar a critério de cada morador, sem aplicação de penalidades pela recusa. A sentença ressaltou a importância da justificativa da escolha pela biometria facial em detrimento de formas menos invasivas e destacou o deslocamento dos riscos de segurança para a base de dados do controlador, justificando a recusa da moradora. Assim, ponderou-se que a coerção no tratamento de dados sensíveis viola direitos fundamentais e que há meios alternativos eficazes para controle de acesso. A decisão ilustra a necessidade de equilíbrio e cautela no uso do reconhecimento facial, em consonância com a LGPD e a proteção da privacidade na esfera condominial. (BRASIL, Tribunal de Justiça do Estado de São Paulo, 2024)

6 ALTERNATIVAS E BOAS PRÁTICAS

Diante dos riscos e limitações apontados, diversas alternativas técnicas menos intrusivas podem ser adotadas por condomínios para controle de acesso, como cartões de proximidade, tags RFID, chaves eletrônicas, senhas pessoais, QR Codes e até biometria oferecida de forma verdadeiramente opcional, sem prejuízo para quem não a aceita. Esses mecanismos permitem, em geral, níveis adequados de segurança patrimonial e registro de entradas e saídas, com menor exposição de dados sensíveis e maior reversibilidade em caso de incidentes.

A LGPD prevê, ainda, o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), instrumento por meio do qual o controlador descreve as operações de

tratamento de dados que podem gerar riscos às liberdades e direitos fundamentais, indicando medidas de mitigação. A adoção de reconhecimento facial em condomínios, dado o tratamento de biometria e o potencial de dano significativo, é forte candidata à exigência de elaboração de RIPD, seja por iniciativa da própria administração, seja por determinação da ANPD. Conforme dispõe o Relatório de Impacto à Proteção de Dados Pessoais previsto no art. 38 da Lei Geral de Proteção de Dados. (BRASIL, 2018).

Boas práticas de governança em privacidade incluem a definição clara de papéis de controlador e operador, a nomeação de encarregado pelo tratamento de dados, a implementação de políticas de segurança da informação, o uso de criptografia forte, controle de acessos, logs de operações e planos de resposta a incidentes. Também é recomendável estabelecer prazos estritos de retenção de dados, evitando a guarda indefinida de imagens e templates biométricos sem justificativa, e garantir transparência aos condôminos e visitantes quanto ao tratamento realizado.

Por fim, o diálogo com moradores, assembleias bem informadas e a participação de comissões de privacidade ou conselhos internos podem contribuir para escolhas tecnológicas mais equilibradas, que considerem as preocupações legítimas com criminalidade, mas também o direito de cada pessoa de não ser submetida a vigilância biométrica permanente para acessar sua própria casa. Esse caminho colaborativo tende a reduzir conflitos, litígios e riscos regulatórios, favorecendo um ambiente condominial mais seguro e, ao mesmo tempo, mais respeitoso da dignidade e da autonomia informacional de seus integrantes.

7 CONCLUSÃO

A análise realizada indica que a imposição do reconhecimento facial como requisito obrigatório e exclusivo de acesso em condomínios é, em regra, incompatível com a LGPD e com o estatuto constitucional da proteção de dados, sobretudo em razão da natureza sensível da biometria e da ausência de alternativas oferecidas aos titulares. O consentimento obtido em contextos de assimetria e sem

opção real de recusa tende a ser considerado viciado, o que invalida a principal base legal usualmente invocada pelos empreendimentos para justificar o tratamento.

Os riscos associados ao armazenamento e possível uso indevido de dados biométricos – incluindo vazamentos, fraudes, vigilância abusiva e comercialização ilícita – são significativos e, muitas vezes, desproporcionais aos benefícios de segurança efetivamente alcançados, sobretudo quando existem meios menos invasivos capazes de atender à mesma finalidade. Além disso, a jurisprudência, a doutrina e entidades de defesa de direitos têm sinalizado interpretação restritiva das hipóteses de tratamento de dados sensíveis, reforçando a centralidade da proporcionalidade, da necessidade e da transparência.

Em termos de política jurídica, mostra-se necessário um equilíbrio entre a legítima preocupação dos condomínios com segurança e a salvaguarda dos direitos fundamentais dos titulares, o que passa pela preferência por soluções híbridas ou alternativas, pela elaboração de Relatórios de Impacto, pela adoção de mecanismos robustos de segurança da informação e por uma cultura de governança em privacidade. Recomenda-se, assim, que condomínios evitem a imposição compulsória do reconhecimento facial, ofereçam meios alternativos de acesso e dialoguem com moradores, órgãos de defesa do consumidor e a ANPD, de modo a alinhar a gestão da segurança predial às exigências da LGPD e da Constituição Federal.

REFERÊNCIAS

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: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em: 11 nov. 2025.

BRASIL. Tribunal de Justiça do Estado de São Paulo. Apelação Cível nº 1012430-21.2024.8.26.0003. Requerente: Condomínio Residencial Villa Bianca. Requerida: Gisleine Dias. Relatora: Juíza Laura Mota Lima de Oliveira Baccin. São Paulo, 5 ago. 2024. Disponível em: https://esaj.tjsp.jus.br/pastadigital/pg/abrirConferenciaDocumento.do. Acesso em: 13 nov. 2025.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República. Disponível em:

https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 13 nov. 2025.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para atribuir à União a competência privativa para legislar sobre proteção e tratamento de dados pessoais. *Diário Oficial da União*, Brasília, DF, 11 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 13 nov. 2025.

G1. Reconhecimento facial se espalha por prédios no Brasil com pouca transparência na segurança dos dados. São Paulo: G1, 12 jul. 2025. Disponível em: https://g1.globo.com/tecnologia/noticia/2025/07/12/reconhecimento-facial-se-espalha-por-predios-no-brasil-com-pouca-transparencia-na-seguranca-dos-dados.ghtml. Acesso em: 13 nov. 2025.

IDEC. Câmeras em condomínios: o uso de reconhecimento facial e os direitos de consumidores. Disponível em: https://idec.org.br/dicas-e-direitos/cameras-em-condominios-o-uso-de-reconhecimento-facial-e-os-direitos-de-consumidores. Acesso em: 11 nov. 2025.

SERPRO. Como fica o acesso a condomínios com a LGPD em vigor? 2011. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/condominios-predios-comerciais-residenciais-lgpd/. Acesso em: 11 nov. 2025.

SÍNDICONET. Lei Geral de Proteção de Dados Pessoais e condomínio. 2024. Disponível em: https://www.sindiconet.com.br/informese/lei-geral-de-protecao-de-dados-pessoais-e-condominio-administracao-juridico. Acesso em: 11 nov. 2025.

SÍNDICONET. Polícia Civil investiga vazamento de dados em condomínios no interior de São Paulo; informações incluem fotos e documentos pessoais. Disponível em: https://www.sindiconet.com.br/informese/vazamento-dados-condominios-sp-noticias-seguranca. Acesso em: 11 nov. 2025.

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

O TRATAMENTO DE DADOS PESSOAIS PELO FISCO: CONVERGÊNCIAS NORMATIVAS, TENSÕES CONSTITUCIONAIS E DESAFIOS PRÁTICOS NA COMPATIBILIZAÇÃO ENTRE LGPD E O SIGILO FISCAL

Maísa Anaisse Ribeiro[1]

RESUMO

O presente artigo analisa a relação entre o sigilo fiscal e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709), examinando seus fundamentos jurídicos, pontos de convergência e desafios práticos no contexto da administração tributária brasileira. A digitalização crescente e o uso de tecnologias pelo Estado ampliaram a capacidade de coleta e cruzamento de informações, o que intensificou o debate sobre os limites da atuação fiscal frente aos direitos fundamentais à intimidade e à vida privada. O estudo parte da compreensão do sigilo fiscal como uma garantia derivada da Constituição, destinada a proteger dados sensíveis contra abusos e arbitrariedades. Em seguida, aborda os princípios da LGPD, como finalidade, necessidade, transparência e segurança, que impõem novas exigências à gestão de dados pelo poder público. A análise destaca a tensão entre a eficiência administrativa e a proteção da privacidade, evidenciando riscos como a coleta excessiva, o uso indevido e a ausência de mecanismos claros de controle. São discutidas práticas como o compartilhamento de dados bancários, a integração de bases fiscais e a falta de políticas unificadas de governança. O artigo sustenta que a compatibilização entre LGPD e sigilo fiscal não configura conflito, mas oportunidade para qualificar a atuação estatal, garantindo segurança jurídica, respeito à autodeterminação informativa e fortalecimento da confiança entre contribuinte e Estado. Conclui-se que a adoção de medidas técnicas, administrativas e normativas é essencial para assegurar que a fiscalização tributária ocorra dentro dos limites constitucionais e legais, promovendo uma relação equilibrada entre arrecadação e proteção de direitos.

[1] Graduanda em Direito do Centro Universitário de Brasília - UniCEUB. Aluna da disciplina de Direito, Tecnologia e Inovação. Email: segundomarib@gmail.com

Palavras-chaves: Lei geral de proteção de dados; Sigilo fiscal; Direitos fundamentais; Administração tributária.

SUMÁRIO: 1. Introdução; 2. Fundamentos constitucionais do sigilo fiscal; 3. Poder de fiscalização tributária e seus limites; 4. A LGPD e a proteção de dados pessoais; 5. Compatibilização da lei com o sigilo fiscal; 6. Considerações finais; 7. Referências bibliográficas.

1 INTRODUÇÃO

A crescente digitalização das relações sociais, econômicas e administrativas tem intensificado o debate sobre os limites da atuação estatal frente aos direitos fundamentais dos cidadãos. Em especial, a atuação da administração tributária, que se vale de tecnologias avançadas para coletar, cruzar e analisar dados fiscais e bancários, levanta preocupações quanto à proteção da privacidade individual. O sigilo fiscal, embora não esteja expressamente previsto na Constituição Federal, é reconhecido pela doutrina e jurisprudência como uma extensão do direito à intimidade e à vida privada, funcionando como uma salvaguarda contra abusos na coleta e uso de informações sensíveis.

Por outro lado, a promulgação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), conhecida como LGPD, trouxe ao ordenamento jurídico brasileiro um conjunto de princípios e regras voltados à proteção dos dados pessoais, inclusive aqueles tratados por órgãos públicos. A LGPD estabelece diretrizes claras sobre a finalidade, necessidade, segurança e transparência no tratamento de dados, impondo limites à atuação de qualquer entidade que manipule informações de pessoas naturais, inclusive a administração tributária.

Nesse contexto, surge uma tensão entre dois polos: de um lado, o poder fiscalizador do Estado, legitimado constitucionalmente para arrecadar tributos e combater ilícitos fiscais; de outro, os direitos fundamentais à privacidade e à proteção de dados, que visam garantir a dignidade e a liberdade informacional dos indivíduos. Essa tensão se manifesta de forma concreta em práticas como o compartilhamento de dados bancários com o Fisco, a exigência de informações detalhadas em declarações fiscais e a ausência de políticas claras de privacidade em programas de incentivo fiscal.

A relevância do tema se intensifica diante do volume crescente de dados coletados e da sofisticação dos mecanismos de análise utilizados pelo Estado. A possibilidade de construção de perfis detalhados dos contribuintes, com base em seus hábitos de consumo, rendimentos e relações econômicas, exige uma reflexão profunda sobre os limites éticos e jurídicos dessa atuação. A proteção da privacidade não pode ser vista como obstáculo à eficiência administrativa, mas como elemento essencial para a construção de uma relação de confiança entre o cidadão e o poder público.

Diante disso, o presente artigo tem como objetivo analisar a compatibilidade entre o sigilo fiscal e a LGPD, explorando os fundamentos jurídicos de ambos os institutos, suas interseções e os desafios práticos que emergem dessa relação. Busca-se compreender como o Estado pode exercer seu poder de fiscalização sem violar os direitos fundamentais dos contribuintes, propondo uma leitura equilibrada que respeite tanto a necessidade de arrecadação quanto a proteção da dignidade informacional.

2 FUNDAMENTOS CONSTITUCIONAIS DO SIGILO FISCAL

O sigilo fiscal, embora não esteja expressamente previsto no texto constitucional, é amplamente reconhecido como uma derivação direta dos direitos fundamentais à intimidade e à vida privada, consagrados no artigo 5º, inciso X, da Constituição Federal de 1988. Esses direitos garantem ao indivíduo a proteção contra interferências indevidas em sua esfera pessoal, incluindo o acesso e divulgação de informações sensíveis, como dados financeiros e patrimoniais. A doutrina e a jurisprudência brasileiras têm interpretado que o sigilo fiscal é uma forma de assegurar a inviolabilidade da privacidade, especialmente no contexto da relação entre o contribuinte e o Estado.

A proteção ao sigilo fiscal decorre, portanto, de uma leitura sistemática dos direitos fundamentais, que reconhece a necessidade de limitar o poder estatal de acesso a informações pessoais. O Estado, ao exercer sua função arrecadatória e fiscalizadora, lida com dados que revelam aspectos íntimos da vida dos cidadãos, como seus rendimentos, hábitos de consumo, investimentos e movimentações

bancárias. Por isso, é essencial que essa atuação seja pautada por critérios de legalidade, proporcionalidade e necessidade, evitando a exposição indevida de informações que pertencem à esfera privada do indivíduo.

A jurisprudência do Supremo Tribunal Federal tem contribuído para consolidar essa visão. Em diversos julgamentos, o STF reconheceu que o acesso a dados fiscais e bancários deve respeitar os direitos fundamentais, sendo necessário justificar a quebra de sigilo com base em interesse público relevante e previsão legal específica. Essa proteção indireta, via direitos fundamentais, reforça a ideia de que o sigilo fiscal não é apenas uma prerrogativa técnica da administração tributária, mas uma garantia constitucional que protege o cidadão contra abusos e arbitrariedades.

Além disso, o sigilo fiscal desempenha um papel importante na preservação da confiança entre o contribuinte e o Estado. A segurança de que suas informações não serão utilizadas de forma indevida ou expostas publicamente é essencial para que o cidadão cumpra suas obrigações tributárias com tranquilidade. A quebra injustificada desse sigilo pode gerar efeitos negativos, como constrangimento, discriminação ou até mesmo perseguição política ou econômica, comprometendo a legitimidade da atuação estatal.

Nesse sentido, o sigilo fiscal deve ser compreendido como um instrumento de equilíbrio entre o poder de fiscalização do Estado e os direitos individuais dos contribuintes. Ele não impede a atuação legítima da administração tributária, mas impõe limites que garantem a proteção da dignidade e da liberdade informacional. A sua observância é, portanto, condição essencial para a conformidade constitucional das práticas fiscais, especialmente em um cenário de crescente digitalização e compartilhamento de dados.

3 PODER DE FISCALIZAÇÃO TRIBUTÁRIA E SEUS LIMITES

A Constituição Federal de 1988, ao estabelecer as competências tributárias dos entes federativos, confere à administração tributária não apenas o poder de instituir tributos, mas também os meios necessários para sua apuração, arrecadação e fiscalização. Essa prerrogativa é essencial para garantir o funcionamento do Estado e

o cumprimento de suas obrigações sociais. O artigo 145, §1º, da Carta Magna autoriza expressamente a identificação do patrimônio, dos rendimentos e das atividades econômicas dos contribuintes, desde que respeitados os direitos individuais e nos termos da lei. Trata-se, portanto, de uma competência constitucional que legitima o acesso a informações pessoais para fins fiscais.

No exercício dessa função, o Fisco utiliza uma série de instrumentos tecnológicos e administrativos que permitem a coleta e o cruzamento de dados em larga escala. Entre os principais mecanismos estão o Sistema Público de Escrituração Digital (SPED), a declaração de Imposto de Renda (IR) e a emissão de notas fiscais eletrônicas. Esses sistemas exigem que os contribuintes forneçam informações detalhadas sobre suas operações financeiras, comerciais e patrimoniais, o que resulta na formação de grandes bancos de dados sob controle da Receita Federal e das Secretarias de Fazenda estaduais.

A sofisticação desses mecanismos permite à administração tributária construir perfis detalhados dos cidadãos, com base em seus hábitos de consumo, evolução profissional, relações familiares e movimentações bancárias. Embora essa capacidade represente um avanço na eficiência da fiscalização, ela também levanta sérias preocupações quanto à proteção da privacidade. A ausência de limites claros sobre o uso desses dados pode resultar em práticas abusivas, como o monitoramento excessivo ou a utilização de informações para fins não autorizados.

Um marco importante na discussão sobre os limites da fiscalização tributária foi o julgamento do Recurso Extraordinário nº 601.314 pelo Supremo Tribunal Federal. Antes dessa decisão, prevalecia o entendimento de que o acesso a dados bancários pelo Fisco só poderia ocorrer mediante autorização judicial, especialmente em casos envolvendo suspeitas de crimes como sonegação, lavagem de dinheiro ou corrupção. Com o julgamento, o STF reconheceu a constitucionalidade do artigo 6º da Lei Complementar nº 105/2001, que permite o compartilhamento direto de informações entre instituições financeiras e a administração tributária, desde que observadas as garantias legais.

Essa flexibilização, embora tenha sido justificada pela necessidade de aprimorar o combate à evasão fiscal, gerou críticas quanto à possível violação dos

direitos fundamentais à intimidade e à proteção de dados. A ampliação do acesso estatal a informações bancárias sem controle judicial prévio exige uma atuação ainda mais rigorosa no cumprimento dos princípios da legalidade, proporcionalidade e finalidade. O risco de invasão à privacidade é real, especialmente quando não há mecanismos eficazes de supervisão e transparência sobre o tratamento dos dados coletados.

Dessa forma, o poder de fiscalização tributária, embora legítimo e necessário, deve ser exercido com responsabilidade e respeito aos direitos fundamentais. A compatibilização entre eficiência administrativa e proteção da privacidade exige uma abordagem equilibrada, que reconheça os limites constitucionais da atuação estatal e promova a segurança jurídica dos contribuintes.

A ampliação da capacidade fiscalizatória do Estado, especialmente por meio da digitalização dos processos tributários, trouxe ganhos significativos em termos de eficiência e controle. No entanto, essa evolução também acentuou os riscos relacionados à violação da privacidade dos contribuintes. A coleta massiva de dados, muitas vezes realizada sem o devido esclarecimento sobre sua finalidade e sem mecanismos de controle externo, pode comprometer direitos fundamentais, como a autodeterminação informativa e a intimidade.

O uso de tecnologias como o SPED, que integra informações contábeis e fiscais em tempo real, permite ao Fisco uma visão abrangente das operações empresariais e pessoais. A emissão de notas fiscais eletrônicas, por sua vez, registra cada transação comercial, vinculando-a ao CPF ou CNPJ do consumidor. Já a declaração de Imposto de Renda exige a exposição detalhada da situação patrimonial e financeira do contribuinte. Esses instrumentos, embora legítimos, operam sobre uma base de dados extremamente sensível, cuja proteção deve ser rigorosamente observada.

A ausência de uma política nacional unificada de proteção de dados no âmbito tributário, anterior à LGPD, permitia que cada ente federativo adotasse suas próprias regras de coleta, armazenamento e compartilhamento de informações. Isso gerava um cenário de insegurança jurídica, no qual o contribuinte não sabia exatamente como seus dados estavam sendo utilizados, nem por quem. A falta de

transparência e de controle social sobre essas práticas favorecia o uso excessivo ou desproporcional de dados, muitas vezes sem relação direta com a finalidade fiscal.

O julgamento do RE 601.314, embora tenha reconhecido a constitucionalidade do acesso direto do Fisco a dados bancários, também reafirmou a necessidade de observância dos princípios constitucionais. A decisão não eliminou o sigilo bancário, mas condicionou seu acesso à existência de processo administrativo formalizado, com garantias mínimas ao contribuinte. Ainda assim, a flexibilização desse direito gerou preocupações legítimas sobre o potencial de abuso, especialmente em contextos de fiscalização ampla e automatizada.

Outro ponto crítico é a possibilidade de cruzamento de dados entre diferentes bases, como informações bancárias, fiscais, cadastrais e até mesmo de consumo. A integração desses dados permite a construção de perfis comportamentais extremamente precisos, que podem ser utilizados para fins diversos, inclusive fora do escopo tributário. Sem uma delimitação clara da finalidade e sem mecanismos de auditoria independentes, essa prática pode configurar uma violação direta à LGPD e aos direitos fundamentais.

Portanto, o poder de fiscalização tributária deve ser exercido dentro de um marco normativo que respeite os limites constitucionais e legais. A eficiência administrativa não pode justificar a supressão de garantias individuais. É necessário que o Estado adote políticas de governança de dados, com transparência, prestação de contas e respeito à finalidade da coleta. A proteção da privacidade não é um obstáculo à fiscalização, mas uma condição para sua legitimidade.

4 A LGPD E A PROTEÇÃO DE DADOS PESSOAIS

A promulgação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), conhecida como LGPD, representou um marco na consolidação do direito à privacidade no Brasil. Inspirada em legislações internacionais, como a Convenção 108 do Conselho da Europa e a Diretiva Europeia 95/46/CE, a LGPD introduziu um conjunto de princípios e regras voltadas à proteção dos dados pessoais, com aplicação tanto no setor privado quanto no público. Sua principal

finalidade é garantir que o tratamento de informações relativas a pessoas naturais ocorra de forma transparente, segura e respeitosa aos direitos fundamentais.

A LGPD define dado pessoal como qualquer informação relacionada a pessoa natural identificada ou identificável. Isso inclui, por exemplo, nome, CPF, endereço, dados bancários, informações fiscais, entre outros. No contexto tributário, esses dados são amplamente coletados pela administração pública para fins de arrecadação e fiscalização. No entanto, a lei impõe limites claros ao uso dessas informações, exigindo que o tratamento seja realizado com base em uma finalidade legítima, respeitando os princípios da necessidade, adequação e segurança.

Entre os princípios fundamentais da LGPD, destacam-se: (i) a finalidade, que exige que os dados sejam coletados para propósitos específicos e legítimos; (ii) a necessidade, que determina que apenas os dados estritamente necessários sejam tratados; (iii) a transparência, que obriga o controlador a informar ao titular sobre o uso de seus dados; (iv) a segurança, que impõe medidas técnicas e administrativas para proteger os dados contra acessos não autorizados; e (v) o livre acesso, que garante ao titular o direito de consultar, corrigir e excluir suas informações.

A aplicação da LGPD à administração tributária exige uma mudança significativa na cultura institucional. Historicamente, o Estado brasileiro tem operado com grande liberdade na coleta e uso de dados dos cidadãos, especialmente no âmbito fiscal. Programas como o SPED, a declaração de IR e a emissão de notas fiscais envolvem o tratamento de grandes volumes de dados pessoais, muitas vezes sem que o contribuinte tenha clareza sobre como essas informações serão utilizadas. A LGPD, nesse sentido, impõe uma nova lógica, baseada na responsabilização e na prestação de contas.

Um dos principais desafios é compatibilizar a atuação fiscalizadora do Estado com os direitos dos titulares de dados. A administração pública, ao tratar dados pessoais, deve observar os mesmos princípios aplicáveis ao setor privado, inclusive no que diz respeito à limitação de finalidades e à adoção de medidas de segurança. Isso significa que não é mais admissível o uso indiscriminado de informações fiscais para fins diversos, como análise de crédito, políticas públicas genéricas ou compartilhamento com outros órgãos sem base legal específica.

Além disso, a LGPD introduz o conceito de autodeterminação informativa, segundo o qual o titular dos dados tem o direito de controlar o uso de suas informações. Esse princípio reforça a ideia de que o cidadão não é apenas objeto da coleta de dados, mas sujeito ativo na definição dos limites e propósitos desse tratamento. No contexto tributário, isso implica a necessidade de maior transparência por parte do Fisco, com a disponibilização de políticas de privacidade claras, canais de comunicação acessíveis e mecanismos de revisão de decisões automatizadas.

Portanto, a LGPD não representa um obstáculo à atuação da administração tributária, mas sim um instrumento de qualificação dessa atuação. Ao estabelecer parâmetros legais para o tratamento de dados, a lei contribui para a construção de uma relação mais equilibrada entre o Estado e o cidadão, baseada na confiança, na legalidade e na proteção dos direitos fundamentais.

5 COMPATIBILIZAÇÃO DA LEI COM O SIGILO FISCAL

A relação entre o sigilo fiscal e a Lei Geral de Proteção de Dados Pessoais (LGPD) não deve ser compreendida como uma colisão normativa, mas como uma oportunidade de integração entre dois regimes jurídicos que compartilham objetivos comuns: a proteção da privacidade e a limitação do uso indevido de informações pessoais. Ambos os institutos, embora com origens e finalidades distintas, convergem na defesa da dignidade da pessoa humana frente ao poder informacional do Estado.

O sigilo fiscal, como já abordado, decorre do direito à intimidade e à vida privada, funcionando como uma barreira contra a exposição indevida de dados financeiros e patrimoniais. Já a LGPD, ao regulamentar o tratamento de dados pessoais, estabelece princípios que devem ser observados por qualquer agente público ou privado que manipule informações de pessoas naturais. Entre esses princípios, destaca-se o da autodeterminação informativa, que confere ao titular dos dados o poder de decidir sobre o uso e a finalidade de suas informações.

No contexto da administração tributária, essa compatibilização exige uma mudança de paradigma. Tradicionalmente, o Fisco operava com ampla liberdade na

coleta e uso de dados, amparado pela legislação tributária e pela presunção de legitimidade de seus atos. Com a entrada em vigor da LGPD, essa atuação passa a ser condicionada ao respeito aos princípios da finalidade, necessidade, transparência e segurança. Isso significa que o tratamento de dados fiscais deve ser limitado ao estritamente necessário para o cumprimento das obrigações legais, com clareza sobre os propósitos e com garantias de proteção contra acessos indevidos.

Um dos principais pontos de tensão entre os dois regimes é a ausência de controle externo efetivo sobre o uso de dados pela administração tributária. Em muitos casos, como nos programas de incentivo fiscal estaduais ou na emissão de notas fiscais eletrônicas, não há políticas públicas claras de privacidade, nem mecanismos de supervisão que permitam ao contribuinte saber como seus dados estão sendo utilizados. A LGPD, ao exigir a prestação de contas e a transparência, impõe ao Estado o dever de informar e justificar suas práticas de tratamento de dados.

Além disso, a compatibilização entre LGPD e sigilo fiscal demanda a adoção de medidas técnicas e administrativas que garantam a segurança da informação. O vazamento de dados fiscais, além de comprometer a privacidade do contribuinte, pode gerar prejuízos econômicos e sociais significativos. A implementação de sistemas de proteção, auditoria e resposta a incidentes é essencial para assegurar que o tratamento de dados ocorra dentro dos limites legais e éticos.

Outro aspecto relevante é a necessidade de delimitação clara das finalidades do tratamento de dados. A coleta de informações pelo Fisco deve estar vinculada a objetivos específicos, como a apuração de tributos ou a prevenção de ilícitos fiscais. O uso desses dados para outras finalidades, como políticas públicas genéricas ou compartilhamento com outros órgãos sem base legal, configura violação direta à LGPD. A definição de propósitos legítimos e a limitação do uso são elementos centrais para a compatibilização entre os dois regimes.

A compatibilização entre o sigilo fiscal e a LGPD exige não apenas uma leitura técnica das normas envolvidas, mas também uma compreensão sistêmica da função do Estado e dos direitos dos cidadãos em uma sociedade democrática. O sigilo fiscal, como garantia de proteção à intimidade, não pode ser relativizado pela

simples alegação de interesse público. Da mesma forma, a LGPD não deve ser interpretada como um entrave à atuação legítima da administração tributária, mas como um instrumento que qualifica essa atuação, impondo limites e responsabilidades.

Um dos principais pontos de convergência entre os dois institutos é o reconhecimento de que os dados fiscais e bancários são, por natureza, dados pessoais. Isso significa que, mesmo quando coletados por obrigação legal, esses dados devem ser tratados com base nos princípios da LGPD. O princípio da finalidade, por exemplo, exige que a coleta e o uso de informações pelo Fisco estejam diretamente relacionados à atividade de fiscalização e arrecadação, vedando o uso para fins diversos ou genéricos. Já o princípio da necessidade impõe que apenas os dados estritamente indispensáveis sejam tratados, evitando a coleta excessiva ou desproporcional.

Outro aspecto relevante é o dever de transparência. A administração tributária deve informar aos contribuintes, de forma clara e acessível, quais dados estão sendo coletados, para que finalidade, por quanto tempo serão armazenados e com quem poderão ser compartilhados. Essa obrigação, embora já prevista em normas de direito administrativo, ganha reforço com a LGPD, que estabelece o direito do titular de obter informações sobre o tratamento de seus dados, inclusive no âmbito público.

A compatibilização também passa pela implementação de medidas de segurança da informação. O vazamento de dados fiscais pode gerar consequências graves, como fraudes, discriminação ou perseguições indevidas. A LGPD exige que o controlador adote medidas técnicas e organizacionais capazes de proteger os dados contra acessos não autorizados, destruição, perda ou alteração indevida. No caso da administração tributária, isso implica a adoção de sistemas robustos de proteção, auditoria e resposta a incidentes, além da capacitação contínua dos servidores públicos envolvidos no tratamento de dados.

Além disso, é necessário considerar o papel da Autoridade Nacional de Proteção de Dados (ANPD) na fiscalização do cumprimento da LGPD por órgãos públicos. A atuação da ANPD pode contribuir para a harmonização entre os regimes, oferecendo diretrizes específicas para o setor tributário, promovendo boas práticas e

garantindo que os direitos dos titulares sejam respeitados mesmo diante da atuação fiscalizadora do Estado.

6 CONSIDERAÇÕES FINAIS

Por fim, é importante destacar que essa integração normativa não enfraquece a atuação fiscalizadora do Estado, mas a qualifica. Ao respeitar os direitos dos contribuintes e adotar práticas transparentes e seguras, a administração tributária fortalece sua legitimidade e promove uma relação mais equilibrada com a sociedade. A compatibilização entre LGPD e sigilo fiscal é, portanto, um passo necessário para a construção de um modelo de governança pública baseado na proteção de direitos e na confiança mútua.

Além disso, a análise evidencia que a harmonização entre os dois regimes jurídicos não deve ser vista como um obstáculo à eficiência administrativa, mas como um mecanismo essencial para garantir segurança jurídica e preservar a dignidade informacional dos cidadãos. A adoção de políticas claras de governança de dados, associadas a medidas técnicas e organizacionais robustas, é indispensável para prevenir abusos, reduzir riscos de vazamentos e assegurar que o tratamento de informações ocorra dentro dos limites constitucionais e legais.

Outro ponto relevante é a necessidade de maior transparência e prestação de contas por parte do Estado, permitindo que os contribuintes compreendam como seus dados são coletados, utilizados e protegidos. Essa postura reforça a confiança social e contribui para a legitimidade das práticas fiscais. A atuação da Autoridade Nacional de Proteção de Dados também se mostra fundamental para fiscalizar e orientar a aplicação da LGPD no âmbito público, garantindo que os princípios da lei sejam efetivamente observados.

Conclui-se que a integração entre LGPD e sigilo fiscal representa não apenas um desafio jurídico e técnico, mas também uma oportunidade para consolidar um modelo de fiscalização tributária mais ético, transparente e alinhado aos direitos fundamentais. Esse equilíbrio é indispensável para que o Estado exerça seu poder informacional sem comprometer a liberdade e a privacidade dos cidadãos,

promovendo uma relação baseada na legalidade, na confiança e na proteção da dignidade humana.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília: Presidência da República, [s.d.]. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 20 nov. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 20 nov. 2025. [canaltech.com.br], [educacaoeu...oio.com.br]

BRASIL. **Lei Complementar nº 105, de 10 de janeiro de 2001.** Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Diário Oficial da União, Brasília, DF, 11 jan. 2001. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/LCP/Lcp105.htm>. Acesso em: 20 nov. 2025. [planalto.gov.br]

COUNCIL OF EUROPE. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).** Strasbourg, 28 Jan. 1981. Disponível em: <https://www.coe.int/en/web/data-protection/convention108-and-protocol>. Acesso em: 20 nov. 2025. [coe.int], [rm.coe.int]

MELO, A. C. C. **O sigilo fiscal e sua "quebra": análise das previsões legais excepcionantes à luz da Constituição.** Revista Tributária e de Finanças Públicas, São Paulo, v. 82, p. 44, set. 2008.

FEDERIGHI, A. C. P.; CHOW, B. G. **Os sigilos fiscal e bancário e a LGPD: direito fundamental à autodeterminação informacional no âmbito do direito tributário.** Revista de Direito Bancário e do Mercado de Capitais, São Paulo, v. 89, p. 231-256, jul./set. 2020.

MAGNAVITA, A. M. G.; SACRAMENTO, A. R. S.; RAUPP, F. M.; ALMEIDA, D. R. **Entre a transparência e o sigilo fiscal: um estudo dos limites a partir da Secretaria Especial da Receita Federal do Brasil.** Revista Humanidades e Inovação, Palmas, v. 10, n. 9, p. 47-61, 2023. Disponível em: <https://falabr.cgu.gov.br/>. Acesso em: 20 nov. 2025.

BRASIL. **Supremo Tribunal Federal. Recurso Extraordinário nº 601.314/SP.** Relator: Min. Edson Fachin. Julgado em 24 fev. 2016. Publicado no Diário da Justiça Eletrônico em data correspondente. Tema 225 da repercussão geral.

Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur356216/false>. Acesso em: 20 nov. 2025.

Ementa: RECURSO EXTRAORDINÁRIO. REPERCUSSÃO GERAL. DIREITO TRIBUTÁRIO. DIREITO AO SIGILO BANCÁRIO. DEVER DE PAGAR IMPOSTOS. REQUISIÇÃO DE INFORMAÇÃO DA RECEITA FEDERAL ÀS INSTITUIÇÕES FINANCEIRAS. ART. 6º DA LEI COMPLEMENTAR 105/01. MECANISMOS FISCALIZATÓRIOS. APURAÇÃO DE CRÉDITOS RELATIVOS A TRIBUTOS DISTINTOS DA CPMF. PRINCÍPIO DA IRRETROATIVIDADE DA NORMA TRIBUTÁRIA. LEI 10.174/01.

CONSTRUINDO CONFIANÇA SOCIAL: COMO OS ÓRGÃOS DE EMERGÊNCIA PODEM DIVULGAR SUAS AÇÕES RESPEITANDO A LGPD

Lucas Caetano Leão[1]
Nilsa Antonia de Oliveira[2]

RESUMO

A comunicação institucional em órgãos de emergência, como o Serviço de Atendimento Móvel de Urgência (SAMU) e o Corpo de Bombeiros Militar do Distrito Federal (CBMDF), assume papel estratégico na construção da confiança social. O avanço das mídias digitais ampliou as possibilidades de interação com a sociedade, mas também trouxe riscos relacionados à exposição de dados pessoais e à preservação da dignidade das vítimas. Este artigo analisa como esses órgãos podem estruturar práticas de divulgação que conciliem a transparência exigida pela Lei de Acesso à Informação (Lei nº 12.527/2011) com a proteção de dados sensíveis prevista na Lei Geral de Proteção de Dados (Lei nº 13.709/2018). A partir de revisão teórica contextualizada, foram discutidos quatro eixos centrais: o marco legal, a imagem institucional, o uso das redes sociais e a ética na proteção das vítimas. Os resultados apontam que a comunicação responsável deve evitar o sensacionalismo, adotar protocolos internos de divulgação e priorizar narrativas institucionais de caráter educativo e preventivo. Conclui-se que a integração entre conformidade normativa, ética comunicacional e estratégias pedagógicas é indispensável para fortalecer a legitimidade e a credibilidade social do SAMU e do CBMDF.

Palavras-chave: Comunicação institucional; SAMU; CBMDF; LGPD; Lei de Acesso à Informação; Confiança social.

SUMÁRIO: Introdução; 1. Fundamentação Teórica; 1.1. Marco Legal: LGPD e Lei de Acesso à Informação; 1.2. Imagem Institucional e Confiança Social; 1.3. Comunicação Institucional e Redes Sociais; 1.4. Ética e Proteção das Vítimas; 2. Discussão; 3. Conclusão; Referências.

1 INTRODUÇÃO

[1] Graduando em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: lucas.cl@sempreceub.com.
[2] Graduanda em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: nilsa.oliveira@sempreceub.com.

Os órgãos de emergência exercem papel estratégico na proteção da saúde e da segurança pública, sendo reconhecidos pela sociedade como instituições de alta visibilidade e confiança. No Brasil, o Serviço de Atendimento Móvel de Urgência (SAMU) e o Corpo de Bombeiros Militar do Distrito Federal (CBMDF) são exemplos emblemáticos: sua atuação cotidiana impacta diretamente a vida da população e, ao mesmo tempo, projeta uma imagem institucional que deve refletir eficiência, ética e compromisso social.

Nos últimos anos, a expansão do uso de mídias e redes sociais transformou a comunicação dessas instituições. Se, por um lado, os canais digitais ampliaram a interação com a comunidade — permitindo divulgar ocorrências, prestar contas e promover campanhas educativas —, por outro, trouxeram novos desafios relacionados à proteção da privacidade das vítimas e à preservação da credibilidade institucional.

Nesse contexto, a entrada em vigor da Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) e a consolidação da Lei de Acesso à Informação (LAI – Lei nº 12.527/2011) redefiniram os limites da transparência governamental. O desafio para órgãos de emergência não é apenas cumprir obrigações legais, mas equilibrar a divulgação responsável de informações com a salvaguarda da dignidade humana. Trata-se de um campo ainda pouco explorado na literatura, sobretudo em relação a serviços de emergência brasileiros, onde a pressão por transparência convive com riscos de exposição e revitimização.

A fim de enfrentar essa lacuna, este artigo adota como metodologia uma revisão teórica de caráter exploratório e analítico, baseada em legislação, literatura acadêmica recente e estudos aplicados ao campo da comunicação institucional e da gestão pública. A seleção das referências buscou contemplar autores que discutem diretamente os marcos legais (LGPD e LAI), bem como pesquisas sobre imagem institucional, uso de redes sociais e ética na proteção das vítimas. A finalidade metodológica, portanto, não é apresentar um estudo empírico, mas integrar diferentes perspectivas teóricas e normativas para construir diretrizes que orientem práticas comunicacionais de órgãos de emergência no Brasil.

Assim, a discussão não se restringe ao aspecto jurídico: envolve também dimensões comunicacionais, éticas e sociais. A imagem institucional construída pelo SAMU e pelo CBMDF depende da capacidade de conciliar eficiência técnica com responsabilidade na comunicação, evitando práticas sensacionalistas e reforçando a confiança coletiva.

O objetivo deste artigo é analisar como esses órgãos de emergência podem estruturar práticas de comunicação institucional que conciliem a transparência exigida pela LAI com a proteção de dados prevista na LGPD, fortalecendo, ao mesmo tempo, a legitimidade e a confiança social. A análise será desenvolvida a partir de uma revisão teórica contextualizada e resultará na proposição de diretrizes aplicáveis ao SAMU e ao CBMDF para uma promoção institucional responsável.

2 FUNDAMENTAÇÃO TEÓRICA

A construção da confiança social em órgãos de emergência exige não apenas eficiência técnica no atendimento, mas também clareza normativa, legitimidade institucional e responsabilidade ética na comunicação. Nesse sentido, o referencial teórico deste artigo organiza-se em quatro eixos interdependentes: (i) o marco legal representado pela LGPD e pela LAI; (ii) a imagem institucional e sua relação com a confiança social; (iii) as práticas de comunicação institucional em redes sociais; e (iv) a dimensão ética da proteção das vítimas. O objetivo é integrar aspectos jurídicos, comunicacionais e éticos para sustentar a análise de como o SAMU e o CBMDF podem adotar estratégias de divulgação responsáveis e socialmente legitimadas.

2.1 Marco legal: LGPD e Lei de Acesso à Informação

O tratamento de dados pessoais é inerente à atuação de órgãos de emergência como o SAMU e o CBMDF, uma vez que o atendimento a ocorrências frequentemente envolve informações sensíveis, tais como condições clínicas, histórico de saúde e registros que permitem a identificação das vítimas. A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) estabelece que esse

tratamento deve observar princípios como finalidade, adequação, necessidade, transparência e segurança, de modo a assegurar que os dados sejam utilizados apenas para fins legítimos e compatíveis com a preservação da vida e a continuidade da assistência em saúde.

No caso específico dos serviços de emergência, a LGPD autoriza o tratamento de dados pessoais em duas bases principais: a tutela da saúde, prevista no art. 7º, inciso VIII, que abrange o uso das informações para salvaguarda da vida e integridade física, e o cumprimento de obrigação legal ou regulatória, previsto no art. 7º, inciso III, aplicável às instituições públicas em seu dever de prestar serviços essenciais. Dessa forma, o uso dos dados no contexto do atendimento pré-hospitalar encontra respaldo normativo claro, ainda que limitado a finalidades específicas relacionadas à assistência e à gestão pública.

De modo complementar, a Lei de Acesso à Informação (Lei nº 12.527/2011 – LAI) assegura à sociedade o direito de acesso a informações de interesse coletivo ou geral, incluindo dados sobre a gestão, os custos e a eficiência dos serviços públicos. Entretanto, a própria LAI ressalva que informações de caráter pessoal devem ser resguardadas, especialmente quando sua divulgação possa afetar a intimidade, a honra ou a imagem de indivíduos.

Assim, a LGPD e a LAI estabelecem um marco regulatório que orienta os órgãos de emergência a equilibrar duas dimensões fundamentais: a obrigação de proteger os dados sensíveis das vítimas e o dever de garantir transparência em suas ações perante a sociedade. Essa tensão normativa constitui a base para a análise das práticas de comunicação institucional do SAMU e do CBMDF, que será aprofundada nas seções seguintes.

2.2 Imagem institucional e confiança social

A imagem institucional corresponde à forma como uma organização é percebida pelos diferentes públicos com os quais se relaciona. Em instituições públicas de alta visibilidade, como o SAMU e o CBMDF, essa imagem constitui um ativo de legitimidade que influencia diretamente o grau de confiança social.

Diferentemente de organizações privadas, em que a reputação pode estar associada ao desempenho econômico, nos serviços de emergência ela está vinculada à eficiência no atendimento, à transparência das ações e à postura ética diante da sociedade.

A literatura acadêmica confirma a relevância da reputação institucional na geração de vínculos de confiança. Horz et al. (2022), ao analisarem a responsabilidade social corporativa em cooperativas de crédito, demonstram que práticas éticas e transparentes fortalecem tanto a satisfação interna quanto a credibilidade externa. Embora situados em outro contexto, os resultados podem ser tomados como analogia útil para órgãos públicos de emergência: quando os cidadãos percebem que instituições como o SAMU e o CBMDF atuam com responsabilidade social, respeito à privacidade e compromisso com o bem coletivo, tende a haver maior cooperação comunitária e confiança nas suas ações.

Por outro lado, a ausência de mecanismos de accountability pode comprometer essa legitimidade. Rocha, Zuccolotto e Teixeira (2020), ao investigarem os Tribunais de Contas brasileiros, mostram que estruturas pouco permeáveis ao controle social tendem a gerar desconfiança e isolamento institucional. Embora não se trate de estudos sobre serviços de emergência, o raciocínio é aplicável: práticas comunicacionais restritivas, a omissão na prestação de contas ou a adoção de narrativas sensacionalistas podem fragilizar a imagem de órgãos como o SAMU e o CBMDF, reduzindo o capital de confiança acumulado junto à sociedade.

Nesse debate, Laranja (2024) introduz o conceito de Inteligência Pública, definido como uma forma de governança orientada para transparência, integração de dados e ampliação da participação social. A perspectiva é relevante para o contexto dos serviços de emergência, pois sugere que a imagem institucional deve ser entendida não como mero recurso de comunicação ou marketing, mas como elemento integrante de uma estratégia de governança democrática, em que a credibilidade institucional depende da forma como as informações são geridas e compartilhadas com a comunidade.

Assim, os estudos revisados indicam que a imagem institucional resulta de uma combinação entre eficiência técnica, transparência comunicacional e responsabilidade ética. Esses fatores, ao serem considerados como fundamentos teóricos, permitem compreender como a percepção social sobre o SAMU e o CBMDF se forma e se consolida. Nas seções seguintes, esses referenciais serão retomados para analisar de que modo a comunicação em redes sociais e a proteção das vítimas se articulam à construção da confiança social.

2.3 Comunicação institucional e redes sociais

A comunicação institucional deixou de ser apenas um instrumento de informação unidirecional para se consolidar como um espaço de diálogo entre instituições públicas e a sociedade. No caso de órgãos de emergência como o SAMU e o CBMDF, a presença nas redes sociais tem se mostrado estratégica por três razões principais: prestação de contas à população, fortalecimento da imagem institucional e conscientização social em torno da prevenção de riscos.

A literatura aponta que a comunicação institucional pode assumir caráter pedagógico quando bem estruturada. Freitas et al. (2025), ao analisarem estratégias de ensino em saúde, demonstram que metodologias participativas e práticas de simulação favorecem a retenção de conhecimento e o fortalecimento da confiança profissional. Embora o estudo não trate de redes sociais, sua lógica pode ser transposta: assim como a simulação contribui para consolidar práticas no campo da saúde, a comunicação digital pode transformar ocorrências em oportunidades educativas, oferecendo orientações preventivas à população.

Por outro lado, a utilização de redes sociais por órgãos de emergência envolve riscos significativos. O emprego de imagens com viés sensacionalista, a divulgação precipitada de informações não verificadas ou a participação de servidores não autorizados em postagens institucionais podem comprometer a credibilidade da organização. Além disso, a velocidade de circulação das informações nas plataformas digitais potencializa a difusão de críticas infundadas e de notícias falsas. Nesse sentido, estudos sobre políticas públicas de enfrentamento à desinformação no Brasil evidenciam que a disseminação de fake news fragiliza a

confiança social e ameaça a legitimidade das instituições públicas, incluindo aquelas ligadas à saúde e à segurança (SANTOS; SILVA; FERREIRA, 2023).

Diante desse cenário, a literatura destaca a importância de condições que assegurem uma comunicação institucional responsável. Isso implica a adoção de protocolos internos que definam fluxos de aprovação de conteúdos, a capacitação das equipes de comunicação em conformidade com a LGPD e a delimitação de critérios sobre quais informações podem ser divulgadas sem comprometer a privacidade das vítimas. O uso de imagens institucionais, como viaturas, equipamentos e equipes em ação, é frequentemente apontado como alternativa adequada à exposição de indivíduos, enquanto a linguagem deve manter caráter técnico e institucional, evitando a espetacularização de ocorrências.

As redes sociais, ao mesmo tempo, oferecem oportunidades para campanhas de conscientização contínua. O SAMU pode utilizar seus canais oficiais para difundir informações sobre o uso adequado do número 192 e sobre cuidados básicos de primeiros socorros, enquanto o CBMDF pode direcionar campanhas sazonais de prevenção de incêndios ou de segurança viária. Nessas situações, a comunicação cumpre dupla função: além de reforçar a imagem institucional, contribui para a formação de uma cultura de prevenção e cidadania.

Assim, a literatura permite compreender que a comunicação em redes sociais, no âmbito do SAMU e do CBMDF, não deve ser reduzida a um instrumento de visibilidade institucional, mas entendida como parte de uma estratégia mais ampla de governança comunicacional. Essa perspectiva teórica fornece subsídios para analisar, nas seções seguintes, como a dimensão ética e a proteção das vítimas se articulam à construção da confiança social.

2.4 Ética e proteção das vítimas

A dimensão ética da comunicação institucional em órgãos de emergência está intrinsecamente ligada ao princípio da dignidade da pessoa humana, consagrado pela Constituição Federal de 1988, e aos direitos da personalidade que asseguram a inviolabilidade da intimidade, da vida privada, da honra e da imagem (art. 5º, X). No

caso do SAMU e do CBMDF, esse aspecto assume relevância singular, uma vez que tais instituições atuam cotidianamente em situações de extrema vulnerabilidade, como acidentes, doenças súbitas, violência doméstica, tentativas de suicídio e emergências envolvendo idosos ou crianças.

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) aprofunda essa preocupação ao classificar como sensíveis as informações relacionadas à saúde, à vida sexual, à origem étnica ou às convicções pessoais. Fotografias, vídeos ou relatos de atendimentos que permitam a identificação de pacientes devem ser tratados com máxima cautela, uma vez que a divulgação indevida pode configurar violação legal e revitimização. A literatura ressalta que esse cuidado não se limita à esfera normativa, mas constitui igualmente uma exigência ética, pois a exposição pública da vulnerabilidade individual compromete a legitimidade institucional e fragiliza a confiança social.

Pesquisas específicas reforçam essa compreensão. De Lima e Moraes (2023), em revisão integrativa sobre o cuidado a pessoas que tentaram suicídio atendidas em serviços de emergência hospitalar, evidenciam fragilidades no preparo das equipes e destacam a necessidade de protocolos que contemplem não apenas a dimensão biomédica, mas também aspectos psicossociais e comunicacionais. Os autores alertam que a divulgação de ocorrências dessa natureza em redes sociais, ainda que de forma indireta, pode gerar efeitos negativos irreversíveis para vítimas e familiares, além de reforçar estigmas sociais.

No campo dos cuidados paliativos, Bammann et al. (2022) identificam que a sensibilidade ética é fundamental para fortalecer a confiança nos serviços pré-hospitalares, apontando que narrativas institucionais centradas na ação do serviço preservam melhor a dignidade dos pacientes em fim de vida. Da mesma forma, estudos sobre o atendimento pré-hospitalar ao idoso revelam o crescimento das demandas desse grupo e a ausência de protocolos específicos, o que reforça a importância de iniciativas comunicacionais voltadas à prevenção e à proteção de populações vulneráveis.

Essas contribuições teóricas convergem para a compreensão de que ética e proteção das vítimas não se restringem ao cumprimento formal da LGPD, mas

integram a missão pública dos serviços de emergência. A comunicação institucional deve, portanto, evitar a exposição individualizada e assumir caráter educativo e preventivo, em consonância com a preservação da dignidade humana. Esses referenciais constituem a base para a análise que será desenvolvida na seção seguinte, voltada à discussão das implicações práticas para a comunicação responsável do SAMU e do CBMDF.

3 DISCUSSÃO

A análise do referencial teórico evidencia que a comunicação institucional dos órgãos de emergência se estrutura em um campo de tensões, em que a necessidade de transparência convive com a obrigação de resguardar a privacidade das vítimas. No caso do SAMU e do CBMDF, essas tensões são ainda mais visíveis, pois a exposição de suas atividades ocorre em situações de forte impacto social, nas quais qualquer falha comunicacional pode repercutir diretamente na confiança da sociedade.

O marco normativo, representado pela LGPD (Lei nº 13.709/2018) e pela LAI (Lei nº 12.527/2011), delimita os contornos jurídicos desse processo. Como apontam Oliveira e Aureliano (2024) e Rios (2024), a adequação à LGPD exige protocolos institucionais claros para o tratamento e a divulgação de dados, enquanto a LAI impõe a obrigação de garantir acesso às informações de interesse coletivo. Na prática, SAMU e CBMDF precisam encontrar mecanismos de compatibilização, como o uso de dados anonimizados e a publicação de relatórios institucionais, que permitam conciliar transparência e proteção da privacidade.

Além da dimensão normativa, a literatura ressalta a importância da imagem institucional como recurso estratégico para sustentar a confiança social. Horz et al. (2022) demonstram que práticas responsáveis fortalecem vínculos internos e externos, enquanto Rocha, Zuccolotto e Teixeira (2020) alertam para os riscos de isolamento institucional quando não há accountability efetiva. Aplicados ao SAMU e ao CBMDF, esses achados indicam que a imagem construída pela comunicação não deve se limitar à autopromoção, mas refletir responsabilidade ética, clareza informacional e abertura ao diálogo social.

As redes sociais acrescentam complexidade a esse cenário. Por um lado, oferecem meios de aproximação com a população, viabilizando campanhas educativas e prestação de contas mais ágil. Por outro, aumentam os riscos de sensacionalismo e de disseminação de fake news, o que pode corroer a legitimidade institucional. Freitas et al. (2025) mostram que estratégias comunicacionais podem ter caráter pedagógico, e esse raciocínio pode ser transposto para o uso das plataformas digitais: ocorrências divulgadas de forma responsável podem ser convertidas em oportunidades de aprendizagem social. Contudo, sem protocolos internos, a velocidade da informação pode gerar erros irreparáveis para a credibilidade dos serviços.

Por fim, a dimensão ética se revela central na construção da confiança coletiva. Estudos sobre atendimento em situações de vulnerabilidade — como os de De Lima e Moraes (2023) sobre tentativas de suicídio e de Bammann et al. (2022) sobre cuidados paliativos — demonstram que a comunicação deve priorizar a preservação da dignidade humana, evitando a exploração da dor individual. Esse cuidado ético não se restringe ao cumprimento formal da LGPD, mas constitui fundamento da legitimidade dos serviços de emergência perante a sociedade.

Assim, os quatro eixos analisados convergem para a compreensão de que a comunicação institucional de órgãos como SAMU e CBMDF não é uma dimensão acessória de sua atuação, mas parte integrante de sua missão pública. O desafio está em integrar marcos legais, práticas comunicacionais responsáveis, estratégias de fortalecimento da imagem e compromissos éticos em uma abordagem coerente, capaz de sustentar a confiança social em longo prazo.

4 CONCLUSÃO

A análise desenvolvida neste artigo demonstrou que a comunicação institucional dos órgãos de emergência, em especial o SAMU e o CBMDF, deve ser entendida como parte essencial de sua missão pública. A partir da revisão teórica, verificou-se que quatro dimensões estruturam esse processo: o marco legal, a imagem institucional, o uso das redes sociais e a ética na proteção das vítimas.

No campo normativo, a compatibilização entre a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e a Lei de Acesso à Informação (Lei nº 12.527/2011) mostra que transparência e privacidade não se contrapõem, mas se complementam. A divulgação de dados anonimizados, relatórios institucionais e indicadores de desempenho permite conciliar o dever de prestar contas à sociedade com a proteção dos direitos individuais.

No plano da imagem institucional, constatou-se que a legitimidade de serviços de emergência não se sustenta apenas pela eficiência técnica, mas também pela percepção de que atuam com ética, responsabilidade e abertura ao controle social. Práticas comunicacionais que evitam o sensacionalismo e priorizam a clareza reforçam a confiança da população e consolidam o papel dessas instituições como referência de proteção coletiva.

As redes sociais, embora representem espaço de riscos pela velocidade da informação e pela possibilidade de difusão de notícias falsas, também oferecem oportunidades para aproximar a população, difundir campanhas educativas e reforçar a imagem institucional. Para que cumpram essa função, é indispensável a existência de protocolos internos de comunicação, que orientem o conteúdo e a forma de divulgação, evitando a exposição indevida de indivíduos e fortalecendo o caráter pedagógico da informação.

A dimensão ética, por sua vez, constitui o eixo orientador de toda prática comunicacional. O respeito à dignidade humana em situações de vulnerabilidade — como tentativas de suicídio, atendimentos a idosos ou cuidados em fim de vida — exige narrativas institucionais centradas na ação do serviço, e não na exposição da dor individual. Essa postura preserva a legitimidade e contribui para a construção de confiança duradoura.

Conclui-se, portanto, que a comunicação institucional responsável, alicerçada nos marcos legais, orientada pela ética e articulada a estratégias educativas, é condição indispensável para que o SAMU e o CBMDF mantenham e fortaleçam sua credibilidade junto à sociedade. Como perspectiva futura, indica-se a elaboração de protocolos específicos de comunicação para serviços de emergência no Brasil, bem como estudos empíricos que avaliem como a população percebe a imagem dessas

instituições diante da adoção de práticas comunicacionais em conformidade com a LGPD e a LAI.

REFERÊNCIAS

BAMMANN, Luísa Helena Maurell; CORDEIRO, Franciele Roberta; CORRÊA, Izadora Martins; SILVA, Felipe Ferreira. Estratégias para a atuação pré-hospitalar diante de pacientes com doença avançada em final de vida e suas famílias: revisão integrativa. Research, Society and Development, v. 11, n. 1, e34611125207, 2022. DOI: http://dx.doi.org/10.33448/rsd-v11i1.25207. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/25207. Acesso em: 7 set. 2025.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 7 set. 2025.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso à informação previsto na Constituição Federal. Diário Oficial da União: Brasília, DF, 18 nov. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 7 set. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 7 set. 2025.

DE LIMA, Dorlivete Moreira; MORAES, Ana Cláudia Souto. Cuidado às pessoas que tentam suicídio atendidas em emergência hospitalar: uma revisão integrativa. Revista Psicologia e Pesquisa, v. 16, n. 2, p. 1–18, 2023. DOI: https://doi.org/10.24879/2023001600200574. Disponível em: https://editora.sepq.org.br/rpq/article/view/574. Acesso em: 7 set. 2025.

FREITAS, Marisa Ferreira de; BERNARDINELLI, Fabiana Cristina Pires; RUIZ, Mariana Torreglosa; AMARAL, Eliana Maria Scarelli; CHAVAGLIA, Suzel Regina Ribeiro. Estratégias pedagógicas voltadas à assistência em saúde na parada cardiorrespiratória em gestantes: revisão integrativa. Revista de Enfermagem Atenção à Saúde, v. 15, n. 1, p. e20257725, 2025. DOI: https://doi.org/10.18554/reas.v15i1.7725. Disponível em: https://seer.uftm.edu.br/revistaeletronica/index.php/enfer/article/view/7725. Acesso em: 7 set. 2025.

HORZ, Vagner; ACCADROLLI, Monique Couto; FRARE, Anderson Betti; CRUZ, Ana Paula Capuano da. Implicações da reputação de responsabilidade social corporativa no comprometimento organizacional: o papel mediador da satisfação no trabalho. Globalización, Competitividad y Gobernabilidad, Georgetown University,

v. 16, n. 1, p. 115–127, 2022. DOI: https://doi.org/10.3232/GCG.2022.V16.N1.06. Acesso em: 7 set. 2025.

LARANJA, Lara Silva. Inteligência pública, gestão e governança para o desenvolvimento no Sul Global: considerações e aplicações para o Brasil e a saúde. 2024. 300 f. Tese (Doutorado em Desenvolvimento, Sociedade e Cooperação Internacional) – Universidade de Brasília, Brasília; Instituto Politécnico Nacional, Cidade do México, 2024. Disponível em: https://repositorio.unb.br/bitstream/10482/51923/1/LaraSilvaLaranja_TESE.pdf. Acesso em: 7 set. 2025.

OLIVEIRA, Sheilane Karla Martins de; AURELIANO, Viviane Cristina Oliveira. LGPD e guias de adequação à lei: uma revisão sistemática da literatura. Monografia (Especialização em Gestão e Qualidade em Tecnologia da Informação e Comunicação) – Instituto Federal de Pernambuco, Campus Jaboatão dos Guararapes, Jaboatão dos Guararapes, 2024. Disponível em: https://repositorio.ifpe.edu.br/xmlui/handle/123456789/1348. Acesso em: 7 set. 2025.

RIOS, Isaac Rozas. Tratamento dos dados pessoais nas universidades federais do Brasil: proposta de modelo de maturidade sob a perspectiva dos marcos legais brasileiros. 2024. 533 f. Tese (Doutorado em Ciência da Informação) – Universidade Federal da Paraíba, João Pessoa, 2024. Disponível em: https://repositorio.ufpb.br/jspui/handle/123456789/34794. Acesso em: 7 set. 2025.

ROCHA, Diones Gomes da; ZUCCOLOTTO, Robson; TEIXEIRA, Marco Antonio Carvalho. Insulados e não democráticos: a (im)possibilidade do exercício da social accountability nos Tribunais de Contas brasileiros. Revista de Administração Pública, Rio de Janeiro, v. 54, n. 2, p. 201–219, mar./abr. 2020. DOI: http://dx.doi.org/10.1590/0034-761220190294. Acesso em: 7 set. 2025.

SANTOS, Gustavo; SILVA, Mariana; FERREIRA, Lucas. Políticas públicas de combate às fake news aplicadas no Brasil. Revista de Políticas Públicas e Comunicação, v. 12, n. 1, p. 45–63, 2023. Disponível em: https://editora.sepq.org.br/rpq/article/view/574. Acesso em: 7 set. 2025.

MEU INSS: FACILIDADE DIGITAL OU FONTE DE INSEGURANÇA NO PLANEJAMENTO DA APOSENTADORIA?

Daniela de Brito Olinto[1]

RESUMO

Este artigo analisa as limitações do aplicativo oficial Meu INSS e seu impacto no planejamento previdenciário do trabalhador, questionando se a digitalização dos serviços representa uma facilidade ou uma fonte de insegurança jurídica. O estudo se justifica pela vasta gama de dados pessoais de pessoas físicas, ou seja, pessoas naturais, que são tratadas por entidades públicas e privadas, e que, no contexto previdenciário, englobam informações cruciais para a garantia de direitos sociais. Busca-se responder ao seguinte questionamento: como as deficiências do aplicativo oficial, aliadas à proliferação de plataformas privadas não regulamentadas, expõem o trabalhador a riscos digitais e comprometem a segurança jurídica de seu planejamento previdenciário? A pesquisa baseia-se na necessidade de garantir os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo, princípios que devem nortear a prestação de serviços digitais, públicos ou privados. Por meio da contextualização da falha regulatória e da exposição a riscos de dados (analogamente a cenários de megavazamento de dados), conclui-se que o acesso à previdência na era digital exige urgentemente uma abordagem que incorpore os princípios da LGPD (Lei nº 13.709/2018) e mecanismos de fiscalização robustos para os agentes de tratamento de dados que operam fora da esfera oficial, como Fintechs e escritórios privados.

Palavras-chave: Meu INSS; Previdência; LGPD; Segurança Jurídica; Aplicativos Privados; Dados Pessoais.

SUMÁRIO: Introdução. 1. O Direito Social à Previdência e a Inserção Digital do Meu INSS; 2. O Caráter Vastíssimo dos Dados Pessoais Previdenciários e a Proteção Legal; 3. A Proliferação de Aplicativos Privados e a Insegurança Jurídica; 4. A Necessidade de Mecanismos de Fiscalização e de Indicadores Auditáveis; Conclusões; Referências.

1 INTRODUÇÃO

[1] Graduanda em Direito do UniCEUB – Centro Universitário de Brasília.

A tecnologia digital transformou radicalmente a maneira como o cidadão acessa serviços públicos, e o aplicativo Meu INSS é um exemplo proeminente dessa mudança na esfera previdenciária. Contudo, essa inserção digital, apesar de promover a celeridade e a simplificação de processos, inaugurou uma nova onda de problemáticas e questões sensíveis, especialmente no que tange à segurança jurídica e ao planejamento da aposentadoria.

2 O DIREITO SOCIAL À PREVIDÊNCIA E A INSERÇÃO DIGITAL DO MEU INSS

No direito social à previdência busca garantir uma condição mínima de existência para os membros da sociedade, sendo a moradia e a segurança elementos essenciais, conforme previsto na Constituição Federal. A digitalização do acesso a esses direitos, mediada por plataformas como o Meu INSS, exige que a segurança jurídica seja mantida, algo que nem sempre é evidente quando o serviço oficial apresenta deficiências ou falhas operacionais.

O problema central reside nas limitações funcionais do Meu INSS, que levam o trabalhador a buscar soluções em plataformas alternativas, como aplicativos feitos por escritórios de advocacia, serviços privados, Fintechs e Startups de Previdência. Essa migração para o ambiente não oficial, ou não diretamente fiscalizado, gera uma falta de segurança jurídica na liberdade das pessoas na internet ao lidar com dados de natureza financeira e previdenciária altamente sensíveis. É necessário, portanto, refletir até que ponto essa liberdade de acesso digital pode afetar o cidadão e comprometer a garantia dos seus direitos fundamentais.

3 O CARÁTER VASTÍSSIMO DOS DADOS PESSOAIS PREVIDENCIÁRIOS E A PROTEÇÃO LEGAL

Quando o aplicativo oficial Meu INSS falha em prover informações claras ou permite inconsistências, o trabalhador é impelido a procurar alternativas em plataformas privadas, como as oferecidas por escritórios de previdência, Fintechs ou Startups. A ascensão de plataformas digitais, como as Fintechs, faz parte de um mercado que usa estratégias avançadas para atrair e manter usuários, mas que, no

campo previdenciário, lida com a expectativa de ganhar algo em troca (uma aposentadoria mais vantajosa ou mais rápida), expondo o usuário a riscos se a regulamentação for frágil.

Tais plataformas não tão reconhecidas, ao operarem com dados previdenciários, assumem o papel de agentes de tratamento de dados (Controlador e/ou Operador). No entanto, a falta de clareza sobre como essas entidades privadas cumprem a legislação de proteção de dados e a segurança de suas infraestruturas (especialmente quanto ao tratamento de dados sensíveis) cria um vácuo de insegurança jurídica.

4 A PROLIFERAÇÃO DE APLICATIVOS PRIVADOS E A INSEGURANÇA JURÍDICA

Este problema se assemelha à fragilidade regulatória observada em outros setores digitais, onde o crescimento substancial e a movimentação de recursos exigem fiscalização. No Brasil, a experiência tem demonstrado que, mesmo havendo legislação (como a LGPD, Lei nº 13.709), a falta de fiscalização adequada pode comprometer a eficácia das normas. A Constituição e a jurisprudência buscam garantir a segurança jurídica, mas isso é desafiado quando os prestadores de serviços digitais operam com regras pouco claras ou com deficiências de fiscalização.

A complexidade é amplificada pelo fato de que o risco de vazamento de dados, mesmo os não sensíveis, pode gerar dano moral presumido, e a responsabilidade civil por danos causados é objetiva. Assim, a escolha do trabalhador por um aplicativo privado, em busca de uma facilidade, pode inadvertidamente resultar na exposição de seu histórico de vida profissional a riscos de segurança digital.

5 A NECESSIDADE DE MECANISMOS DE FISCALIZAÇÃO E DE INDICADORES AUDITÁVEIS

Para mitigar a insegurança gerada pelas limitações do Meu INSS e pela presença de aplicativos privados, o arcabouço legal brasileiro deve ser mobilizado

para exigir maior transparência e controle. O debate legislativo deve focar em regras mais claras que possam garantir mais direitos e reforçar a segurança jurídica.

A fiscalização e sanções (Arts. 52–54) previstas na LGPD, aplicáveis pela Autoridade Nacional de Proteção de Dados (ANPD), devem ser rigorosamente observadas. As Fintechs e Startups de Previdência devem estar sujeitas a estas sanções, que incluem multas, advertência, suspensão e bloqueio. A ameaça de multas por irregularidades pode chegar a R$ 50 milhões, o que demonstra a seriedade com que a legislação trata a violação de dados.

É essencial que, no contexto previdenciário digital:

1. Haja rastreabilidade e integridade: Para que o cidadão possa confiar na internet, o aplicativo deve garantir a rastreabilidade da origem dos dados publicados e a integridade das informações. O anonimato é vedado pela Constituição na manifestação do pensamento, e no tratamento de dados previdenciários, a identificação clara e a responsabilidade são cruciais para combater abusos e crimes virtuais.

2. Sejam exigidos indicadores auditáveis: A natureza principiológica da LGPD implica que todos os agentes de tratamento (incluindo aplicativos privados) devem fornecer mecanismos que permitam a auditoria de suas operações, garantindo que a interpretação constitucional seja um caminho para concretizar direitos.

3. Seja assegurada a defesa do consumidor: A defesa do consumidor é um princípio da ordem econômica. Os usuários de aplicativos previdenciários (públicos ou privados) devem ter a garantia da efetiva prevenção e reparação dos danos, especialmente em um campo onde há hipossuficiência técnica por parte do trabalhador.

O sistema exige uma abordagem dialógica na separação de poderes, onde o Judiciário (STF) e o Legislativo precisam construir conjuntamente regras que confiram maior segurança jurídica para direitos. A ausência de regras claras ou a ineficácia da fiscalização do Meu INSS levanta preocupações que exigem a atenção do Poder Legislativo.

4 CONCLUSÕES

A digitalização do acesso à Previdência Social, embora promova a comodidade (facilidade digital), introduz novos vetores de risco e insegurança no planejamento da aposentadoria. As limitações do aplicativo oficial Meu INSS e a busca por soluções em plataformas privadas (Fintechs, Startups ou escritórios) expõem o trabalhador a um tratamento de dados vastíssimo e sensível que, se não for rigorosamente regulamentado, viola os direitos fundamentais de privacidade e liberdade.

A LGPD é o pilar para lidar com essa ameaça, exigindo indicadores auditáveis e responsabilizando os agentes de tratamento. A garantia da segurança jurídica no ambiente digital depende tanto da atuação proativa do Poder Público para melhorar e fiscalizar o aplicativo oficial, quanto da aplicação rigorosa da legislação de proteção de dados sobre as plataformas privadas.

O cidadão comum, por sua vez, deve adotar medidas de proteção, como reforçar senhas e ser diligente ao não confirmar dados por canais não oficiais. Contudo, a responsabilidade primordial recai sobre o Estado e os agentes privados que detêm e tratam esses dados, para que a inovação tecnológica não sirva como um atalho para a violação dos direitos e garantias fundamentais. A busca por mais direitos, reconhecidos em leis editadas pelo Congresso Nacional, deve seguir o compromisso de assegurar a dignidade humana no planejamento previdenciário digital.

REFERÊNCIAS

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 26 out. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União**: seção 1, Brasília, DF, ano 155, n. 157, p. 59-64, 15 ago.

2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 out. 2025.

CIRNE, Mariana Barbosa; MARTINS, Amanda Ribeiro; ROSELLI, Igor Andrey (Org.). **Constituição, processo legislativo e Supremo Tribunal Federal**: interagindo por mais direitos. Brasília: CEUB, 2025. 143 p.

CNN BRASIL ECONOMIA. **Entenda o risco do vazamento de dados pessoais**. YouTube, 2021. Disponível em: https://www.youtube.com/watch?v=f5vygiM5-00. Acesso em: 29 set. 2025.

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

MOURÃO, Daniela Machado. Estudo sobre o impacto de eventos climáticos extremos na vida das pessoas em situação de vulnerabilidade econômica. In: CIRNE, Mariana Barbosa; MARTINS, Amanda Ribeiro; ROSELLI, Igor Andrey (Org.). **Constituição, processo legislativo e Supremo Tribunal Federal**: interagindo por mais direitos. Brasília: CEUB, 2025. p. 62-74.

POLITIZE!. O IMPÉRIO das BETS: **A verdade OBSCURA por trás das apostas online**. YouTube, 2024. Vídeo (28:23). Disponível em: https://www.youtube.com/watch?v=fpPFzA2KDds. Acesso em: 29 set. /2025.

SCHNEIDER, Leonardo Calice. **A liberdade de expressão na internet**: regulação, corregulação ou autorregulação? Editora Dialética, 2024. p 140.

SILVA, Gabriel Henrique Leite da. Liberdade de expressão na internet: estudo dos projetos de lei sobre a liberdade de expressão e como esse direito é garantido na internet. In: CIRNE, Mariana Barbosa; MARTINS, Amanda Ribeiro; ROSELLI, Igor Andrey (Org.). **Constituição, processo legislativo e Supremo Tribunal Federal**: interagindo por mais direitos. Brasília: CEUB, 2025. p. 9-22.

SILVA, Mel Luiza Rodrigues de Alcântara e. Liberdade de expressão e seus limites: avaliação do alcance da garantia constitucional do artigo 5º da constituição federal. In: CIRNE, Mariana Barbosa; MARTINS, Amanda Ribeiro; ROSELLI, Igor Andrey (Org.). **Constituição, processo legislativo e Supremo Tribunal Federal**: interagindo por mais direitos. Brasília: CEUB, 2025. p. 104-117.

PARTE III – DIREITO DIGITAL, CIBERCRIMINALIDADE E SEGURANÇA

CRIMES CIBERNÉTICOS: A EFICÁCIA DAS LEGISLAÇÕES BRASILEIRAS

Bárbara Moon[1]

RESUMO

Este artigo analisa a crescente incidência dos crimes cibernéticos no Brasil e a efetividade das legislações nacionais na prevenção, investigação e punição dessas condutas. A partir da evolução normativa, especialmente após a promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD), observa-se um avanço significativo na proteção de dados pessoais e na responsabilização de agentes públicos e privados. Apesar disso, desafios persistem em razão da sofisticação das ameaças digitais, da transnacionalidade dos delitos e das limitações estruturais enfrentadas pelos órgãos de segurança e pela própria Administração Pública. A análise deste estudo é ilustrada por dois casos concretos de grande repercussão nacional: o megavazamento de dados de 223 milhões de brasileiros ocorrido em 2021, considerado um dos maiores crimes cibernéticos da história do país, e o ataque hacker ao Superior Tribunal de Justiça (2020), que paralisou o funcionamento da Corte. Ambos os episódios evidenciam vulnerabilidades críticas em sistemas públicos e privados, bem como a urgência de um fortalecimento da governança de dados no Brasil. Os exemplos demonstram que, embora a legislação brasileira seja robusta em teoria — com marcos como a Lei Carolina Dieckmann, o Marco Civil da Internet, a LGPD e a Lei nº 14.155/2021 —, sua eficácia depende de políticas públicas de inclusão digital, investimentos contínuos em tecnologia de segurança e cooperação técnica internacional. O artigo discute ainda impactos sociais, econômicos e políticos dos crimes cibernéticos, apresenta comparações com sistemas normativos estrangeiros e propõe medidas de aprimoramento do modelo brasileiro.

Palavras-chave: Crimes Cibernéticos; Direito Penal; Proteção de Dados; LGPD; Marco Civil da Internet; Cibersegurança; Responsabilidade Jurídica.

1 INTRODUÇÃO

[1] Graduanda em Direito do UniCEUB – Centro Universitário de Brasília. Email: barbara.moon@sempreceub.com

A revolução digital inaugurou um novo paradigma de relações sociais, econômicas e políticas. A internet deixou de ser apenas um meio de comunicação e passou a integrar a estrutura essencial da vida cotidiana, do mercado financeiro à administração pública. Nesse contexto, emergem os crimes cibernéticos, caracterizados por elevado potencial ofensivo, alcance global e sofisticação técnica. Embora o Brasil tenha avançado na criação de dispositivos legais específicos, ainda persiste o debate sobre sua real eficácia.

Este artigo analisa criticamente a evolução da legislação brasileira destinada a enfrentar crimes cibernéticos, com destaque para a Lei Geral de Proteção de Dados (LGPD). Além disso, serão examinados casos concretos que evidenciam vulnerabilidades da sociedade e do Estado.

2 CRIMES CIBERNÉTICOS: CONCEITO E TIPOLOGIA

Os crimes cibernéticos consistem em condutas ilícitas praticadas com o uso de sistemas informatizados, dispositivos eletrônicos ou redes digitais. Podem afetar bens jurídicos individuais — como patrimônio, privacidade, honra — e bens coletivos — como segurança nacional e estabilidade institucional. A doutrina costuma classificá-los em três grupos:

- **Crimes cibernéticos puros** – aqueles que só podem ocorrer no ambiente digital, como invasão de sistemas, ransomware, DDoS, phishing e distribuição de malware.
- **Crimes cibernéticos mistos** – condutas tradicionais praticadas por meio da internet, como fraudes bancárias, estelionato eletrônico, pornografia infantil e crimes contra a honra.
- **Crimes cibernéticos conexos** – situações em que a internet serve como meio acessório para facilitar práticas ilícitas, como a comunicação entre membros de organizações criminosas.

Essa classificação evidencia a diversidade e complexidade das ameaças contemporâneas que cercam o ambiente virtual.

3 EVOLUÇÃO NORMATIVA BRASILEIRA E A LGPD

Por muito tempo, o Brasil enfrentou crimes digitais utilizando tipos penais tradicionais, o que tornava difícil responsabilizar autores de ataques complexos. Nos últimos anos, porém, o arcabouço jurídico se tornou mais robusto.

3.1 Principais marcos legislativos

- **Lei nº 12.737/2012 (Lei Carolina Dieckmann)** – tipificou a invasão de dispositivo informático e a obtenção de dados sem autorização.
- **Lei nº 12.965/2014 (Marco Civil da Internet)** – estabeleceu direitos e deveres no uso da internet, com destaque para regras de guarda e fornecimento de registros.
- **Lei nº 13.709/2018 (LGPD)** – regulamentou o tratamento de dados pessoais e estabeleceu princípios, bases legais e sanções administrativas.
- **Lei nº 14.155/2021** – aumentou penas para estelionatos e fraudes cometidas por meio eletrônico.

3.2 A LGPD e sua importância

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, consolidou-se como um dos marcos regulatórios mais relevantes na construção de um ambiente digital mais seguro e transparente no Brasil. Sua criação decorreu da necessidade de estabelecer parâmetros claros para o tratamento de informações pessoais, em um cenário de crescente digitalização das relações sociais, expansão do comércio eletrônico e aumento significativo dos crimes cibernéticos envolvendo dados sensíveis. Ao regulamentar como dados podem ser coletados, utilizados, armazenados e compartilhados por agentes públicos e privados, a LGPD promove uma cultura de responsabilização e reforça a proteção dos direitos fundamentais à privacidade, à autodeterminação informativa e à inviolabilidade da intimidade.

A importância da LGPD é evidenciada pela abrangência de seus princípios, entre os quais se destacam a finalidade, a necessidade, a transparência, a segurança e a responsabilização. Tais princípios orientam as práticas de tratamento de dados e exigem que empresas e órgãos públicos adotem medidas técnicas e administrativas robustas para garantir a integridade, confidencialidade e disponibilidade das informações sob sua guarda. O artigo 7º estabelece as bases legais que legitimam o tratamento de dados, enquanto o artigo 46 impõe a adoção de mecanismos capazes de prevenir incidentes de segurança. Já os artigos 48 e 50 tratam da comunicação de vazamentos e da implementação de programas de governança, reforçando a obrigação de gestão ativa e preventiva dos riscos.

A criação da Autoridade Nacional de Proteção de Dados (ANPD) representa outro avanço significativo, ao conferir fiscalização efetiva e padronização regulatória ao tema. A atuação da ANPD tem sido fundamental para orientar instituições, promover boas práticas e aplicar sanções administrativas quando necessário, garantindo maior segurança jurídica. Esse fortalecimento institucional também posiciona o Brasil de maneira mais competitiva no cenário internacional, alinhando-o às diretrizes de legislações avançadas, como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR).

Além de seu papel regulatório, a LGPD exerce função essencial no enfrentamento dos crimes cibernéticos, uma vez que incidentes envolvendo vazamento ou uso indevido de dados pessoais podem resultar em graves prejuízos econômicos, sociais e emocionais às vítimas. Ao impor controles rigorosos, a lei contribui para a redução de vulnerabilidades exploradas por criminosos e reforça mecanismos de rastreabilidade que auxiliam investigações. A conformidade com a LGPD, portanto, não se limita ao cumprimento formal da legislação, mas se revela elemento estratégico de segurança cibernética, mitigação de riscos e preservação da confiança nas relações digitais.

A LGPD representa marco essencial no combate a crimes cibernéticos, fortalecendo a prevenção e garantindo direitos fundamentais dos cidadãos.

4 CASOS PRÁTICOS

4.1 Megavazamento de dados de 223 milhões de brasileiros (2021)

O megavazamento de dados ocorrido em janeiro de 2021 é considerado um dos maiores incidentes de segurança da história do Brasil e um dos maiores do mundo. O caso envolveu a exposição ilícita de informações pessoais de aproximadamente 223 milhões de brasileiros, incluindo pessoas falecidas, demonstrando a dimensão do nível de vulnerabilidade presente em bancos de dados públicos e privados no país. Entre os dados vazados estavam nomes completos, CPF, datas de nascimento, endereços, telefones, informações de renda, fotografias de documentos, vínculos empregatícios, scores de crédito e até mesmo detalhes sensíveis relacionados a beneficiários de programas sociais.

As informações foram colocadas à venda em fóruns da dark web e oferecidas em pacotes segmentados, com valores variáveis conforme a sensibilidade dos dados. A forma como esses dados foram compilados sugeriu a possibilidade de múltiplas fontes, incluindo bases de órgãos governamentais e instituições financeiras, embora a origem exata jamais tenha sido oficialmente confirmada. A amplitude das informações expostas, abrangendo praticamente toda a população brasileira, evidenciou a existência de extensas fragilidades de segurança na gestão e no armazenamento de dados.

As consequências foram imediatas e graves. O vazamento ampliou o risco de práticas de estelionato eletrônico, abertura de contas bancárias fraudulentas, golpes de phishing altamente personalizados e ataques direcionados contra indivíduos e empresas. Para milhões de cidadãos, a exposição significou vulnerabilidade permanente, já que dados como CPF e data de nascimento são imutáveis e dificilmente podem ser protegidos após sua divulgação pública.

Do ponto de vista jurídico, o incidente representou um marco decisivo para o debate sobre a eficácia da LGPD e sobre a necessidade de fortalecimento da Autoridade Nacional de Proteção de Dados (ANPD). O megavazamento levou à abertura de investigações pela Polícia Federal, pelo Ministério Público e pela própria ANPD, além de gerar intensa pressão social para o aprimoramento dos mecanismos de governança e segurança cibernética. O caso também demonstrou como delitos

dessa natureza desafiam as estruturas investigativas tradicionais, uma vez que envolvem atuação transnacional, anonimização de autores, técnicas avançadas de ocultação digital e exploração de vulnerabilidades sistêmicas.

Em síntese, o megavazamento de 2021 expôs não apenas falhas técnicas na proteção de dados pessoais, mas também fragilidades estruturais na capacidade estatal de prevenção e resposta a incidentes de grande escala. O episódio permanece como um dos exemplos mais emblemáticos da urgência em fortalecer políticas públicas de segurança da informação, investir em infraestrutura tecnológica e aprimorar o aparato legislativo e investigativo voltado ao enfrentamento dos crimes cibernéticos no Brasil.

4.2 Invasão Hacker ao Superior Tribunal de Justiça (2020)

O ataque cibernético sofrido pelo Superior Tribunal de Justiça (STJ) em novembro de 2020 tornou-se um dos episódios mais graves de violação à segurança institucional no Brasil, revelando fragilidades significativas na proteção de dados e na governança digital do Poder Judiciário. A ofensiva, atribuída a um sofisticado grupo de hackers, consistiu na infiltração nos servidores internos da Corte e na execução de um ataque de ransomware, que criptografou completamente bancos de dados, documentos processuais e sistemas essenciais. Como consequência imediata, o STJ teve suas atividades paralisadas por vários dias, impossibilitando o funcionamento de sistemas processuais e administrativos.

A investigação conduzida pela Polícia Federal apontou que os invasores exploraram vulnerabilidades técnicas em servidores internos, possivelmente decorrentes de falhas de atualização e ausência de mecanismos robustos de segmentação de rede. Embora o ataque tenha sido controlado, o impacto foi profundo: processos em andamento ficaram inacessíveis, o tribunal precisou acionar protocolos emergenciais e a integridade dos dados processuais ficou sob risco. O episódio evidenciou que, mesmo órgãos públicos de alta relevância institucional, responsáveis por decisões de alcance nacional, podem ser alvos de agentes cibernéticos altamente organizados.

A LGPD desempenha papel essencial na análise desse caso. Seus dispositivos determinam que órgãos públicos adotem medidas técnicas e administrativas aptas a proteger dados pessoais e sensíveis (art. 46), além de exigir a comunicação imediata de incidentes que possam acarretar risco ou dano aos titulares (arts. 48 e 50). Embora o ataque ao STJ anteceda a plena vigência das sanções administrativas da LGPD, ele revelou a urgência de implementação efetiva dessa legislação em instituições estatais, sobretudo aquelas que lidam com informações sigilosas e estratégicas.

Esse caso também impulsionou debates sobre segurança nacional, soberania digital e a necessidade de investimentos contínuos em infraestrutura tecnológica. O ataque ao STJ demonstrou que crimes cibernéticos não apenas afetam indivíduos ou empresas, mas podem comprometer o próprio funcionamento do Estado, exigindo políticas públicas permanentes, cooperação internacional e fortalecimento da segurança da informação em todas as esferas da administração pública.

5 DESAFIOS DE APLICAÇÃO PRÁTICA

A aplicação das legislações brasileiras voltadas ao enfrentamento dos crimes cibernéticos enfrenta desafios estruturais, tecnológicos, jurídicos e operacionais que comprometem a efetividade do sistema de prevenção, investigação e responsabilização. Embora o país disponha de um arcabouço normativo consistente — composto pela Lei Carolina Dieckmann, Marco Civil da Internet, LGPD e normas penais específicas —, a realidade prática revela limitações que dificultam a resposta estatal diante de ameaças altamente sofisticadas.

Um dos principais desafios é a dificuldade probatória, já que a identificação de autores de crimes digitais muitas vezes depende de rastreamento de endereços IP, logs de acesso, metadados e cooperação com provedores de aplicação. Muitos desses registros são voláteis, possuem prazos curtos de guarda e podem estar armazenados em servidores localizados no exterior, o que exige mecanismos de colaboração jurídica internacional nem sempre céleres. A transnacionalidade dos delitos, portanto, cria entraves significativos, sobretudo porque muitos crimes são executados a partir de países sem tratados de cooperação com o Brasil.

Outro obstáculo relevante decorre da insuficiência estrutural das instituições responsáveis pela persecução penal. Delegacias, varas judiciárias e unidades ministeriais especializadas em crimes cibernéticos ainda são poucas e, em muitos estados, inexistem. Além disso, há carência de peritos capacitados em tecnologia da informação, limitando o trabalho de análise forense digital. A alta demanda por investigações contrasta com recursos escassos, o que compromete a agilidade e a eficácia das apurações.

Soma-se a isso a rápida evolução tecnológica, que frequentemente supera a capacidade do Estado de atualizar suas próprias ferramentas e protocolos de segurança. Golpes, ataques e técnicas de invasão tornam-se cada vez mais sofisticados, explorando vulnerabilidades ainda desconhecidas, enquanto servidores públicos e cidadãos, muitas vezes, não possuem capacitação contínua para se protegerem adequadamente.

A vulnerabilidade social, sobretudo entre idosos, crianças e pessoas com baixo grau de inclusão digital, constitui outro ponto crítico. Esses grupos são alvos frequentes de golpes, fraudes e manipulação, e a legislação, por si só, não é suficiente para garantir proteção efetiva sem políticas de educação digital, campanhas de conscientização e acesso democratizado a tecnologias seguras.

No âmbito institucional, a LGPD ainda enfrenta desafios quanto à sua implementação integral. Muitas empresas e órgãos públicos ainda não possuem programas de governança de dados, encarregados de proteção de dados (DPO) ou políticas internas robustas de segurança da informação. O próprio poder público, conforme demonstrado pelos casos recentes de megavazamentos e ataques a órgãos de alto escalão, carece de investimentos sistemáticos em infraestrutura tecnológica, protocolos de resposta a incidentes e auditorias contínuas.

Por fim, o enfrentamento aos crimes cibernéticos exige cooperação multissetorial, envolvendo Estado, setor privado, plataformas digitais, instituições financeiras e sociedade civil. Sem integração entre esses atores e sem protocolos de resposta ágeis, a legislação tende a ter eficácia limitada diante da complexidade do ambiente digital contemporâneo.

6 IMPACTOS SOCIAIS, ECONÔMICOS E POLÍTICOS

Os megavazamentos de dados ocorridos no Brasil nos últimos anos — como o caso emblemático do vazamento de informações de mais de 223 milhões de cidadãos — produziram efeitos profundos nas esferas social, econômica e política. A exposição massiva de dados pessoais compromete a privacidade, fragiliza estruturas institucionais e afeta diretamente o funcionamento da economia digital.

No âmbito social, tais incidentes contribuem para a erosão da sensação de segurança e de autonomia dos indivíduos. A divulgação de informações sensíveis — como nome completo, dados bancários, hábitos de consumo, endereços e até dados de saúde — aumenta exponencialmente o risco de fraudes, golpes de engenharia social e subtração de identidade. Isso também gera impactos psicológicos significativos, como medo, ansiedade e sentimento de impotência. Grupos vulneráveis, como idosos e pessoas de baixa renda, tendem a sofrer ainda mais com golpes que se aproveitam da exposição de seus dados.

Do ponto de vista econômico, os efeitos são igualmente graves. No plano individual, vítimas enfrentam prejuízos financeiros, comprometimento do crédito e a necessidade de acionar instituições financeiras e órgãos de proteção ao consumidor. Para empresas públicas e privadas, incidentes dessa magnitude geram custos elevados com respostas a incidentes, investigações de segurança, implementação de novas medidas técnicas, pagamento de multas e reparações civis. Há ainda danos à reputação organizacional, perda de clientes e diminuição da confiança do mercado. Em escala nacional, os megavazamentos afetam a competitividade do Brasil no cenário internacional, já que países com elevados índices de insegurança digital atraem menos investimentos e enfrentam dificuldades para desenvolver ecossistemas inovadores.

No campo político, os megavazamentos provocam desgaste institucional e questionamentos sobre a capacidade do Estado de proteger informações sensíveis da população. A fragilidade dos sistemas governamentais afeta a confiança pública e abre espaço para disputas partidárias, uso político de incidentes cibernéticos e narrativas de insegurança generalizada. Em momentos eleitorais, o risco é ainda

maior, pois a manipulação de dados pode influenciar o debate público, favorecer estratégias de desinformação e comprometer a lisura de processos democráticos. Além disso, o debate político passa a pressionar pela ampliação da atuação da Autoridade Nacional de Proteção de Dados (ANPD), pela adoção de políticas públicas mais rígidas de segurança da informação e por reformas legais que fortaleçam o aparato estatal no enfrentamento ao cibercrime.

Em síntese, os impactos sociais, econômicos e políticos dos megavazamentos de dados evidenciam que a proteção da informação é um elemento fundamental para a garantia de direitos individuais, para o funcionamento saudável da economia e para a estabilidade das instituições democráticas. Por isso, o enfrentamento desse tipo de crime exige não apenas avanços tecnológicos, mas sobretudo um esforço conjunto entre Estado, iniciativa privada e sociedade civil para promover uma cultura robusta de proteção de dados.

7 COMPARATIVO INTERNACIONAL

A análise comparativa das práticas internacionais de enfrentamento aos crimes cibernéticos revela diferenças marcantes entre os modelos adotados por países desenvolvidos e o cenário brasileiro. Enquanto o Brasil avança de forma gradual na modernização de seu arcabouço jurídico e institucional, nações como Estados Unidos, Reino Unido, Alemanha, Estônia e Israel possuem estruturas consolidadas de prevenção, resposta e investigação de incidentes digitais. Entender tais modelos é fundamental para identificar boas práticas e propor estratégias que fortaleçam o sistema nacional.

Nos Estados Unidos, o combate ao crime cibernético é fortemente baseado na articulação entre agências especializadas, como o FBI, o Cybersecurity and Infrastructure Security Agency (CISA) e o National Security Agency (NSA). O país adota políticas rígidas de segurança de infraestrutura crítica e investe continuamente em inteligência cibernética, com destaque para a cooperação entre governo e setor privado. A legislação norte-americana também prevê sanções severas para cibercriminosos, o que aumenta o caráter dissuasório das normas.

Na União Europeia, especialmente em países como Alemanha e França, prevalece um modelo focado na proteção de dados pessoais e na segurança digital como direitos fundamentais. O Regulamento Geral de Proteção de Dados (GDPR) é um marco global, influenciando inclusive a criação da LGPD no Brasil. A União Europeia mantém ainda o "EU Cybersecurity Act", que estabelece padrões de certificação de segurança e fortalece a atuação da Agência da União Europeia para a Cibersegurança (ENISA). A responsabilidade das empresas é tratada com rigor e as multas por incidentes são significativamente mais elevadas do que no Brasil.

A Estônia é frequentemente considerada referência mundial, tendo se transformado em uma sociedade digital altamente integrada após sofrer um ataque cibernético massivo em 2007. O país criou o Centro de Excelência em Defesa Cibernética Cooperativa da OTAN e implementou um modelo de governança unificado, com infraestrutura de segurança distribuída, autenticação digital avançada e políticas robustas de resiliência cibernética. A alta digitalização, aliada ao investimento em educação e treinamento especializado, resultou em uma das populações mais preparadas para lidar com ataques digitais.

Israel também se destaca como potência em cibersegurança, com forte integração entre governo, universidades e indústria de tecnologia. Sua Autoridade Nacional de Cibernética coordena ações de defesa digital, enquanto investimentos massivos em pesquisa e inovação permitiram o surgimento de um ecossistema internacionalmente reconhecido. A estratégia israelense combina inteligência avançada, defesa proativa e cooperação global.

Comparado a esses modelos, o Brasil ainda enfrenta desafios significativos, como a falta de coordenação entre órgãos públicos, baixa padronização de protocolos de segurança, limitações orçamentárias e déficit de profissionais especializados. Embora a LGPD e a atuação da Autoridade Nacional de Proteção de Dados tenham representado um importante avanço, o país ainda carece de uma política nacional mais integrada e de investimentos contínuos em educação digital.

A observação do cenário internacional demonstra que países que tratam a cibersegurança como prioridade estratégica apresentam maior resiliência e menor vulnerabilidade a ataques. Portanto, o Brasil pode aprimorar sua atuação por meio da

adoção de práticas internacionais consolidadas, como cooperação ampliada entre setores, incentivos à pesquisa, fortalecimento institucional e políticas rígidas de responsabilização.

8 PROPOSTAS DE APRIMORAMENTO

A complexidade e a expansão acelerada dos crimes cibernéticos exigem do Brasil uma atuação estratégica e multidimensional. Embora o país tenha avançado com marcos normativos, ainda há lacunas significativas na prevenção, investigação e responsabilização dos delitos digitais. Para enfrentar esse cenário, é necessário adotar um conjunto de medidas estruturais capazes de fortalecer o ambiente digital, promover segurança jurídica e ampliar a resiliência das instituições públicas e privadas.

O primeiro eixo fundamental é o aprimoramento institucional. O Brasil precisa consolidar uma política nacional de cibersegurança que integre governo federal, estados, municípios e iniciativa privada. A atuação da Autoridade Nacional de Proteção de Dados (ANPD) deve ser ampliada, garantindo-lhe maior autonomia administrativa e orçamentária, bem como capacidade fiscalizatória mais robusta. A criação de centros regionais de resposta a incidentes também contribuiria para padronizar procedimentos e agilizar a cooperação entre diferentes órgãos.

Outro ponto essencial é o investimento em infraestrutura tecnológica e segurança da informação. Sistemas públicos e privados ainda dependem de arquiteturas defasadas, frequentemente vulneráveis a ataques. A adoção de políticas de atualização contínua, criptografia avançada, autenticação multifatorial e auditorias periódicas de segurança deve tornar-se obrigatória para setores sensíveis, como saúde, finanças, educação e administração pública. Ao mesmo tempo, é indispensável incentivar o desenvolvimento de tecnologias nacionais para reduzir a dependência externa.

No campo jurídico, o Brasil precisa ampliar e atualizar sua legislação, incorporando modalidades mais complexas de crimes cibernéticos, como deepfakes, manipulação algorítmica, espionagem digital e ataques a infraestrutura crítica.

Também é recomendável aprimorar os mecanismos de cooperação com outros países, por meio de tratados e acordos internacionais voltados ao compartilhamento de informações, extradição de criminosos e investigação transnacional. A adesão plena à Convenção de Budapeste sobre Crime Cibernético representaria importante avanço nesse sentido.

A formação e capacitação de profissionais especializados constitui outro pilar indispensável. A carência de peritos em computação forense, analistas de segurança e investigadores treinados limita a eficácia das respostas estatais. A criação de programas permanentes de capacitação para policiais, promotores, juízes e servidores públicos é medida urgente. Parcerias com universidades e centros de excelência internacionais também podem contribuir para transferência de conhecimento e evolução técnica.

Ao lado dessas medidas institucionais e tecnológicas, é crucial investir em educação digital e conscientização da população. A maior parte das fraudes eletrônicas depende da exploração de falhas humanas, como cliques em links maliciosos ou compartilhamento indevido de informações pessoais. Campanhas massivas de educação digital, inclusão nos currículos escolares e treinamentos em empresas privadas podem reduzir significativamente a superfície de ataques.

Por fim, é necessário promover uma cultura nacional de proteção de dados, que valorize a privacidade como direito fundamental e incentive práticas responsáveis no uso das tecnologias. Esse processo envolve mudanças estruturais, mas também culturais, que dependem da cooperação entre Estado, mercado e sociedade civil. O fortalecimento da confiança no ambiente digital é essencial não apenas para reduzir crimes cibernéticos, mas também para impulsionar inovação, competitividade e desenvolvimento econômico.

Em síntese, as propostas de aprimoramento aqui discutidas apontam para um modelo de cibersegurança mais integrado, moderno e eficiente. A construção desse modelo exige visão estratégica, investimentos contínuos e um esforço coordenado em múltiplas frentes. Somente assim o Brasil poderá enfrentar, com segurança e eficácia, os desafios complexos impostos pela criminalidade no ambiente digital.

9 CONCLUSÃO

A crescente sofisticação dos crimes cibernéticos impõe ao Estado brasileiro, às instituições públicas e privadas e à própria sociedade o dever de repensar suas estratégias de proteção, prevenção e resposta a incidentes digitais. Os casos analisados – o megavazamento de dados de 223 milhões de brasileiros e o ataque ao Superior Tribunal de Justiça – demonstram a gravidade das vulnerabilidades estruturais presentes no país e evidenciam que a simples existência de legislações avançadas não é suficiente para garantir segurança plena. Esses episódios revelam que, em um ambiente digital altamente dinâmico e complexo, a eficácia do sistema normativo depende de sua constante atualização e, sobretudo, da implementação prática de medidas de governança, segurança e educação digital.

A LGPD emerge como marco fundamental nesse cenário, ao estabelecer diretrizes claras sobre o tratamento de dados pessoais e ao reforçar a necessidade de adoção de mecanismos de segurança por parte do poder público e da iniciativa privada. No entanto, sua plena aplicação ainda enfrenta desafios, como a insuficiência da infraestrutura tecnológica, a carência de profissionais especializados e a dificuldade de investigação de crimes transnacionais. Para que a LGPD cumpra integralmente sua função, é indispensável fortalecer a Autoridade Nacional de Proteção de Dados (ANPD), ampliar a fiscalização e consolidar uma cultura nacional de respeito à privacidade.

O enfrentamento aos crimes cibernéticos requer, portanto, políticas públicas integradas, investimentos contínuos em tecnologia, capacitação de profissionais e campanhas permanentes de conscientização da população. É essencial que o Brasil avance na cooperação internacional, na modernização institucional e no aprimoramento da legislação penal voltada ao ambiente digital. Somente com a união e desenvolvimento desses esforços será possível reduzir vulnerabilidades, proteger direitos fundamentais e promover um ambiente digital seguro, confiável e democrático.

REFERÊNCIAS

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. *Diário Oficial da União*, Brasília, DF, 31 dez. 1940. Disponível em: https://legis.senado.gov.br/norma/527942. Acesso em: 10 de nov de 2025

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos (Lei Carolina Dieckmann). *Diário Oficial da União*, Brasília, DF, 3 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 10 de nov de 2025

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. *Diário Oficial da União*, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 de nov de 2025

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. *Diário Oficial da União*, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709compilado.htm. Acesso em: 10 de nov de 2025

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Código Penal para agravar penas de crimes cometidos por meios eletrônicos. *Diário Oficial da União*, Brasília, DF, 28 maio 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 19 de nov de 2025

POLÍCIA FEDERAL. Relatório técnico sobre o ataque ao STJ. Brasília, DF, 2020. Disponível em: https://g1.globo.com/politica/noticia/2020/11/05/pf-diz-que-instaurou-inquerito-para-apurar-invasao-de-computadores-do-stj.ghtml. Acesso em: 10 de nov de 2025

CARVALHO, P. H. O "Marco Civil da Internet": uma análise sobre a constitucionalidade do artigo 19. *Revista da Faculdade de Direito do Sul de Minas*, v. 33, n. 2, 2017. Disponível em: https://revista.fdsm.edu.br/index.php/revistafdsm/article/view/140. Acesso em: 19 nov. 2024.

CIBERCRIME CONTRA CRIANÇAS E ADOLESCENTES: ADULTIZAÇÃO

Karen Menéndez[1]
Leticia Sol Barbosa[2]
Mariana Marques[3]

RESUMO

Este artigo analisa o fenômeno da adultização de crianças e adolescentes por meio das mídias sociais e como a evolução digital expõe menores consequências negativas, incluindo exploração sexual, onde são incentivados a assumir uma imagem adulta para monetizar e obter engajamento. O estudo se baseia no caso recente do influenciador Hitalo Santos, denunciado por crimes de exploração sexual de crianças e adolescentes e produção/tráfico de conteúdo pornográfico. Estes crimes são enquadrados no Código Penal e no Estatuto da Criança e do Adolescente. A Lei Geral de Proteção de Dados (LGPD) reforça a proteção ao exigir consentimento específico dos pais para o tratamento de dados de crianças, visando seu melhor interesse. Em resposta a esse cenário, foi sancionada a Lei nº 15.211/25 (ECA Digital), que estabelece regras contra a adultização na internet. Essa lei obriga as plataformas a adotar medidas de prevenção, como ferramentas de controle parental e restrições de comunicação para menores. As plataformas digitais têm a responsabilidade de fiscalizar e garantir a remoção imediata de conteúdos ilícitos, como abuso ou exploração sexual. O descumprimento destas obrigações pode gerar sanções graves, incluindo multas por infração. A exposição antecipada traz consequências prejudiciais e, por vezes, irreparáveis à saúde e ao desenvolvimento das crianças, como ansiedade e estresse, tornando urgente a proteção jurídica e social.

Palavras Chaves: Adultização. Exploração Sexual Infantil Digital. Código Penal. LGPD. ECA. Prevenção. Aspectos sociais. Impactos psicológicos na criança.

SUMÁRIO: Introdução. 1. Momento histórico. Surgimento da era digital; 1.1 Cibercrime; 2. Adequação legal. Caso concreto; 2.1 Código Penal 2.2 ECA (Estatuto da Criança e do Adolescente); 2.3 LGPD (Lei de Proteção de Dados); 3

[1] Graduanda em Direito do UniCEUB - Centro Universitário de Brasília, Aluna da disciplina de Direito, Tecnologia e Informação. E-mail: m.karen2@sempreceub.com
[2] Graduanda em Direito do UniCEUB - Centro Universitário de Brasília, Aluna da disciplina de Direito, Tecnologia e Informação. E-mail: leticia.sbarbosa@sempreceub.com.
[3] Graduanda em Direito do UniCEUB - Centro Universitário de Brasília, Aluna da disciplina de Direito, Tecnologia e Informação. E-mail: mariana.amaral@sempreceub.com.

Regulamentação das redes sociais (aspectos negativos e positivos); 3.1 Responsabilidade das plataformas digitais; 4. Aspecto social e a adultização das crianças; 4.1 Impacto à saúde e ao desenvolvimento da criança; 5. Políticas Públicas e medidas de proteção on-line; 5.1 Medidas a serem tomadas pela sociedade para enfrentar a situação e prevenir a ocorrência dos crimes; Conclusão; Referências.

1 INTRODUÇÃO

A evolução acelerada da sociedade e o surgimento das mídias digitais trouxeram consigo uma série de consequências tanto positivas como negativas para todos como grupos sociais e especialmente para esses grupos mais vulneráveis como crianças e adolescentes.

A inocência carregada por estes, em ainda desenvolvimento e maturação, faz a causa principal do uso banalizado das mídias, somado a outros fatores estruturais familiares e sociais, as crianças seguem tendências que as expõem aos olhos maldosos de uma mente perversa que os assiste na maioria das vezes sem saber quem são e quais as intenções de assistir conteúdo de crianças dançando sexualmente, com roupas adultas, maquiadas passando uma imagem adultiçada da criança.

Este artigo faz uma análise profunda da situação com base no caso recente de Hitalo Santos e a adultização das crianças e nas legislações vigentes no território nacional que protegem às crianças e adolescentes.

A partir da análise é mestre conscientizarmos com a situação. Para tanto, também serão abordadas algumas das medidas para a proteção das crianças e adolescentes como também para a prevenção dos crimes relacionados.

2 MOMENTO HISTÓRICO. SURGIMENTO DA ERA DIGITAL.

Em 1991 ocorreu a primeira conexão à internet no Brasil, realizada pela Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp). Esse marco histórico representou o início de uma nova era, de troca de informações no país, abrindo caminho para o desenvolvimento tecnológico. (SILVA; SILVA, 2023)

Posteriormente, o Brasil começou a fazer negociações com os Estados Unidos da América (EUA), com o objetivo de que houvesse o compartilhamento de dados e informações entre instituições de pesquisa. (SILVA; SILVA, 2023)

Em 1992, o projeto começou a ser colocado em prática de forma mais ampla, com as universidades brasileiras implantando a primeira rede de computadores conectada à internet. Essa fase foi essencial para a disseminação do conhecimento digital e para o fortalecimento da comunicação acadêmica, permitindo que pesquisadores brasileiros tivessem acesso a informações, estudos e publicações internacionais com muito mais agilidade. (SILVA; SILVA, 2023)

Um tempo depois, em 1997, houve uma grande expansão do acesso à internet no Brasil. Com o surgimento das chamadas “redes locais de conexão” e o avanço das tecnologias de telecomunicação, o acesso começou a se popularizar, saindo do ambiente acadêmico e alcançando empresas, órgãos públicos e, gradualmente, os lares brasileiros. (SILVA; SILVA, 2023)

Entretanto, à medida que a tecnologia avançava e a rede se tornava mais acessível, surgiram novas ameaças. Questões como a segurança da informação, crimes virtuais e o uso indevido de dados pessoais passaram a representar grandes desafios para os usuários e para as autoridades. (SILVA; SILVA, 2023)

2.1 Cibercrime

Cibercrime é entendida como qualquer atividade criminosa que envolve um computador, rede de computadores ou dispositivo em rede. Esses crimes podem ser classificados em duas categorias principais: crimes nos quais o computador é o alvo, como ataques de hackers; e crimes nos quais o computador é utilizado como estelionato e disseminação de malware. (BRASIL, Câmara dos Deputados)

Dentre os crimes, um recentemente abordado foi o de adultização de crianças e adolescentes no ambiente digital, recentemente foi sancionada a lei 15.211/25 para a proteção desses menores. (BRASIL, Câmara dos Deputados)

Essa lei estabelece obrigações para aplicativos, jogos eletrônicos, redes sociais e serviços digitais, como verificação de idade confiável, ferramentas de

supervisão familiar, remoção de conteúdos relacionados a abuso ou exploração infantil e regras para tratamento de dados e publicidade voltada a menores. (BRASIL, Câmara dos Deputados)

Essas medidas buscam tornar o ambiente digital mais seguro, reforçando a importância da proteção e do respeito aos direitos dos menores de idade na era da tecnologia. (BRASIL, Câmara dos Deputados)

3 ADEQUAÇÃO LEGAL - CASO CONCRETO

Como abordado anteriormente, são vários os casos que diariamente observamos de crianças com perfis em mídia social fazendo vídeos dançando vestidas sexualmente. Isto é um cenário cada vez mais comum em rede social. Recentemente viu-se o caso de Hitalo Santos, o qual reunia um grupo de jovens e adolescentes menores de idade, os quais eram levados para uma casa sob responsabilidade dele como único adulto.

Se acompanhavam o perfil do mesmo em Instagram, nele observa-se os vídeos das diversas festas realizadas no local, com consumo de bebidas alcoólicas. Os vídeos mostram como os jovens consumiam o álcool, em lugares que propiciavam a pouca vestimenta como piscinas, dançando uns com os outros, estes trocavam namorados dentro do grupo, tinham brigas e muito mais. O influenciador Felca fez um vídeo no seu canal no YouTube, que atualmente possui ao redor de 6,46 milhões de pessoas inscritas falando sobre a situação.

Dada a repercussão total que teve o vídeo e as denúncias feitas pelo influenciador o Ministério Público da Paraíba (MPPB), por meio do Grupo de Atuação Especial de Combate ao Crime Organizado (Gaeco), ofereceu em 15 de setembro de este ano, denúncia criminal contra Hitalo José Santos Silva e Israel Nata Vicente por tráfico de pessoas exploração sexual de crianças, produção de conteúdo pornográfico e monetização com estes.

3.1 Código Penal

Conforme a denúncia os crimes imputados seriam: em primeiro lugar, tráfico de pessoas, para fins de exploração sexual. Previsto no Art. 149- A, V do Código Penal. A continuar diz a lei:

> Art. 149-A. Agenciar, aliciar, recrutar, transportar, transferir, comprar, alojar ou acolher pessoa, mediante grave ameaça, violência, coação, fraude ou abuso, com a finalidade de:
>
> V - Exploração sexual.

Configura-se o fato criminoso pelo agenciamento e aliciamento de adolescentes e suas famílias, com promessas ilusórias, visando ao controle da liberdade e da vida íntima das vítimas para fins de exploração sexual.

Em segundo lugar, imputado o crime previsto no Art. 218-B do Código penal, sendo o favorecimento da prostituição ou exploração sexual de vulnerável. Diz a lei:

> Art. 218-B. Submeter, induzir ou atrair à prostituição ou outra forma de exploração sexual alguém menor de 18 (dezoito) anos ou que, por enfermidade ou deficiência mental, não tem o necessário discernimento para a prática do ato, facilitá-la, impedir ou dificultar que a abandone.

Neste caso observamos que se configura o fato criminoso quando se induz à prática de atos sexuais com terceiros, também menores de 18 (dezoito anos), inclusive em situações de extremo constrangimento e em ambientes destinados à exploração sexual.

Ambos os crimes descritos na nossa legislação penal se adequam a nosso caso concreto. Mas outras legislações como a LGPD (lei de proteção de dados) e o ECA (Estatuto da Criança e do Adolescente) trazem proteções e prevenções antes à vulnerabilidade das crianças e adolescentes.

3.2 ECA (Estatuto da Criança e do Adolescente)

Na Denúncia feita pelo Ministério Público da Paraíba, imputa-se também o crime previsto no art. 240. Pela produção de material pornográfico envolvendo crianças ou adolescentes e a divulgação dos conteúdos em rede social para monetização e aumento de engajamento digital. Diz o Estatuto:

> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente.

Hítalo Santos por meio de seu perfil do Instagram que contava com mais de 20 milhões de seguidores que engajaram com este conteúdo monetizando milhões de reais com os conteúdos que faziam com as crianças.

3.3 LGPD (Lei de Proteção de Dados)

A Lei de Proteção de Dados não foi mencionada na denúncia, mesmo assim ela traz uma seção dedicada ao tratamento de dados pessoais de crianças e de adolescentes que vale a pena analisar. O art. 14 já direciona o tratamento de dados pessoais da criança e do adolescente para o melhor interesse destes

> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
>
> § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

A criança ainda não é capaz de realizar os atos da vida civil, é por isso que até a maioria de idade estes precisam de consentimento de seus representantes legais para praticá-los em segurança e para o melhor interesse da vida destes.

> § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

Todo o tratamento destes dados deve ser feito de forma pública e transparente, dessa forma a legislação permite que os titulares saibam como são tratados seus dados e como estes são usados.

> § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
>
> § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de

> informações pessoais além das estritamente necessárias à atividade.

Neste último parágrafo a legislação permite que as crianças tenham total autonomia, não precisando de consentimento dos pais para participar em jogos e aplicações de internet. Aqui o legislador é insuficiente, pois como bem temos observado esse uso frequente de aplicativos online, sem supervisão dos genitores, tem dado espaço cada vez mais a conteúdos de crianças e adolescentes nestes aplicativos.

Veja-se a necessidade de um maior monitoramento no lar e por parte dos tutores para prevenir que as crianças e adolescentes sejam alvos e vítimas da exploração sexual infantil digital.

> § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
>
> § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Assim, a Lei LGPD traz a refletir sobre a acessibilidade das crianças e adolescentes em meios digitais que podem ocasionar danos irreparáveis a seus dados pessoais, mas além disso, à sua saúde e desenvolvimento.

4 REGULAMENTAÇÃO DAS REDES SOCIAIS (ASPETOS NEGATIVOS E POSITIVOS)

Em setembro de 2025 foi sancionada a Lei nº 15.211/2025, conhecida como Estatuto Digital da Criança e do Adolescente (ECA Digital), estabelecendo regras para a proteção de crianças e adolescentes contra a adultização na internet. As plataformas de redes sociais são obrigadas a adotar medidas de prevenção contra conteúdos e práticas abusivas, como exploração sexual, além de fornecerem ferramentas de controle parental, o que inclui a vinculação de contas de menores a responsáveis e restrições de comunicação.

Essa regulamentação das redes sociais no combate da adultização de crianças e adolescentes traz pontos positivos como negativos.

No entanto, os positivos sobressaem aos negativos, pois há uma necessidade de restringir o uso das redes sociais em crianças e adolescentes, um deles é a exigência que as plataformas removam conteúdo inadequado, que exploram, o abuso, a violência, o assédio, o bullying. A remoção pode ser imediata em casos graves, sem necessidade de ordem judicial.

Ao limitar o tempo de uso da tela e a exposição de conteúdos que geram comparação e ansiedade, a regulamentação contribui para diminuir o impacto negativo na saúde mental infantil. Também devolve aos pais o controle no monitoramento das redes sociais dos seus filhos, sendo obrigados as plataformas oferecer mecanismos de controle para os pais.

A responsabilização das plataformas nessa nova redação ficam sujeitas a sanções, como multas e suspensão de operações, caso não cumpra as obrigações impostas para as empresas de tecnologia. Nesse sentido, ao proibir a publicidade direcionada e enganosa para menores, a regulamentação protege as crianças da exploração comercial precoce. Isso coloca a segurança da criança acima do lucro das empresas, incentivando o desenvolvimento de publicidades e produtos seguros.

Apesar que o objetivo de proteção seja aceito, a regulamentação das redes sociais para combater a adultização de crianças e adolescentes enfrenta desafios e críticas, um dos principais argumentos é o risco dessa proteção ser considerada um risco de censura e limitação da liberdade de expressão, a responsabilização das plataformas, a remoção do conteúdo após denúncia sem uma ordem judicial, deixa as plataformas sem contradição e apagam conteúdo legítimos por precaução. Pela quantidade de conteúdos postados nas redes sociais, torna a fiscalização manual ineficaz, e o uso da IA pode ocorrer falhas, permitindo conteúdo ofensivos e negando os inofensivos.

A regulamentação pode levar à implementação de mecanismos de vigilância em massa para monitorar postagens e interações, com preocupações sobre a privacidade dos usuários. A criação de limites para a interação entre adultos e

menores pode impedir a comunicação legítima, como entre familiares distantes ou educadores e alunos.

A criação de mecanismos de verificação de idade, embora prevista em projetos de lei, pode não ser totalmente eficaz, além de levantar questões sobre privacidade e acesso a dados pessoais. A restrição do tempo de permanência nas redes pode ser vista como uma medida paternalista e de difícil fiscalização, além de não abordar a causa principal do problema, que é o tipo de conteúdo consumido.

Assim, a regulamentação visa criar um ambiente digital mais seguro e apropriado para a faixa etária de crianças e adolescentes, protegendo-os de riscos à sua saúde mental, física e desenvolvimento, no entanto, deve-se observar quais mecanismos serão usados nesse combate, para não prejudicar as plataformas ou se tornar uma censura. (BRASIL,2025)

4.1 Responsabilidade das plataformas digitais

Entre as principais responsabilidades, destacam-se a prevenção ao acesso de menores a conteúdos prejudiciais, a remoção de publicações ilícitas e a implementação de mecanismos de supervisão parental. (BRASIL,2025)

No que se refere à remoção de conteúdo, as empresas devem eliminar, de forma imediata, materiais que envolvam abuso sexual, sequestro, aliciamento ou exploração de menores, comunicando as autoridades competentes. Da mesma forma, conteúdos que violem direitos infanto juvenis devem ser retirados assim que a violação for notificada, independentemente de ordem judicial.

Em relação às denúncias e recursos, o texto prevê que o usuário seja previamente notificado sobre a exclusão de publicações, com a devida justificativa e indicação do tipo de análise utilizada. A norma também prevê sanções a denúncias abusivas, incluindo suspensão ou exclusão de contas, e determina que plataformas com mais de um milhão de usuários menores publiquem relatórios semestrais sobre denúncias e medidas de segurança adotadas. (BRASIL,2025)

Sendo às penalidades, no descumprimento das obrigações podendo acarretar advertência, multa, suspensão ou proibição de atividades. As multas podem alcançar

até 10% do faturamento do grupo econômico no Brasil ou R$50 milhões por infração, sendo as medidas mais severas aplicáveis apenas por decisão judicial.

A supervisão parental é tratada como elemento central, impondo a obrigatoriedade de vinculação das contas de usuários com menos de 16 anos a um responsável legal. As plataformas deverão oferecer ferramentas de controle acessíveis e configuradas, com o nível máximo de proteção, permitindo aos responsáveis acompanharem o uso, restringir interações, controlar recomendações e limitar o tempo de acesso.

Por fim, o projeto proíbe o tratamento indevido de dados pessoais de crianças e adolescentes e veda o direcionamento de publicidade a esse público, inclusive mediante técnicas de análise emocional ou o uso de tecnologias imersivas, como realidade aumentada e virtual. (BRASIL, 2025)

Nesse viés, o texto busca reforçar a responsabilidade das plataformas digitais e assegurar um ambiente virtual mais seguro e adequado ao desenvolvimento de crianças e adolescentes.

5 ASPECTO SOCIAL E A ADULTIZAÇÃO DAS CRIANÇAS

O surgimento acelerado das redes sociais veio acompanhado de uma pandemia que obrigou às pessoas a se refugiarem no uso de aplicativos para manter-se informados, em conexão com os outros e até na criação de conteúdo para o entretenimento e o lazer.

No início observa-se a presença de um aspeto positivo, certo é que os aspetos negativos foram surgindo com o tempo, observe-se um vício desenvolvido pelas pessoas no uso de estes aparelhos e aplicativos, além disso, todos são permitidos a criarem conteúdo das mais diferentes naturezas, entre elas sexuais, ao mesmo tempo expostos para todos.

A pandemia trouxe também o desemprego massivo de muitas pessoas, que começaram a usar este meio digital como renda, posto que alcançado o engajamento necessário, estes aplicativos viabilizam a monetização dos conteúdos gerando uma entrada de renda fácil e basta para os donos dos perfis.

Cada tornou-se mais recorrente a criação de perfis com este fim, muitos de crianças e adolescentes que por meio de trend de dança monetizaram com o engajamento dos vídeos e conteúdo. Muitos a monitoramento dos pais que colocaram aos filhos a fazer os vídeos para ganharem dinheiro com estes, expondo-os com roupas curtas mostrando seus corpos.

Outros se aproveitam da vulnerabilidade que estas crianças têm em seus lares prometendo renda, trabalho, melhoria para suas vidas e as de seus familiares, assim induzindo a estes por meio de bebidas e ambientes à criação de conteúdo para exploração sexual das crianças e adolescentes.

5.1 Impacto à saúde e ao desenvolvimento da criança

É claro que essa exposição antecipada da infância à adultização traz consequências prejudiciais e às vezes irreparáveis na criança e ao adolescente e na sua formação para se converter em um adulto saudável.

Algumas das consequências demonstradas são a ansiedade e estresse. Quando expostas a grandes responsabilidades ou pressões para atingir padrões adultos frequentemente desenvolvem ansiedade e estresse. A constante preocupação com desempenho na aparência pode gerar um estado de tensão permanente, o que consequentemente traz baixa autoestima, posto que estas não conseguem se encaixar em padrões que não condizem com sua realidade.

Além disso, a criança ao se ver determinada a alcançar padrões adultos, vai ter dificuldade de socializar em ambientes infantis com outras crianças, isso o levará a tentar se relacionar com outros adultos. Consequentemente as responsabilidades aumentam e o tempo para atividades recreativas diminuem, levando à criança a apresentar comportamento violentos, agressivos e problemáticos por meio da rebeldia e desobediência.

O dano mais prejudicial para a saúde da criança é a perda no aproveitamento da sua infância. A infância é um momento da vida crucial para o ser humano, nele aprendemos a interagir com o mundo e em sociedade, criamos princípios e bases sólidas para nossa vida adulta. Sem a contemplação desse tempo precioso e de todas

suas experiências, o resultado é um adulto despreparado para à vida, para a tomada de decisões e para a sobrevivência no mundo.

6 POLÍTICAS PÚBLICAS E MEDIDAS DE PROTEÇÃO ON-LINE

As políticas públicas para proteção online de crianças e adolescentes envolvem legislação, como a Lei nº 14.811/2024, que combate à violência digital e estabelece diretrizes para o ambiente digital, e diretrizes como a Resolução nº 245 do CONANDA, que prevê a colaboração do poder público e empresas na divulgação de informações e riscos online. Medidas de proteção incluem o uso de controles parentais, diálogo aberto sobre segurança e privacidade na internet, e acompanhamento do uso das redes sociais.

O Brasil aprovou o Estatuto Digital da Criança e do Adolescente (Lei nº 15.211/2025), que estabelece políticas públicas e medidas para proteger jovens na internet contra a adultização e outros perigos, como exploração sexual, pornografia e bullying. A Lei nº 14.811/2024: Cria medidas de prevenção e combate a diversas formas de violência contra crianças e adolescentes, incluindo o cyberbullying e o abuso e exploração sexual, no ambiente digital. A Resolução nº 245 do CONANDA: Estabelece a necessidade de colaboração entre o poder público e empresas para informar sobre direitos, riscos e oportunidades no ambiente digital, além de promover a ética digital e a cidadania infanto-juvenil. Plano Nacional de Enfrentamento da Violência contra Crianças e Adolescentes: Busca proteger contra crimes digitais e violações de direitos, através de um conjunto de ações integradas.

Algumas medidas são ferramentas de monitoramento são importantes para proteger crianças e adolescentes no ambiente digital, mantenha um diálogo constante para que crianças e adolescentes se sintam à vontade para compartilhar situações incômodas online e relatar problemas, ensine sobre o uso seguro da internet, a importância de senhas seguras, verificação em duas etapas e a não compartilhar informações pessoais, tenha conhecimento dos aplicativos e plataformas que os jovens utilizam e acompanhe suas atividades online, crie regras claras para o uso da internet, buscando um equilíbrio saudável entre o tempo online e off-line e conheça

os canais para denunciar crimes digitais e compartilhe essa informação com a família e a sociedade.

No site do Gov.br tem um Guia sobre Usos de Dispositivos Digitais para Crianças e Adolescentes, o Guia é um documento oficial com análises e recomendações sobre o tema, baseado em evidências científicas e nas melhores práticas internacionais, inteiramente comprometido com a construção de um ambiente digital mais saudável. Além disso, o Guia serve de base às políticas públicas nas áreas de saúde, educação, assistência social e proteção.

6.1 Medidas a serem tomadas pela sociedade para enfrentar a situação e prevenir a ocorrência dos crimes.

Para enfrentar o uso excessivo e descontrolado das redes sociais em crianças e adolescentes para prevenir a ocorrência de crimes digitais, a sociedade pode adotar medidas que vão desde a colaboração direta com as autoridades até a promoção de ações sociais de longo prazo. É fundamental que a segurança pública não seja vista apenas como uma responsabilidade estatal, mas como um dever de todos os cidadãos.

Promover a inclusão de jovens em atividades educativas, esportivas e culturais. A falta de acesso a oportunidades é um dos principais fatores que levam ao uso descontrolado da internet, e a educação é uma ferramenta poderosa para a prevenção para excluir as propagandas enganosas e perfis falsos.

Exigir e apoiar programas de assistência social, saúde, lazer e saneamento básico com as crianças e os pais. A oferta de serviços de qualidade contribui para a prevenção do acesso à internet de crianças e adolescentes e ocupa a mente deles com ações saudáveis.

Em casos de violação de direitos ou suspeita de exploração, o cidadão pode entrar em contato com o Disque 100 (Disque Direitos Humanos), o Conselho Tutelar ou a Delegacia de Proteção à Criança e ao Adolescente.

7 CONCLUSÕES

O panorama apresentado pelas mídias sociais em relação às crianças e adolescentes é um panorama assustador e preocupante para nossa sociedade. Após as análises do Caso do Hitalo Santos e à adultização das crianças, nos resta muito para denunciar e fazer na proteção destas. O caso de adultização do Hitalo Santos não é uma situação isolada, milhares de perfis têm a finalidade de explorar às crianças sexualmente e compartilhar conteúdo pornográfico das mesmas.

Apesar das legislações atuais e a proteção às crianças e adolescentes garantidas por estas, precisamos fazer um árduo trabalho jurídico e social a respeito da situação visando o melhor interesse das nossas crianças e adolescentes.

REFERÊNCIAS

Adultização infantil: como reconhecer, prevenir e proteger crianças e adolescentes. Disponível em:https://www.tjdft.jus.br/institucional/imprensa/noticias/2025/agosto/adultizacao-infantil-como-reconhecer-prevenir-e-proteger-criancas-e-adolescentes

BRASIL. Lei nº 15.211, de 17 de setembro de 2025. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Diário Oficial da União, Brasília, 17 set. 2025.

BRASIL, E. M. Educa Mais Brasil - Bolsas de Estudo de até 85% para Faculdades – Graduação e Pós-graduação. Disponível em: https://www.educamaisbrasil.com.br/educacao/noticias/adultizacao-infantil-causas-impactos-e-como-proteger-as-criancas.

COMUNICAÇÃO – Todas as notícias – Núcleo de Gestão do Conhecimento – NGC. Gaeco MPPB oferece denúncia criminal contra o influenciador Hitalo Santos e Israel Vicente.

L15211. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm.

Nova lei protege crianças contra adultização na internet. (s. d.). Portal da Câmara dos Deputados. Recuperado em 12 de outubro de 2025, de https://www.camara.leg.br/noticias/1201525-nova-lei-protege-criancas-contra-adultizacao-na-internet/.

SILVA, Alessandra; SILVA, Luísa. Evolução histórica dos crimes cibernéticos no Brasil e o rigor da aplicabilidade das penalidades pela legislação. 2023. Disponível em: https://digital-camscanner.onelink.me/P3GL/g26ffx3k. Acesso em: 12 out. 2025.

A PEDOFILIA NAS REDES SOCIAIS CONTRA CRIANÇAS E ADOLESCENTES DO SEXO FEMINO

Carolina Almeida Alavrenga[1]
Letícia Silva Costa[2]

RESUMO

A crescente presença de crianças e adolescentes nas redes sociais, especialmente no Instagram e no TikTok, tem ampliado sua exposição a riscos como o contato com predadores sexuais. Apesar das plataformas estabelecerem idade mínima de 13 anos, muitos menores utilizam esses espaços sem supervisão adequada, facilitando interações abusivas que começam de forma discreta, por meio de emojis ou elogios, e podem evoluir para assédio explícito. A dinâmica algorítmica das redes também contribui para essa vulnerabilidade, impulsionando conteúdos com alta interação, mesmo quando visualizados por usuários mal-intencionados.Do ponto de vista jurídico, o problema é enfrentado por um conjunto de normas que visam proteger crianças e adolescentes, como o artigo 227 da Constituição, o ECA, o Código Penal, o Marco Civil da Internet e a LGPD. Essas legislações estabelecem deveres de proteção, criminalizam práticas de exploração sexual e atribuem responsabilidade às plataformas digitais. O artigo evidencia que a pedofilia online é um fenômeno estrutural que envolve falhas individuais, sociais, tecnológicas e institucionais, exigindo ações preventivas e coordenadas entre Estado, sociedade, famílias e empresas digitais.

Palavras-chave: Pedofilia; Redes sociais; Crianças e adolescentes; Vulnerabilidade digital; Instagram; TikTok; Proteção infantojuvenil; Algoritmos; Exploração sexual online.

SUMÁRIO: 1. Introdução; 2. Fundamentação teórica e legal; 3. O problema da pedofilia nas redes sociais; 4. Análise dos impactos e responsabilidade das redes sociais; 5. Considerações Finais.

1 INTRODUÇÃO

[1] Graduando em Direito do CEUB – Centro Universitário de Brasília. E-mail: carolina.almeidaa@sempreceub.com
[2] Graduando em Direito do CEUB – Centro Universitário de Brasília. E-mail: leticiasilvacosta7@sempreceub.com

Com o avanço da internet, o acesso a ela se tornou, e se torna, cada vez mais fácil, seja por adultos, seja por adolescentes ou crianças. Conforme dados coletados pelo IBGE e divulgados em seu canal oficial em 2023, cerca de 88% dos adolescentes a partir de 10 anos fazem uso da internet para fins diversos. Tendo 83% da percentagem prévia contas em redes sociais como Instagram e Tiktok, sendo esse dado, no mínimo, curioso, tendo em vista que, as principais plataformas têm como idade mínima 13 anos. E é aqui que surge o problema, tendo em vista a ampla gama de usuários dessas redes, tais quais possuem idades diversas, o contato entre adolescentes e adultos é, de certo, muito facilitado. O que é comprovado pelo fato de que 29% dos usuários entre 9 e 17 anos, conforme pesquisa divulgada no site de notícias G1, afirmam ter passado por situações constrangedoras.

A popularização das redes sociais entre crianças e adolescentes transformou profundamente as formas de interação, comunicação e construção de identidade na sociedade contemporânea. Plataformas como Instagram, TikTok, Facebook e aplicativos de mensagens instantâneas se tornaram parte essencial da rotina desses jovens, oferecendo entretenimento, sociabilidade e espaços de expressão. Contudo, essa inserção precoce ocorre, muitas vezes, sem a formação psicológica e cognitiva necessária para compreender e enfrentar riscos complexos, o que torna meninas especialmente vulneráveis a práticas como aliciamento, manipulação emocional e exploração sexual por parte de pedófilos que atuam no ambiente virtual.

A arquitetura das redes sociais, baseada em algoritmos, comunicação privada, perfis anônimos e alcance global, facilita a aproximação silenciosa de agressores, que utilizam estratégias sofisticadas para se aproximar e conquistar a confiança das vítimas. Esse cenário contribui para a naturalização de interações abusivas e dificulta a identificação e responsabilização dos autores, produzindo impactos psicológicos, sociais e jurídicos graves, que ultrapassam o ambiente digital e atingem diretamente o desenvolvimento integral da criança e da adolescente.

Diante dessa realidade, a pedofilia nas redes sociais configura um problema estrutural, multidisciplinar e transnacional, que demanda respostas coordenadas entre Estado, sociedade e empresas provedoras de serviços digitais. Nesse sentido, analisar o fenômeno exige compreender não apenas o comportamento dos agressores

e as vulnerabilidades das vítimas, mas também a atuação, ou omissão, das plataformas digitais.

Ante o exposto, é crucial a atenção em como a pedofilia sai de um âmbito majoritariamente físico, ou seja, em locais palpáveis e migra para o digital, onde a possibilidade de vítimas é inegavelmente maior, tendo em vista o rápido e fácil contato entre os usuários. Ocorrendo tal fato, por exemplo, em comentários de um vídeo ou foto postados ou até mesmo em chat de mensagens diretas que tais aplicativos disponibilizam.

Tendo isso em vista, o seguinte trabalho tem como objetivo explorar a problemática da pedofilia nas redes sociais, principalmente contra adolescentes do sexo feminino e com enfoque nas redes sociais Instagram e TikTok, tendo em vista a popularidade dessas entre o público feminino e de tal faixa etária.

Inicialmente será abordada a fundamentação teórica e legal que versa diretamente sobre o problema, a fim de proporcionar ao leitor um saber jurídico inicial a fim de que a problemática seja entendida com mais clareza. Sendo usado como base o estabelecido na Constituição Federal de 1988, o Estatuto da Criança e do Adolescente, a Lei de Proteção Geral de Dados e Código Penal.

Em seguida, a temática problema será de fato exposta e trabalhada, trazendo exemplos reais por meio de imagens que comprovam a existência de pedofilia nas redes sociais, além de explicar melhor como isso acontece, a linguagem utilizada pelos criminosos. Será utilizado como fundamentação também a opinião de profissionais das áreas jurídicas e jornalística.

No próximo tópico, visto o texto legal e o problema em si e como ele se desenvolve, serão analisados os impactos negativos que a pedofilia tem na vida das vítimas e qual é a responsabilidade das redes sociais, meio onde o crime acontece, ante ao problema. Por fim, será abordado brevemente o que está sendo feito e o que deve ainda ser feito por parte não só das redes sociais, mas também do Estado, da sociedade como um todo e dos responsáveis diretos por essas crianças e adolescentes.

2 FUNDAMENTAÇÃO TEÓRICA E LEGAL

A pedofilia nas redes sociais representa uma das formas mais graves de violação aos direitos da criança e do adolescente, configurando-se como uma ameaça concreta à dignidade sexual e à integridade psicossocial desses indivíduos. O avanço tecnológico e o fácil acesso à internet ampliaram os meios de interação social, mas também possibilitaram o surgimento de novos espaços para a prática de crimes sexuais virtuais, especialmente contra adolescentes do sexo feminino, que se mostram mais vulneráveis diante da exploração e manipulação digital.

Do ponto de vista teórico, o fenômeno da pedofilia pode ser compreendido como uma desordem de natureza psicossocial e sexual, caracterizada pela atração de um adulto por crianças e adolescentes, de forma persistente e patológica. No ambiente virtual, essa conduta ganha novas dimensões, pois os agressores utilizam diversas estratégias para obter material de cunho sexual de crianças e adolescentes.

Um fator contemporâneo que potencializa esse tipo de prática criminosa é o uso dos algoritmos personalizados das redes sociais. Esses sistemas são programados para identificar e sugerir conteúdos com base nos interesses e interações de cada usuário. Pedófilos, cientes dessa lógica, podem utilizar o algoritmo a seu favor, assistindo e curtindo vídeos ou fotos de crianças e adolescentes realizando atividades cotidianas, como dançar, brincar, participar de desafios ou postar selfies, conteúdos que, para pessoas comuns, são vistos como inocentes, mas que para esses indivíduos adquirem conotação sexual. Com isso, as próprias plataformas acabam, inadvertidamente, alimentando um ciclo de recomendação que facilita o acesso contínuo a esse tipo de material e reforça o comportamento predatório.

No campo jurídico, a Constituição Federal de 1988 assegura, em seu artigo 227, que é dever da família, da sociedade e do Estado assegurar à criança e ao adolescente, com absoluta prioridade, o direito à dignidade, ao respeito e à proteção contra qualquer forma de negligência, discriminação, exploração, violência e opressão. Esse mandamento constitucional serve como base para toda a legislação infraconstitucional voltada à proteção infanto-juvenil. *In verbis:*

> Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão. (Redação dada Pela Emenda Constitucional nº 65, de 2010). Constituição Federal, 1988.

O Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) reforça esse compromisso, tipificando condutas relacionadas à exploração sexual e à divulgação de imagens pornográficas envolvendo menores de 18 anos. Além disso, a Lei nº 11.829/2008 alterou o ECA para incluir dispositivos específicos que criminalizam a posse, a produção e o compartilhamento de material pornográfico infantil em meios digitais, reconhecendo a internet como um espaço passível de práticas criminosas. Vejamos o seguinte dispositivo da Lei nº 8.069/1990:

> Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso:
>
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
>
> Parágrafo único. Nas mesmas penas incorre quem:
>
> I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso;
>
> II – pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita (Estatuto da Criança e do Adolescente)

O Código Penal brasileiro também prevê sanções severas para crimes sexuais contra vulneráveis, especialmente nos artigos 217-A e seguintes, que tratam do estupro de vulnerável e da corrupção de menores. Ademais, a Lei nº 12.965/2014 (Marco Civil da Internet) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) introduziram princípios fundamentais sobre a responsabilidade das plataformas digitais e a proteção de dados pessoais, buscando coibir práticas abusivas e garantir maior segurança no ambiente virtual. Vejamos:

> Art. 217-A. Ter conjunção carnal ou praticar outro ato libidinoso com menor de 14 (catorze) anos: (Incluído pela Lei nº 12.015, de 2009)
>
> Pena - reclusão, de 8 (oito) a 15 (quinze) anos. (Incluído pela Lei nº 12.015, de 2009) (Código Penal)

> ***
>
> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
>
> § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. (Lei Geral de Proteção de Dados)

Assim, a fundamentação teórica e legal demonstra que a pedofilia nas redes sociais não se limita ao contato direto entre agressor e vítima, mas envolve também a utilização indevida de recursos tecnológicos e algorítmicos que ampliam o alcance e a gravidade dessas condutas. Diante disso, torna-se imprescindível uma atuação conjunta entre o Estado, as plataformas digitais e a sociedade civil para garantir uma efetiva proteção aos adolescentes, sobretudo às meninas, mais expostas e vulneráveis a esse tipo de violência digital.

3 O PROBLEMA DA PEDOFILIA NAS REDES SOCIAIS

Exposta a fundamentação teórica e legal, é cabível dizer que o problema começa realmente com o acesso dessas crianças às redes sociais, por mais que diversas dessas possuam diretrizes que estabeleçam uma idade mínima para criação de uma conta em seu domínio - como os termos estabelecidos pelo Instagram a seguir - não é isso que acontece, ou seja, meninas muito novas postam e interagem com outras pessoas na rede social.

> 4. Seus compromissos
>
> Em troca de nosso compromisso [...].
>
> 4.1 Quem pode usar o Instagram. Queremos que nosso Serviço seja o mais aberto e inclusivo possível, mas também desejamos que ele seja seguro e esteja em conformidade com a lei. Por isso, precisamos que você se comprometa em relação a algumas restrições para fazer parte da comunidade do Instagram.
>
> - Você deve ter pelo menos 13 anos ou a idade mínima legal em seu país para usar o Instagram.

E, por mais que existam essas regras, como já dito, elas não são respeitadas. O que primeiro indica uma falta de supervisão paterna ou de responsáveis pelas menores de idade e, também, uma falta por parte da gestão feita pelas redes sociais.

Como as fotos que serão fornecidas mostram, é muito fácil a indicação de que o detentor da conta, não é um adulto, mas sim adolescentes e até crianças tendo em vista que, conforme o ECA, aqueles que possuem até 12 anos ainda são considerados crianças.

Figura 1 - Legenda: usuária de 10 anos, post de comemoração de seu aniversário.

Fonte: Instagram.

Figura 2 - Legenda: usuária de 11 anos, post de comemoração de seu aniversário

Fonte: Instagram.

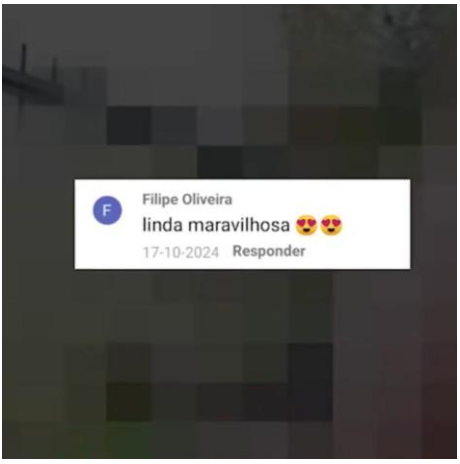
Por mais que as redes sociais sejam uma fonte de entretenimento de fácil e rápido acesso, elas não são "locais" apropriados para públicos de certas idades na maior parte do tempo. Para que esse uso não seja tão prejudicial seria necessária uma supervisão constante por parte dos pais, o que não é uma expectativa tão realista no Brasil. Conforme a revista Guarulhos, 63% dos pais e mães não passam tempo suficiente com seus filhos, principalmente por conta da alta carga trabalhista, então a pergunta que fica é: como os pais que mal passam uma hora com seus filhos vão conseguir supervisionar seu uso das redes sociais?

Essa falta de supervisão e uso desenfreado gera uma enorme gama de problemas, sejam eles mentais ou sociais. A taxa de ansiedade em jovens após a grande expansão da internet aumentou drasticamente, por exemplo, mas também surge outro problema que merece atenção redobrada. Com o acesso ilimitado, vem as interações muitas vezes ilimitadas. Crianças e adolescentes querem ser influencers, afinal elas são influenciadas a isso, para isso o contato com outros usuários é enxergado como algo necessário, entretanto, muitas vezes aqueles que interagem, principalmente com meninas, são homens adultos e é aqui que o problema se intensifica. Muitos desses homens, não são meros expectadores, mas sim predadores sexuais. Em meio a publicações, curtidas e comentários eles se mostram presentes, seja salvando esses vídeos com segundas intenções, escrevendo comentários com duplo sentido, ou até de forma mais direta como será apresentado. Tal fato é inegável, pedófilos estão presentes, fazem questão de se mostrarem presentes e esse problema precisa ser reconhecido e tratado com mais seriedade.

Os criminosos começam de forma mais discreta, com comentários que possuem apenas emojis, de coração ou que representem paixão. A juíza Vanessa Cavalieri, responsável pela Vara da Infância e Juventude do Rio de Janeiro durante sua entrevista para o programa "Encontro com Patrícia Poeta" deixou claro que pedófilos costumam usar emojis específicos que escondem seu verdadeiro significado nas postagens, como meio de identificação entre os predadores sexuais para que eles entrem em contato uns com os outros, mas também emojis usados com cunho sexual com o foguinho representando que a criança seria sensual. Após esse uso exclusivo dos emojis, se nada acontece, os comentários passam a ser escritos,

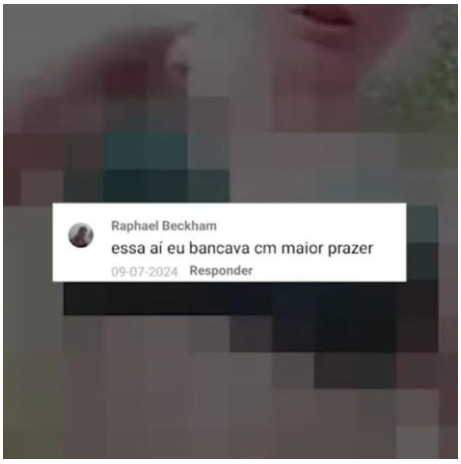
principalmente elogios, mas a conduta continua a evoluir e são escritas mensagens mais explícitas nas publicações, como pode ser observado a seguir nas imagens a seguir, que são prints de comentários deixados em um vídeo curto de uma adolescente dançando nas redes sociais.

Figura 3 - Imagem com print de comentário "linda maravilhosa"



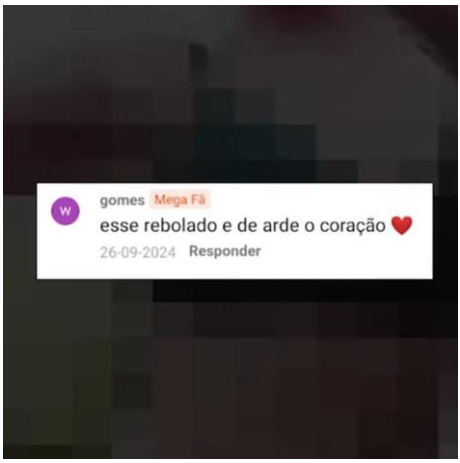
Fonte: YouTube. Adultização [vídeo].

Figura 4 - Imagem com print de comentário: "essa aí eu bancava 'cm' maior prazer"



Fonte:YouTube. Adultização [vídeo].

Figura 5 - Imagem contendo print de comentário: “esse rebolado ‘e’ de arde o coração”



Fonte:YouTube. Adultização [vídeo].

Além disso, investigações conduzidas pelo Wall Street Journal em parceria com pesquisadores de Stanford e da Universidade de Massachusetts Amherst revelaram que o Instagram tem desempenhado um papel ativo na facilitação do problema da pedofilia em seu domínio por conectar e promover contas dedicadas produção de conteúdo infantil. São também promovidas contas que utilizam hashtags explícitas para sinalizar interesse e comercialização de conteúdo que seja do interesse dos predadores sexuais, mesmo que associadas a práticas ilegais. Logo, embora a Meta reconheça falhas significativas em seus mecanismos de moderação, incluindo problemas que descartavam denúncias de usuários, e afirme ter removido hashtags, conteúdos e criado uma equipe interna esse problema em específico, os pesquisadores destacam que a escala e a gravidade do problema indicam uma insuficiência estrutural nas políticas de segurança infantil da plataforma.

4 ANÁLISE DOS IMPACTOS E RESPONSABILIDADE DAS REDES SOCIAIS

A presença de pedófilos em plataformas digitais produz impactos significativos e duradouros na vida de crianças e adolescentes, sobretudo do sexo feminino, que constituem um dos grupos mais vulneráveis no ambiente virtual. A dinâmica das redes sociais, marcada por rapidez, anonimato relativo, algoritmos que

intensificam a exposição e mecanismos frágeis de verificação, cria um cenário propício para que comportamentos predatórios ocorram de maneira silenciosa, cotidiana e altamente repetitiva. Os impactos dessa realidade se manifestam em diferentes níveis: psicológico, social, emocional e até mesmo jurídico.

No plano psicológico, meninas expostas a comportamentos sexualizados, mensagens invasivas ou solicitações inadequadas tendem a desenvolver sentimentos de medo, culpa, vergonha, ansiedade e confusão emocional. Esses danos se agravam pela incapacidade, típica da idade, de compreender completamente a gravidade das condutas que sofrem. O processo de grooming, ao criar vínculos artificiais de confiança entre vítima e agressor, intensifica esse impacto, pois muitas adolescentes, especialmente as mais jovens, não distinguem a manipulação emocional do afeto genuíno. Assim, a violência digital não se encerra no momento do contato, ela reverbera, podendo comprometer o desenvolvimento saudável, a autoestima e a percepção de segurança.

Além disso, há o impacto social. Meninas vítimas desse tipo de violência tendem a apresentar isolamento, retração, queda no desempenho escolar e dificuldades de interação. Em casos mais graves, quando ocorrem vazamentos de imagens íntimas ou ameaças, o dano se expande para o coletivo: a vítima é exposta a julgamentos, humilhações e repercussões que podem persistir por anos. A internet, por sua natureza permanente e replicável, agrava ainda mais esses prejuízos.

Esses impactos não ocorrem isoladamente, mas dentro de um ambiente em que as redes sociais têm papel determinante. Embora as plataformas se apresentem como espaços neutros de socialização e entretenimento, elas detêm controle sobre ferramentas, algoritmos e políticas capazes de reduzir ou ampliar riscos. O modelo de funcionamento dessas redes, que promove conteúdos altamente visualizados e engajados, acaba, ainda que de forma não intencional, contribuindo para a circulação de vídeos e fotos de meninas muito jovens. Isso ocorre porque o algoritmo não distingue interesse legítimo de interesse predatório: quanto mais um conteúdo envolvendo crianças é visualizado, salvo ou comentado, ainda que por pedófilos, mais ele é impulsionado, aumentando a exposição da vítima.

Assim, a responsabilidade das plataformas não pode ser ignorada. Elas operam com plena capacidade tecnológica para criar sistemas de detecção automática, bloquear contas suspeitas, identificar padrões de comportamento predatório e exigir verificação de idade mais rigorosa. Contudo, em grande parte dos casos, as medidas existentes são superficiais e insuficientes, limitadas a ferramentas básicas de denúncia que dependem da iniciativa da vítima ou de terceiros. Diante da vulnerabilidade intrínseca do público infantil, essas plataformas deveriam atuar de forma mais ativa, preventiva e contínua, não apenas reativa.

Do ponto de vista jurídico, esse entendimento encontra respaldo no Marco Civil da Internet, na LGPD e no ECA, que atribuem deveres às plataformas de garantir segurança, proteção de dados e prevenção de práticas ilícitas, sobretudo quando envolvem usuários menores de idade. Também deriva do princípio da proteção integral previsto no artigo 227 da Constituição, que impõe à sociedade, incluindo empresas privadas, o dever inafastável de resguardar crianças e adolescentes.

Portanto, a análise dos impactos revela que o problema da pedofilia nas redes sociais não pode ser compreendido somente como conduta individual de criminosos, mas como resultado de uma estrutura digital que falha em proteger adequadamente seus usuários mais frágeis. As redes sociais, ao permitirem a circulação de conteúdo infantil sem mecanismos eficazes de controle e ao criarem ambientes em que a interação com adultos desconhecidos é comum e incentivada, assumem responsabilidade direta na mitigação ou perpetuação desse fenômeno. Cabe a elas, em conjunto com o Estado e a sociedade civil, adotar práticas rigorosas e tecnologias avançadas que garantam um ambiente virtual mais seguro e saudável para crianças e adolescentes, prevenindo a continuidade dessa forma de violência.

5 CONSIDERAÇÕES FINAIS

O presente estudo demonstrou que a pedofilia nas redes sociais é um fenômeno complexo, estrutural e amplamente facilitado pelo ambiente digital. A análise realizada evidenciou que a exposição precoce de crianças e adolescentes, especialmente meninas, a plataformas como Instagram e TikTok vem de lacunas por

parte da supervisão parental e falhas institucionais que potencializam comportamentos predatórios, mesmo que de forma não intencional.

Verificou-se que, embora exista um vasto material legal voltado à proteção infanto-juvenil, sua eficácia objetiva depende de um fiscalização mais severa no meio digital que ainda não acontece. A atuação estatal e o sistema normativo mostram-se insuficientes diante da velocidade de circulação de conteúdo, da dificuldade em identificar agressores e da insuficiência dos mecanismos de verificação de idade e moderação das plataformas. A responsabilização das redes sociais, portanto, é peça central nessa discussão, não apenas como intermediadoras tecnológicas, mas como agentes que possuem meios técnicos para reduzir significativamente os casos de pedofilia por estar atento não só a idade real dos usuários, mas também ao comportamento de outros nos comentários.

Além disso, ficou evidente que os impactos da violência sexual digital ultrapassam o campo jurídico. As consequências psicológicas, emocionais e sociais para as vítimas podem ser profundas e duradouras, afetando sua autoestima, desenvolvimento e relações interpessoais. Assim, o combate à pedofilia online não deve se limitar à punição de criminosos, mas envolver políticas preventivas e responsabilidade compartilhada entre Estado, sociedade, família e empresas privadas. Conclui-se, portanto, que a proteção de crianças e adolescentes nas redes sociais exige uma articulação contínua e integrada entre todos os atores envolvidos, pois somente a partir de uma ação conjunta, consciente e permanente será possível construir um ambiente virtual mais seguro que minimize vulnerabilidades e garanta uma experiência saudável para os usuários.

REFERÊNCIAS

BRASIL. **Código Penal: Decreto-Lei nº 2.848, de 7 de dezembro de 1940.** Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 12 nov. 2025.

BRASIL. **Constituição (1988). Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 nov. 2025.

BRASIL. **Estatuto da Criança e do Adolescente: Lei nº 8.069, de 13 de julho de 1990.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 12 nov. 2025.

BRASIL. **Em 2023, 88,0 % das pessoas com 10 anos ou mais utilizaram Internet.** Agência de Notícias do Instituto Brasileiro de Geografia e Estatística (IBGE), 16 ago. 2024. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/41026-em-2023-87-2-das-pessoas-com-10-anos-ou-mais-utilizaram-internet. Acesso em: 12 nov. 2025.

BRASIL. **Lei Geral de Proteção de Dados Pessoais: Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l13709.htm. Acesso em: 12 nov. 2025.

BRSILVA, Victor Hugo. **83% das crianças e adolescentes que usam internet no Brasil têm contas em redes sociais, diz pesquisa.** G1 – Tecnologia, 23 out. 2024. Disponível em: https://g1.globo.com/tecnologia/noticia/2024/10/23/83percent-das-criancas-e-adolescentes-que-usam-internet-no-brasil-tem-contas-em-redes-sociais-diz-pesquisa.ghtml. Acesso em: 12 nov. 2025.

YouTube. **Adultização** [vídeo]. Disponível em: https://www.youtube.com/watch?v=FpsCzFGL1LE. Acesso em: 18 nov. 2025.

INC, Meta Platafoms. **Termos de uso**. Disponível em: https://help.instagram.com/581066165581870/?locale=pt_ . Acesso em: 18 nov. 2025.

GSHOW. **Juíza expõe emojis e gifs usados por pedófilos nas redes sociais; aprenda a identificar.** Gshow - Tecnologia, 15 out. 2025. Disponível em: https://gshow.globo.com/tv/encontro-com-patricia-poeta/noticia/juiza-expoe-emojis-e-gifs-usados-por-pedofilos-nas-redes-sociais-aprenda-a-identificar.ghtml. Acesso em: 18 nov. 2025.

HORWITZ, Jeff. **How Instagram's Algorithm Connects and promotes Pedophile Network.** WSJ Podcast - Tecnologia, 8 jun. 2023. Disponível em: https://www.wsj.com/podcasts/tech-news-briefing/how-instagrams-algorithm-connects-and-promotes-pedophile-network/a683c0b4-2e6f-4661-9973-10bd455db895. Acesso em: 18 nov. 2025.

GOLPES CONTRA IDOSOS A PARTIR DE INFORMAÇÕES PROCESSUAIS PÚBLICAS

Laís Eduarda Leal da Fonseca[1]

RESUMO

O presente artigo analisa o crescente fenômeno dos golpes aplicados contra pessoas idosas a partir da exposição de informações processuais públicas em meio digital. A pesquisa parte da constatação de que a publicidade judicial, embora consagrada como princípio fundamental do Estado Democrático de Direito e instrumento de controle social da Justiça, tem produzido efeitos colaterais preocupantes na era da informação. O estudo propõe uma reflexão crítica sobre a necessidade de compatibilização entre a transparência processual e a tutela da privacidade, sobretudo diante da vulnerabilidade dos idosos. A partir de casos concretos e de uma análise teórica sobre o papel contemporâneo da publicidade judicial, argumenta-se que a ampla divulgação de dados pessoais, sem critérios de necessidade e proporcionalidade, viola direitos fundamentais e favorece práticas criminosas. Defende-se, portanto, uma reinterpretação do princípio da publicidade de modo a garantir a efetiva dignidade humana sem comprometer a confiança pública no sistema de Justiça.

Palavras-chave: Consulta Pública; LGPD; idosos; golpes digitais; dignidade da pessoa humana; crimes cibernéticos.

SUMÁRIO:1. Introdução; 2.O paradoxo da publicidade processual na era digital e o princípio da publicidade; 2.1 A transição do contexto histórico-analógico para a exposição irrestrita de dados; 2.2 O desvio de finalidade; 3. O Estatuto do idoso e o dever de proteção na Constituição Federal; 3.1 A inexperiência digital como fator de hipervulnerabilidade é alvo para fraudes; 3.2 Dados processuais públicos como vetor de fraude; 4. Modus operandi e o “golpe do falso advogado"; 4.1 Casos concretos; 5. Medidas de enforcement da LGPD pelo judiciário; 5.1 Soluções técnicas e a anonimização em camadas; 5.2 Mecanismos de acesso qualificado para fins de pesquisa; 5.3 Tutela da dignidade humana e do hipossuficiente digital como prioridade; 6. Conclusão; Referências.

1 INTRODUÇÃO

[1] Graduanda em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: lais.leal@sempreceub.com

A era da informação redefiniu o conceito de transparência no Direito. O princípio da publicidade processual, consolidado no artigo 93, inciso IX, da Constituição Federal, constitui um baluarte do Estado Democrático de Direito, garantindo o controle social e a legitimidade das decisões judiciais.

Contudo, a transição do contexto histórico-analógico para o ambiente digital irrestrito do Poder Judiciário desencadeou um paradoxo: o mecanismo desenhado para assegurar a justiça está, agora, funcionando como um canal de exposição permanente de dados pessoais. Esta digitalização, embora inerente ao avanço tecnológico, desvirtua o conceito clássico de "garantia da garantia" e coloca em profunda tensão a transparência com os direitos fundamentais à intimidade, imagem e segurança (Art. 5º, X e LXXIX).

O epicentro deste conflito recai sobre a população idosa, um grupo reconhecido por sua hipervulnerabilidade digital e social, que se torna o alvo preferencial de crimes cibernéticos. Ao divulgar nomes, valores de causas e vínculos familiares sem qualquer filtro de segurança ou necessidade, o próprio sistema de Justiça oferece o insumo para fraudes sofisticadas.

Diante da urgência imposta pela escalada do dano patrimonial e moral, este artigo propõe uma reflexão fundamental: é crucial que o princípio da publicidade seja intrinsecamente acompanhado por um limite protetivo, impedindo que a ampla divulgação de dados se torne um fator de risco para a população hipervulnerável. Portanto, há necessidade de o Poder Judiciário reinterpretar o princípio da publicidade sob o prisma da dignidade da pessoa humana, implementando maiores medidas de segurança.

2 O PARADOXO DA PUBLICIDADE PROCESSUAL NA ERA DIGITAL E O PRINCÍPIO DA PUBLICIDADE (ART. 93, IX, CF)

A transparência é um pilar essencial do Estado Democrático de Direito. No âmbito do Poder Judiciário, o princípio da publicidade processual, consagrado no artigo 93, inciso IX, da Constituição Federal, assegura que todos os julgamentos

sejam públicos e que as decisões sejam fundamentadas, garantindo controle social e legitimidade às decisões judiciais.

O que deveríamos compreender é: até que ponto a ampla disponibilização de informações processuais na internet, contendo dados pessoais e sensíveis, realmente serve ao interesse público? Conforme o Art. 6º, I, da Lei Nº 13.709 LGPD, todo tratamento de dados deve observar o princípio da finalidade, sendo realizado para propósitos legítimos, específicos, explícitos e sendo informados ao titular, observando as exceções.

O autor Luigi Ferrajoli diz que ao tornar o processo transparente " à luz do sol" conseguiríamos estabelecer a "garantia da garantia" que permite um controle duplo de maneira que seria assegurado externamente e internamente; o controle externo é a ideia de permitir com que qualquer cidadão ou até mesmo a imprensa tenha o poder de acessar o trabalho de todos os atuantes no processo judicial; o controle interno se dá quando as partes e seus defensores possuem a segurança de que os atos não ocorrerão em segredo.

Afinal, de acordo com esse pensamento doutrinário é pela a visibilidade dos atos processuais que se asseguram o respeito às demais garantias constitucionais, como o contraditório, a ampla defesa e o devido processo legal.

2.1 A transição do contexto histórico-analógico para a exposição irrestrita de dados

Apesar do inegável valor histórico, essa concepção clássica do princípio da publicidade foi formulada em um contexto histórico analógico, no qual a publicidade se materializava de modo físico e limitado por audiências presenciais, publicações em murais e acesso local aos autos. Na contemporaneidade digital, entretanto, a disponibilização irrestrita de dados nos portais eletrônicos do Judiciário modificou completamente essa dinâmica.

Na contemporaneidade, entretanto, a digitalização dos processos e a disponibilização irrestrita de dados nos portais eletrônicos do Judiciário modificaram completamente essa dinâmica. Essa mudança drástica sem nenhum preparo técnico

torna o dado facilmente minerável e pesquisável, é o cerne da exposição irrestrita que facilita novas vulnerabilidades.

2.2 O desvio de finalidade

Conforme se observa, a exposição irrestrita de dados configura um ponto de inflexão na lógica garantista, onde a suposta "garantia da garantia" começa, então, a se transformar em ameaça à própria essência das garantias constitucionais. Se, de um lado, a publicidade assegura controle social, de outro, pode violar a intimidade, a imagem e a segurança dos jurisdicionados que são valores tutelados pela Constituição Federal, especialmente em seu artigo 5º, incisos X e LXXIX.

A ideia de que a visibilidade absoluta constitui condição necessária para a justiça ignora que, em tempos de *big data*[2] e mineração automatizada de informações, a exposição pública não serve apenas ao controle democrático, mas também sendo uma facilitadora de práticas ilícitas, alimentando o modus operandi de criminosos especialistas em golpes contra idosos comprometendo o próprio sentido garantista do princípio.

3 O ESTATUTO DO IDOSO E O DEVER DE PROTEÇÃO NA CONSTITUIÇÃO FEDERAL.

Em contraponto à exposição de dados, o ordenamento jurídico impõe um dever claro de proteção ao grupo vulnerável, como se observa no Estatuto do Idoso, que, em seu artigo 10, impõe à sociedade e ao poder público a prioridade absoluta de garantir diversos direitos à pessoa idosa, como a vida, à saúde, à alimentação, à educação, o trabalho e a dignidade (BRASIL, 2003).

A Constituição Federal, em seu artigo 230, estabelece o dever da família, da sociedade e do Estado de apoiar as pessoas idosas, garantindo sua participação comunitária, defendendo sua dignidade, o bem-estar e o direito à vida. Com base

[2] Big data: Termo que define o conjunto de dados extremamente volumosos, variados e que são gerados em alta velocidade. No contexto de segurança e privacidade, refere-se à capacidade tecnológica de coletar, armazenar e analisar massas de dados para identificar padrões e perfis, sendo crucial tanto para a prevenção de crimes.

nisso, até que ponto a consulta processual pública extrapola o limite da relevância social e passa a representar uma ameaça à privacidade e à segurança dos cidadãos, sobretudo quanto à hipervulnerabilidade dos idosos que é deixada de lado.

3.1 A inexperiência digital como fator de hipervulnerabilidade é alvo para fraudes

Apesar das garantias legais existentes, a realidade prática dos crimes cibernéticos revela um descompasso alarmante: idosos são considerados alvos fáceis de crimes cibernéticos, conforme um levantamento global da Kaspersky, fabricante de softwares de segurança. Segundo Fábio Assolini, pesquisador sênior de Segurança Digital da empresa, "O fraudador, quando vai fazer o ataque, mira a todos, mas quando vê que a pessoa já tem alguma idade, costuma aperfeiçoar golpes". Ele ainda explica que, por não possuírem amplo conhecimento em segurança ou fraudes na web, os idosos não conseguem diferenciar o que é legítimo de uma fraude, o que demonstra a propensão desse grupo a um risco maior. (KASPERSKY, [2018]).

A crescente digitalização da vida cotidiana transformou a forma como as pessoas interagem, consomem e acessam serviços públicos, inclusive os judiciais. Entretanto, essa transformação não ocorreu de forma igual para todos. Os idosos, muitas vezes alijados dos avanços tecnológicos ou com menor domínio sobre ferramentas digitais, tornaram-se um dos principais alvos dos crimes cibernéticos. Essa vulnerabilidade não é apenas tecnológica, mas também jurídica e social, exigindo uma resposta estatal mais cuidadosa e preventiva.

3.2 Dados processuais públicos como vetor de fraude

No ambiente de consulta pública judicial, os dados processuais assumem o papel de vetor para atividades criminosas, pois a mera divulgação de informações como nomes, valores de causas e advogados pode representar uma porta de entrada para práticas fraudulentas, pois não exige nenhuma condição prévia de acesso pode representar uma porta de entrada para práticas fraudulentas, contrariando a

finalidade protetiva da legislação. O mesmo idoso que busca o Judiciário para ter obter um direito reconhecido, muitas vezes passa a ser vítima de golpes telefônicos, mensagens falsas e extorsões, em razão da exposição involuntária de suas informações pessoais.

Estudos recentes reforçam essa percepção Wojahn et al. (2022), ao analisarem a vulnerabilidade social dos idosos frente a golpes digitais, concluem que, embora o artigo 230 da Constituição Federal e o Estatuto do Idoso garantam proteção integral a essa faixa etária, tais dispositivos não têm sido suficientes para evitar a ocorrência de fraudes tecnológicas.

Segundo os autores, a ingenuidade tecnológica e a ausência de políticas públicas de educação digital contribuem para que os idosos se tornem vítimas recorrentes de crimes cibernéticos, o que evidencia um grave descompasso entre as garantias legais e a realidade prática.

Segundo o Radar Febraban 2024, 40% das pessoas acima de 60 anos já foram vítimas ou sofreram tentativas de algum tipo de golpe envolvendo sua conta bancária, número que cresce a cada ano e que parte de origens lícitas de dados, porém utilizados de maneira indevida, como informações disponíveis em sites de tribunais e diários oficiais. Há inúmeros relatos de criminosos que se passam por advogados, servidores ou representantes de instituições bancárias, valendo-se de detalhes extraídos de processos públicos para dar verossimilhança às suas abordagens.

4 MODUS OPERANDI E O “GOLPE DO FALSO ADVOGADO”

Um dos exemplos mais emblemáticos da fragilidade da publicidade judicial é o "golpe do falso advogado", um *modus operandi*[3] que se beneficia diretamente do acesso a informações sensíveis através de processos judiciais públicos.O contato é

[3] *Modus operandi:* É uma expressão em latim que significa "modo de operar" ou "maneira de funcionar". No campo do Direito, da Criminologia e da Segurança Digital, o *Modus Operandi* designa o conjunto de métodos, hábitos, técnicas e padrões de comportamento recorrentes que um indivíduo ou um grupo criminoso utiliza para cometer seus atos ilícitos.

realizado, via de regra, por telefone ou aplicativos de mensagens (como WhatsApp), onde o golpista se apresenta como assessor jurídico ou funcionário do escritório, alegando que o advogado principal não pode falar no momento. A tática de persuasão frequentemente envolve o uso de linguagem jurídica, perfis falsos com fotos de profissionais e, crucialmente, a imposição de uma urgência exagerada, forçando a vítima a agir sem tempo para desconfiar ou verificar a informação. "O golpe do falso advogado tem se tornado endêmico, em nível nacional, o que afeta não apenas cidadãos, mas também a credibilidade da advocacia", defendeu Paulo Maurício Siqueira, o atual presidente da OAB/DF.

O ponto central do golpe reside na imposição de uma falsa condição para a liberação do processo judicial. A vítima é levada a crer que deve pagar antecipadamente "custas processuais", "impostos" ou "taxas cartorárias" que seriam necessárias para liberar um valor de indenização. Esse falso pagamento é, então, solicitado via PIX ou depósito para contas de terceiros ("laranjas"), configurando o estelionato e o dano patrimonial.

Essa falha atual e concretizada no modelo de publicidade apenas comprova mais uma vez o paradoxo alarmante desse princípio. Pois, embora o acesso ao teor completo dos autos seja restrito por senhas ou *tokens*, a disponibilização de dados sensíveis na consulta pública como nome da parte, valor da causa e nome do advogado fornece os dados primários para que a dignidade da pessoa idosa seja lesada e seu patrimônio, roubado.

4.1 Casos concretos

A eficácia deste tipo de fraude é lamentavelmente comprovada por casos concretos de dano patrimonial.

Em São José do Rio Preto (SP), no dia 31 de outubro de 2025, uma idosa de 74 anos foi vítima, perdendo mais de R$ 47 mil. O boletim de ocorrência revela o *modus operandi* que se beneficia da publicidade de dados sensíveis e da vulnerabilidade emocional. O golpista iniciou o contato com a vítima afirmando que

ela teria valores a receber em razão do falecimento de uma irmã, citando dados específicos do óbito (ocorrido após um AVC em um restaurante) (G1, 2025).

A menção a detalhes familiares e ao evento do óbito, combinada com a promessa de valores, demonstra que esta fraude é construída em uma base de dados que extrapola um "mero cadastro telefônico". A facilidade de acesso a documentos processuais, que inevitavelmente contém informações sobre heranças, inventários, vínculos familiares e valores financeiros, permite que o criminoso atue com uma precisão cirúrgica.

A urgência nesse debate é sublinhada também pela audácia e frieza dos criminosos. Uma reportagem no domingo espetacular mostra além da constatação da fraude o quanto a idade dessas pessoas é levada em consideração.

Durante uma investigação policial que foi transmitida nesse programa, é mostrado que os golpistas chegam a gravar vídeos e compartilhar tutorias internos para seus comparsas e revela a frieza que demonstram em zombar das vítimas como "bora velha", "olha aí, nem preciso falar nada, a velha já ta indo sozinha! ó!" , "vai sua velha sem dente", os golpistas ridicularizam e fazem piadas das vítimas de maneira hostil tirando proveito da falta de conhecimento. Nessa reportagem foi enfatizado que o alvo são pessoas com mais de 60 anos de idade.

Estes casos não são isolados; eles são as evidências concretas de que a exposição pública dos dados não atende mais à finalidade constitucional de transparência, agindo como um vetor de insegurança que exige intervenção imediata de autoridades competentes.

5 MEDIDAS DE *ENFORCEMENT* DA LGPD PELO JUDICIÁRIO

A condição de hipervulnerabilidade digital da população idosa impõe ao Poder Judiciário uma reavaliação imediata de suas práticas de divulgação de dados. Ao operar sistemas de informação processual e publicar atos em Diários Eletrônicos, o Judiciário assume o papel de Controlador de Dados, tornando-se diretamente

responsável pela segurança das informações pessoais de seus usuários, conforme previsto na Lei Geral de Proteção de Dados (LGPD).

Este cenário exige que o Judiciário transcenda a mera conformidade formal e adote uma postura ativa de *enforcement*,[4] isso significa dizer portanto que sejam aplicados rigorosamente nas políticas de acesso os princípios da LGPD como o da necessidade e o da prevenção.

A efetivação da justiça, em uma sociedade digital, não pode ser medida apenas pela quantidade de informações disponibilizadas, mas sim pela capacidade do sistema em garantir a proteção dos direitos fundamentais sem gerar novas exclusões . O Judiciário deve, portanto, reconhecer que a proteção de dados não se opõe totalmente à transparência mas ela a qualifica, estabelecendo o limite protetivo necessário para salvaguardar a dignidade da pessoa idosa no ambiente digital.

5.1 Soluções técnicas e a anonimização em camadas

Dentre as medidas mais eficazes e necessárias, destaca-se a proposta de anonimização de dados de identificação. Em processos que não tramitam em segredo de Justiça, mas que envolvam partes hipervulneráveis, deve-se adotar a pseudonimização ou anonimização parcial na consulta pública. Isso implica em limitar a possibilidade de busca pelo nome completo de pessoas idosas nos sistemas de consulta. A busca deveria ser prioritariamente feita pelo número do processo para fins de controle institucional ou pelo CPF/OAB (para as partes e advogados).

Além disso, propõe-se a ocultação seletiva de endereços/dados de contato, ocultando ou rasurando automaticamente em documentos públicos acessíveis por terceiros não autorizados.

Por fim, a implementação de Limitação de Requisições (*Rate Limiting*) é fundamental, definindo um limite diário ou por hora de quantas consultas por CPF/Nome podem ser feitas a partir do mesmo endereço de IP (ou máquina) quando a consulta for pública impede a mineração de dados em grande escala, tornando a

[4] Enforcement: Termo de origem inglesa que, no contexto jurídico e regulatório, designa a aplicação, execução e fiscalização ativa das normas e sanções previstas em lei e um dos aspectos mais importantes do enforcement é a sua capacidade de promover a confiança no sistema jurídico.

coleta de uma lista grande de vítimas financeiramente e tecnicamente inviável para os golpistas.

5.2 Mecanismo de acesso qualificado para fins de pesquisa

Para que essas limitações não afetem estudantes, pesquisadores e a imprensa, que possuem interesse legítimo, a forma de solucionar isso é criar um "filtro na legitimidade" ou mecanismo de acesso qualificado.

O CNJ como proposta deve criar um cadastro simples e obrigatório para essas pessoas, idealmente dentro do próprio portal GOV.br, vinculando a identidade do usuário. Para estudantes, a plataforma poderia solicitar até uma autorização da instituição de ensino e, nos demais casos, poderia ser solicitado um Termo de Responsabilidade e Compromisso dentro da plataforma por essas pessoas.

Mesmo que tenham esse credenciamento, após fazer a consulta e antes de abrir qualquer processo, o usuário deverá responder um questionário e justificar o motivo de interesse real ao acesso.

Assim, poderiam ter uma versão mais completa de processos dentro de uma plataforma específica de consultas processuais, garantindo que o acesso à informação sirva ao estudo e ao controle social, e não à fraude.

5.3 Tutela da dignidade humana e do hipossuficiente digital como prioridade

A reinterpretação do princípio da publicidade já não é mais apenas uma recomendação e sim um fator necessário e indiscutível que priorize a autodeterminação informativa e a tutela do hipervulnerável.

A adoção de um novo paradigma de publicidade digital, que equilibre o acesso à informação com a proteção à dignidade e à segurança, é um imperativo ético e legal. Neste cenário, o Poder Judiciário deve internalizar o entendimento de que sua função como garantidor da justiça se estende à segurança digital de seus usuários.

Isso implica reconhecer que a ampla e irrestrita divulgação de dados pessoais em plataformas de consulta pública não cumpre integralmente a finalidade democrática da publicidade. Portanto, a tutela da dignidade humana requer que o Judiciário adote uma publicidade qualificada, em que a exposição de dados seja sempre minimizada.

A proteção ao hipervulnerável deve ser o filtro inegociável, assegurando que o sistema não apenas puna o dano após sua ocorrência, mas que atue proativamente para prevenir a fraude, garantindo que o direito à informação não se sobreponha ao direito fundamental à proteção de dados e à integridade patrimonial dos cidadãos.

6 CONCLUSÃO

O presente estudo jurídico-social confirmou a existência de um grave desajuste entre a garantia legal de proteção à pessoa idosa e os riscos concretos impostos pela dinâmica da informação digital. A pesquisa demonstrou que a publicidade inerente aos sistemas processuais, embora vital para a transparência democrática, transformou-se em uma fonte acessível e rica de dados para a prática do estelionato digital, sendo o *modus operandi* do falso advogado a expressão mais grave dessa vulnerabilidade.

Concluiu-se que o problema reside na aplicação irrestrita do princípio da publicidade, que falha em considerar a hipervulnerabilidade do jurisdicionado idoso. Este contexto exige que a doutrina e a jurisprudência abandonem uma leitura formalista da publicidade e avancem para uma perspectiva teleológica, onde o direito fundamental à dignidade humana e à autodeterminação informativa se sobrepõe ao interesse genérico na exposição plena de dados.

A solução defendida se materializa em uma proposta de atuação bifacetada, coordenada pelo Poder Judiciário em sua função de Controlador de Dados, nos termos da LGPD.

Primeiramente, é imperativo o desenvolvimento de soluções tecnológicas de mitigação de risco, como a pseudonimização de dados pessoais e valores de causa nas consultas abertas, bem como a implementação de controles sistêmicos (*rate*

limiting) para frustrar a coleta massiva de dados por *softwares* maliciosos. Em segundo lugar, e de forma complementar, faz-se necessária a criação de um regime de acesso qualificado, que garanta a pesquisa acadêmica e o controle da imprensa mediante credenciamento e termo de responsabilidade, preservando assim o interesse público sem comprometer a segurança individual.

Em síntese, o desafio contemporâneo imposto ao Judiciário não é o de escolher entre a transparência e a segurança, mas sim o de fundi-las. A verdadeira eficácia do sistema de justiça, na era digital, será medida pela sua capacidade de garantir que o princípio da publicidade cumpra seu papel democrático sem que o processo judicial gere suas próprias vítimas.

É hora de o Direito evoluir, utilizando a tecnologia para blindar o cidadão mais frágil e reafirmar o compromisso inegociável com a proteção do patrimônio e da dignidade da pessoa idosa.

REFERÊNCIAS

A VULNERABILIDADE social dos idosos frente a golpes no âmbito digital. Pesquisa, Sociedade e Desenvolvimento, [S. l.], v. 11, n. 11, p. e452111133652, 2022. DOI: $10.33448/rsd-v11i11.33652$. Disponível em: https://rsdjournal.org/rsd/article/view/33652. Acesso em: 13 out. 2025.

ARAUJO, Gabriely; LIMA, Galeno. Idoso é alvo fácil de invasores na internet. Estadão, São Paulo, [s.d.]. Disponível em: https://infograficos.estadao.com.br/focas/planeje-sua-vida/idoso-e-alvo-facil-de-invasores-na-internet. Acesso em: 7 out. 2025.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Presidência da República, [2025]. Disponível em: [https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm]. Acesso em: [7 de out. 2025].

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 out. 2025.

CONSELHO NACIONAL DE JUSTIÇA – CNJ. Tribunal do DF e OAB-DF se unem para combater golpe do falso advogado. Portal CNJ, 18 jun. 2025. Disponível em: https://www.cnj.jus.br/tribunal-do-df-e-oab-df-se-unem-para-combater-golpe-do-falso-advogado/. Acesso em: [19 de novembro de 2025].

(5315) Falso advogado: criminosos roubam dados de processos para aplicar golpes online. YouTube. Disponível em: [https://www.youtube.com/watch?v=kPfbkjtX1ws]. Acesso em: [20 de nov. de 2025].

FEDERAÇÃO BRASILEIRA DE BANCOS (FEBRABAN). Abuso econômico contra idosos e mulheres. 2024. Disponível em: https://meubolsoemdia.com.br/Materias/abuso-economico-contra-idosos-e-mulheres. Acesso em: 15 out. 2025.

FERRAJOLI, Luigi. Direito e Razão: Teoria do Garantismo Penal. Tradução de Ana Paula Zomer et al. 3. ed. São Paulo: Editora Revista dos Tribunais, 2002.

G1. Golpe do 'falso advogado': idosa perde mais de R$ 47 mil ao receber ligação em Rio Preto. G1, São Paulo, 1 nov. 2025. Disponível em: https://g1.globo.com/sp/sao-jose-do-rio-preto-aracatuba/noticia/2025/11/01/golpe-do-falso-advogado-idosa-perde-mais-de-r-47-mil-ao-receber-ligacao-em-rio-preto.ghtml. Acesso em: 12 nov. 2025.

LEGALE. Fraude de falso advogado: como identificar e agir no Direito Digital. Legale: Blog de Direito Digital. [04 de nov. 2025]. Disponível em: https://legale.com.br/blog/fraude-de-falso-advogado-como-identificar-e-agir-no-direito-digital/. Acesso em: 21 nov. 2025.

MINISTÉRIO DO DESENVOLVIMENTO E ASSISTÊNCIA SOCIAL, FAMÍLIA E COMBATE À FOME. Princípios da LGPD. Brasília, DF, [2021]. Disponível em: https://www.gov.br/mds/pt-br/acesso-a-informacao/lgpd/principios-da-lgpd. Acesso em: [21 de nov. de 2025].

TRIBUNAL DE JUSTIÇA DE SANTA CATARINA. Agravo de Instrumento n. 5057163-04.2023.8.24.0000, Rel. João de Nadal, Sexta Câmara, julgado em 30/01/2024. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sc/2155313938?origin=serp. Acesso em: [19 de novembro de 2025].

A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NAS ATIVIDADES DE INVESTIGAÇÃO POLICIAL

Ana Thereza Santana Pessoa[1]

RESUMO

O presente artigo tem como objetivo analisar até que ponto a Lei Geral de Proteção de Dados (LGPD) limita ou regula o uso de informações pessoais em investigações policiais, além de analisar o direito fundamental à privacidade e à proteção de dados e o conflito existente com à segurança pública. Com maior enfoque no seu artigo 4°, inciso III, que trata da inaplicabilidade da LGPD em alguns casos, o estudo revisa o raciocínio manifestado pela Advocacia-Geral da União (AGU) e o posicionamento do Supremo Tribunal Federal (STF). Além disso, tratará do pré-projeto da Lei Geral de Proteção de Dados Penal, prevista no § 1° do artigo 4°, que dispõe sobre a necessidade de legislação específica.

Palavras-chave: LGPD, Tratamento de dados, Investigações, Segurança do Estado.

ABSTRACT

The present article aims to analyze the extent to which the General Data Protection Law (LGPD) limits or regulates the use of personal information in police investigations, as well as to examine the fundamental right to privacy and data protection and its conflict with public security. With a greater focus on Article 4, item III, which addresses the inapplicability of the LGPD in certain cases, the study reviews the reasoning presented by the Office of the Attorney General (AGU) and the position adopted by the Federal Supreme Court (STF). Additionally, it discusses the draft bill of the General Law on Criminal Data Protection, provided for in paragraph 1 of Article 4, which establishes the need for specific legislation.

KEYWORDS: LGPD, Data processing, Investigations, State security.

SUMÁRIO: Introdução. 1. Princípios do tratamento de dados pessoais, direito à privacidade e à proteção de dados; 2. Inaplicabilidade da LGPD e consequência das lacunas normativas; 3. Manifestação da AGU e do STF; 4. O anteprojeto da Lei Geral de Proteção de Dados Penal; 5. Fishing expedition no processo penal; Conclusões; Referências.

[1] Graduanda em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: ana.spessoa@sempreceub.com.

1 INTRODUÇÃO

Inicialmente, faz-se necessário destrinchar a Lei Geral de Proteção de Dados (LGPD) para uma melhor compreensão do assunto. A LGPD regula o tratamento de dados pessoais no setor público e no setor privado, impondo obrigações que garantam a segurança, a transparência e o uso adequado de informações. Tem como objetivo proteger os direitos individuais, a privacidade, a liberdade e o livre desenvolvimento da personalidade, além de criar uma segurança jurídica na proteção de dados dos cidadãos. A lei estabelece uma autoridade com a finalidade de fiscalizar e aplicar penalidades pelos eventuais descumprimentos de normas. Tal atividade ficou a encargo da Autoridade Nacional de Proteção de Dados Pessoais (ANPD). Além disso, a LGPD trata os dados de acordo com suas particularidades, por exemplo, dados de crianças e adolescentes possuem um tratamento diferenciado, assim como dados sensíveis, classificados dentro do rol do artigo 11 da LGPD[2].

Apesar de a lei ter como objetivo proteger a privacidade dos cidadãos, há um conflito com o interesse público quando relacionado à segurança pública. Isso porque o artigo 4° dispõe sobre restrições à aplicação da Lei. Ei-lo:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
>
> I - Realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
>
> II - Realizado para fins exclusivamente:
>
> a) jornalístico e artísticos; ou
>
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
>
> III - realizado para fins exclusivos de:
>
> a) segurança pública;
>
> b) defesa nacional;
>
> c) segurança do Estado; ou
>
> d) atividades de investigação e repressão de infrações penais; ou

[2] O que é a LGPD? Disponível em: O que é a LGPD? — Lei Geral de Proteção de Dados Acesso em 15 de outubro de 2025.

> IV - Provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.
>
> § 1º 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.
>
> § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.
>
> § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos ... responsáveis relatórios de impacto à proteção de dados pessoais.
>
> § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei nº 13.853, de 2019) Vigência[3]

Ao observar o artigo 4°, inciso III, alíneas a, b, c e d, é possível verificar que a Lei não se aplica ao tratamento de dados pessoais com fins exclusivos de segurança pública, segurança do Estado ou atividades de investigação e repressão de infrações penais. Apesar da exceção prevista, seguindo esse dispositivo, há outras determinações que visam regular o uso de dados, conforme §§ 1° e 3°, os quais determinam a utilização de uma legislação específica que observe o devido processo legal, os princípios gerais de proteção e as medidas proporcionais que atendam ao interesse público.

[3] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

2 PRINCÍPIOS DO TRATAMENTO DE DADOS PESSOAIS, DIREITO À PRIVACIDADE E À PROTEÇÃO DE DADOS.

O tratamento de dados com fins investigativos deve ser feito por meios especiais, visto que a referida lei não se aplica. Entretanto, os princípios da Lei Geral de Proteção de Dados devem ser observados, pois, apesar da exclusão, existem limites a serem respeitados. Os princípios do tratamento de dados pessoais estão dispostos no art. 6° da Lei n° 13.709/18. Nota-se:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> I - Finalidade: realização do tratamento para propósitos legítimos,
>
> específicos, explícitos e informados ao titular, sem possibilidade de
>
> tratamento posterior de forma incompatível com essas finalidades;
>
> II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
>
> IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
>
> V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
>
> VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
>
> VII - segurança: utilização de medidas técnicas e administrativas aptas a protegeros dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
>
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

> IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
>
> X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. [4]

À vista disso, a lei é clara com relação aos princípios, mas é necessário tratar de alguns de seus incisos com maior atenção. O inciso II aborda a necessidade de adequar os dados à finalidade objetivada, para evitar que haja desvio de finalidade dos dados e para evitar que os dados sejam utilizados inadequadamente.

O inciso III, por sua vez, versa sobre o princípio da necessidade, o qual dispõe que o Estado só pode acessar os dados quando for estritamente indispensável para atingir a finalidade da investigação. Além disso, a solicitação dos dados deve ser definida, caracterizada por período, tipo de dado e objetivo de obter a informação.

O inciso VI cuida da transparência e tem como objetivo tornar as informações do que foi feito com os dados acessíveis. Envolve a rastreabilidade interna e a possibilidade de controle, por exemplo, por meio de registro de quem acessou os dados e o motivo do acesso.

O inciso VII trata da segurança, sendo certo que o Estado precisa proteger os dados que coletou, por meio de ferramentas, como por exemplo, acesso aos dados somente em computadores que possuem criptografia de ponta a ponta, para evitar o vazamento de dados. No contexto de investigações policiais, há de se ter um cuidado com as redes abertas, a fim de evitar que haja vazamento de dados investigativos e outros.

Há, ainda, a proporcionalidade, que não está explícita no art. 6° da Lei, mas que merece destaque. A proporcionalidade dispõe que o acesso aos dados não pode ser invasivo aos extremos, ou seja, faz-se necessário que o tratamento de dados seja

[4] **BRASIL**. Câmara dos Deputados. Anteprojeto de Lei Geral de Proteção de Dados. Câmara dos Deputados, abr 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459&filename=Tramitacao-PL+5276/2016. Acesso em: 21 de nov. 2025

feito com a menor quantidades de dado possível, apenas o suficiente. Nas investigações policiais, por exemplo, os agentes devem recorrer a outros meios antes de utilizar do tratamento de dados.

Sendo assim, ainda que a LGPD tenha exclusões no art. 4° inciso III, os princípios se aplicam ao conteúdo destas e precisam ser observados pelas autoridades. É notório que a ausência da LGPD-Penal aumenta o risco de violação desses princípios, visto que no início da Lei 13.709/18 há exclusão e nos entendimentos jurisprudenciais tais princípios se aplicam às exclusões, causa de confusão na vida prática.

O direito à privacidade está disposto em vários instrumentos normativos, como na Declaração Universal de Direitos Humanos, no Pacto Internacional sobre Direitos Civis e Políticos e na Constituição Federal. Confira-se:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> X - São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; [5]

Esses dispositivos reconhecem que os indivíduos têm direito a vida privada, a honra, a liberdade e, dentre eles, à proteção de dados pessoais. A Constituição brasileira garante tais direitos aos cidadãos, o que significa que todos têm direito de usufruí-los e gozá-los. Para estes fins a Lei Geral de Proteção de Dados foi criada, a fim de que haja segurança nas informações pessoais.

3 INAPLICABILIDADE DA LGPD E CONSEQUÊNCIAS DAS LACUNAS NORMATIVAS

A inaplicabilidade da LGPD está prevista no art. 4° inciso III, alíneas “a”, “b”, “c” e “d”. Tal inviabilidade ocorre, nos casos de segurança pública, segurança do Estado, defesa nacional, atividades de investigação e repressão de infrações

[5] BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Diário Oficial da União, Brasília, DF, 5 out. 1988.

penais, porque muitas vezes a coleta e o monitoramento de dados podem invadir a privacidade das pessoas, violando seus direitos fundamentais para fins de prevenção de crimes e ameaças à segurança.[6] São casos em que o interesse público de garantir a segurança prevalece sobre interesses individuais. No intuito de elucidar melhor o exemplo, utiliza-se a compreensão de que em uma investigação penal na qual é necessário a coleta e monitoramento de dados, haverá duas opções:

a) Seguir as disposições da LGPD e não violar os direitos e, assim, obter resultados, quais sejam:

i. O interesse do Estado não comprometido ou;

ii. O interesse do Estado comprometido

Não seguir as disposições, violar alguns direitos eventualmente e assim obter as informações necessárias. Os resultados podem ser:

iii.O interesse do Estado em garantir segurança é alcançado ou;

iv.Os direitos são violados e não é possível chegar em nenhuma conclusão, sendo assim, o Estado não consegue garantir seus interesses.

De qualquer maneira, a referida lei prevê que é necessária uma lei específica para tratar de tais casos, lei esta que é conhecida como LGPD-penal. Desta forma, é possível notar que há uma lacuna normativa que causa consequências práticas.

Um dos efeitos que a lacuna causa é a ausência de critérios legais de proporcionalidade e necessidade que definam um limite às autoridades. Até onde os órgãos de inteligência podem ir em suas investigações? Como podem fazê-lo? A ausência de normas que regulem esse tipo de questionamento abre espaço para arbitrariedades. Ainda nessa linha de argumentos, qual órgão fiscaliza as atividades de inteligência, já que a ANPD fiscaliza os dados regulados pela LGPD? Há uma incerteza na fiscalização, na competência da fiscalização.

[6] SAMPAIO, Ricardo Ramos. Inaplicabilidade da Lei Geral de Proteção de Dados: a interpretação do art. 4º, inciso III e §1º da LGPD à luz do direito comparado. Revista da AGU, Brasília, v. 20, n. 2, p. 231-258, 2021. Disponível em: https://revistaagu.agu.gov.br/index.php/AGU/article/view/3142. Acesso em: 15 out. 2025.

Além desta consequência, há a falta de controle de registros e auditoria, como adequa o princípio da responsabilização e prestação de contas [7]. Por fim, é notório que as consequências acima elencadas acarretam um risco de abuso dos dados, como por exemplo, o compartilhamento de dados sem ordem judicial, quando dela dependerem.

4 MANIFESTAÇÃO DA AGU E DO STF

A Advocacia-Geral da União apresentou entendimento em relação à inaplicabilidade da LGPD às atividades de segurança pública e firmou como posicionamento a necessidade de legislação própria para o tratamento de dados que resguarde a proporcionalidade, o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD.

O Supremo Tribunal Federal, por sua vez, reconheceu, por decisão do Ministro Gilmar Mendes, que "o próprio texto da LGPD escusa a aplicação dos seus princípios e diretrizes ao tratamento de dados para fins de segurança pública, defesa nacional ou segurança do Estado". (ADPF,2020)[8]

5 O ANTEPROJETO DA LEI GERAL DE PROTEÇÃO DE DADOS PENAL

No dia 26 de novembro de 2019 foi constituída Comissão de Juristas para elaboração do Anteprojeto para segurança pública e persecução penal (LGPD-Penal). O anteprojeto regulamentou apenas as alíneas "a" e "d" do inciso III, do art. 4°, deixando um vazio nas alíneas "b" e "c". Veja-se:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais realizado por autoridades competentes para atividades de

[7] **BRASIL**. Câmara dos Deputados. Anteprojeto de Lei Geral de Proteção de Dados. Câmara dos Deputados, abr 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459&filename=Tramitacao-PL+5276/2016. Acesso em: 21 nov. 2025

[8] BRASIL. Supremo Tribunal Federal (2. Turma). Arguição de Descumprimento de Preceito Fundamental n° 695. Compartilhamento de dados pessoais pelo Serpro à ABIN. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15343579920&ext=.pdf. Acesso em: 17 out. 2025

> segurança pública e de persecução penal, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O anteprojeto prevê o respeito à privacidade em seu art. 2°:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamento o respeito à privacidade e:
> I - a autodeterminação informativa;
> II - a liberdade de expressão, de comunicação e de opinião;
> III - a inviolabilidade da intimidade, da vida privada, da honra e da imagem;
> IV - o desenvolvimento econômico e tecnológico; e
> V - a livre iniciativa, a livre concorrência e a defesa do consumidor.

Além de tais fundamentos, é preciso que sejam aplicadas medidas preventivas a fim de evitar abusos no tratamento de dados da pessoa. Como já exposto alhures, terão violações no que toca a direitos à privacidade, sendo, pois, imprescindível que sejam pensadas formas de tais violações ocorrerem de maneira menos danosa. Por exemplo, poderiam viabilizar essas violações apenas em último caso, ou seja, assim como o direito penal deve funcionar como *ultima ratio*, o acesso aos dados deveria ser dado apenas quando não houvesse nenhum outro meio que fosse igualmente eficaz ou menos ofensivo. Além disso, deveria ter uma fiscalização com relação ao acesso e uso dos dados porque além de acesso à privacidade de outrem há o risco de abusos durante a atividade de tratamento de dados.[9]

5 FISHING EXPEDITION NO PROCESSO PENAL

Fishing expedition é uma busca com base especulativa para auxiliar a acusação. A definição a seguir explicita de maneira mais clara. (Rosa, 2021)

> Fishing expedition é a procura especulativa, no ambiente físico ou digital, sem causa provável, alvo definido, finalidade tangível ou para além dos limites autorizados (desvio de finalidade), de elementos capazes de atribuir responsabilidade penal a alguém (...) Prática relativamente comum de se aproveitar dos espaços de exercício de poder para subverter a

[9] COSTA, Rafael Di Lorenzo. Lei Geral de Proteção de Dados e a atividade de inteligência em segurança pública: uma análise profícua entre a privacidade individual e a segurança coletiva. Recima21 – Revista Científica Multidisciplinar, v. 6, n. 1, p. 1-15, 2025. Disponível em: https://recima21.com.br/index.php/recima21/article/view/5813. Acesso em: 15 out. 2025.

> lógica das garantias constitucionais, vasculhando-se a intimidade, a vida privada, enfim, os direitos fundamentais, para além dos limites legais [10]

Como se vê, trata-se de procedimento fundado em convicções e suspeitas infundadas, na qual a lógica do processo penal, de proteger o acusado do Estado, é posta em risco. Esta é, logo, mais uma linha de ação que a lei deve prever e prevenir, uma vez que se a conduta for praticada e não houver sanção, estará tudo bem, porque não haverá prejudicados. Por outro lado, se a prática incorrer em um processo criminal e os direitos da pessoa forem violados, por exemplo, uma pessoa que perde a sua liberdade de ir e vir a partir de convicções, de suspeitas sem qualquer fundamento, então haverá um problema: uma injustiça ocorrendo devido à prática de fishing expedition. Portanto, é muito importante que a LGPD-Penal lide com essas práticas que inicialmente parecem inofensivas, mas que podem acarretar problemas muito maiores.

6 CONCLUSÃO

Ante o exposto, conclui-se necessário que a LGPD-Penal seja elaborada com uma certa urgência, de maneira que consiga abarcar todos os princípios e garantias constitucionais expostos da forma mais eficiente possível. Além de impor restrições aos dados e ao seu tratamento, a fim de evitar abusos e maiores complicações no decorrer das investigações.

É preciso que seja definido um órgão que faça a fiscalização, que haja determinação de como será feita, como será regulada - por meio de relatórios ou auditorias - além de possíveis sanções quando houver irregularidades.

Ademais, é essencial que a lei disponha sobre como será feito o tratamento de dados, em quais momentos poderão ser usadas as informações, quando e para que serão usados os dados caracterizados como sigilosos. É necessário que haja limites e hipóteses para seguir com as investigações sem a necessidade do uso de informações

[10] A prática de fishing expedition no processo penal. Disponível em: A prática de fishing expedition no processo penal Acesso em: 17 out. 2025

que sejam invasivas e que violem o direito à privacidade, respeitando a proporcionalidade disposta na LGPD e nos princípios constitucionais.

Por fim, há necessidade da criação de outra lei específica, para tratar dos demais dispositivos (alíneas "b" e "c", do inciso III art. 4°) ou que, na mesma lei, LGPD Penal, haja normas distintas para cada uma das hipóteses dos incisos. Este artigo trata apenas de duas hipóteses excluídas da LGPD, entretanto, com certeza, as outras duas hipóteses têm sua urgência com relação ao tratamento de dados.

REFERÊNCIAS

ABIN. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15343579920&ext=.pdf. Acesso em: 17 out. 2025

ALVES, Pedro de Oliveira; OLIVEIRA FILHO, Felipe Gustavo Ramos de. O direito fundamental de proteção de dados no processo penal brasileiro: a ilicitude dos mandados de busca e apreensão como práticas de *fishing expedition*. *Revista Acadêmica da Faculdade de Direito do Recife*, Recife: UFPE, v. 93, n. 2, p. 245-269, 2022. Disponível em: https://periodicos.ufpe.br/revistas/ACADEMICA/article/view/253037. Acesso em: 15 out. 2025.

A prática de fishing expedition no processo penal. Disponível em: A prática de fishing expedition no processo penal Acesso em: 17 out. 2025

BRASIL. Câmara dos Deputados. Anteprojeto de Lei Geral de Proteção de Dados. Câmara dos Deputados, abr 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459&filename=Tramitacao-PL+5276/2016. Acesso em: 17 out. 2025

BRASIL. Câmara dos Deputados. Anteprojeto de Lei Geral de Proteção de Dados Penal. Câmara dos Deputados, nov 2020. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em: 17 out. 2025

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. *Diário Oficial da União*, Brasília, DF, 5 out. 1988.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União: seção 1*, Brasília, DF, 15 ago. 2018.

BRASIL. Supremo Tribunal Federal (2. Turma). Arguição de Descumprimento de Preceito Fundamental n° 695. Compartilhamento de dados pessoais pelo Serpro à

COSTA, Rafael Di Lorenzo. Lei Geral de Proteção de Dados e a atividade de inteligência em segurança pública: uma análise profícua entre a privacidade individual e a segurança coletiva. *Recima21 – Revista Científica Multidisciplinar*, v. 6, n. 1, p. 1-15, 2025. Disponível em: https://recima21.com.br/index.php/recima21/article/view/5813. Acesso em: 15 out. 2025.

O que é a LGPD? Disponível em: O que é a LGPD? — Lei Geral de Proteção de Dados Acesso em 15 de out. de 2025.

SAMPAIO, Ricardo Ramos. Inaplicabilidade da Lei Geral de Proteção de Dados: a interpretação do art. 4º, inciso III e §1º da LGPD à luz do direito comparado. *Revista da AGU*, Brasília, v. 20, n. 2, p. 231-258, 2021. Disponível em: https://revistaagu.agu.gov.br/index.php/AGU/article/view/3142. Acesso em: 15 out. 2025.

DIREITO E TECNOLOGIA: A RESPONSABILIDADE DAS PLATAFORMAS, O DEVER DE CUIDADO E O ENFRENTAMENTO AOS CIBERCRIMES, COM ÊNFASE NA PROTEÇÃO INTEGRAL DE CRIANÇAS E ADOLESCENTES

Ariely Vitória Lopes Lima[1]
Bruna Aquino Carvalho[2]
Maria Luísa Barbosa Guerra[3]
Naylani James de Oliveira[4]
Sofia Viana do Vale[5]

RESUMO

O presente artigo abordará os desafios enfrentados dentro da internet para manter a segurança de seus usuários e seus dados pessoais, como também a influência que a sociedade, principalmente crianças e adolescentes, vem sofrendo em razão do que é exposto e publicado na internet. A hipersexualização de menores de idade, o desenvolvimento de crianças e adolescentes, a proteção dos dados pessoais e as leis que versam sobre isso são temas que serão abordados e analisados neste artigo como forma de alertar os seus usuários, mostrar a evolução da tecnologia e das leis nesse âmbito e trazer uma reflexão sobre a devida importância que os provedores de internet têm dado aos seus usuários e ao que eles guardam e fazem dentro da internet.

Palavras-chave: Internet. Dados. Crimes cibernéticos. Hiperssexualização. Usuários.

SUMÁRIO: Introdução. 1. A dificuldade de conciliar a moderação do conteúdo com os princípios de proteção de dados e privacidade; 2. A hipersexualização e o uso deturpado das redes por menores de idade; 3. A responsabilidade civil no âmbito da internet e como meio de proteção dos dados pessoais; 4. Como o uso desenfreado

---

[1] Graduanda em Direito pelo Centro Universitário de Brasília, concluiu o projeto de extensão da Clínica de Direitos Humanos pelo CEUB.
[2] Graduanda em Direito pelo Centro Universitário de Brasília
[3] Graduanda em Direito pelo Centro Universitário de Brasília, escritora com dois livros publicados, concluiu o projeto de extensão da Clínica de Direitos Humanos pelo CEUB.
[4] Graduanda em Direito pelo Centro Universitário de Brasília
[5] Graduanda em Direito pelo Centro Universitário de Brasília, concluiu o projeto de extensão da Clínica de Direitos Humanos pelo CEUB.

das redes pode inibir o crescimento saudável e maduro de uma criança; 5. Como o marco civil da internet foi um avanço no âmbito de direito civis, mas se fez tão omisso no quesito da regulação do uso da internet; 5.1. O Marco Civil como avanço nos direitos civis; 5.2. A omissão na regulação da internet e o âmbito penal; 5.3 A responsabilidade; 5.4. O contraste com a jurisprudência anterior; 5.4. O ambiente digital atualmente e o dever de cuidado; 6. O dever geral de cuidado nas plataformas digitais; Considerações finais; Bibliografia.

1 INTRODUÇÃO

O presente artigo propõe a análise do dinâmico campo do Direito e Tecnologia no Brasil, examinando a evolução e os desafios do arcabouço normativo estabelecido para conciliar o desenvolvimento tecnológico com a proteção dos direitos fundamentais dos usuários.

Inicialmente, são resgatados os esforços legislativos no país, que datam de mais de três décadas, para o enfrentamento dos crimes cometidos na rede mundial de computadores. Neste contexto, destaca-se a promulgação da Lei n.º 12.965/2014, o Marco Civil da Internet (MCI), uma norma crucial para estabelecer princípios, garantias e deveres para o uso da rede. Não obstante, o regime de responsabilidade civil das plataformas digitais (provedores de aplicação) por danos decorrentes de conteúdo gerado por terceiros, conforme previsto no Artigo 19 do MCI, gerou intensa controvérsia. Essa regra é criticada por especialistas por condicionar a remoção de conteúdo ilícito à prévia ordem judicial específica, o que se configura como um obstáculo moroso para a vítima e um "flagrante retrocesso" que se aproxima de um regime de irresponsabilidade para os provedores.

Em contraste com a premissa de que as plataformas seriam "meras intermediárias passivas", a análise se aprofunda no atual ambiente digital, onde esses agentes exercem grande protagonismo e controle sobre o fluxo informacional por meio de algoritmos, atuando na chamada "economia da atenção". Diante dessa realidade, impõe-se a interpretação do MCI em conjunto com o ordenamento jurídico brasileiro (como o Código Civil e o CDC) para sustentar a exigência do dever geral de cuidado (duty of care) às plataformas. Tal dever implica uma atuação ativa e preventiva, que deve incidir inclusive sobre o design algorítmico da

plataforma, visando evitar a criação de riscos desarrazoados e a propagação de ilícitos.

Sob esse viés, o trabalho investiga os crimes cibernéticos, abordando a necessidade de inovação na legislação penal, impulsionada por casos específicos, como a promulgação da Lei n.º 12.737/2012 (Lei Carolina Dieckmann), que tipifica a invasão de dispositivo informático. É dada ênfase à análise de condutas de alta gravidade, como a apologia e incitação a crimes contra a vida e os massacres em escolas, crimes estes que são disseminados e incentivados por meio das redes sociais, muitas vezes utilizando referências cifradas que dificultam a moderação por algoritmos. Com a disseminação da tecnologia, internet e o uso desenfreado e inconsciente das redes sociais, a tipificação e observação ao cumprimento do que está tipificado possui uma alta relevância para a efetividade da proteção e garantia da segurança dos meios tecnológicos e de seus usuários.

Ademais, é dedicado um olhar especial à proteção integral de crianças e adolescentes (P & A). Dada a hiper vulnerabilidade desses usuários, o dever de cuidado é considerado mais rigoroso e exigente. Discute-se o desafio de conciliar a moderação de conteúdo com os princípios de privacidade e proteção de dados e a tutela assegurada pela Lei Geral de Proteção de Dados (LGPD), que impõe a observância do melhor interesse da criança. São analisados os riscos específicos que afetam esse público, como a exposição a discursos de ódio e a exploração comercial (publicidade abusiva e propaganda direcionada), destacando a necessidade de limites claros às plataformas para garantir o desenvolvimento saudável dos jovens.

2 A DIFICULDADE DE CONCILIAR A MODERAÇÃO DO CONTEÚDO COM OS PRINCÍPIOS DE PROTEÇÃO DE DADOS E PRIVACIDADE.

A moderação de conteúdos a serem veiculados nas principais plataformas digitais encontra diversos desafios, na tentativa de conciliar a proteção de dados e a privacidade das crianças e adolescentes. Nesse sentido, equilibrar a liberdade de expressão e a proteção da dignidade de usuários digitalmente vulneráveis faz-se um entrave a ser refletido e debatido, visando a proteção dos direitos de tais grupos. Os

processos de análise e de remoção de postagens veiculadas estão associados ao acesso às informações pessoais, fato que pode ocasionar riscos de vazamento de dados sensíveis e de exposição de menores. Por conseguinte, tal contexto ocasiona dilemas éticos, os quais envolvem a tentativa de conciliar, de um lado, a proteção de usuários contra conteúdos nocivos, e de outro, o respeito à liberdade de expressão e à privacidade. Dessa forma, a Lei Geral de Proteção de Dados (LGPD) atribui rigorosas obrigações de transparência e de consentimento e retrata, em tópicos específicos, sobre a forma especial como os dados de crianças e adolescentes devem ser tratados.

Nesse cenário, a proteção de crianças e adolescentes, no contexto virtual, deve ocorrer de forma mais cautelosa, tendo em vista os riscos e danos oriundos do ambiente digital, principalmente frente aos avanços tecnológicos e à dificuldade de controlá-los. A crescente oferta de conteúdos ao público infantil, muitas vezes de forma gratuita e sem filtros, abre a reflexão para o tema em questão, de grande relevância social. Trata-se de um problema de todos, o qual precisa ser analisado em um âmbito geral e por variadas fontes. Dessa forma, o tema ganha relevância, também, diante dos benefícios oriundos do uso das plataformas digitais, envolvendo o acesso a informações e notícias, ambiente de pesquisas e de interação, além de potencializar o desenvolvimento econômico e promover o bem-estar. De acordo com dados do CNJ, no Brasil cerca de 93% das crianças e adolescentes, entre 9 e 17 anos, fazem uso constante da internet. As tecnologias de informação e de comunicação ganharam ainda mais relevância no contexto da Pandemia do Covid-19, o que ratificou a importância do acesso digital no cotidiano da população, com destaque para o dia a dia das crianças e jovens.

A moderação de conteúdo nas redes sociais trata-se do processo de filtrar, aprovar, revisar ou até mesmo remover comentários, imagens, publicações e outros tipos de conteúdo em plataformas digitais. Isso ocorre, pois, as mídias digitais não são espaços neutros, em que se pode publicar ou consumir qualquer conteúdo sem filtros. Pelo contrário, existem regras privadas de "moderação de conteúdos", definindo o que será ou não publicado e consumido. Tal moderação ocorre para que aquilo que for compartilhado esteja em consonância com regras legais, políticas internas e padrões éticos de conduta. Esta moderação pode se dar de forma

automática, por meio de algoritmos e inteligência artificial que detectam palavras-chave e termos naturalmente impróprios ou suspeitos, ou de modo manual, por moderadores humanos em que se utiliza a capacidade humana e subjetiva de avaliar casos mais complexos, tais como discursos de ódio ou bullying.

Tal monitoramento de conteúdo se faz indispensável para a proteção dos usuários vulneráveis, os quais são mais suscetíveis a estarem expostos a conteúdos perigosos, tais como violência, cyberbullying ou exploração sexual. Dessa forma, a moderação do conteúdo atua em conformidade com o cumprimento da lei, em que muitas legislações exigem que as plataformas excluam conteúdos ilegais, como aqueles associados ao discurso de ódio e ao abuso infantil, por exemplo. Ademais, esta supervisão dos conteúdos ocorre como uma forma de preservar a reputação das plataformas, já que os cenários com pouco ou nenhum controle podem perder usuários, por se tornarem hostis. Por fim, tem-se a importância da moderação dos conteúdos digitais para a segurança e a saúde mental, pois os conteúdos sensíveis, se não filtrados, podem afetar psicologicamente os usuários, aumentando os casos de ansiedade e de assédio, entre outros problemas que podem surgir.

Um ponto importante a ser refletido é a questão do conflito entre a moderação e a privacidade. Isso se dá, pois, a moderação exige, muitas vezes, a análise de dados pessoais para se identificar possíveis riscos, e a coleta de informações sensíveis pode entrar em conflito com os termos da LGPD e os princípios da privacidade, o que gera o seguinte dilema ético: até que ponto o monitoramento para proteção invade a privacidade dos usuários? Tal questão precisa ser debatida, diante da sua relevância no contexto virtual e social. Sabe-se que, para que os moderadores atuem, de forma automática ou manual, precisa-se do acesso às mensagens, fotos e históricos de atividades para detectar os conteúdos tidos como impróprios. Por conseguinte, isso requer o acesso à informações pessoais dos usuários, e as informações sensíveis, de menores, podem ser expostas, aumentando-se o risco de vazamento de dados.

Tal análise também abre a reflexão sobre o impacto gerado na experiência do usuário, os quais, incluindo crianças e jovens, podem se sentir monitorados ou até mesmo censurados, ainda que o objetivo seja a segurança virtual. Exige-se, portanto, uma transparência e medidas de segurança que mitiguem o acesso às informações

sensíveis, da mesma forma que se deve priorizar o acesso a dados de modo que garantam a privacidade e não comprometam a liberdade de uso das plataformas pelos usuários. Uma possível alternativa a ser adotada é a anonimização de dados – processo técnico em que se remove ou modifica informações, com o intuito de que os dados não possam ser associados a um indivíduo específico. Tal processo possui como vantagens a redução dos riscos de privacidade, ao proteger os titulares dos dados contra vazamentos e acessos indevidos, diminuindo a exposição. Outra medida possível seria o uso de filtros específicos para menores, em que esteja presente o consentimento parental, de modo a evitar o acesso a conteúdos prejudiciais, sem a necessidade de violar a privacidade.

Somado a isso, é válido discutir os limites entre a proteção, pela moderação dos conteúdos, e a liberdade de expressão- direito fundamental assegurado pela Constituição Federal. É nítido que a proteção dos menores deve ser a prioridade, de forma a evitar que eles sejam expostos a conteúdos sensíveis, os quais podem causar traumas psicológicos futuros. Observa-se, entretanto, que o direito fundamental à liberdade de expressão se torna ameaçado, na medida em que a moderação de conteúdos de maneira excessiva ou a partir de algoritmos muito restitutivo pode gerar, por exemplo, censuras de conteúdos educativos, de atividades artísticas ou de assuntos saudáveis e importantes para o desenvolvimento de crianças e jovens. A censura excessiva se faz um entrave, pois esta é proibida pela Constituição Cidadã. O artigo 220 estabelece que "A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição" e seu parágrafo segundo a forma que é vedada toda e qualquer censura de natureza política, ideológica e artística".

Desse modo, também há o problema da moderação automática, a qual nem sempre é capaz de interpretar contextos culturais, de humor ou ironia, podendo bloquear conteúdos inofensivos e muitas vezes necessários ao público infantil. O desafio se torna constituir políticas que sejam capazes de proteger crianças e adolescentes, sem restringir, de forma incorreta, a liberdade de expressão como um todo. As possíveis soluções envolvem filtros diferenciados para menores, transparência nas regras de moderação e recursos de contestação, para que se possa reavaliar conteúdos removidos. O ECA (Estatuto da Criança e do Adolescente) e a

LGPD fornecem diretrizes sobre proteção, mas não tratam diretamente do limite entre censura e liberdade de expressão. Por isso, as plataformas necessitam equilibrar os direitos constitucionais, implementando políticas responsáveis, mas que também consigam proteger os usuários, principalmente aqueles mais suscetíveis a conteúdos ofensivos e prejudiciais.

A big tech alterou, recentemente, suas políticas de moderação de conteúdo, colocando fim aos filtros que coibiam falas odiosas e finalizando o programa de checagem de fatos. As novas diretrizes passaram a valer nos Estados Unidos e podem ser adotadas também no Brasil, despertando a preocupação de pais e responsáveis e de organizações defensoras dos direitos das crianças e adolescentes. A pesquisa TIC Kids Online Brasil 2024, do Comitê Gestor da Internet no Brasil, mostrou que 3 a cada 10 crianças e adolescentes brasileiros de até 17 anos que acessam a internet afirmam já ter vivenciado alguma situação ofensiva. Isso reflete a necessidade de se abordar e discutir o assunto de forma crítica e detalhada, diante da sua relevância social.

O novo modelo, de acordo com a Meta, permitirá que os indivíduos se expressem mais, "eliminando restrições sobre alguns assuntos que são parte de discussões em voga na sociedade e focando a moderação de conteúdo em postagens ilegais e violações de alta severidade". Tais alterações na política de moderação da Meta se fazem preocupantes, pois as crianças e jovens são os mais vulneráveis aos discursos de ódio circulantes nas plataformas, tendo os seus reflexos ultrapassados do cenário digital, ato de extrema preocupação. "Se você não coloca nenhum tipo de limite em relação ao discurso de ódio e diz que tudo isso será tratado como uma forma legítima de liberdade de expressão, a tendência é que você favoreça esse tipo de conteúdo", analisa o jurista João Coelho, do Programa Criança e Consumo do Instituto Alana.

Com a mudança na plataforma, outro cuidado a ser tomado é a questão da vulnerabilidade de crianças e adolescentes à propagandas de jogos de apostas – as Bets. "A partir do momento em que são desmanteladas as políticas contra o discurso de ódio e as estruturas internas da empresa que lidam com a proteção dos consumidores, terminam também a proteção contra outras violações, inclusive outras

formas de conteúdo que podem ser extremamente prejudiciais para as crianças, que são as propagandas de Bets feitas por influenciadores" aponta Coelho. Dessa forma, as principais plataformas não apenas permitem, mas incentivam a participação de crianças e jovens em jogos de azar, oferecendo bônus e atrativos que chamam a atenção desse público mais vulnerável. O Brasil possui leis que protegem os direitos de crianças e adolescentes e que se estendem ao ambiente digital, como o Estatuto da Criança e do Adolescente (ECA), de 1990. Entretanto, ainda não existe uma legislação específica sobre as obrigações das empresas controladoras de plataformas digitais e como essa governança deve ser estruturada.

Nesse contexto, a proteção de dados pessoais de crianças e adolescentes é um dos grandes desafios do ambiente digital contemporâneo. No Brasil, esse tema encontra respaldo em um conjunto de normas jurídicas que visam garantir a privacidade, a dignidade e a segurança de usuários em situação de vulnerabilidade, com destaque para a Lei Geral de Proteção de Dados Pessoais (LGPD) e o Estatuto da Criança e do Adolescente (ECA). Tais legislações estabelecem os limites e deveres das plataformas digitais, dos responsáveis legais no tratamento de informações pessoais de menores e do Estado. O artigo 14 da LGPD estabelece que "O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente" e deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. Outro ponto essencial é o princípio da minimização de dados, que impõe que apenas informações estritamente necessárias sejam coletadas, evitando o rastreamento desnecessário ou o uso comercial indevido.

Assim, a LGPD busca equilibrar o avanço tecnológico com a proteção integral da infância e da adolescência, conforme previsto na Constituição Federal. Já o ECA (Lei nº 8.069/1990) é a base da proteção jurídica da infância e adolescência no Brasil. Embora criado antes da era digital, seus princípios continuam fundamentais na interpretação das normas contemporâneas de proteção de dados. O Estatuto reconhece a criança e o adolescente como sujeitos de direitos, devendo ser colocados a salvo de qualquer forma de negligência, discriminação, exploração, violência ou opressão (art. 5º).

O ECA também reforça o direito à privacidade e à preservação da imagem, especialmente nos meios de comunicação (art. 17), princípios que se aplicam à exposição em redes sociais e ao uso de dados pessoais. Ambas as leis reforçam a importância da transparência, do consentimento informado e das plataformas e agentes de tratamento de dados, além de enfatizarem o dever do Estado em fiscalizar e promover políticas públicas de proteção digital. Apesar dos avanços, ainda existem dificuldades na efetiva fiscalização e implementação de tais normas, já que, ainda hoje, muitas plataformas atuam com políticas pouco claras e com termos genéricos, dificultando o controle parental e o exercício do direito à informação. Assim, faz-se essencial o fortalecimento de ações educativas e de medidas de orientação e punição de condutas que violem os direitos de crianças e adolescentes no ambiente virtual.

3 A HIPERSEXUALIZAÇÃO E O USO DETURPADO DAS REDES POR MENORES DE IDADE.

A presença massiva de crianças e adolescentes nas redes sociais tem revelado um fenômeno preocupante: a hipersexualização precoce e a adultização digital. Em um ambiente marcado pela busca incessante por visibilidade, engajamento, dinheiro e popularidade, menores de idade passam a reproduzir comportamentos, gestos e linguagens que extrapolam sua maturidade emocional, impulsionados por algoritmos e influenciadores que reforçam padrões estéticos, erotizados e irreais. Essa exposição, além de afetar o desenvolvimento psíquico e a formação identitária, coloca em risco a privacidade, a integridade e a segurança digital desse público, constituindo uma grave violação de direitos.

O vídeo “Adultização”, publicado em agosto de 2025 pelo influenciador Felipe Bressanim Pereira (Felca), deu visibilidade nacional ao tema. Felca denunciou a exploração de menores nas redes sociais, mostrando como determinados influenciadores expunham adolescentes em contextos de conotação sexual, controlavam suas redes sociais, restringiam seu acesso à comunicação e usavam sua imagem para gerar lucro e engajamento. As denúncias provocaram uma onda de repercussão pública, política e jurídica: o número de denúncias sobre conteúdos abusivos envolvendo menores cresceu 114% na ONG SaferNet, e o Ministério

Público da Paraíba (MPPB) intensifica investigações já em curso sobre exploração de menores vinda do influenciador digital Hytalo Santos. Paralelamente, o Congresso Nacional recebeu dezenas de projetos de lei voltados à proteção de crianças e adolescentes no ambiente digital, abordando temas como verificação etária, monetização de conteúdo com menores e responsabilização de plataformas.

Esses fatos expõem uma realidade em que a exposição e a mercantilização da infância se normalizam sob o disfarce de entretenimento, enquanto as plataformas digitais lucram com visualizações, curtidas e compartilhamentos. Tal contexto fere princípios básicos do Estatuto da Criança e do Adolescente (ECA – Lei nº 8.069/90), que, em seu art. 5º, proíbe qualquer forma de negligência, exploração ou violência contra menores, punindo todo atentado aos direitos fundamentais. A adultização e a hipersexualização constituem formas de exploração moral e psicológica, violando ainda o art. 17, que assegura a inviolabilidade da integridade física, psíquica e moral, abrangendo a preservação da imagem, identidade e autonomia. O art. 18 reforça que é dever de todos, Estado, sociedade e família, zelar pela dignidade da criança e do adolescente, pondo-os a salvo de qualquer tratamento vexatório, constrangedor ou desumano.

Em muitos casos, o material publicado nas redes ultrapassa o limite ético e legal, configurando crimes expressamente tipificados no ECA. O art. 240 criminaliza a produção de cenas pornográficas com menores, enquanto os arts. 241- A e 241- B tratam, respectivamente, da divulgação, troca, armazenamento ou distribuição de imagens de teor sexual envolvendo crianças e adolescentes, práticas que ganharam destaque após denúncias sobre o chamado “trade” — comunidades virtuais de pedófilos que trocam conteúdos de abuso infantil. O art. 244 - A, por sua vez, pune quem submete menores à exploração sexual, o que pode incluir situações em que responsáveis permitem ou incentivam a produção de conteúdo sexualizado com seus filhos.

Sob o âmbito penal, o Código Penal complementa essa proteção. O art. 217-A tipifica o estupro de vulnerável, o art. 218 - A criminaliza a satisfação de lascívia mediante a presença de criança ou adolescente, e o art. 218-B prevê punição para o favorecimento da prostituição ou exploração sexual de vulnerável. Ainda que em

muitos casos não haja contato físico direto, a indução de menores a situações de conotação sexual, a manipulação de sua imagem ou o uso de sua exposição para lucro e entretenimento configuram exploração sexual digital, que deve ser combatida com o mesmo rigor jurídico.

Além das implicações penais, essas práticas violam de forma grave a Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente no que se refere ao tratamento de dados de crianças e adolescentes. O art. 14, caput, determina que esse tratamento deve ocorrer em seu melhor interesse, o que evidentemente não ocorre quando a imagem e os dados de menores são utilizados para fins comerciais, sensacionalistas ou sexualizados. O § 1º exige consentimento específico e destacado de ao menos um dos responsáveis legais, mas esse consentimento, quando serve para permitir uma prática abusiva, é juridicamente inválido, pois nenhum responsável pode autorizar algo que fira a dignidade e a integridade do menor. Já o § 3º impõe aos controladores (como plataformas e influenciadores) o dever de manter transparência sobre o tipo de dado coletado, sua utilização e os mecanismos de controle disponíveis, o que raramente é cumprido na prática.

Outro fator agravante é o papel dos algoritmos de recomendação, que, movidos pela lógica do engajamento, frequentemente amplificam a exposição de menores, inclusive direcionando conteúdos sexualizados para públicos predatórios. Essa opacidade algorítmica representa uma violação direta aos princípios da finalidade, necessidade e segurança previstos na LGPD, pois dados sensíveis como imagem, voz e comportamento digital são processados e distribuídos sem controle ou justificativa legítima. O resultado é a criação de ambientes digitais permissivos à exploração, em que o lucro e o engajamento se sobrepõem ao dever de proteger a infância.

É importante ressaltar que muitos adolescentes também passam a reproduzir comportamentos nocivos, incentivados por essa lógica. O uso deturpado das redes, sem discernimento crítico, faz com que alguns se tornem vítimas e agentes involuntários de práticas de exposição, desafios perigosos, discursos de ódio e compartilhamento de conteúdo íntimo. Esse ciclo reforça a necessidade de aplicar os princípios da proteção integral e do melhor interesse do menor, previstos tanto no

ECA quanto na LGPD, e de responsabilizar as plataformas por omissão ou negligência no dever de moderação e segurança.

A partir do caso Felca, o debate sobre hipersexualização e adultização digital transcendeu o campo moral e ganhou o caráter de urgência jurídica e social. As ameaças sofridas por Felca após a denúncia evidenciam a resistência de parte da sociedade em reconhecer o problema, mas também demonstram a importância do papel social dos influenciadores quando agem com responsabilidade e consciência ética.

Portanto, a questão não se restringe à moralidade dos conteúdos, mas à proteção dos direitos fundamentais da criança e do adolescente, expressos em múltiplos diplomas legais. A violação da LGPD nesses casos reflete não apenas o descumprimento técnico da norma, mas a negação do direito à infância, à dignidade e à segurança digital. É dever do Estado, das plataformas, das famílias e da sociedade civil zelar pela integridade desse público vulnerável, prevenindo que dados pessoais e imagens sejam utilizados como mercadoria e que a infância continue sendo explorada em troca de audiência e lucro.

Assim, discutir a hipersexualização e o uso deturpado das redes é discutir a própria efetividade das garantias legais que protegem a infância. O enfrentamento desse problema exige políticas públicas, regulação tecnológica, fiscalização e educação digital para que as crianças e adolescentes possam existir online sem que sua inocência, sua privacidade e seus dados sejam transformados em instrumentos de consumo. Garantir isso é reafirmar o compromisso ético e jurídico de que dados não são mercadoria e a infância não é entretenimento.

4 A RESPONSABILIDADE CIVIL NO ÂMBITO DA INTERNET E COMO MEIO DE PROTEÇÃO DOS DADOS PESSOAIS

Tendo em vista o elevado desenvolvimento tecnológico com o decorrer dos anos, e o seu uso tornando-se mais corriqueiro, mais costumeiro no meio social, as redes sociais e outras plataformas digitais começaram a fazer parte do cotidiano das pessoas, do mesmo modo com que isso facilitou as atividades econômicas,

educativas, trabalhistas, também surgiram acontecimentos de crimes, abusos, violação de direitos, o aumento da propagação de conteúdos pornográficos envolvendo crianças e adolescentes, violação e vazamento de dados pessoais e também sua adultização e hipersexualização, como já foi mencionado no tópico anterior. E justamente em razão de tais acontecimentos que foram surgindo leis e normas para cuidar dos seus usuários e sancionar aqueles que a usarem de forma deturpada e ilegal.

A responsabilidade civil na internet existe para atuar como uma maneira de assegurar que os sujeitos que utilizarem a internet, redes sociais, sites de forma indevida, de uma forma que prejudique seus usuários sejam responsabilizados por suas ações dentro do âmbito digital, dentro da internet, ou seja, se alguém publicar algo ofensivo ou compartilhar algo que propague a prática de crimes, abusos, seja ele contra menores, mulheres, idosos, pedofilia ou incite de alguma forma essas práticas, ou propague sites, jogos, conteúdos que são proibidos no país ou até mesmo se algum dado pessoal ou alguma informação pessoal de alguém vazar na internet, ele será responsabilizado por tais ações de acordo com as normas, com as leis estabelecidas na justiça brasileira.

Para que os dados pessoais fossem protegidos dentro da internet foi criada a Lei Geral de Proteção de Dados (LGPD) que está em vigor desde 2020. Essa lei estabeleceu normas para o uso e compartilhamento de dados pessoais, justamente para evitar que essas informações pessoais fossem violadas, vazadas ou usadas para fins ilegais ou que pudessem de alguma forma trazer prejuízo, seja ele material ou não, para o indivíduo aos quais pertencem esses dados, essas informações. É importante salientar, que isso inclui também as redes sociais.

Quando falamos de responsabilidade civil no âmbito da internet falamos também da responsabilidade que a sociedade como um todo deve ter ao utilizar a internet, as redes sociais, ao terem acessos a dados pessoais como por exemplo algo relacionado à saúde ou relacionado a questões bancárias, salariais. A Lei do Marco Civil da Internet foi criada justamente com o intuito de estabelecer normas e punições para aqueles que usam de forma indevida a internet, mas também para proteger os seus usuários e seus fornecedores. Isso não tira a responsabilidade da

sociedade de denunciar caso veja algo que seja ilegal ou que estejam violando, ameaçando algum direito, pelo contrário, isso faz com que mais pessoas fiquem atentas quanto as suas práticas dentro da internet ou dentro de suas redes sociais, e ajuda até mesmo a evitar a prática de crimes como a pedofilia, o vazamento de dados pessoais. A LGPD veio para contribuir de forma significativa na proteção dos usuários e dos seus dados, com seu estabelecimento o direito à privacidade foi bastante lembrado dentro da internet, o vazamento de dados obteve um certo controle e hoje podemos ter uma segurança sobre o que iremos ver, o que iremos colocar e como isso irá se propagar dentro do âmbito digital.

5 COMO O USO DESENFREADO DAS REDES PODE INIBIR O CRESCIMENTO SAUDÁVEL E MADURO DE UMA CRIANÇA

A infância é uma fase no qual a criança descobre o mundo e a si mesma, é o tempo no qual sua visão de mundo é mais colorida, sensível e risonha, bem como a busca do seu desenvolvimento cognitivo, social e emocional. Dessa forma, falar de infância é falar de inocência e proteção. No contexto atual, a infância tem se escondido atrás das plataformas digitais, que estão gerando maior entretenimento e distração nas crianças, impactando negativamente na criatividade, aprendizagem e maturação dessa idade.

Nesse mesmo viés, é importante pontuar que o foco não é acabar com a interação digital, mas dar ênfase ao descontrole, que se torna o fator limitante e disfuncional para a criança, que acaba passando muito tempo na frente das telas, podendo desenvolver déficits em sua vida comum e no aprendizado e aqui, a qualidade e quantidade caminham juntas. Segundo a Fundação Abrinq, no seu artigo que trata sobre crianças e telas, ‘’a qualidade do conteúdo é tão importante quanto a quantidade de tempo que a criança passa em frente a uma tela’’, nesse sentido, não somente importa as horas ou minutos que passam nas telas, mas o que está sendo absorvido e gerando influência (positiva ou negativa) para as mesmas, que ainda não sabem discernir e separar o conteúdo edificante de um conteúdo prejudicial. Portanto, é necessário que haja uma regulamentação e vigilância por parte dos

responsáveis e educadores, protegendo seus pequenos de qualquer tipo de conteúdo danoso; é crucial, também, que os responsáveis não venham a utilizar a internet como forma de distrair a criança e acabar gerando vícios desnecessários e incomuns, os meios digitais não foram feitos para ser um escape, mas um meio de entretenimento temporário, não rotineiro.

Diante de todo o exposto, fica o questionamento: qual o impacto do uso dos dispositivos eletrônicos na saúde física e emocional das crianças? Como já fora discutido, o uso excessivo de telas acaba prejudicando o desenvolvimento cognitivo e social da criança, fazendo com que o tempo disponível e o lazer se reduzam à interação digital, afetando na sua criatividade e inibindo os tipos de brincadeiras que somente uma criança é capaz de produzir. Não obstante, o crescimento maduro também é afetado, não sendo alcançado de maneira completa e consciente, tendo em vista que o crescimento de uma criança se dá por suas experiências sensoriais, a exploração de atividades dinâmicas que busquem exercer o raciocínio lógico, a maneira de pensar por si mesma e por fim, ter a chance de demonstrar seu comportamento em face à outras crianças, instigando o senso de coletividade e humanização. Segundo uma pesquisa realizada pelo TIC Kids Online Brasil, 93% da população entre 09 e 17 anos usa internet no país, o que equivale a 25 milhões de crianças e adolescentes e aproximadamente 23% desse público alegam ter acessado à internet pela primeira vez aos 06 anos de idade - tão somente é um risco e números que só tendem a aumentar, caso não haja um ponto de equilíbrio entre tempo, entretenimento e a vida prática. Portanto, estimulá-las a ter uma rotina e vida fora das telas é o primeiro passo para uma liberdade a longo prazo, pois será de muito mais proveito investir tempo e energia na proteção e inteligência dos pequenos, garantindo uma educação digital e equilibrada, do que permitir que o fiquem em constante tédio e ociosos.

Por fim, essa educação digital não se limita somente ao público infantil e jovem, mas também aos responsáveis, para que tenham consciência do impacto das redes dentro dos lares e na área educacional, que é demasiadamente afetada nos desafios de ensino, buscando alternativas e meios de entreter os alunos com a mínima de interação digital possível. Ademais, a imposição de limites às plataformas digitais é uma segurança jurídica e social, evitando, portanto, ameaças diretas e

significativas ao seu desenvolvimento integral e garantindo o suporte e políticas necessárias para que nenhuma criança seja alvo de um crescimento imaturo e danoso. Garantir a proteção integral e em todos os meios é um dever social, jurídico e familiar.

6 COMO O MARCO CIVIL DA INTERNET FOI UM AVANÇO NO ÂMBITO DE DIREITO CIVIS, MAS SE FEZ TÃO OMISSO NO QUESITO DA REGULAÇÃO DO USO DA INTERNET.

O Marco Civil da Internet (MCI), promulgado pela Lei n.º 12.965/2014, é reconhecido internacionalmente como um avanço significativo, mas carrega consigo um paradoxo notável: enquanto estabeleceu princípios fundamentais no âmbito dos direitos civis, revelou-se omisso e restritivo quanto à regulação da responsabilidade dos provedores, especialmente na moderação de conteúdo ilícito.

V.I O Marco Civil como Avanço nos Direitos Civis

O MCI foi considerado um grande marco na proteção de direitos civis dos usuários de internet. O Projeto de Lei que o originou visava estabelecer a base para a regulamentação de temas sensíveis no ciberespaço, como a proteção de dados, o comércio eletrônico e a tipificação de cibercrimes.

A legislação estabelece princípios, garantias, direitos e deveres essenciais para o uso da Internet no Brasil, baseados em valores como a liberdade, a privacidade e a neutralidade da rede. Seu objetivo era garantir segurança jurídica quanto às decisões sobre remoção de conteúdo, evitar a censura preventiva e assegurar o máximo grau de proteção ao direito à liberdade de expressão. Contudo, este avanço nos direitos fundamentais veio acompanhado de críticas relativas à sua efetividade regulatória, especialmente no tocante à esfera penal e à responsabilidade dos intermediários.

V.II A Omissão na Regulação da Internet e o Âmbito Penal

A principal problemática do Marco Civil reside em sua omissão na regulação da internet no âmbito penal. O Poder Legislativo tem se esquivado da

responsabilidade de regulamentar o uso da internet no campo penal para combater práticas lesivas perpetradas por meios digitais. Essa insuficiência legislativa transfere ao Poder Judiciário a tarefa de realizar manobras interpretativas para enquadrar condutas praticadas no ciberespaço em tipos penais comuns.

O MCI foi um projeto que, em sua formulação final, criou barreiras para a remoção de conteúdos nocivos que circulam no ciberespaço. Em vez de atuar como um regulamento que acompanha a evolução tecnológica e a diversidade de eventos danosos, o MCI resultou em um modelo que tende a ruir.

V.III A Responsabilidade Civil

A omissão regulatória do MCI manifesta-se de forma mais aguda no regime de responsabilidade civil dos provedores de aplicações (como redes sociais e websites) por danos decorrentes de conteúdo gerado por terceiros. Com o propósito de "assegurar a liberdade de expressão e impedir a censura", o Artigo 19 do MCI condicionou a responsabilização civil dos provedores de aplicações ao descumprimento de uma ordem judicial específica para tornar o conteúdo infringente indisponível.

A redação literal deste dispositivo sugeriu a existência de uma ampla isenção em relação a quaisquer deveres de cuidado por parte do provedor. Para muitos especialistas, essa regra criou um regime próximo da irresponsabilidade das plataformas digitais pelos danos decorrentes do conteúdo gerado por terceiros, servindo como uma "blindagem da responsabilidade".

V.IV O Contraste com a Jurisprudência Anterior

Este regime de "aviso judicial e remoção" (judicial notice and takedown) representou um flagrante retrocesso em comparação com a jurisprudência brasileira anterior ao MCI. Antes da Lei n.º 12.965/2014, os tribunais brasileiros tendiam a adotar a tese de responsabilidade condicionada à inércia da plataforma na remoção do conteúdo ilícito após a simples notificação do usuário. Ao exigir a ordem judicial para a remoção, o MCI tornou ainda mais estritas as hipóteses de responsabilização e tutela da vítima.

Além disso, o regime estabelecido pelo Artigo 19 é de responsabilidade ex post (após o dano), que visa impedir a sua propagação, mas não a ocorrência. Isso impõe à vítima o ônus de recorrer ao Judiciário, tornando-se uma formalidade morosa e custosa que pode agravar o dano, enquanto as plataformas permanecem inertes.

V.V O Ambiente Digital Atualmente e o Dever de Cuidado

O Artigo 19 parte de uma premissa que se tornou anacrônica: a de que as plataformas figuram como meras intermediárias passivas no fluxo informacional. No ambiente digital atual, as plataformas digitais não são espaços neutros. Elas exercem grande protagonismo e controle sobre a difusão dos conteúdos. Utilizam algoritmos sofisticados para definir qual conteúdo será direcionado aos usuários, o que é a razão do seu modelo de negócios e a fonte de seus lucros. Diante dessa realidade, a doutrina e a jurisprudência mais recentes têm imposto uma interpretação sistemática e finalística do MCI, em conjunto com o Código Civil, o Código de Defesa do Consumidor (CDC) e o Estatuto da Criança e do Adolescente (ECA), para reconhecer o dever geral de cuidado (dever de cuidado) das plataformas.

A ausência de normas claras no âmbito penal, aliada à rigidez do Artigo 19, beneficia aqueles que detêm maior poder econômico e domínio técnico, em detrimento dos usuários. O Supremo Tribunal Federal (STF) discute a constitucionalidade do Artigo 19 (RE 1.037.396 e 1.057.258). Argumenta-se que condicionar a reparação do dano à ordem judicial específica afronta a garantia constitucional de reparação plena e integral por danos à honra, privacidade e imagem.

Ministros do STF sugerem que, enquanto o Artigo 19 possa ser mantido para ilícitos subjetivos (como crimes contra a honra, onde a ilicitude não é clara), deve-se adotar um regime de moderação de conteúdo pautado no dever de cuidado, exigindo que as plataformas atuem ativamente na redução de riscos sistêmicos e na mitigação da exposição dos usuários a conteúdos nocivos. O dever de cuidado, inclusive, deve incidir sobre o próprio design da plataforma, a fim de prevenir danos.

Nesse viés, embora o Marco Civil da Internet tenha sido um avanço crucial na formulação de direitos e garantias digitais, seu engessamento na regulação,

especialmente através do Artigo 19, gerou o efeito indesejável de dificultar a tutela dos direitos fundamentais dos usuários, exigindo uma modernização legislativa que atribua maior responsabilidade aos provedores pelo controle de conteúdo que circula na rede mundial de computadores.

De maneira análoga, ao tratar sobre o MCI, se faz relevante também discorrer sobre a “Lei das Bets”. A relação entre o Marco Civil da Internet (MCI) (Lei n.º 12.965/2014) e a Lei das Bets (Lei n.º 14.790/2023), no atual cenário digital, reside principalmente em um paradoxo regulatório comum: a dificuldade do ordenamento jurídico brasileiro em acompanhar a dinâmica da internet e impor efetiva responsabilidade às grandes plataformas frente aos riscos sistêmicos e sociais gerados por atividades digitais.

O MCI trata da fundação dos direitos civis e da responsabilidade dos intermediários (provedores de aplicação) no ciberespaço, enquanto a Lei das Bets regula uma atividade econômica específica – as apostas de quota fixa – que se tornou massiva e geradora de graves externalidades sociais através da internet. O Marco Civil da Internet foi um esforço para estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Contudo, o regime de responsabilidade civil que instituiu para os provedores de aplicações (como redes sociais) é amplamente criticado por ser um "flagrante retrocesso" e uma "blindagem da responsabilidade" em relação a danos decorrentes de conteúdo gerado por terceiros.

Como fora supracitado, a chave desse regime é o Artigo 19, que condiciona a responsabilização civil do provedor ao descumprimento de uma ordem judicial específica para tornar o conteúdo indisponível. Esse mecanismo, conhecido como judicial notice and takedown, impede a censura prévia, mas impõe à vítima uma formalidade morosa e custosa, incompatível com a rápida difusão de conteúdo ofensivo no mundo virtual.

A premissa do MCI de que as plataformas são meras intermediárias passivas no fluxo informacional é vista como anacrônica. Na realidade, essas plataformas são gatekeepers que utilizam algoritmos para fazer a curadoria e gerenciamento de informações, definindo que conteúdos serão direcionados aos usuários e obtendo lucros com essa atividade. Essa ausência de normas claras no âmbito penal e a

rigidez do Artigo 19 beneficiam quem detém maior poder econômico e domínio técnico.

A Lei n.º 14.790/2023 surgiu em resposta ao crescimento exponencial das casas de apostas online (BETs). Esta atividade, que não se confunde com a contravenção penal de exploração de jogos de azar (art. 50, §2°, da Lei n.º 3.688/41), movimentou valores altíssimos e gerou preocupações sociais e econômicas.

A principal preocupação social em relação às "bets" reside no seu impacto no vício patológico em apostas e no comprometimento da renda das famílias, especialmente as mais pobres. Além disso, a circulação de dinheiro em um mercado inicialmente desregulado favoreceu a prática de crimes financeiros, como sonegação e lavagem de dinheiro. Embora a nova legislação traga regras sobre tributação, licença e fiscalização, ela é criticada por ser "muito frouxa", focando mais nos interesses dos empresários do que em gerar um ambiente seguro para a população. Dessa forma, a lei possui externalidades não abordadas pelo MCI.

A conexão crucial entre o MCI e a Lei das Bets, no cenário digital atual, reside na forma como a atividade de apostas é promovida e disseminada pelas plataformas, expondo as falhas regulatórias do Marco Civil:

- mercado das apostas (bets) depende da infraestrutura e do modelo de negócios das plataformas digitais para a sua divulgação, que, segundo as fontes, é a principal preocupação do país em relação a essa atividade. As plataformas operam na "economia da atenção", na qual a atenção dos usuários é um bem disputado e a base para a coleta massiva de dados e publicidade direcionada. O uso de algoritmos personalizados para filtrar conteúdo conforme os hábitos e preferências dos usuários é um motor poderoso para a veiculação de anúncios de apostas, potencialmente agravando o vício e o endividamento.
- MCI, em seu artigo 19, restringiu a responsabilidade civil das plataformas a danos decorrentes de conteúdo gerado por terceiros. No entanto, o problema da publicidade e do risco sistêmico gerado pela Lei das Bets não se limita ao conteúdo de terceiros. Danos decorrentes

> da publicidade abusiva ou direcionada (uma externalidade econômica da plataforma) não têm relação direta com o conteúdo postado pelos usuários, mas sim com a conduta da própria plataforma e seus contratos com anunciantes. Nesses casos (que podem incluir a promoção de apostas), os Artigos 19 e 21 do MCI não se aplicam. Portanto, o MCI, ao focar estritamente na responsabilidade por conteúdo de terceiros (e torná-la dependente de ordem judicial), deixou lacunas em relação à responsabilidade das plataformas por outros tipos de danos inerentes ao seu modelo de negócio, como a promoção agressiva de atividades legalizadas, mas socialmente danosas. A discussão atual no Supremo Tribunal Federal (STF) sobre a constitucionalidade do Artigo 19 (REs 1.037.396 e 1.057.258) e o debate sobre o dever geral de cuidado (design de plataformas) buscam exatamente corrigir a insuficiência do MCI.

Ante o exposto, a relação entre o MCI e a Lei das Bets é que o MCI forneceu o arcabouço digital permissivo (com baixa responsabilidade do provedor por danos de conteúdo) que, no cenário da Lei das Bets, permite a proliferação e amplificação de danos sociais (vício e endividamento) por meio da publicidade agressiva e algorítmica, reforçando a urgência de uma legislação digital mais clara e impositiva que não sirva como "blindagem" e que obrigue as plataformas a mitigar riscos sistêmicos, para além do mero conteúdo de terceiros.

6 O DEVER GERAL DE CUIDADO NAS PLATAFORMAS DIGITAIS

O dever geral de cuidado das plataformas digitais é um princípio interpretativo e obrigacional que tem sido cada vez mais exigido pela doutrina e pela jurisprudência para determinar a responsabilidade e as ações esperadas dos provedores de aplicações de internet (como redes sociais e sites) devendo ser interpretado de forma sistemática com o ordenamento jurídico brasileiro.

Esse conceito surge em grande parte para confrontar a interpretação literal do Artigo 19 do Marco Civil da Internet (MCI), que condiciona a responsabilização

civil das plataformas por conteúdo de terceiros ao descumprimento de uma ordem judicial específica. O dever de cuidado, por sua vez, exige uma conduta mais ativa e preventiva dessas empresas, baseada em diversos fundamentos legais e constitucionais.

1. Boa-fé Objetiva: No direito brasileiro, o dever geral de cuidado é um dever anexo que decorre da boa-fé objetiva (Art. 422 do Código Civil), que impõe às partes de uma relação contratual (incluindo a relação entre plataformas e usuários) a adoção de comportamento compatível com a lealdade e a confiança recíprocas. O objetivo desses deveres de proteção é que os contratantes não causem danos uns aos outros ou a seus patrimônios.

2. Relação de Consumo: A relação entre plataformas e usuários é amplamente considerada uma relação de consumo. O Código de Defesa do Consumidor (CDC) impõe ao fornecedor o dever de observância do cuidado, exigindo a segurança e a prevenção de danos ao consumidor (Art. 6º, VI, e Art. 8º).

3. Prevenção de Danos Injustos: O dever de cuidado impõe às plataformas a obrigação de adotar medidas de proteção para prevenir danos injustos aos seus usuários, mesmo quando os danos decorrem de conteúdos gerados por terceiros, seguindo um parâmetro de razoabilidade.

O dever de cuidado não pode ser definido em abstrato, mas deve ser densificado (detalhado) a partir de critérios como a previsibilidade do risco e a gravidade do dano. A interpretação mais ampla do dever de cuidado busca afastar a "blindagem da responsabilidade" proporcionada pelo Artigo 19 do MCI.

- **Rompimento com a Inércia:** A plataforma digital não pode alegar que está impedida de exercer controle de conteúdo sob pena de violação à liberdade de expressão. As plataformas já realizam a curadoria e moderação de conteúdo e, ao impulsionar e controlar a difusão de conteúdo, tornam-se responsáveis pela propagação do dano.
- **Ações Ativas (Mitigação de Riscos Sistêmicos):** O dever de cuidado exige que as plataformas atuem ativamente na redução de riscos sistêmicos de exposição dos usuários a conteúdos nocivos.

- **Conteúdos Flagrantemente Ilícitos:** Em casos de ilicitude flagrante (como pornografia infantil ou racismo), defende-se que a plataforma teria o dever de remover o conteúdo, independentemente de notificação judicial ou extrajudicial, e a inércia pode caracterizar culpa.

- **Reinserção de Conteúdos:** A inércia da plataforma em criar mecanismos de filtro ou bloqueio para conteúdos que já foram reconhecidos como ilícitos (e que são reinseridos) caracteriza falta do dever de cuidado.

Uma abordagem mais moderna do dever de cuidado estende-se para além do mero controle de conteúdos, focando na própria arquitetura da plataforma.

- **Design Algorítmico:** O dever de cuidado deve incidir sobre o design do código algorítmico, incentivando os agentes econômicos a evitar a criação de riscos desarrazoados. As plataformas utilizam algoritmos para fazer a curadoria automática de informações, e esses mesmos mecanismos, que hoje promovem lucros, devem ser usados para proteger os usuários e evitar a propagação de ilícitos.

- **Prevenção de Danos:** O dever de cuidado deve ser preventivo, exigindo das plataformas uma conduta ativa para evitar danos injustos.

- **Transparência:** O dever de cuidado está intrinsecamente ligado à necessidade de transparência na forma como as plataformas gerenciam os fluxos informacionais e na forma como exercem a curadoria e remoção de conteúdo.

e na forma como exercem a curadoria e remoção de conteúdo.

O dever de cuidado é mais rigoroso e exigente quando se trata da proteção de crianças e adolescentes, em razão da tutela especial e prioritária assegurada a esses sujeitos de direito pela Constituição Federal (Art. 227) e pelo Estatuto da Criança e do Adolescente (ECA).

- **Melhor interesse:** A interpretação de todas as leis, incluindo o MCI, deve ser compatível com os princípios constitucionais e legais que impõem a ampla proteção desse grupo hipervulnerável. Na dúvida, deve ser tomada a medida mais compatível com a necessidade de prevenir danos.

- **Publicidade e LGPD:** O dever de cuidado aplica-se a danos que não decorrem de conteúdo de terceiros, como a coleta e tratamento de dados pessoais (Lei Geral de Proteção de Dados - LGPD) e a publicidade abusiva ou direcionada. A LGPD impôs tratamento diferenciado e mais rigoroso aos dados de crianças, exigindo, por exemplo, que a coleta e tratamento se deem sempre no melhor interesse da criança e do adolescente.

- **Design Razoável:** É fundamental que o design do sistema possibilite a identificação das crianças e adolescentes para operacionalizar medidas de prevenção de danos.

O dever geral de cuidado das plataformas digitais representa uma tentativa de atualizar o regime de responsabilidade do MCI, exigindo que as grandes empresas digitais, que lucram com a gestão do fluxo informacional, assumam responsabilidades proporcionais ao seu poder e ajam de forma diligente, proativa e transparente para proteger seus usuários de danos.

7 CONSIDERAÇÕES FINAIS

O artigo em questão foi decisivo ao analisar a intersecção entre Direito e Tecnologia no Brasil, com ênfase nos desafios em conciliar o desenvolvimento tecnológico com a proteção dos direitos fundamentais, especialmente no que tange à responsabilidade das plataformas digitais e a necessidade do dever de cuidado. Nesse sentido, conforme mencionado, o Marco Civil da internet (MCI), embora crucial ao estabelecer princípios e garantias, gerou intensa controvérsia em seu regime de responsabilização por danos decorrentes de conteúdos gerados por

terceiros, conforme o artigo 19 do MCI, que condiciona a remoção à prévia ordem judicial específica.

Diante da premissa de que as plataformas digitais seriam "meras intermediárias passivas", o artigo demonstrou que estes agentes exercem protagonismo e controle sobre o fluxo informacional por meios dos algoritmos. Tal realidade impõe a interpretação do Marco Civil da Internet em consonância com o ordenamento jurídico brasileiro, para sustentar a exigência do dever de cuidado – duty of care. Este dever exige que as plataformas atuem de forma ativa e preventiva na mitigação de riscos e na propagação de ilícitos. A necessidade desse cuidado se faz ainda mais decisiva na proteção de crianças e adolescentes, público hiper vulnerável, cuja proteção se faz prioritária.

O artigo destacou os desafios em conciliar a moderação de conteúdos com os princípios de privacidade, a partir de uma análise da Lei Geral de Proteção de Dados (LGPD). Foram analisados os riscos específicos, tais como a exposição a discursos de ódio, a propagação de cibercrimes e o uso deturpado das redes sociais para fomentar a hipersexualização e a adultização digital. A moderação deve sempre priorizar o melhor interesse da criança, conforme a LGPD.

Dessa forma, o enfrentamento de tais desafios exige a superação das lacunas regulatórias do artigo 19 do MCI, assim como o fortalecimento da fiscalização e da implementação de políticas responsáveis e transparentes pelas plataformas. Faz-se indispensável que as garantias legais protejam a criança, prevenindo que os dados pessoais e as imagens sejam transformados em mercadoria, e evitando que a inocência seja explorada em troca de audiência e de lucro. Reafirma-se o compromisso ético das plataformas, as quais devem assumir responsabilidades proporcionais ao seu poder, a fim de garantir um cenário digital seguro para todos os usuários.

Ademais, foi analisada a complexa dicotomia entre a moderação de conteúdo e a preservação dos princípios de proteção de dados, privacidade e liberdade de expressão no ambiente digital. O desafio central reside em conciliar a proteção de usuários, principalmente crianças e adolescentes, contra conteúdos nocivos, em respeito às suas liberdades fundamentais. A moderação de conteúdos exige o acesso

a informações pessoais e sensíveis, o que gera dilemas éticos sobre até que ponto o monitoramento invade a privacidade, sobretudo de menores, cujos dados exigem tratamentos diferenciados e mais cautelosos, conforme as diretrizes da LGPD.

Foi constatado, também, que a vulnerabilidade digital de crianças e adolescentes é exacerbada não apenas pela dificuldade em controlar os avanços tecnológicos, mas também pelas omissões regulatórias. Esta insuficiência regulatória amplia desafios, tais como hiperssexualização e a adultização, como já mencionado. O enfrentamento de tais impasses exige uma resposta multifacetada, o que envolve, por exemplo, adaptações legislativas, com atribuição de responsabilidade proporcional aos provedores, bem como a efetiva fiscalização das normas já existentes, como a Lei Geral de Proteção dos Dados e o Marco Civil da Internet. Medidas como a anonimização de dados para mitigar os riscos de privacidade, o uso de filtros diferenciados mediante consentimento parental e a garantia de recursos transparentes contra a censura excessiva são determinantes para garantir um ambiente digital mais seguro e equilibrado.

Por fim, conclui-se que a proteção de dados, a moderação responsável e a exigência do dever de cuidado refletem o compromisso ético e jurídico com a proteção integral da infância e da adolescência. Discutir temas como a hiperssexualização e uso deturpado das redes sociais é debater a própria efetividade das garantias legais que protegem os infantes. Portanto, faz-se imperativo que o Estado, as plataformas, a sociedade e as famílias zelem pela dignidade e pela integridade desse público naturalmente vulnerável, a fim de garantir que, no cenário virtual, a privacidade e os dados não sejam transformados em instrumentos de consumo, e que a infância não seja explorada em troca de audiência e lucro.

REFERÊNCIAS

BRASIL. Código Penal (Decreto-Lei nº 2.848, de 7 de dezembro de 1940). Disponível em: https://www.planalto.gov.br. Acesso em: 17 de Novembro de 2025.

BRASIL. Crianças, adolescentes e telas – Guia sobre uso de dispositivos digitais. Governo Federal do Brasil, [s.d.]. Disponível em: https://fadc.org.br/noticias/criancas-e-telas. Acesso em: 17 de Novembro de 2025.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 17 de Novembro de 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 de Novembro de 2025.

EDUCAÇÃO E TERRITÓRIO. Mudanças na moderação de conteúdo em redes sociais deixam crianças mais vulneráveis. [S.l.], [s.d.]. Disponível em: https://educacaoeterritorio.org.br/reportagens/mudancas-na-moderacao-de-conteudo-em-redes-sociais-deixam-criancas-mais-vulneraveis/. Acesso em: 17 de Novembro de 2025.

FRAZÃO, Ana. *Dever geral de cuidado das plataformas digitais diante de crianças e adolescentes.* Brasília, 2020. Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2021/11/dever-geral-de-cuidado-das-plataformas.pdf Acesso em: 17 de Novembro de 2025.

FRAZÃO, Ana. *Marco Civil da Internet: impactos, evoluções e perspectivas – 10 anos.* Brasília, 2024. Análise jurídica e crítica sobre a década de vigência do Marco Civil da Internet, incluindo avanços, desafios regulatórios e perspectivas futuras. Disponível em: https://bibliotecadigital.stf.jus.br/xmlui/handle/123456789/8055 Acesso em: 17 de Novembro de 2025.

INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR (IDEC). Direitos nas mídias. [S.l.], [s.d.]. Disponível em: https://idec.org.br/direitos-nas-midias. Acesso em: 17 de Novembro de 2025.

MILAGRE, José Antônio; DE JESUS, Damásio. Manual de crimes informáticos. São Paulo: Saraiva, 2016.

SILVA, Marco Civil da Internet: avanço ou retrocesso? Disponível em: https://www.academia.edu/28711449/Marco_Civil_da_Internet_Avan%C3%A7o_ou_Retrocesso. Acesso em: 17 de Novembro de 2025.

TEIXEIRA, Bernardo Spencer da Fontoura. **Liberdade De Expressão E Moderação De Conteúdo Nas Redes Sociais**. 2020. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2020. Disponível em: https://tede2.pucrs.br/tede2/bitstream/tede/11640/2/BERNARDO_SPENCER_DA_FONTOURA_TEIXEIRA_DISS.pdf. Acesso em: 17 de Novembro de 2025.

DEEPFAKE E O DIREITO BRASILEIRO: DESAFIOS CONTEMPORÂNEOS DA MANIPULAÇÃO DIGITAL E DA TRANSFORMAÇÃO TECNOLÓGICA

Maria Fernanda Siebra da Silva[1]
Natália Sousa Maciel[2]
Nicole Lopes Marinho Bandeira[3]

RESUMO

O artigo analisa os desafios jurídicos contemporâneos decorrentes da disseminação de deepfakes, demonstrando como as tecnologias de manipulação digital desestabilizam conceitos tradicionais de prova, autenticidade e confiabilidade no ordenamento jurídico brasileiro. Ao examinar a insuficiência do direito convencional para lidar com conteúdo sintético com potencial risco, o texto evidencia que normas pensadas para falsificações materiais não são suficientes para enfrentar fraudes audiovisuais produzidas por inteligência artificial. A análise também aborda a atuação institucional do STF e do STJ, que, embora ainda não possuam jurisprudência consolidada sobre esse tipo de material, já estabelecem diretrizes relevantes sobre responsabilidade das plataformas, preservação de registros, autenticidade das provas digitais e proteção de direitos fundamentais no ambiente virtual. Além disso, discute-se a necessidade de fortalecer políticas públicas de educação midiática como estratégia essencial para reduzir a vulnerabilidade social à desinformação e ampliar a capacidade cidadã de identificar manipulações audiovisuais. Conclui-se que o enfrentamento dos deepfakes demanda uma abordagem integrada, combinando atualização normativa, aprimoramento pericial, atuação coordenada das instituições e formação crítica da população, a fim de preservar a integridade da informação e assegurar a proteção de direitos na sociedade digital.

Palavras-chave: Deepfake; Manipulação digital; Direito brasileiro; Prova digital. Desinformação; Inteligência artificial; Plataformas digitais; STF; STJ; Educação midiática.

SÚMARIO: Introdução; 2. Liveness: proteção contra deepfakes; 3. Análise comportamental: protegendo com identidade digital; 3.1 Responsabilidade de plataformas e normas globais; 4 Educação sobre mídias e conscientização; 5. A

[1] Discente do curso de Direito do UniCEUB – Centro Universitário de Brasília
[2] Discente do curso de Direito do UniCEUB – Centro Universitário de Brasília
[3] Discente do curso de Direito do UniCEUB – Centro Universitário de Brasília

inadequação do direito convencional; 6. Atuação do STF e do STJ diante dos desafios jurídicos dos deepfakes; Conclusões; Referências.

1 INTRODUÇÃO

O deepfake é uma forma de inteligência artificial (IA) utilizada para criar imagens, sons e vídeos falsos altamente convincentes. O termo resulta da combinação entre deep learning e fake, indicando justamente o uso de aprendizado profundo para produzir conteúdos artificiais que imitam a realidade. A tecnologia funciona por meio da compilação de imagens e sons fraudulentos, que são combinados por algoritmos de aprendizado de máquina, gerando pessoas, falas e eventos que não existem ou que nunca ocorreram. Embora possa ser utilizada de maneira recreativa, como em vídeos humorísticos, tem ganhado notoriedade pelo seu uso em práticas nocivas, como a disseminação de desinformação, a manipulação política e a criação de conteúdos pornográficos não consensuais.

A produção desse conteúdo envolve um processo complexo dividido em etapas. Inicialmente, ocorre a coleta de dados, que exige grande quantidade de imagens ou vídeos da pessoa que se pretende "clonar". Quanto maior o volume de dados, maior será o realismo da reprodução. Esses dados são então utilizados no treinamento de uma rede neural, geralmente baseada em Generative Adversarial Networks (GANs), compostas por duas partes, o gerador, responsável por criar o conteúdo sintético, e o discriminador, que tenta identificar se o material apresentado é real ou artificial. Em sucessivas interações, ambos os sistemas se aperfeiçoam, até que o discriminador não consiga mais reconhecer a diferença entre o original e o criado, resultando em deepfakes cada vez mais verossímeis.

Após o treinamento, a rede neural pode gerar novos vídeos ou imagens a partir de um material de referência, manipulando expressões faciais, movimentos labiais e gestos para simular falas ou ações específicas. Esses conteúdos, quando utilizados de forma mal-intencionada, apresentam riscos significativos. Entre eles estão a desinformação, capaz de manipular percepções políticas e sociais; a pornografia não consensual, que utiliza a imagem de indivíduos sem autorização;

fraudes financeiras, como vídeos falsos de CEOs anunciando decisões empresariais; violação de privacidade; além de cyberbullying e difamação.

No Brasil, ainda não existe legislação específica sobre deepfakes, mas alguns dispositivos legais podem ser aplicados ao tema. A Lei Geral de Proteção de Dados (LGPD) protege a privacidade e o uso indevido de dados pessoais; o Marco Civil da Internet (Lei nº 12.965/2014) estabelece direitos e deveres no uso da rede; a Lei Carolina Dieckmann (Lei nº 12.737/2012) tipifica crimes informáticos; e o Código Penal aborda crimes como difamação, calúnia e falsidade ideológica. Além disso, tramitam no Congresso Nacional projetos de lei voltados especificamente à criminalização da manipulação digital por IA, como o PL nº1.272/2023 e o PL nº 5.695/2023.

2 LIVENESS: PROTEÇÃO CONTRA DEEPFAKES

A solução de liveness, também chamada de prova de vida, tem como objetivo garantir que a captura biométrica seja feita a partir de uma pessoa real, e não por meio de fotos, vídeos, gravações ou até máscaras extremamente parecidas com um rosto humano. Com o avanço dos deepfakes, essa verificação se tornou indispensável, já que hoje é possível criar imagens e movimentos muito próximos da realidade.

Esse tipo de tecnologia consegue analisar detalhes que só um rosto humano apresenta, como pequenos movimentos naturais, textura da pele, mudanças de iluminação e até a forma como a imagem reage ao ambiente. Muitas soluções fazem a análise de vários quadros (frames) ao mesmo tempo, o que ajuda a identificar se aquela imagem realmente corresponde a uma pessoa presente no momento da validação.

Além disso, alguns sistemas utilizam o chamado liveness passivo, que não exige que o usuário faça movimentos específicos, deixando o processo mais simples e rápido, sem perder a segurança. Essa abordagem ajuda a identificar fraudes produzidas por inteligência artificial, que normalmente apresentam falhas, como falta de profundidade, bordas distorcidas ou aparência artificial.

A união de diferentes medidas de segurança em uma mesma etapa de validação é essencial para tornar as transações mais seguras, especialmente quando envolvem dados pessoais sensíveis ou operações financeiras. Quando biometria, verificação documental e prova de vida atuam juntas, a detecção de fraude se torna muito mais eficiente do que quando apenas uma dessas técnicas é usada isoladamente.

Outro ponto importante é garantir que o usuário verdadeiro, que age de boa-fé, consiga realizar a validação sem dificuldades. Isso significa pensar em acessibilidade, ambientes com pouca luz e até problemas de conexão, evitando que medidas de segurança acabem prejudicando quem realmente precisa acessar o sistema. Dessa forma, a tecnologia deve equilibrar proteção e facilidade de uso, bloqueando o fraudador, mas permitindo que o usuário legítimo consiga concluir o processo sem complicações.

3 ANÁLISE COMPORTAMENTAL: PROTEGENDO COM IDENTIDADE DIGITAL

A análise comportamental é uma estratégia moderna de prevenção a fraudes que se baseia nos hábitos naturais do usuário ao utilizar seus dispositivos. Cada pessoa tem um jeito próprio de interagir com a tecnologia como segura o celular, como digita, a velocidade dos toques, ou até a forma de mover o cursor. Esses padrões formam uma espécie de identidade digital única, difícil de ser copiada por fraudadores.

Com isso, sistemas de inteligência artificial conseguem perceber quando há um comportamento diferente do normal e identificam possíveis tentativas de fraude. A grande vantagem é que essa verificação acontece de forma contínua e silenciosa, sem exigir ações extras do usuário. Dessa forma, o processo de autenticação fica mais seguro, mas também mais simples, superando métodos tradicionais como senhas, códigos e tokens.

Além da análise do comportamento em si, o monitoramento em tempo real dos fluxos de negócio é fundamental. Os algoritmos avaliam registros, horários de acesso, rotinas e padrões de navegação. Quando percebem algo fora do comum,

geram alertas automáticos para que medidas preventivas sejam tomadas imediatamente. Assim, muitas fraudes podem ser barradas antes mesmo de causar prejuízos.

Essa abordagem preventiva fortalece a proteção tanto das instituições quanto dos usuários, garantindo mais confiança nas operações digitais e reduzindo a possibilidade de ataques bem-sucedidos

3.1 Responsabilidade de plataformas e normas globais

Considerando o alcance mundial do material digital, a normatização dos deepfakes demanda uma ação conjunta entre as diversas nações. Países como EUA, União Europeia e China já elaboram leis que exigem clareza, identificação e retirada de materiais adulterados. O Brasil, mesmo sem leis próprias, pode usar tais exemplos para criar normas que envolvam tanto o governo quanto as empresas de tecnologia.

As plataformas digitais são essenciais nesse cenário. Elas devem criar sistemas de identificação automática, ter políticas de remoção rápida e colaborar com órgãos governamentais e centros de pesquisa. O uso de marcas d'água digitais e metadados criptografados se mostra como soluções técnicas boas para atestar a origem e a veracidade dos materiais. A regulamentação dessa tecnologia virou um dos maiores desafios legais e políticos na era digital, já que lida com a circulação global de informações alteradas e dos limites cada vez menores entre o real e o imaginário. Em um contexto em que conteúdos sintéticos podem ser espalhados rapidamente para muitos, nenhum país resolve essa questão sozinho. Essa natureza transnacional destaca a necessidade de cooperação internacional e exige que as plataformas digitais assumam responsabilidades inéditas na comunicação humana. A União Europeia avançou com o AI Act, que impõe regras rígidas de clareza e exige a rotulagem obrigatória dos conteúdos sintéticos, além de sistemas de rastreamento que identifiquem a origem do material manipulado (União Europeia, 2024).

Já os Estados Unidos optaram por uma abordagem fragmentada, com leis estaduais que focam em temas eleitorais, como as regras da Califórnia e do Texas que proíbem a divulgação de deepfakes que afetem a escolha do eleitor antes das

eleições (Keller; Levine, 2023). Essa diferença na regulamentação causa brechas exploradas em ambientes digitais que ultrapassam fronteiras, permitindo que materiais ilícitos migrem para áreas com normas mais leves ou com menos estrutura na fiscalização de manipulações audiovisuais. Hoje, o Brasil enfrenta uma situação complexa e multifacetada. Por um lado, temos uma estrutura de salvaguarda de dados e dos direitos individuais notavelmente robusta, impulsionada pela Lei Geral de Proteção de Dados e pelo Marco Civil da Internet, que servem como pilares jurídicos fundamentais. Por outro, a lacuna na legislação específica sobre deepfakes facilita o uso inadequado dessa tecnologia, sobretudo em casos de calúnia, pornografia não consentida e disseminação de informações falsas. O trâmite do Projeto de Lei 3821/2024 representa um avanço essencial para uma regulamentação apropriada, ao classificar como crime a adulteração digital de imagens por meio de inteligência artificial com o objetivo de provocar danos morais, chantagem, agressão psicológica ou influenciar eleições.

Essa proposta é o ponto de partida para integrar o Brasil ao debate mundial sobre veracidade digital e segurança da informação. Todavia, a obrigação das plataformas digitais vai além da mera retirada de conteúdos ilícitos após denúncias. A escala e a velocidade da criação demandam que essas empresas adotem uma atitude ativa, comumente chamada de gestão algorítmica. Essa nova perspectiva exige que plataformas como Meta, Google, TikTok e X implementem sistemas complexos capazes de identificar manipulações audiovisuais antes que se propaguem. Estudos apontam que a união da análise humana com modelos de aprendizado profundo resulta em índices de identificação superiores, realçando a importância de equipes especializadas que trabalhem em paralelo com instrumentos automáticos. Em paralelo, padrões globais, como os propostos pela Coalition for Content Provenance and Authenticity (C2PA), estão se tornando essenciais para a criação de um sistema técnico que viabilize a certificação de vídeos e imagens por meio de metadados codificados e assinaturas digitais, assegurando o rastreamento da origem desse material.

Contudo, a simples adoção dessas tecnologias não resolve questões éticas cruciais. As plataformas precisam equilibrar a proteção contra fraudes com a liberdade de expressão, garantindo que os sistemas de moderação automatizados não

gerem erros, excluam conteúdo válido ou agravem desigualdades já existentes. Como destaca Pawelec, a autorregulação das plataformas deve vir acompanhada de meios para promover a transparência e a auditoria externa, dando ao público a chance de supervisionar as decisões dos algoritmos e impedindo a criação de estruturas de poder centralizadas em empresas que decidem o que é verdade ou aceitável online. A desinformação causada por esse tipo de informação é uma ameaça mundial à integridade das democracias, à dignidade humana e à confiança na sociedade atual.

Nesse sentido, estudiosos brasileiros como Santaella e Salgado (2021) ressaltam que vivemos um novo tipo de comunicação, onde a própria ideia de verdade se torna instável, criando um ambiente perfeito para a "mecanização da desconfiança", ou seja, uma dúvida constante sobre qualquer imagem ou declaração. É nesse contexto de incerteza que responsabilidade das plataformas e a criação de normas internacionais se tornam vitais: sem critérios mínimos de verificação técnica e responsabilidade legal, o espaço digital pode virar um terreno fértil para manipulações que podem prejudicar instituições, reputações e processos democráticos. Assim, a regulamentação dos deepfakes deve ser vista não só como uma solução legal para problemas específicos, mas como algo essencial para defender a informação como um bem público global. A união entre normas internacionais, leis nacionais e políticas internas das plataformas é crucial para restaurar a confiança na comunicação digital e proteger as pessoas de práticas prejudiciais que exploram fraquezas tecnológicas e sociais. O futuro da autenticidade na internet depende dessa colaboração e do fortalecimento de uma ética algorítmica que garanta transparência, responsabilidade e respeito aos direitos fundamentais em todas as etapas de criação, distribuição e moderação de conteúdos sintéticos.

4 EDUCAÇÃO SOBRE MÍDIAS E CONSCIENTIZAÇÃO

No contexto atual, onde deepfakes ganham espaço, a educação midiática transcende o papel de mero complemento educacional. Ela se impõe como política estatal essencial para proteger a democracia e a qualidade da informação. A complexidade do ambiente digital, com seus algoritmos, manipulações e notícias

falsas velozes, exige que o cidadão saiba identificar falsificações e compreenda o sistema informacional. Alfabetização midiática significa formar pessoas capazes de analisar mensagens, entender a circulação da informação e questionar as plataformas de comunicação. Assim, essa educação visa menos a "ver" o conteúdo e mais a preparar para identificar intenções, narrativas, discursos e manipulações emocionais. Estudos de Miranda e Maciel (2024) mostram que eles exploram falhas cognitivas e emocionais, exigindo o desenvolvimento do pensamento crítico desde a infância. Estudos globais apontam que combater isso exige educação constante, não só tecnologia. Uma pesquisa no International Journal of Media Literacy (2024) revela que treinamentos práticos e interativos aumentam a detecção e o ceticismo em relação a conteúdos virais. Essa metodologia enfatiza que a educação midiática deve ser engajada, prática e contextual, indo além da teoria e da memorização. No Brasil, a desinformação e os vídeos de IA levaram a educação e a mídia a pedir programas de alfabetização digital. Reportagens de O Globo (2024) e UOL (2024) indicam que jovens brasileiros, mesmo conectados, pecam na análise da credibilidade das fontes. Isso revela uma contradição, estar conectado não garante competência informacional. A população enfrenta excesso de conteúdo, mas faltam ferramentas críticas, principalmente em relação à inteligência artificial.

No Brasil, o meio acadêmico também busca solucionar essa carência. A USP, através da sua plataforma de Tecnologia e Educomunicação, sustenta que a alfabetização midiática só funciona de verdade quando integrada em várias matérias, incluindo pontos de sociologia, filosofia, língua portuguesa e tecnologia. Essa visão multidisciplinar corresponde à "competência interpretativa ampliada" de Santaella e Salgado (2021), crucial para se virar em um mundo onde a confiança está em risco., em sua pesquisa, ainda argumenta que a conscientização tem que ter um lado político, além disso, a educação sobre mídia precisa cobrir as emoções ao receber coisas online.

Os deepfakes enganam não só pela aparência, mas porque usam nossas emoções. As pessoas acreditam mais no que confirma o que já pensam, dá medo ou irrita. Essa parte emocional é tão importante que aulas de alfabetização digital em vários países da Europa ensinam a controlar as emoções, reconhecer o que nos afeta e analisar as táticas psicológicas de quem cria notícias falsas. No Brasil, poucos

projetos pensam nisso, mesmo sendo importante. A união entre escolas, jornais, universidades, políticos, ONGs e plataformas online é essencial. Sites que checam notícias, como Aos Fatos, Agência Lupa e Fato ou Fake, ajudam a conferir informações, mesmo não substituindo o pensamento crítico. Mas, para isso virar costume, as pessoas precisam entender por que checar os fatos é importante e ver o papel do jornalismo profissional como elo entre o que acontece e o que as pessoas pensam. Hoff e Barbosa (2025) mostram que, com a inteligência artificial, o jornalismo também ensina, mostrando como a manipulação funciona e como se proteger dela. É crucial entender que criar consciência é uma jornada contínua.

Não basta oferecer workshops isolados ou campanhas passageiras; é preciso criar diretrizes duradouras, integradas ao ensino, apoiadas pelo governo, ligadas ao trabalho da imprensa e fortalecidas pelas mídias digitais. A proteção da sociedade contra essa problemática exige um esforço conjunto, já que visa defender não só a forma como cada pessoa enxerga a realidade, mas também a veracidade das informações que sustentam a democracia. Um cidadão que compreende a criação das falsificações, reconhece as técnicas de manipulação, questiona conteúdos com forte apelo emocional e checa informações antes de divulgar, é essencial para um ambiente de informação saudável. Assim, a educação sobre mídia vai além de apenas combater as notícias falsas, tornando-se um alicerce vital para o futuro das sociedades interligadas. Um ponto pouco explorado, mas essencial, é a inclusão digital consciente de pessoas em situação de fragilidade. Grupos com menos estudo, baixa escolaridade ou moradores de áreas afastadas são mais vulneráveis a manipulações, especialmente em eleições ou momentos de crise. Oferecer educação midiática a esses grupos exige políticas públicas específicas, métodos participativos e materiais que respeitem a realidade social de cada comunidade. Sem essa ação, esses vídeos falsos podem ampliar a desigualdade na informação e aumentar a diferença de poder na sociedade.

Além disso, é crucial entender que a educação sobre mídias não é apenas um fim em si mesma, mas sim um pedaço de uma mudança cultural muito maior. Essa mudança envolve criar uma forma de pensar em conjunto sobre como verificar informações, tornar a checagem um costume diário, dar valor ao trabalho dos

jornalistas, incentivar que tudo seja mais claro e reforçar a confiança entre as pessoas em um mundo cheio de informações por todos os lados.

No fim das contas, saber usar as mídias ajuda a diminuir os problemas causados pelos deepfakes e fortalece o quanto as pessoas se importam com o saber, a verdade e a proteção da democracia. Quando notamos que combater as notícias falsas na internet não é só uma questão de tecnologia ou leis, mas também de educação e de como as pessoas vivem em sociedade, fica claro que a conscientização é o jeito mais importante de lidar com a situação de hoje. A tecnologia pode descobrir as mentiras, as leis podem punir quem as espalha, mas só a educação pode construir uma sociedade forte, preparada e capaz de resistir aos perigos das informações falsas que ainda estão por vir

5 A INADEQUAÇÃO DO DIREITO CONVENCIONAL

Ao analisarmos os deepfakes no Brasil, notamos uma transformação radical na relação entre o Direito e conceitos fundamentais como prova, veracidade e autoria. O ordenamento jurídico brasileiro foi construído em um momento em que a autenticidade das evidências era avaliada principalmente através de elementos físicos e sinais visíveis de fraude. A natureza documental das provas permite que juízes, especialistas e partes interessadas reconstruam os eventos com base em evidências concretas, possibilitando também um controle eficaz da cadeia de custódia. No entanto, as tecnologias de inteligência artificial generativa, capazes de criar imagens e sons inexistentes com notável precisão, rompem com esse modelo ao gerar simulações que não são meras falsificações, mas criações inéditas que replicam comportamentos, expressões faciais e até emoções de pessoas reais. Santaella e Salgado (2021) defendem que essas tecnologias inauguram uma nova era de hiper-realidade, onde a percepção sensorial já não basta para distinguir o real do artificial, impactando a confiança epistemológica que sustentava o valor probatório das imagens. Esse descompasso entre tecnologia e legislação fica evidente na tentativa de classificar as ações relacionadas a esses vídeos. Os tipos penais previstos no Código Penal, como falsidade documental, falsidade ideológica ou uso de documento falso, foram criados para proteger a autenticidade de documentos com

existência material e finalidade jurídica específica. Entretanto, deepfakes não alteram documentos, mas sim criam simulações audiovisuais sem base em conteúdo original, dificultando sua inclusão nas classificações tradicionais do direito penal. Isso ajuda a entender por que a resposta jurídica no Brasil tem sido fragmentada, frequentemente se restringindo a adaptações parciais a crimes contra a honra ou delitos cibernéticos, que não refletem a gravidade e a singularidade da manipulação digital da identidade. Miranda e Maciel (2024) destacam que o Direito brasileiro ainda opera com categorias concebidas para um mundo analógico, resultando na permanência de grande parte das condutas envolvendo mídias sintéticas em uma zona cinzenta, sem definição precisa. O debate legislativo em torno do Projeto de Lei 3821/2024 ilustrou essa lacuna. O projeto visa preencher a ausência de um tipo penal específico para a manipulação digital por inteligência artificial, com foco em contextos eleitorais, libidinosos e difamatórios.

Durante a discussão no congresso, ficou claro que os efeitos desses conteúdos extrapolam a simples difamação, podendo destruir trajetórias políticas, influenciar a validade de pleitos eleitorais e gerar traumas psicológicos severos em pessoas expostas em montagens falsas de nudez ou agressão. Limitar-se às leis de injúria ou difamação desconsidera que o deepfake inventa um contexto completo, conferindo uma aparência real a eventos que jamais aconteceram. É um prejuízo ampliado que atinge não só a reputação, mas a própria individualidade da pessoa representada, visto que sua imagem é capturada e alterada com uma precisão técnica impressionante. No contexto das provas, a insuficiência das leis tradicionais se mostra ainda mais preocupante.

A credibilidade que sempre foi atribuída às provas em vídeo e áudio é profundamente abalada pelas novas tecnologias de criação. Antes, um vídeo era tido como uma prova praticamente incontestável; contudo, hoje em dia, ele pode suscitar dúvidas válidas devido à alta qualidade das manipulações digitais. Os juízes começam a se deparar com casos em que se alega falsificação em vídeos reais, ou, em contrapartida, onde a veracidade é exageradamente defendida em vídeos adulterados. Segundo estudos da USP (2024), a crise de veracidade nas mídias audiovisuais afeta diretamente a confiabilidade do sistema judicial, uma vez que a imagem perde sua força simbólica de retratar a realidade de forma clara.

Isso implica a necessidade de repensar os critérios de avaliação das provas, além de definir normas para a realização de perícias digitais em um ambiente de crescente instabilidade tecnológica. A atividade pericial se mostra um prisma cheio de conflitos, refletindo a inadequação do direito mesmo. Métodos de análise de vídeo, antes normais, serviam pra achar manipulações e inconsistências. Porém, essas formas não se encaixam mais na sofisticação dos modelos hoje em dia, que imitam com uma veracidade assustadora. Hoff e Barbosa (2025) dizem que a análise precisa de habilidades que vão além da perícia criminal comum, como entender redes neurais e achar rastros de algoritmos. Essa nova situação exige uma colaboração interdisciplinar.

O sistema judiciário brasileiro precisa sempre de especialistas em ciência de dados e engenharia da computação. A fragmentação do conhecimento impede uma compreensão completa da justiça diante da complexidade das informações sintéticas. O Direito sozinho, perde sua capacidade de interpretar diante das tecnologias digitais; só vai conseguir lidar bem com os deepfakes incorporando uma cultura institucional que priorize a interdisciplinaridade, vista como muito importante na investigação criminal e na busca pela verdade no processo. Além dos efeitos práticos a insuficiência do direito tradicional por assim dizer em relação aos conteúdos, provoca uma crise nos princípios teóricos do Direito Penal e da teoria da prova. A compreensão da autoria, por exemplo, complica-se bastante com a possibilidade de um vídeo ser gerado automaticamente por um modelo aberto de inteligência artificial sem intervenção humana direta ou com a colaboração mínima daquele que partilha o material.

A própria definição de dolo exige, na realidade, uma revisão a fim de incluir situações em que o indivíduo não cria o instrumento, mas o usa, com pleno conhecimento da sua falsidade para influenciar as percepções sociais. A materialidade da prova que outrora se baseava em evidências físicas, agora depende de padrões computacionais intangíveis, cuja interpretação precisa de ferramentas e conhecimentos técnicos que superam, em muito, o arsenal jurídico usual. Este fenômeno também interfere na noção de verdade processual. Numa conjuntura de simulações, torna-se gradualmente mais difícil assegurar a veracidade dos fatos. A realidade, construída em outro tempo por discussões e fatos agora se submete a

minuciosas avaliações técnicas, além de estruturas institucionais preparadas pra acompanhar as mudanças rápidas na tecnologia. A questão das provas em áudio e vídeo levanta uma desconfiança, cada vez maior, sobre a confiança no sistema judicial, pois a galera questiona decisões que se baseiam em elementos que podem ser manipulados facilmente. Essa queda na crença do povo é um dos maiores problemas que as pesquisas brasileiras sobre a desinformação indicam, e abala a base da democracia, que é a fé na honestidade das decisões do governo. Diante disso tudo, é perceptível que a fraqueza do direito tradicional não se resolve só criando leis novas.

É crucial repensar a forma como o Direito lida com a prova, a autoria, a intenção, e as responsabilidades. A tecnologia cria situações que exigem do sistema legal não só aplicar as regras, mas também entender, como um detetive experiente, os complexos ambientes digitais. Isso demanda reformas estruturais na formação em direito, aperfeiçoamento dos profissionais, métodos de investigação, e na própria cultura do Judiciário. Para enfrentar os desafios postos, uma reestruturação profunda dos alicerces da epistemologia jurídica é vital, assegurando a capacidade do Direito em responder com eficácia num ambiente em que a representação do real pode ser totalmente artificial. A análise da inaplicabilidade do direito tradicional perante os deepfakes revela que o desafio dessas inovações tecnológicas ultrapassa o âmbito jurídico, abrangendo aspectos estruturais e civilizacionais. O sistema penal no Brasil foi pensado pra operar em um cenário em que a verdade, mesmo que manipulada, tinha limites materiais perceptíveis. Agora, diante de simulações que reproduzem a realidade com muita precisão, o Direito se depara com uma transformação de paradigmas, exigindo uma revisão teórica, metodológica e institucional. As limitações das definições criminais clássicas, a prova audiovisual insuficiente, a necessidade cada vez maior de exames tecnológicos complicados, e a necessidade de uma parceria intersetorial urgente, mostram que a estrutura legal atual já não dá conta das exigências resultantes da nova ecologia da informação. A aceitação dessa condição na verdade não proíbe o Direito, mas destaca uma modernização urgente. Em sincronia com as rápidas mudanças sociais, o sistema jurídico brasileiro terá que redefinir suas categorias, promover educação interdisciplinar, avaliar a epistemologia da prova e expandir sua visão sobre tecnologias.

As discussões legislativas atuais e investigações em andamento revelam uma direção possível, porém, isso vai precisar de decisões institucionais que entendam a complexidade do contexto e que o combate aos deepfakes vá além da simples criminalização, isso é importante pois implicará em uma mudança na proteção da verdade, dignidade e confiabilidade pública. Por fim, o Direito brasileiro está em um momento chave, o que o força a sair da zona de conforto interpretativa e a buscar uma renovação. Esta temática específica reflete as fraquezas de um sistema legal construído sobre analogias, que hoje está em choque com o mundo digital, o qual transforma os conceitos de prova, autoria e responsabilidade de maneira dramática. Ultrapassar essas insuficiências exigirá, além de elaborar dispositivos legais inovadores, um esforço em grupo para remodelar as instituições, garantindo, face a manipulações complicadas, que a busca da verdade nos processos judiciais permaneça justa e executável.

6 ATUAÇÃO DO STF E STJ DIANTE DOS DESAFIOS JURÍDICOS DOS DEEPFAKES

A atuação do Supremo Tribunal Federal STF e do Superior Tribunal de Justiça STJ tem evoluído constantemente, apesar disso, demonstra uma adaptação institucional impressionante diante da complexidade labiríntica das fraudes digitais. Nenhum tribunal, presentemente, sentenciou qualquer caso notável relativo ao uso disto como crime independente. Contudo, os dois tribunais já emitiram decisões, declarações e diretrizes com efeito direto nesta área, especialmente em tópicos como desinformação, integridade eleitoral e a responsabilidade das plataformas digitais. Esse conjunto de decisões estabelece os alicerces legais que, depois, farão possível o desenvolvimento de jurisprudência específica sobre as manipulações sintéticas, criadas por inteligência artificial. No STF, destaca-se uma decisão em colegiado, emitida em 2025, onde a Corte definiu que as plataformas digitais podem ser civilmente responsabilizadas pela manutenção de conteúdos evidentemente ilegais, após serem notificadas extrajudicialmente, sem a exigência de uma determinação judicial prévia. Mesmo que a decisão não aborde diretamente o tema, ela abre um precedente importante, reforçando o dever das plataformas de retirar conteúdo

potencialmente ofensivo dos direitos básicos, até mesmo os feitos por inteligência artificial.

Essa interpretação conecta-se intimamente, sabe, à essência dos vídeos falsos, que têm o poder de causar danos graves e imediatos a honra, imagem e ao processo eleitoral, quando espalhados pelas mídias sociais. O tribunal, igualmente, tomou uma posição institucional sobre a temática, o Ministro Luís Roberto Barroso, avisou sobre a falta de ferramentas tecnológicas que consigam parar completamente os impactos das mídias sintéticas. Em sua fala destacou a urgente necessidade de mais estratégias educacionais e regulatórias, pensadas pra proteger o processo democrático. Além disso, o STF agiu em iniciativas educacionais, como o Guia Ilustrado contra Deepfakes, pra tentar ensinar a galera sobre os sinais de manipulação audiovisual. Apesar de não ser uma decisão judicial final, essa medida mostra o reconhecimento, da Corte, da importância social do tema e prova que lutar contra a inteligência artificial maliciosa vai além do campo penal. É um avanço simbólico grande, porque aumenta a conscientização da população e reforça o papel do Judiciário, como protetor da integridade da informação. Em relação ao Superior Tribunal de Justiça, mesmo que não haja precedentes precisos acerca da tecnologia dos vídeos sintéticos, é possível perceber um conjunto de decisões, que lançam alicerces legais importantes para encarar esse problema nos próximos anos. O Tribunal tem aprofundado as suas ideias, sobre a responsabilidade civil das plataformas digitais, sobre a importância de manter registros, e a necessidade de tirar do ar conteúdos ilegais, depois da vítima avisar. Esses posicionamentos criam bases importantes que podem ser usadas, em decisões futuras, sobre a distribuição de vídeos manipulados, com a intenção de difamar, extorquir, ou causar danos morais e existenciais.

Pesquisas acadêmicas brasileiras têm apontado que o STJ já fez menção ao termo deepfake em algumas decisões de forma incidental, especialmente ao lidar com alegações de manipulação audiovisual, mas ainda sem desenvolver uma tese clara sobre a temática. A atuação dos tribunais superiores ainda não resultou na criação de normas específicas para a responsabilização penal relacionada ao material sintético, embora já possua as bases necessárias para uma interpretação tanto constitucional quanto infraconstitucional que possa abordar essa questão. O

movimento atual indica que tanto o STF quanto o STJ reconhecem que as manipulações digitais geradas por inteligência artificial representam uma ameaça clara à integridade das instituições democráticas, ao devido processo legal e à salvaguarda da personalidade civil. À medida que casos específicos forem levados ao Judiciário, é provável que as diretrizes existentes sejam fortalecidas e aprofundadas.

7 CONCLUSÕES

A discussão apresentada ao longo deste artigo mostra que os deepfakes não são apenas uma inovação tecnológica, mas um fenômeno que desafia diretamente a forma como lidamos com a informação, a verdade e os direitos individuais. A possibilidade de produzir imagens e vídeos extremamente convincentes altera profundamente nossa relação com a realidade e coloca em risco a confiança que depositamos no que vemos e ouvimos. Isso afeta não apenas instituições e processos democráticos, mas também a vida cotidiana de pessoas que podem ter sua imagem, sua privacidade e sua reputação gravemente comprometidas.

Fica evidente que o Direito brasileiro ainda não está totalmente preparado para enfrentar essas manipulações digitais. As normas existentes oferecem ferramentas importantes, mas foram criadas em um contexto anterior à inteligência artificial generativa e, por isso, não conseguem abarcar todas as nuances desse novo risco tecnológico. A falta de legislação específica gera insegurança e deixa lacunas que dificultam tanto a punição dos responsáveis quanto a proteção das vítimas.

Também se percebe que a resposta jurídica não pode se limitar a criar novos crimes ou ampliar punições. Os deepfakes introduzem problemas complexos que exigem preparo técnico, capacidade de investigação digital e conhecimento interdisciplinar. Para identificar uma manipulação, não basta a análise tradicional de provas; é preciso integrar saberes da computação, comunicação, psicologia e direito. Isso mostra que o próprio sistema de justiça precisa se adaptar para continuar garantindo segurança jurídica em um ambiente cada vez mais instável.

Outro ponto fundamental é a responsabilidade compartilhada. Plataformas digitais, instituições públicas, escolas, meios de comunicação e cidadãos têm papel ativo na construção de uma cultura de verificação e responsabilidade informacional. A educação midiática surge como uma das formas mais eficazes de fortalecer essa cultura, permitindo que as pessoas desenvolvam olhar crítico e sejam capazes de reconhecer sinais de manipulação. Quanto mais a sociedade estiver preparada, menores serão os impactos da desinformação e maiores serão as chances de preservar um ambiente democrático saudável.

Diante de tudo isso, é possível afirmar que o enfrentamento aos deepfakes precisa ser visto como um esforço coletivo e contínuo. Não se trata apenas de acompanhar a tecnologia, mas de compreender seus efeitos humanos e sociais. Somente com legislação atualizada, preparo institucional, alfabetização digital e compromisso com a transparência será possível proteger a integridade das informações e garantir que a tecnologia continue servindo ao bem-estar social, e não como instrumento de violência e manipulação.

REFERÊNCIAS

SAAD, Elizabeth. **Desinformação e alfabetização midiática – uma parceria necessária.** Jornal da USP, São Paulo, 16 jan. 2019. Disponível em: https://jornal.usp.br/artigos/desinformacao-e-alfabetizacao-midiatica-uma-parcerianecessaria/. Acesso em: 17 nov. 2025.

UNIÃO EUROPEIA. **Artificial Intelligence Act. Parlamento Europeu, 2024.** Disponível em: https://eur-lex.europa.eu. Acesso em: 19 out. 2025

CÂMARA DOS DEPUTADOS. Projeto de Lei n. 3821, de 2024. **Institui tipificação criminal para manipulação digital por IA e dá outras providências.** Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2461213. Acesso em: 12 out. 2025.

HOFF, Rafael Sbeghen; BARBOSA, Cristiane de Lima. **Educação midiática e jornalismo na era da inteligência artificial. Ámbitos: Revista Internacional de Comunicación,** n. 68, p. 45–63, 2025. Disponível em: https://revistascientificas.us.es/index.php/Ambitos/article/view/28115. Acesso em: 12 out. 2025.

MIRANDA, Felipe da Cruz; MACIEL, Cristiano. **Educação midiática como alternativa à desinformação e a deepfake. Anais da Conferência Latino-Americana de Ética em**

Inteligência Artificial, 2024. Disponível em: https://sol.sbc.org.br/index.php/laai-ethics/article/view/32454. Acesso em: 12 out. 2025

SANTAELLA, Lucia; SALGADO, Marcelo de Mattos. **Deepfake e as consequências sociais da mecanização da desconfiança. TECCOGS: Revista Digital de Tecnologias Cognitivas,** n. 23, p. 90–103, 2021. Disponível em: https://revistas.pucsp.br/index.php/teccogs/article/view/55981. Acesso em: 18 out. 2025.

UNIVERSIDADE DE SÃO PAULO (USP). **Educação midiática e combate à desinformação. São Paulo: USP, 2024.** Disponível em: https://www.iea.usp.br/noticias/educacao-midiatica-pode-ser-chave-para-combate-a-desinfor macao. Acesso em: 18 out. 2025.

SUPREMO TRIBUNAL FEDERAL (STF). **Guia Ilustrado Contra as Deepfakes. Brasília:**

STF, 2024. Disponível em: https://bibliotecadigital.stf.jus.br/xmlui/bitstream/handle/123456789/7797/Guia_ilustrado_dee pfakes.pdf?isAllowed=y&sequence=1. Acesso em: 4 nov. 2025.

O GLOBO. **Barroso defende 'educação midiática' para combater deepfake.** O Globo, Rio de Janeiro, 03 out. 2024. Disponível em: https://oglobo.globo.com/politica/noticia/2024/10/03/barroso-defende-educacao-midiatica-par a-combater-deepfake.ghtml. Acesso em: 12 out. 2025.

SIQUEIRA, M. de; ANDRADE, E. J. de. **DEEPFAKE E PRIVACIDADE: UMA ANÁLISE JURÍDICA ACERCA DA MANIPULAÇÃO DA IMAGEM DOS USUÁRIOS. REVISTA FOCO**, *[S. l.]*, v. 17, n. 8, p. e5679 , 2024. DOI: 10.54751/revistafoco.v17n8-014. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/5679. Acesso em: 17 nov. 2025.

PAWELEC, M. **Decent deepfakes? Professional deepfake developers' ethical consideratios and their governance potential. AI and Ethics,** v. 5, p. 2641-2666, 2025

KELLER, Daphne. **Internet Platforms: Observations on Speech, Danger, and Money. Hoover Institution Essay, Hoover Institution** – Stanford University, Paper No. 1807, 2019. Disponível em: https://law.stanford.edu/wp-content/uploads/2019/04/keller_webreadypdf_final.pdf. Acesso em: 17 nov. 2025.

Instituto Nacional de Tecnologia da Informação – ITI. **Congresso da Cidadania Digital 2025 reúne especialistas em Brasília para debater integração nacional e inovação tecnológica.**

Brasília, 29 set. 2025. Disponível em: https://www.gov.br/iti/pt-br/assuntos/noticias/indice-de-noticias/congresso-da-cidadania-digit al-2025-reune-especialistas-em-brasilia-para-debater integracao-nacional-e-inovacao-tecnologica. Acesso em: 17 nov. 2025.

BRASIL. Banco Central do Brasil. **Relatório integrado 2022. Brasília: Banco Central do Brasil, 2023**. Disponível em: https://www.bcb.gov.br/content/publicacoes/rig/rig_2022.pdf. Acesso em: 17 nov. 2025.

FEBRABAN – Federação Brasileira de Bancos. **Relatório Anual da Autorregulação**

Bancária 2024. São Paulo: FEBRABAN, 2024. Disponível em: https://portal.febraban.org.br/pagina/3396/52/pt-br/relatorio-autorregulacao-2024 Acesso em: 17 nov. 2025.

MIRANDA, Gustavo Alves. **Lei Geral de Proteção de Dados e suas repercussões no direito e nas relações de consumo.** Volta Redonda/RJ: Universidade Federal Fluminense, Instituto de Ciências Humanas e Sociais, 2022. Trabalho de Conclusão de Curso (Graduação em Direito). Disponível em: https://app.uff.br/riuff/bitstream/handle/1/28844/GUSTAVO%20ALVES%20MIRANDA.pdf? sequence=1&isAllowed=y. Acesso em: 17 nov. 2025.

PARTE IV - TRANSPARÊNCIA, PUBLICIDADE E GOVERNO DIGITAL

A TENSÃO ENTRE A PUBLICIDADE DOS ATOS PROCESSUAIS E A PROTEÇÃO DE DADOS PESSOAIS

Ana Júlia Guimarães Ferreira da Silva[1]
Anna Beatriz Dias Amaral[2]
Iasmin de Freitas Soares[3]
Maria Eduarda França Fernandes Beserra[4]

RESUMO

O presente trabalho visa analisar e refletir acerca da proteção de dados pessoais no ambiente do Poder Judiciário, segundo as diretrizes da Lei Geral de Proteção de Dados. Com a digitalização dos processos e a garantia constitucional de publicidade, o que era pra ser um avanço tecnológico apenas para agilidade e celeridade processual, se tornou uma das ferramentas utilizadas por criminosos para aplicar golpes e fraudes, expondo as informações pessoais dos cidadãos a um ambiente perigoso. Com isso, é necessário identificar como isso está sendo realizado e como evitar.

Palavras-chave: publicidade; LGPD; atos processuais; golpes digitais;

SUMÁRIO: 1. Introdução; 2. Papel dos tribunais na exposição de dados; 3. Golpes e fraudes baseados em informações judiciais públicas; 4. Medidas de proteção e anonimização de dados em processos judiciais; 4.1. Estratégias de anonimização e pseudomanização em decisões e repetições; 4.2 Comparação com práticas internacionais e como aplicaria- se no Brasil; 5. O impacto da exposição de dados judiciais na vida dos cidadãos; 6. Medidas de prevenção e combate ao golpe do "falso advogado"; 7. Conclusão; 8. Referências.

1 INTRODUÇÃO

O avanço da tecnologia e a digitalização dos processos judiciais transformaram profundamente a forma como o Poder Judiciário brasileiro atua e se

[1] Graduanda em Direito no Centro Universitário de Brasília – CEUB, estagiária na Mauro Menezes e Advogados, com atuação direta nos tribunais superiores na área trabalhista e constitucional.
[2] Graduanda em Direito no Centro Universitário de Brasília – CEUB.
[3] Graduanda em Direito no Centro Universitário de Brasília – CEUB, estagiária no Tribunal de Justiça do Distrito Federal e Territórios no Núcleo de Assistência ao Jurisdicionado – NAJ.
[4] Graduanda em Direito no Centro Universitário de Brasília – CEUB, estagiária no gabinete de conselheiro no Conselho Nacional de Justiça.

relaciona com a sociedade. A implementação de sistemas eletrônicos, como o Processo Judicial Eletrônico (PJe), permitiu maior celeridade, eficiência e transparência na tramitação das ações. No entanto, esse cenário de modernização também trouxe novos desafios, especialmente no que diz respeito à proteção de dados pessoais e à segurança da informação. O volume expressivo de dados sensíveis sob responsabilidade do Judiciário, como informações pessoais, bancárias e jurídicas, torna o sistema um alvo atrativo para práticas criminosas e fraudes digitais.

Nesse contexto, a necessidade de conciliar a publicidade dos atos processuais com a proteção da privacidade dos cidadãos torna-se uma questão central. O princípio da publicidade, previsto na Constituição Federal, garante a transparência e o controle social sobre as decisões judiciais, mas, ao mesmo tempo, pode expor dados pessoais de forma indevida, facilitando o acesso por pessoas mal-intencionadas. Assim, os tribunais e demais órgãos judiciais precisam adotar medidas de segurança compatíveis com a Lei Geral de Proteção de Dados (LGPD), buscando equilibrar a abertura das informações públicas com a preservação da intimidade e da dignidade dos litigantes.

Contudo, mesmo com essas precauções, o ambiente digital tem se mostrado vulnerável à ação de criminosos que se aproveitam da facilidade de acesso a informações públicas para aplicar golpes e fraudes. A disseminação de documentos digitalizados sem a devida proteção, o envio de comunicações falsas simulando órgãos da justiça e a falsificação de boletos judiciais são apenas alguns exemplos de como os dados disponíveis em plataformas oficiais podem ser utilizados de forma ilícita. Diante disso, torna-se indispensável o fortalecimento das políticas de cibersegurança e a conscientização da população sobre os riscos envolvidos, de modo a assegurar que a digitalização continue sendo uma ferramenta de democratização do acesso à Justiça, e não uma porta aberta para o crime.

2 PAPEL DOS TRIBUNAIS NA EXPOSIÇÃO DE DADOS

Atualmente, o Poder Judiciário concentra um dos maiores volumes de dados pessoais sensíveis no Brasil, segundo o Conselho Nacional de Justiça, por meio do 1º Encontro de Encarregados e Encarregadas do Poder Judiciário, ocorrido em outubro deste ano. Cada tribunal e órgão é responsável por nomear um Encarregado, seguindo as diretrizes da Lei Geral de Proteção de Dados (LGPD).

Essa concentração de dados, que devem ser protegidos, entra em conflito com o princípio da publicidade dos atos processuais, resguardado pelo Art. 5º, inciso LX, da Constituição Federal, que acaba por deixar algumas informações pessoais dos litigantes de fácil acesso ao público. Assim, os tribunais atuam em uma linha tênue entre a obrigação constitucional de publicidade e a necessidade de resguardar dados pessoais, buscando harmonizar o princípio da transparência e a tutela da intimidade e da dignidade humana.

Com a digitalização dos processos por meio de sistemas virtuais dos tribunais, como o PJe, o acompanhamento e desenvolvimento das ações ficaram mais práticos e acessíveis. No entanto, a digitalização de documentos, embora tenha trazido avanços significativos em termos de agilidade e acessibilidade, também abriu espaço para o aumento de golpes e fraudes. Documentos digitalizados, quando armazenados ou compartilhados sem a devida proteção, podem ser facilmente copiados, alterados ou utilizados de forma indevida por criminosos. Golpistas podem empregar técnicas de falsificação digital, como a edição de imagens e PDFs, para criar versões adulteradas de documentos oficiais, como RGs, CPFs, comprovantes de residência e contratos, com o objetivo de aplicar fraudes financeiras, abrir contas bancárias ou realizar compras em nome de terceiros.

Além disso, o armazenamento e o envio desses documentos em plataformas aumentam o risco de vazamentos de dados. Uma vez obtidos, esses arquivos podem ser usados em esquemas de phishing, clonagem de identidade e até em fraudes trabalhistas e previdenciárias.

Recentemente, há um alerta para a sociedade acerca de fraudes aplicadas por meio de aplicativos de mensagens e ligações de supostos escritórios de advocacia, que não existem, para os clientes dos reais escritórios. Os criminosos estão se utilizando das plataformas dos tribunais para pegarem dados dos clientes e se

passarem pelo escritório responsável por suas ações. Por isso, é essencial que tanto os órgãos públicos quanto os particulares adotem medidas de segurança cibernética, garantindo que a digitalização, em vez de fragilizar, contribua para a integridade e a confiabilidade das informações.

3 GOLPES E FRAUDES BASEADOS EM INFORMAÇÕES JUDICIAIS PÚBLICAS

No Brasil, os crimes cibernéticos têm aumentado, principalmente aqueles que aproveitam a estrutura do sistema judiciário para realizar fraudes. O principal objetivo dessas atividades fraudulentas é coletar dados pessoais e bancários das vítimas, além de instalar softwares maliciosos (malwares) em seus dispositivos, o que compromete a segurança da informação e causa perdas financeiras.

Uma das estratégias mais comuns é o envio de e-mails fraudulentos, nos quais se alegam processos judiciais envolvendo o nome da vítima. Essas mensagens comunicam sobre audiências sem data ou local estabelecidos e são assinadas por pessoas que fingem ser advogados ou funcionários da Justiça. Outra prática frequente é o envio de boletos bancários falsificados, com cobranças indevidas em nome de entidades como o Tribunal de Justiça do Distrito Federal e Territórios (TJDFT) ou Justiça do Trabalho. Isso ocorre sob a justificativa de liberar valores que foram retidos em processos judiciais.

Em certas situações, os criminosos usam informações reais obtidas do sistema de acompanhamento processual do Processo Judicial Eletrônico (PJe). Eles enviam mensagens que não apenas parecem autênticas, mas também visam infectar os dispositivos das vítimas e coletar dados sensíveis.

Os jurisdicionados que recorrem aos Juizados Especiais e aos Núcleos de Assistência ao Jurisdicionado são, sem dúvida, os grupos mais suscetíveis a essas práticas. Nesses locais, é frequente que as partes não tenham advogados e não conheçam os procedimentos e atos processuais, o que as deixa mais vulneráveis a tentativas de fraude.

A facilidade de obtenção de informações pessoais como nome completo, CPF e data de nascimento que, por não serem vistas como dados sensíveis, têm um acesso menos restrito, aumenta a eficácia dos golpes. Os criminosos usam essas informações, frequentemente acessíveis nos próprios autos dos processos, para validar suas abordagens. O princípio da publicidade, estabelecido na Constituição Federal, assegura que a maioria dos processos judiciais seja pública. Embora isso seja fundamental para a transparência do Judiciário, também pode facilitar o acesso indevido a informações que podem ser usadas de forma maliciosa.

Em muitos casos, os golpistas usam fotos de advogados tiradas de redes sociais e cópias de processos eletrônicos para dar aparência de legitimidade a seus atos fraudulentos. Nesse contexto, é fundamental que os cidadãos verifiquem a autenticidade das comunicações recebidas, utilizando sempre os canais oficiais dos tribunais e confirmando a origem das mensagens antes de tomar qualquer medida.

4 MEDIDAS DE PROTEÇÃO E ANONIMIZAÇÃO DE DADOS EM PROCESSOS JUDICIAIS

4.1 Estratégias de anonimização e pseudomanização em decisões e repetições

Na Lei Geral de proteção de dados, o dado anonimizado é um dado relativo a titular que não pode ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, conforme o artigo 5º, incisos III e XI.

Ou seja, é aquele que não pode ser associado a uma pessoa natural identificada ou identificável, considerando meios técnicos razoáveis e disponíveis no momento do tratamento. O dado perde o vínculo com a identidade da pessoa, se tornando um dado "despersonalizado". Não podendo ser revertido, a pessoa não é mais identificável, deixando de ser pessoa e saindo do âmbito da LGPD.

E os dados pseudonimizado é aquele que passa por um processo que dificulta a associação a uma pessoa, mas ainda permite a reversão com informações

adicionais, conforme o artigo 13, parágrafo 4º. Dados que ainda são considerados pessoais e continuam sobre a proteção da LGPD.

Para a proteção destes dados em processos judiciais, utilizam-se algumas estratégias, como, a substituição de nomes, endereços e números de documentos por etiquetas genéricas, a remoção de informações sensíveis quando não forem essenciais à compreensão da decisão, uso de identificadores fixos internos que mantenham coerência entre documentos, sem revelar identidades reais. E mesmo em casos de anonimização automática, a revisão por especialista jurídico é imprescindível para evitar a exposição indevida.

Outros, como remover atributos de dados que não se utilizaram, sendo qualquer atributo que não seja claramente necessário no conjunto de dados, deve ser suprimido. Avaliar a solução, examinar os conjuntos de dados para avaliar se vai ter utilidade, sendo a utilidade insuficiente, processo de anonimização pode ter de ser redesenhado.

No caso de repetições, utilizam-se métodos mais específicos, como o K-anonimato, sendo aplicado para assegurar que os identificadores diretos e/ou indiretos do registo são partilhados por pelo menos k-1 outros registos, por isso não é possível ligar ou isolar o registro de um indivíduo. E o Tokenização rotativa, que é utilizado para a alteração periódica dos pseudônimos utilizados em diferentes publicações para reduzir a rastreabilidade entre releases.

Portanto, as estratégias de anonimização e pseudonimização constituem instrumentos indispensáveis para conciliar a transparência pública com a proteção de dados pessoais. Sendo fundamental para prevenir riscos, identificação e assegurar o equilíbrio entre publicidade, privacidade e segurança jurídica.

4.2 Comparação com práticas internacionais e como aplicaria- se no Brasil

No Estados Unidos, ainda não adotaram uma lei federal que abrangente sobre a privacidade e proteção de dados, mesmo que as leis estejam se tornando eficazes em um nível estadual. Porém estabelecem critérios de anonimização semelhantes

com o Brasil, minimizando atributos identificáveis e no uso de modelos probabilísticos para impedir a reidentificação.

Tendo umas agências, como o U.S. Census Bureau aplicam a differential privacy desde 2020 em seus censos, tornando-se referência mundial na anonimização de dados de larga escala. E um projeto de lei, a American Data Privacy Protection Act (ADPPA), que se tornaria a primeira lei federal de privacidade após quase duas décadas de discussão. Para proporcionar aos consumidores direitos fundamentais de privacidade de dados, criar fortes mecanismos de supervisão e estabelecer uma aplicação significativa.

Na Europa, a anonimização e a pseudonimização são através de agências de proteção de dados independentes, como a CNIL (França) e o ICO (Reino Unido), que estabelecem guias técnicos detalhados sobre boas práticas de anonimização, categorizando os riscos de reidentificação, definindo níveis de ruído aceitáveis e padronizando metodologias de auditoria.

E o RGPD da UE torna obrigatória a eliminação ou anonimização de dados pessoais quando não existir uma finalidade (mais) legal para a sua conservação, de forma a permitir a identificação de um indivíduo. No entanto, as técnicas de pseudonimização oferecem medidas técnicas e organizacionais para mitigar os riscos à proteção de dados quando (ainda) for necessário tratar dados pessoais de indivíduos.

Também incentiva o uso de privacidade diferencial (Differential Privacy) e dados sintéticos em bases públicas, especialmente em setores como saúde e justiça, para equilibrar transparência e sigilo.

5 O IMPACTO DA EXPOSIÇÃO DE DADOS JUDICIAIS NA VIDA DOS CIDADÃOS

Com o crescimento exponencial da tecnologia e a inauguração da era digital, o acesso à informação obteve maior visibilidade, e com isso, medidas do próprio Estado para assegurar que esse acesso seja efetivado. Entretanto, é de suma

importância que o referido acesso seja viabilizado em conformidade com o que preceitua a LGPD.

Não obstante, a exposição de dados pessoais pode acarretar riscos e prejuízos aos indivíduos envolvidos, ao serem usados de forma fraudulenta para atingir fins criminosos. Dessa forma, em vista da crescente quantidade de golpes que estão sendo aplicados a partir do acesso a dados judiciais, os quais são encontrados em processos dotados de acesso irrestrito, é fundamental analisar o impacto que esse tipo de golpe tem causado na vida das vítimas.

Sob esse viés, a partir de plataformas de acesso público do Poder Judiciário é possível consultar diversos dados estritamente pessoais, como telefone, endereço e CPF, o que pode acarretar no roubo de identidade, em que criminosos utilizam as informações divulgadas para abrir contas bancárias fraudulentas. Além do uso crescente dessas informações por estelionatários que fingem ser advogados, utilizando os referidos dados para enganar os supostos clientes ao informar que possuem sentenças favoráveis, com o fim de auferirem vantagem financeira.

Como exposto, o golpe do falso advogado encontra-se em ascensão, a partir da sofisticação das atividades fraudulentas, decorrente desse livre acesso a informações processuais e pessoais das partes. Assim, o funcionamento dessa fraude acontece com o acesso aos referidos dados, por meio das plataformas dos Tribunais, assim, os golpistas informam o número real do processo, em nome do próprio advogado, e passam atualizações falsas do processo, muitas vezes informando que existem valores liberados, ou a necessidade do pagamento de alguma taxa.

Sob essa perspectiva, as principais vítimas desse tipo de golpe são, sobretudo, pessoas com processos judiciais em andamento, com destaque para idosos, indivíduos em situação de vulnerabilidade financeira e pessoas com baixo nível de escolaridade. Por sua vez, os autores das fraudes utilizam estratégias de convencimento e linguagem jurídica complexa, valendo-se do desconhecimento técnico e da vulnerabilidade de grande parte da população para obter vantagens indevidas.

Conforme noticiado pelo portal O Dia (2025), uma professora aposentada do Rio de Janeiro foi vítima de um golpe aplicado por falsos advogados, resultando em expressivo dano financeiro, conforme segue:

> A reportagem relata que a vítima participou de uma suposta audiência e, acreditando estar sendo assistida por advogados, acabou transferindo valores e contratando empréstimos, acumulando um prejuízo de aproximadamente R$300 mil (O DIA, 2025).

Outrossim, de acordo com dados levantados pela OAB Nacional, de janeiro a agosto foram registradas 84 denúncias do golpe do falso advogado apenas no Distrito Federal, sendo ainda um assunto amplamente debatido não só pela OAB-DF e o TJDFT, como também a nível nacional, porquanto, segundo outro levantamento da OAB Nacional, desde 2024, apenas em São Paulo, foram registradas 1,6 mil denúncias de golpes envolvendo falsos advogados. Em Minas Gerais, já são 516 casos, e no Acre, quase 400. A estimativa da instituição é que milhares de vítimas em todo o país tenham sido enganadas por esse tipo de fraude.

Nessa toada, os números supracitados são tão expressivos e preocupantes que a OAB criou a plataforma "ConfirmADV" com o objetivo de reduzir a quantidade de golpes, porém como demonstrado, ainda não obteve a eficiência almejada, visto que grande parcela da população ainda vem sofrendo essa extorsão.

Diante do exposto, conclui-se que o livre acesso a informações processuais, embora essencial para garantir a transparência do Poder Judiciário, tem se mostrado vulnerável à exploração por criminosos, especialmente no contexto do golpe do falso advogado. A divulgação de dados pessoais em plataformas públicas, quando associada à falta de conhecimento técnico por parte de parcela significativa da população, possibilita que indivíduos mal-intencionados obtenham vantagens financeiras de forma ilícita, causando prejuízos expressivos às vítimas.

6 MEDIDAS DE PREVENÇÃO E COMBATE AO GOLPE DO "FALSO ADVOGADO"

O aumento recente de fraudes cometidas por pessoas que se apresentam como advogados demanda uma resposta institucional sólida e coordenada. As ações recentes da OAB e do CNJ demonstram que medidas eficazes estão sendo adotadas. Em colaboração com suas 27 seccionais, a OAB Nacional iniciou uma campanha de conscientização que combina orientação pública e tecnologia. A plataforma ConfirmADV permite que os cidadãos confirmem a inscrição de um advogado na Ordem. Essa ferramenta, que está integrada ao Cadastro Nacional dos Advogados (CNA), envia um pedido para o e-mail do profissional em questão, solicitando confirmação em até cinco minutos, o que assegura uma resposta rápida e transparente.

Os números refletem a aceitação da população à medida: em apenas três semanas, a ConfirmADV registrou quase 10 mil solicitações de verificação, das quais mais de 7,9 mil foram confirmadas. Ademais, a OAB disponibiliza um canal de denúncias para casos de fraude, enfatizando que a prevenção também envolve a responsabilização institucional.

O Conselho Nacional de Justiça (CNJ), por outro lado, implementou medidas estruturais para reduzir o golpe. A partir de 3 de novembro de 2025, a autenticação em dois fatores (2FA/MFA) foi introduzida no sistema PJe para usuários externos, como advogados, partes e interessados, aumentando consideravelmente a segurança no acesso aos sistemas judiciais. Essa camada extra torna mais difícil para os fraudadores acessarem o sistema com credenciais roubadas ou usadas de forma inadequada.

A identificação de assistentes de advogados no PJe, mesmo com a implementação do 2FA, é outro aspecto relevante. Isso implica que funcionários de escritórios podem acessar processos sem a necessidade de compartilhar senhas, tokens ou certificados do titular, diminuindo assim o risco de uso indevido de credenciais e melhorando a rastreabilidade das ações no sistema. Ademais, mesmo com o compartilhamento de funções administrativas, operações sensíveis, como assinatura eletrônica e ciência de intimações, permanecem exclusivas ao advogado titular, assegurando a integridade e a responsabilidade pelos atos realizados.

Essas ações combinadas conscientização do público, verificação da identidade profissional por meio da ConfirmADV e fortalecimento da segurança digital no sistema judicial com etapa de dois fatores constituem uma estratégia sólida para combater o golpe do "falso advogado". A conexão entre as ações da OAB e do CNJ evidencia que uma prevenção eficiente se sustenta em três pilares: conscientização da sociedade, disponibilidade de ferramentas tecnológicas e garantia de segurança nos sistemas institucionais. Essas medidas, em última análise, não só protegem os cidadãos vulneráveis a golpes, mas também fortalecem a credibilidade da advocacia e aumentam a confiança no Judiciário digital.

7 CONCLUSÃO

Diante do cenário apresentado, torna-se evidente que o Poder Judiciário brasileiro enfrenta o grande desafio de equilibrar dois princípios constitucionais de igual relevância: a publicidade dos atos processuais e a proteção da privacidade dos cidadãos. A digitalização e a ampliação do acesso aos processos judiciais foram marcos importantes na modernização da Justiça, mas também expuseram fragilidades que têm sido exploradas por criminosos. A crescente ocorrência de golpes e fraudes, baseadas em informações públicas e documentos processuais, evidencia a urgência de repensar as formas de divulgação e armazenamento dos dados, para que a transparência não se converta em vulnerabilidade.

Nesse sentido, a aplicação efetiva da Lei Geral de Proteção de Dados (LGPD) deve ser prioridade absoluta dentro dos tribunais, exigindo políticas de segurança cibernética mais rigorosas e práticas de anonimização e pseudonimização mais amplas. O uso dessas técnicas é essencial para garantir que as informações mantidas em processos públicos não possam ser utilizadas para identificar ou prejudicar as partes envolvidas. Além disso, é necessário o investimento em capacitação contínua dos servidores e operadores do Direito, assegurando que todos compreendam a importância da proteção dos dados e saibam lidar com os riscos tecnológicos de forma responsável e preventiva.

Outro aspecto fundamental é o fortalecimento da cooperação entre o Poder Judiciário, o Conselho Nacional de Justiça (CNJ), a Ordem dos Advogados do Brasil

(OAB) e as autoridades de segurança digital. Essa integração é indispensável para o desenvolvimento de protocolos padronizados de proteção de dados, de mecanismos eficientes de monitoramento e da criação de canais de denúncia e verificação acessíveis à população. A atuação conjunta dessas instituições pode não apenas reduzir a incidência de golpes, mas também ampliar a confiança social na Justiça, mostrando que a tecnologia pode ser aliada da segurança, e não uma ameaça.

Por fim, é imprescindível promover a conscientização da sociedade sobre os riscos associados à exposição de informações pessoais em ambientes digitais, especialmente entre os grupos mais vulneráveis. Campanhas educativas, verificações de autenticidade em comunicações jurídicas e o estímulo ao uso exclusivo de canais oficiais podem reduzir significativamente os prejuízos decorrentes de fraudes. Portanto, a proteção dos dados no Judiciário não deve ser vista como um obstáculo à transparência, mas como uma condição indispensável para garantir uma Justiça moderna, segura e comprometida com a dignidade e os direitos fundamentais de todos os cidadãos.

REFERÊNCIAS

CONSELHO NACIONAL DE JUSTIÇA (CNJ). *Judiciário reafirma compromisso com proteção de dados pessoais*. Brasília, 2023. Disponível em: https://www.cnj.jus.br/judiciario-reafirma-compromisso-com-protecao-de-dados-pessoais.Acesso em: 10 out. 2025.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). *Minuta do guia de anonimização e pseudonimização – versão limpa pós-revisão CGN*. Brasília, [s. d.]. Acesso em: 10 out. 2025.

ESTADÃO VERIFICA. *Como identificar e se proteger de golpes virtuais*. São Paulo, 2023. Disponível em: https://www.estadao.com.br/estadao-verifica/como-identificar-proteger-golpes-virtuais/?srsltid=AfmBOooe_9Wb0Qvbjo-LQoq70g3pfHNvc0c2VrLuslOFGWsk_f7JpLte. Acesso em: 11 out. 2025.

EUROPEAN DATA PROTECTION SUPERVISOR (EDPS). *Pseudonymous data: processing personal data while mitigating risks.* EDPS Blog, 2023. Disponível em: https://www.edps.europa.eu/press-publications/press-news/blog/pseudonymous-data-processing-personal-data-while-mitigating_en. Acesso em: 09 out. 2025.

IUBENDA. *A Lei de Proteção e Privacidade de Dados dos EUA (ADPPA): uma visão geral.* 2024. Disponível em: https://www.iubenda.com/pt-br/help/124064-a-lei-de-protecao-e-privacidade-de-dados-dos-eua-adppa-uma-visao-

geral#:~:text=O%20que%20%C3%A9%20a%20ADPPA%20(American%20Data%20Privacy%20Protection%20Act)%3F&text=Como%20lei%20federal%2C%20a%20ADPPA,ou%20a%20VCDPA%20da%20Virg%C3%ADnia. Acesso em: 11 out. 2025.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E TERRITÓRIOS (TJDFT). *Alerta para tentativa de golpes envolvendo supostos processos criminais do TJDFT.* Disponível em: https://www.tjdft.jus.br/institucional/imprensa/noticias/2022/marco/alerta-para-tentativa-de-golpes-envolvendo-supostos-processos-criminais-do-tjdft. Acesso em: 09 out. 2025.

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO (TRT-2). *Relembre alguns golpes praticados em nome da Justiça do Trabalho da 2ª Região.* Disponível em: https://ww2.trt2.jus.br/noticias/noticias/noticia/relembre-alguns-golpes-praticados-em-nome-da-justica-do-trabalho-da-2a-regiao-1. Acesso em: 10 out. 2025.

TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO (TRT-4). *Golpes aplicados em nome da Justiça do Trabalho: saiba como se proteger.* Disponível em: https://www.trt4.jus.br/portais/trt4/modulos/noticias/586046. Acesso em: 11 out. 2025.

UNIVERSIDADE FEDERAL DO CARIRI (UFCA). *Guia para técnicas básicas de anonimização de dados – LGPD.* Juazeiro do Norte, 2023. Disponível em: https://documentos.ufca.edu.br/wp-folder/wp-content/uploads/2023/08/Guia-para-T%C3%A9cnicas-B%C3%A1sicas-de-Anonimiza%C3%A7%C3%A3o-de-Dados-LGPD.pdf. Acesso em: 11 out. 2025.

FIALHO, Andrea Cristina de Sousa; SEABRA, Cláudia Pessoa Marques da Rocha. *O desafio da proteção de dados pessoais em publicações oficiais do sistema de justiça: equilibrando transparência e privacidade.* Revista Eletrônica do Ministério Público do Estado do Piauí, Teresina, ano 04, edição 02, jul./dez. 2024. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2025/02/11-O-desafio-da-protecao-de-dados-pessoais-em-publicacoes-oficiais-do-sistema-de-justica-equilibrando-transparencia-e-privacidade.pdf. Acesso em: 9 out. 2025.

O DIA. *Professora aposentada sofre prejuízo de R$ 300 mil com golpe do falso advogado.* O Dia, Rio de Janeiro, 8 out. 2025. Disponível em: https://odia.ig.com.br/rio-de-janeiro/2025/10/7142050-professora-aposentada-sofre-prejuizo-de-rs-300-mil-com-golpe-do-falso-advogado.html. Acesso em: 9 out. 2025.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS – TJDFT. *Golpe do falso advogado: TJDFT alerta usuários da Justiça sobre a fraude.* Brasília, 4 ago. 2025. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/noticias/2025/julho/golpe-do-falso-advogado-tjdft-alerta-jurisdicionados-sobre-fraude. Acesso em: 9 out. 2025.

ORDEM DOS ADVOGADOS DO BRASIL – OAB. *Golpe do falso advogado: plataforma ConfirmADV recebe quase 10 mil solicitações em três semanas.* Brasília, 23 maio 2025. Disponível em: https://www.oab.org.br/noticia/63100/golpe-do-falso-advogado-plataforma-confirmadv-recebe-quase-10-mil-solicitacoes-em-tres-semanas. Acesso em: 9 out. 2025.

CONSELHO NACIONAL DE JUSTIÇA – CNJ. *Em combate ao golpe do "falso advogado", CNJ inicia autenticação em dois fatores para usuários do PJe*. CNJ, 3 nov. 2025. Disponível em: https://www.cnj.jus.br/em-combate-ao-golpe-do-falso-advogado-cnj-inicia-autenticacao-em-dois-fatores-para-usuarios-do-pje/. Acesso em: 19 nov. 2025.

CONSELHO NACIONAL DE JUSTIÇA – CNJ. *PJe reforça segurança e permite identificação de assistentes de advogados com autenticação em dois fatores.* CNJ, 3 nov. 2025. Disponível em: https://www.cnj.jus.br/pje-reforca-seguranca-e-permite-identificacao-de-assistentes-de-advogados-com-autenticacao-em-dois-fatores/. Acesso em: 19 nov. 2025.

ORDEM DOS ADVOGADOS DO BRASIL – OAB. *OAB lança campanha nacional e plataforma de verificação contra 'golpe do falso advogado'*. Brasília, 29 abr. 2025. Disponível em: http://www.oab.org.br/noticia/63063/oab-lanca-campanha-nacional-e-plataforma-de-verificacao-contra-golpe-do-falso-advogado. Acesso em: 19 nov. 2025.

ACESSO E REGULAMENTAÇÃO DAS INFORMAÇÕES PÚBLICAS: OS IMPACTOS DA LEI 12.527/2011 NOS ATOS DE GESTÃO PÚBLICA

Luiz Arthur Batista de Figueiredo[1]
Max Efraim Bianchi Godoy[2]

RESUMO

O presente artigo visa avaliar como as decisões sobre pedidos de informações vieram a ser favoráveis aos solicitantes, quando os pedidos vieram a ser julgadas por instancias superiores que venham a compor a Administração pública. Além disto, este trabalho pretende compreender de que forma estas soluções favoráveis ao solicitante, definidas em instâncias superiores, podem vir a gerar efeitos concretos na organização interna e no fluxo de trabalho dos órgãos públicos. Deste modo, também buscamos demonstrar como a implementação da LAI, vem trazendo uma quebra dos paradigmas da cultura do sigilo, a muito tempo imposta e presente nas instituições públicas.

Palavras-chave: Internet; Lei de Acesso a Informação; Lei 12.527/2011; Recursos; Instâncias Superiores; Lei Geral de Proteção de Dados; Transparência Pública.

SUMÁRIO: 1. Introdução; 2. Acesso à informação, abertura governamental e fortalecimento das formas de participação cidadã; 2.1 Fundamentos constitucionais e normativos da transparência no Brasil.; 2.2 A LAI como Marco de Fortalecimento Democrático; 2.3 Transparência e Accountability; 2.3.1 Accountability como princípio democrático e prática institucional; 2.3.2 Transparência centrada na compreensão do cidadão; 3. A LAI e as etapas do processo recursal; 4. Visão crítica sobre o impacto da LAI nas instituições públicas; 5. Conclusão

1 INTRODUÇÃO

[1] Graduado em Superior de Tecnologia em Gestão Pública do UniProjeção - Centro Universitário Projeção.; Graduando em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: luizfigueiredo@sempreceub.com

[2] Graduando em Direito do Uniceub - Centro Universitário de Brasília. E-mail: maxefraim@sempreceub.com

A Lei nº 12.527, conhecida como Lei de Acesso à Informação (LAI), foi aprovada em 18 de novembro de 2011 e passou a valer no ano seguinte. Sendo assim, se faz necessária reflexão com mais profundidade os procedimentos e rotinas administrativas criadas a partir de sua aplicação, que agora já acontece continuamente por 13 anos. Além disso, o sistema recursal instituído pela própria lei funciona como uma garantia adicional ao direito de acesso, permitindo não apenas a consolidação de entendimentos, mas também a identificação de divergências interpretativas sobre seus dispositivos.

O foco deste estudo é avaliar aquilo que foi influenciado por decisões recursais. O propósito central é compreender de que forma soluções favoráveis ao solicitante, definidas em instâncias superiores, podem gerar efeitos concretos na organização interna e no fluxo de trabalho dos órgãos públicos.

A princípio, é necessário analisar conceitos essenciais vinculados ao debate sobre acesso à informação, como transparência, accountability e controle social, e analisa possíveis pontos de encontro entre essas noções e os avanços registrados no Brasil. Prosseguindo, são apresentados a LAI, seus principais dispositivos e o funcionamento do sistema de recursos, acompanhados da descrição do processo de classificação dos recursos examinados e dos resultados observados. Por fim, uma análise baseada em entrevistas com gestores públicos de diferentes ministérios, Relações Exteriores, Fazenda e Trabalho e Emprego, buscando identificar os efeitos práticos da adoção da LAI em suas rotinas institucionais.

2 O ACESSO À INFORMAÇÃO, TRANSPARÊNCIA GOVERNAMENTAL E O FORTALECIMENTO DAS FORMAS DE PARTICIPAÇÃO CIDADÃ.

A ampliação da transparência e a efetivação do acesso à informação constituem fatores indispensáveis tanto para o fortalecimento das instituições democráticas quanto para a melhoria da gestão pública. As informações produzidas, mantidas e administradas por órgãos e entidades em nome da sociedade configuram um verdadeiro patrimônio público. Nesse contexto, a Lei de Acesso à Informação representou um avanço expressivo ao garantir a todos os cidadãos o direito de

consultar dados registrados em documentos oficiais e ao incentivar a criação de mecanismos de divulgação, como os portais de transparência.

Apesar disso, ainda existem obstáculos significativos à consolidação da transparência prevista pela LAI. Um dos desafios mais persistentes é a superação da chamada "cultura do sigilo", ainda fortemente presente em diversas instituições públicas. Trata-se de uma transformação que exige mudanças de postura e comportamento, cujo amadurecimento tende a ocorrer de forma gradual. Assim, a existência de uma legislação assegurando o direito de acesso não basta, por si só, para garantir sua plena efetividade.

Nos últimos anos, observa-se um aumento expressivo no interesse acadêmico pelo tema do acesso à informação e da transparência governamental. A produção de estudos tem crescido em volume e diversidade, demonstrando a relevância e a atualidade desse campo de pesquisa.

2.1 Fundamentos constitucionais e normativos da transparência no Brasil.

No Brasil, o acesso à informação pública é reconhecido constitucionalmente como um direito fundamental, conforme estabelece o artigo 5º, inciso XXXIII da Constituição Federal[3]. Além disso, o artigo 37 do mesmo texto[4] determina que a administração pública deve pautar suas ações pelo princípio da publicidade. A LAI regulamentou esses dispositivos, estabelecendo normas de transparência e assegurando que qualquer pessoa possa solicitar e receber informações públicas de órgãos e entidades governamentais.

[3] Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes [...] XXXIII - Todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

[4] A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte [...].

A discussão sobre transparência no país ganhou destaque com a promulgação da Lei de Responsabilidade Fiscal (Lei Complementar nº 101/2000)[5], que introduziu instrumentos de controle das contas públicas, monitoramento da arrecadação e racionalização do uso dos recursos. A LRF desempenhou papel decisivo na ampliação da visibilidade da gestão fiscal, originando iniciativas como o Portal da Transparência, criado em 2004, e a Lei Complementar nº 131/2009[6], que determinou a divulgação em tempo real das informações orçamentárias e financeiras dos entes federados.

Mesmo com esses avanços, o debate nacional sobre transparência ainda se concentra de forma predominante na esfera orçamentária e financeira. Tais instrumentos representam, ao mesmo tempo, uma obrigação de prestação de contas por parte do Estado e um mecanismo essencial para que a sociedade acompanhe a aplicação dos recursos públicos. Embora muitas vezes marcados por linguagem técnica e de difícil compreensão, são ferramentas relevantes para o monitoramento fiscal. Contudo, a transparência pública não se limita à simples divulgação de dados, tampouco se confunde com o princípio constitucional da publicidade dos atos administrativos.

2.2 A LAI como marco de fortalecimento democrático

A promulgação da Lei de Acesso à Informação e sua implementação prática, ao estabelecer instrumentos que permitem a qualquer indivíduo solicitar e obter informações públicas de órgãos e entidades governamentais, configuram um marco importante para o fortalecimento do regime democrático. Esses mecanismos ampliam as possibilidades de participação cidadã e reforçam o controle social sobre a atuação do poder público.

A Lei de Acesso à Informação inovou ao estabelecer que cabe ao Estado assegurar o direito de acesso às informações públicas, devendo disponibilizá-las por meio de procedimentos claros, transparentes, céleres e expressos em linguagem

[5] BRASIL. Lei complementar n° 101, de 04 de maio de 2000. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp101.htm.
[6] BRASIL. Lei complementar n° 131, de 27 de maio de 2009. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp131.htm.

acessível ao cidadão, conforme art. 5º, Lei nº 12.527/2011[7]. A norma demonstra preocupação não apenas com a entrega da informação, mas também com a forma como ela é comunicada, incorporando a dimensão da compreensão como parte essencial da garantia de acesso.

Entretanto, como já mencionado, a existência de normas jurídicas não assegura, por si só, avanços no controle social e na participação democrática. Para que esses instrumentos se tornem efetivos, é necessário que a sociedade e os agentes públicos se apropriem deles, adotando práticas alinhadas ao interesse coletivo.

2.3 Transparência e accountability

Os conceitos de transparência pública e accountability são fundamentais para a análise proposta. Filgueiras observa que ambos ganharam relevância na teoria política contemporânea, mas muitas vezes são utilizados como sinônimos, apesar de possuírem distinções conceituais importantes. Para esse autor, ainda que a literatura não apresente consenso absoluto, accountability pode ser entendida como o princípio de agentes públicos prestarem contas de seus atos ao público.

> O princípio segundo o qual é dever de todos os agentes públicos prestarem contas de seus atos ao público, de forma que a sociedade possa avaliar não apenas a aplicação dos recursos públicos, mas também as ações e resultados alcançados por políticas, programas e ações propostas e implementadas pelos governos. (FILGUEIRAS, 2015, p. 10)

Essa compreensão amplia o alcance do controle social, que passa a incluir não somente o acompanhamento do gasto público, mas também a avaliação dos resultados concretos das políticas públicas. A accountability, nesse sentido, assume o papel de princípio orientador da atuação de gestores e cidadãos.

2.3.1 Accountability como princípio democrático e prática institucional

[7] BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Lei de Acesso à Informação. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

Segundo Filgueiras, a discussão conceitual precisa considerar dois elementos essenciais, o fortalecimento de uma concepção substantiva de democracia, em que a accountability funciona como princípio normativo, e sua operacionalização no âmbito das instituições políticas e das práticas sociais.

A partir dessa abordagem, o autor desenvolve uma avaliação das políticas de transparência, defendendo que elas constituem regra fundamental da administração pública para assegurar que os governos se tornem efetivamente responsáveis perante a sociedade. Assim, ainda que a transparência envolva a oferta de processos e informações sobre a ação governamental, a accountability vai além, exigindo que políticas, normas e diretrizes sejam executados dentro de padrões adequados de publicidade (FILGUEIRAS, 2011, p. 84)[8].

Dessa forma, accountability não se limita à prestação de contas ou à exposição dos gastos públicos. Trata-se também de garantir que as práticas governamentais sejam compreensíveis e possam ser examinadas pela sociedade.

2.3.2 Transparência centrada na compreensão do cidadão

A transparência pública, quando orientada ao fortalecimento da participação social, não equivale apenas à divulgação de dados. Ela pressupõe que as informações disponibilizadas sejam inteligíveis, dispensando a necessidade de especialistas para traduzi-las. Como destaca Gruman.[9]

> O acesso público à informação, ainda que primordial para a garantia de um Estado transparente e responsável, é instrumental no sentido de que os ganhos advindos das políticas de transparência governamental não se encerram em si mesmos, mas nos resultados trazidos por este tipo de política para a administração pública. A transparência e o acesso não garantem a eficácia do funcionamento da máquina pública, mas, pelo contrário, sua ausência é garantia de mau uso dos recursos públicos porque livres de controle social. O acesso à informação é um instrumento, um meio. (GRUMAN, 2012, p. 104)

[8] FILGUEIRAS, Fernando. Além da transparência: accountability e política da publicidade. Lua Nova, São Paulo, v.84, 2011.
[9] GRUMAN, Marcelo. Lei de Acesso à Informação: notas e um breve exemplo. Revista Debates, Porto Alegre, v. 6, n. 3, 2012.

No caso brasileiro, grande parte dos estudos sobre transparência e acesso à informação concentra-se na análise da implementação da LAI e no monitoramento de seu cumprimento. Há também investigações que discutem a relação entre o acesso à informação e iniciativas de governo eletrônico, bem como documentos governamentais que reúnem orientações e diagnósticos sobre a aplicação da LAI em todo o país.

Esse panorama inicial evidencia que grande parte da produção acadêmica tem priorizado a análise dos instrumentos de transparência a partir de sua contribuição para a efetivação da cidadania, concentrando-se no acesso à informação como um direito assegurado ao cidadão. O objetivo deste texto, contudo, é refletir sobre o modo como esse fornecimento de informações ocorre na prática.

A proposta aqui apresentada direciona o olhar para dentro das instituições públicas, buscando compreender como elas operam ao responder aos pedidos realizados pelos cidadãos. Esse atendimento, sobretudo quando envolve etapas recursais, não ocorre de maneira uniforme, automática ou padronizada na administração pública federal. A regulamentação do direito de acesso provocou impactos heterogêneos nas rotinas dos órgãos, transformando práticas diárias e introduzindo novos desafios.

Dessa forma, pretende-se identificar as possíveis repercussões da LAI no funcionamento administrativo, bem como as dificuldades e lacunas que emergem no enfrentamento da persistente “cultura do sigilo”, ainda fortemente presente em diversas organizações públicas.

3 A LAI E AS ETAPAS DO PROCESSO RECURSAL.

A norma apresenta diretrizes essenciais, a obrigatoriedade de divulgação de informações de interesse coletivo por meio da transparência ativa, o uso de ferramentas de comunicação viabilizadas pela tecnologia da informação, a definição de prazos e procedimentos para atendimento das solicitações, a criação de unidades específicas para atender o cidadão, e o estímulo tanto à cultura da transparência quanto ao controle social dentro da administração pública.

Insere-se, assim, no debate sobre o fortalecimento da transparência como mecanismo de aproximação entre Estado e sociedade, reforçando instrumentos de fiscalização cidadã. A LAI vai além do acompanhamento dos gastos públicos, ao incentivar a divulgação sistemática de informações de interesse geral, consolidando o acesso à informação como um dever estatal.

Compreende-se como transparência ativa a disponibilização espontânea de informações pelo poder público, sem que haja solicitação prévia, sendo o Portal da Transparência o exemplo mais representativo. Já a transparência passiva envolve o fornecimento de informações mediante requerimento dos interessados, como ocorre nos pedidos de acesso à informação feita diretamente a órgãos e entidades públicas.[10]

A abrangência da LAI, entretanto, acaba gerando dificuldades em sua regulamentação. Não há uniformidade entre os decretos regulamentadores nos estados e municípios. No âmbito federal, essa regulamentação se deu pelo Decreto nº 7.724, de 16 de maio de 2012.[11]

Embora a Lei tenha vigência nacional, o presente estudo concentra-se na análise de seus efeitos dentro da administração pública federal, sobretudo no que se refere às rotinas de gestão e aos procedimentos cotidianos dos órgãos, conforme já assinalado anteriormente.

A transparência, enquanto característica fundamental de uma gestão pública democrática exige o abandono de práticas tradicionais baseadas na ideia de que as informações produzidas pelo Estado lhe pertencem exclusivamente. Essa mudança de postura requer o desenvolvimento de métodos que assegurem eficiência, eficácia e efetividade na gestão da informação, em consonância com os princípios de uma administração orientada para o interesse público. Informações produzidas e mantidas para uso restrito, quando organizadas de forma inadequada, tendem a não atender

[10] Gov.br. Disponível em: https://www.gov.br/acessoainformacao/pt-br/lai-para-sic/transparencia-passiva
[11] BRASIL. Decreto n° 7,724, de 16 de maio de 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm

aos requisitos necessários para a efetivação do direito de acesso (ROCHA, 2012, p. 91-92)[12].

É inegável que a implementação da LAI trouxe desafios significativos à administração pública. A questão inicial deste estudo foi identificar em que medida a Lei alterou rotinas internas, procedimentos administrativos e práticas de gestão documental. O processo recursal previsto na LAI, descrito nos artigos 15 a 20, estabelece que, diante da negativa de acesso, o cidadão dispõe de dez dias para recorrer à autoridade imediatamente superior àquela que respondeu o pedido. Caso a resposta permaneça insatisfatória, o requerente poderá dirigir-se à autoridade máxima do órgão. Se ainda assim não houver solução, é possível recorrer à Controladoria-Geral da União e, posteriormente, à Comissão Mista de Reavaliação de Informações, esgotando-se todas as etapas de deliberação.

A apresentação de recursos no âmbito da Lei de Acesso à Informação constitui um direito assegurado ao cidadão. Quando a Controladoria-Geral da União concede provimento ao recurso, não existe a possibilidade de o órgão ou entidade pública contestar essa decisão perante a Comissão Mista de Reavaliação de Informações. O sistema recursal estabelecido pela LAI atribui à CGU a competência para determinar que os órgãos da administração pública federal prestem esclarecimentos ou forneçam as informações solicitadas. A Controladoria-Geral da União atua como a instância responsável por analisar as negativas de acesso proferidas por órgãos federais (Art. 16 da Lei nº 12.527/2011 e Art. 23 do Decreto nº 7.724/2012).

4 VISÃO CRÍTICA SOBRE O IMPACTO DA LAI NAS INSTITUIÇÕES PÚBLICAS

Como vimos ao longo do trabalho, o surgimento da Lei de Acesso à Informação, em 2011, representou um marco fundamental para a democratização da Gestão Pública no Brasil. Pois mesmo tendo enfrentada resistências iniciais, derivadas de uma cultura histórica de sigilo, baixa participação popular e limitações

[12] ROCHA, Heloisa Helena Nascimento. Transparência e accountability no Estado Democrático de Direito: reflexões à luz da Lei de Acesso à Informação. **Revista do TCEMG**. Edição Especial: Transparência e controle social. Belo Horizonte, 2012.

tecnológicas, a LAI inaugurou uma nova era dentro da Administração Pública, estabelecendo a transparência como regra e o sigilo como exceção.

Logo após sua implementação, pesquisas identificaram certas dificuldades, tais como: falta de padronização das informações, resistência de servidores, ausência de treinamentos e deficiência tecnológica nos órgãos públicos. Mesmo assim, os mesmo estudos evidenciaram que a lei, começou a estimular a modernização dos sistemas de divulgação, o uso de portais eletrônicos, o controle social e o acesso mais amplo a dados governamentais. A LAI também impactou positivamente diversas áreas do setor público: fortaleceu o combate à corrupção ao permitir maior fiscalização das ações governamentais, melhorou a prestação de contas por parte dos governantes, ampliou a participação popular nas decisões públicas e induziu uma mudança cultural em direção a práticas mais transparentes e democráticas.

Com o tempo, a transparência evoluiu ainda mais com a chegada da LGPD, que veio a complementar a LAI ao definir limites para proteção de dados pessoais, sem eliminar a obrigatoriedade de divulgar informações públicas de interesse coletivo. Muitos estudos destacam que LAI e LGPD são instrumentos complementares, não conflitantes, onde juntas fortalecem uma governança mais clara, segura e voltada ao cidadão.

Entretanto, apesar das conquistas que surgiram em decorrencia da aplicação das novas normas, ainda restam desafios importantes, desde a necessidade de uma padronização nacional que venha a permitir acesso a documentos que costumeiramente são divulgados impedindo assim a divulgação em certos casos e a não divulgação em outros, investimentos tecnológicos que permitam conferir a coerência dos documentos, treinamento contínuo dos servidores públicos responsáveis pela a gestão dos documentos, melhoria de portais eletrônicos e superação de resistências políticas e culturais.

Apesar desses obstáculos, a LAI começou a produzir efeitos positivos importantes. Ela fortaleceu o combate à corrupção ao permitir maior fiscalização social, favoreceu o controle das ações governamentais, melhorou a prestação de contas e incrementou a participação popular na discussão e acompanhamento das políticas públicas. A lei também induziu mudanças culturais dentro das instituições,

promovendo uma compreensão mais clara do dever de transparência e ampliando a disponibilidade de informações relevantes, como dados sobre gastos públicos, folha de pagamento e despesas do Legislativo. Com o surgimento da Lei Geral de Proteção de Dados, consolidou-se uma fase de ajustes necessária para equilibrar o direito de acesso à informação com a proteção de dados pessoais. Embora alguns órgãos tenham utilizado indevidamente a LGPD para negar acesso a informações públicas, a relação entre as duas leis é complementar: a LAI garante transparência e a LGPD protege a privacidade, resultando em um modelo mais robusto de governança pública.

Em análises recentes, observou-se que a informatização crescente e o uso ampliado de meios digitais aumentaram a capacidade de divulgação, mas exigiram maior cuidado com a qualidade das informações, padronização dos dados, acessibilidade dos portais e combate à desinformação. As pesquisas também revelam avanços em áreas como universidades públicas, sistema judiciário, municípios e o Sistema Único de Saúde, embora ainda persistam desigualdades significativas na implementação da LAI, especialmente no nível municipal. Onde podemos resumir que como surgimento da LAI houve a promoção de transformações profundas na administração pública brasileira, ampliando a transparência, fortalecendo a democracia e promovendo um maior engajamento da sociedade no controle das ações estatais. Contudo, permanecem desafios importantes, como a necessidade de padronização nacional, investimentos em tecnologia, capacitação contínua dos servidores, prevenção ao uso indevido da LGPD e superação de resistências culturais e políticas.

Deste modo, ainda é obvio o impacto nos organizações públicas: a LAI transformou o modo de funcionamento das instituições públicas, aproximou o Estado da sociedade e se consolidou como ferramenta essencial para a transparência pública e para a consolidação da democracia brasileira.

5. CONCLUSÃO

Deste modo, podemos verificar que os avanços nas políticas públicas fomentam a transparência pública no Brasil, onde os seus resultados são visíveis e

altamente significantes, entretanto, ainda se torna necessário investir significativamente para que possamos romper com a cultura de sigilo que ainda persiste nas organizações públicas. Ao mesmo tempo, torna-se essencial garantir a preservação dos sigilos que são permitidos e protegidos legalmente, tais como o fiscal, o bancário e os dados pessoais.

A diversidade de temas e a variação das decisões observadas na análise dos recursos evidenciam a falta de uma padronização no tratamento dos pedidos de acesso à informação entre os diferentes órgãos da administração pública. Em muitos dos casos, solicitações que são idênticas foram atendidas por alguns órgãos e negadas por outros.

Acreditamos que as transformações decorrentes da Lei de Acesso à Informação (LAI) na gestão pública devem ser analisadas sob múltiplos ângulos. Por isso, as entrevistas precisam incluir servidores do Serviço de Informação ao Cidadão (SIC), profissionais das áreas técnicas mais demandadas, equipes responsáveis pelo tratamento das informações e pela gestão documental, entre outros atores envolvidos.

Além disso, ao avaliarmos os impactos da implementação da LAI na administração pública pode gerar resultados relevantes para impulsionar iniciativas inovadoras. Essa análise pode revelar arranjos institucionais mais eficientes, bem como novas metodologias de aplicação da legislação, a partir da identificação de boas práticas e do mapeamento de fragilidades.

O panorama construído a partir da análise dos recursos apresentados com base na LAI evidencia uma administração pública diversa, com ampla variedade de demandas e interpretações. Pois para que a legislação de acesso à informação seja aplicada de forma consistente e saudável, é essencial aprimorar os canais de comunicação dentro e entre as Instituições Públicas. Pois o compartilhamento de experiências vem a fortalecer os mecanismos de acesso à informação e promover mudanças estruturais nos códigos de conduta institucional. Dessa forma, abre-se um conjunto de possibilidades de análise a partir do panorama sintetizado neste texto.

REFERÊNCIAS

BRASIL. *[Constituição (1988)]. Constituição da República Federativa do Brasil de 1988.* Brasília, DF: Presidente da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 nov. 2025.

BRASIL. *Decreto n.º 7.724, de 16 de maio de 2012.* Regulamenta a Lei de Acesso à Informação. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm. Acesso em: 18 nov. 2025.

BRASIL. *Lei Complementar n.º 101, de 04 de maio de 2000.* Estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp101.htm. Acesso em: 18 nov. 2025.

BRASIL. *Lei Complementar n.º 131, de 27 de maio de 2009.* Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp131.htm. Acesso em: 18 nov. 2025.

BRASIL. *Lei n.º 12.527, de 18 de novembro de 2011.* Lei de Acesso à Informação. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 18 nov. 2025.

FILGUEIRAS, Fernando. *O fortalecimento das instituições de accountability do Brasil: relatório final do projeto.* (mimeo), 2015.

FILGUEIRAS, Fernando. Além da transparência: accountability e política da publicidade. *Lua Nova*, São Paulo, n. 84, p. 65–92, 2011.

GOV.BR. *Transparência Passiva.* Disponível em: https://www.gov.br/acessoainformacao/pt-br/lai-para-sic/transparencia-passiva. Acesso em: 18 nov. 2025.

GRUMAN, Marcelo. Lei de Acesso à Informação: notas e um breve exemplo. *Revista Debates*, Porto Alegre, v. 6, n. 3, p. 263–270, 2012.

O “PL DA DEVASTAÇÃO” E O USO DE DADOS

Giovana Brito Carrijo Costa[1]
Laís Carla Conceição Bezerra[2]
Marina Lara Parreira[3]
Pedro Henrique de Souza Mertins[4]
Lorena Portilho Bruno[5]

RESUMO

O presente artigo analisa o Projeto de Lei nº 2.159/2021, popularmente nomeado “PL da Devastação”, interdisciplinarmente, à luz da ótica jurídica, ambiental e econômica. Busca-se compreender as alterações propostas pelo projeto, avaliando o impacto do uso de dados no processo de licenciamento ambiental simplificado. Utilizando-se da revisão bibliográfica relativa à dados ambientais, almeja-se verificar as possíveis consequências da aprovação do referido projeto. Conclui-se que, com sua aprovação, o PL, que tem objetivo de facilitar o licenciamento ambiental, utiliza-se da agilidade e eficiência. Contudo, teme-se que gere efeito contrário, com a fragilização de dados, além de outros prejuízos nos âmbitos políticos, sociais, econômicos e ambientais.

Palavras-chave: Projeto de Lei nº 2.159/2021. “PL da Devastação”. Dados ambientais. LGPD. LAI.

SUMÁRIO: INTRODUÇÃO. 1. REFERENCIAL TEÓRICO; 1.1 Contexto Histórico e Processo do Licenciamento Ambiental; 1.2 Direito Digital e Governança de Dados; 1.3 Lei Geral de Proteção de Dados e o papel dos Dados Ambientais e Públicos; 1.4 Lei de Acesso à Informação - LAI; 2. PERSPECTIVA DA ANÁLISE JURÍDICA; 2.1 Impactos do PL sobre a Transparência Digital; 2.2 Conflitos entre o PL e a LGPD; 2.3 Dados sob ataque: entre a desinformação e a manipulação; 2.4 Ocultação ou restrição de dados ambientais; 3. PERSPECTIVA DA ANÁLISE

[1] Graduanda em Direito do UniCEUB - Centro Universitário de Brasília. E-mail: giovana.bcarrijoc@sempreceub.com
[2] Graduanda em Direito do UniCEUB - Centro Universitário de Brasília. E-mail: lais.carlab@sempreceub.com
[3] Graduanda em Direito do UniCEUB - Centro Universitário de Brasília e graduanda em Ciências Econômicas na Universidade de Brasília. E-mail: marina.lara@sempreceub.com
[4] Graduando em Direito do UniCEUB - Centro Universitário de Brasília. E-mail: pedro.mertins@sempreceub.com
[5] Graduanda em Agronomia da UNB - Universidade de Brasília. E-mail: lorenaportilhobruno@gmail.com

ECONÔMICA; 3.1 Matriz de Riscos; 3.2 Análise de Impacto Regulatório (AIR); CONCLUSÕES; REFERÊNCIAS.

1 INTRODUÇÃO

O Projeto de Lei nº 2.159/2021, popularmente conhecido como "PL da Devastação", tem gerado inúmeras discussões no meio jurídico, político e ambiental brasileiro. O nome, carregado de críticas, expressa a preocupação de ambientalistas, juristas e pesquisadores com os possíveis retrocessos que a proposta pode trazer para a política nacional de licenciamento ambiental. Embora o texto se apresente como uma tentativa de modernizar e simplificar os processos de autorização de atividades econômicas, muitos vêem nele um risco de redução da transparência, enfraquecimento da fiscalização e aumento da degradação ambiental, além da possibilidade de uso inadequado de informações públicas.

Dentro desse cenário, um ponto ganha destaque: o uso e a circulação de dados ambientais e pessoais. O projeto prevê a criação de sistemas digitais voltados à tramitação e integração dessas informações, o que significa lidar com um volume cada vez maior de dados sensíveis. Esse aspecto exige uma análise cuidadosa à luz de duas importantes leis: a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados e a Lei nº 12.527/2011 - Lei de Acesso à Informação. Ambas tratam da forma como o Estado e as instituições devem usar, proteger e divulgar informações, buscando um equilíbrio entre transparência pública e resguardo da privacidade.

A relação entre o referido Projeto de Lei e essas duas normas mostra um desafio importante: como garantir que as informações ambientais sejam acessíveis à sociedade, sendo esta uma condição essencial para a participação e o controle social, sem colocar em risco dados pessoais ou sensíveis. É justamente nesse ponto que este artigo se propõe a atuar, unindo o Direito Ambiental e o Direito Digital para entender como o tratamento de dados no licenciamento ambiental pode afetar tanto o direito à informação quanto o direito à privacidade.

O objetivo central é analisar os impactos do Projeto de Lei nº 2.159/2021 sobre a transparência, a proteção de dados e o acesso à informação, discutindo se o modelo proposto promove o uso ético e responsável dos dados ou se, na prática,

pode representar um retrocesso. Parte-se da ideia de que a regulação clara e equilibrada do uso de dados, sejam eles ambientais ou pessoais, é essencial para fortalecer a gestão ambiental democrática e manter a confiança da sociedade nas instituições públicas.

Em resumo, defende-se que a utilização de dados deve ser guiada pela transparência, pela responsabilidade e pelo respeito às normas de proteção e acesso à informação, conforme os princípios de publicidade e supremacia do poder público da Lei de Acesso à Informação - LAI e princípios de transparência, segurança e responsabilidade da Lei Geral de Proteção de Dados - LGPD, para que a busca por agilidade e eficiência no licenciamento ambiental não se transforme em perda de controle, retrocessos ou fragilização da governança ambiental e digital no país.

2 REFERENCIAL TEÓRICO

2.1 Contexto Histórico e processo do Licenciamento Ambiental

Inicialmente, conforme a atual Constituição Federal de 1988 (DOU, 1988), em seu Capítulo VI, do Título VIII, denominado “Do Meio Ambiente”, define-se o meio ambiente ecologicamente equilibrado como direito de todo cidadão em seu Artigo 225, impondo ao poder público e à coletividade o dever de defendê-lo e preservá-lo. Contudo, a degradação ambiental e o consequente acesso ao dito ambiente ecologicamente equilibrado muitas vezes não é atingido, ora por uma tendência ainda difusionista do setor agrosilvopastoril, ora por um licenciamento ambiental cada vez mais flexível.

Historicamente, como consequência da tendência política e pressão internacional trazida com a Declaração de Estocolmo, consolidada em 1972 (Costa; Costa, 2022) a política ambiental brasileira foi ativamente impactada pelo regramento ambiental, ainda que a tendência do regime estivesse aliado ao difusionismo e a dita “revolução verde”, que promoveu tecnificação e interiorização da agricultura, principalmente no ramo agroexportador (Neto; Charão-Marques, 2023).

Após a Declaração de Estocolmo, em 1973, foi criada a Secretaria Especial de Meio Ambiente (SEMA) como instituição federal responsável por conduzir as políticas ambientais, todavia, sem a formalização de um Licenciamento Ambiental e com um sistema obsoleto de controle através de denúncias, sujeito à falhas de impacto socioambientais e de caráter econômico, sem devida fiscalização, conforme Costa e Albuquerque (2021).

Ademais, quase 10 anos depois urge-se a necessidade de obter um regime jurídico capaz de frear a ação antrópica e os impactos socioeconômicos gerados. Portanto, instituiu-se a Política Nacional do Meio Ambiente (PNMA) por meio da Lei Federal nº 6.938/1981, um marco inicial importante de proteção jurídica e da soberania ambiental brasileira, superando a tutela dispersa e fragmentada entre os entes federativos.

Através do PNMA foi consolidado o Sistema Nacional do Meio Ambiente (SISNAMA), instrumento da referida Lei Federal, organizando a gestão ambiental com estrutura descentralizada e com participação ativa entre entes federativos, in verbis:

> Art 6º - Os órgãos e entidades da União, dos Estados, do Distrito Federal, dos Territórios e dos Municípios, bem como as fundações instituídas pelo Poder Público, responsáveis pela proteção e melhoria da qualidade ambiental, constituirão o Sistema Nacional do Meio Ambiente - SISNAMA, assim estruturado:
>
> I - Órgão Superior: o Conselho Nacional do Meio Ambiente - CONAMA, com a função de assistir o Presidente da República na formulação de diretrizes da Política Nacional do Meio Ambiente;
>
> II - Órgão Central: a Secretaria Especial do Meio Ambiente - SEMA, do Ministério do Interior, à qual cabe promover, disciplinar e avaliar a implantação da Política Nacional do Meio Ambiente;
>
> III - Órgãos Setoriais: os órgãos ou entidades integrantes da Administração Pública Federal, direta ou indireta, bem como as fundações instituídas pelo Poder Público, cujas entidades estejam, total ou parcialmente, associadas às de preservação da qualidade ambiental ou de disciplinamento do uso de recursos ambientais;
>
> IV - Órgãos Seccionais: os órgãos ou entidades estaduais responsáveis pela execução de programas e projetos e de

> controle e fiscalização das atividades suscetíveis de degradarem a qualidade ambiental;
>
> V - Órgãos Locais: os órgãos ou entidades municipais responsáveis pelo controle e fiscalização dessas atividades, nas suas respectivas áreas de jurisdição.

O processo de Licenciamento Ambiental em si, tem como principal objetivo a proteção socioambiental em caso de empreendimentos de grande impacto, conforme (). Segundo a mesma Lei, define-se como grandes empreendimentos os projetos de rodovias de faixas duplas ou triplas, rodovias de portos e aeroportos, mineradoras e empreendimentos agrosilvopastoris (MMA, 2016).

Conforme o disposto na Lei, o processo é divido em três fases ordinárias: Licença Prévia (LP), Licença de Instalação (LI) e Licença de Operação (LO), previstas também na Resolução CONAMA 237/1997. A princípio, torna-se necessário a execução do Estudo de Impacto Ambiental e Relatório de Impacto Ambiental (EIA/RIMA), que determinarão o tipo de impacto do local a ser utilizado. Após análise pelos órgãos fiscalizadores, as licenças serão documentadas e publicadas em Diário Oficial pelo órgão ambiental competente.

Ainda que teoricamente o processo de Licenciamento pareça ser controlado e efetivamente cumprido segundo as normativas vigentes, há uma constante fragilização acerca da transparência, proteção de dados e acesso à informação dos empreendedores impactantes. Como evidenciado nos acidentes envolvendo as barragens de rejeitos minerais em Brumadinho, que, segundo a CPI (Brasil, 2023), as expansões das barragens da empresa VALE S.A. não possuíam EIA/RIMA para comprovar o estudo dos impactos ambientais, sociais e econômicos, contradizendo com todos os princípios da Lei de Acesso à Informação, Lei Geral de Proteção de Dados e principalmente da lei 6.938/81.

Além disso, com o advento do Projeto de Lei 2.159/2021 (Brasil, 2021), há o temor acerca da flexibilização da Legislação Ambiental vigente. Segundo o PL, entre as principais implicações estão a dispensa de licenciamento para atividades de agricultura, pecuária, silvicultura e obras de infraestrutura, consideradas de alto impacto pela Resolução CONAMA 237/1997. Ainda, com o novo PL, pretende-se instituir a Licenças por Adesão e Compromisso (LAC) como forma de “auto-licenciamento” via internet, eliminando análise prévia de órgãos fiscalizadores.

No âmbito do Direito Digital, torna-se ainda mais preocupante pela proposta de restrição da participação de autarquias ambientais, como a FUNAI e ICMBio e da sociedade civil, ferindo gravemente os princípios instituídos pela LAI e LGPD, presentes nos Artigos 3º e 21º da PL. Sem mais, a proposta fere, também, a soberania alimentar e nutricional, afetando diversas políticas públicas conquistadas com a participação popular, como as Leis nº 12.188/2010 (PNATER) e nº 11.326/2006 (Política Nacional de Agricultura Familiar e Empreendimentos Familiares Rurais).

Apesar do sancionamento da PL com vetos aos principais trechos lesivos às normativas e políticas públicas vigentes em agosto de 2025, realizado pelo atual presidente Luiz Inácio Lula da Silva, a Frente Parlamentar Agropecuária (FPA), braço direito da Bancada Ruralista, instituiu uma Medida Provisória (MP 1.308/2025) recuperando os vetos realizados por meio de uma ação coordenada entre parlamentares, com histórica quantidade de emendas enviadas.

A Frente Parlamentar Agropecuária, conforme site próprio, principal interessada no PL da Devastação, foi fundada inicialmente como Frente Ampla Ruralista até 1994, de forma informal. Contudo, em 1995 foi efetivamente fundada e renomeada como FPA em 2008. A princípio, a FPA mobilizou-se para garantir aos grandes empreendedores do agronegócio o “direito à propriedade rural”, que hoje traduz-se como a garantia de tomada de terras de origem dos povos originários, que nunca foram efetivamente regulamentados de forma abrangente.

Atualmente, a FPA está intimamente ligada aos interesses da agropecuária exportadora e da mineração, campeões em impacto ambiental, destacando-se por trabalhos de “modernização” da legislação fundiária e tributária e regulamentação da questão indígena e quilombola. Portanto, a PL da Devastação é de grande interesse para a articulação com o lobby empresarial para agravar o neoextrativismo brasileiro.

2.2 Direito Digital e Governança de Dados

A princípio, é indispensável definir o conceito de direito digital. Este é um novo ramo do Direito, que se ocupa da normatização das relações jurídicas que se desenvolvem por meio das tecnologias da informação.

> O Direito Digital ou Direito Informático é o conjunto de normas e instituições jurídicas que pretendem regular aquele uso dos sistemas de computador - como meio e como fim - que podem incidir nos bens jurídicos dos membros da sociedade; as relações derivadas da criação, uso, modificação, alteração e reprodução do software; o comércio eletrônico e as relações humanas estabelecidas via Internet (PAIVA, 2019, p 18).

Sua pertinência na realidade contemporânea é inegável, considerando a dependência da utilização dos meios virtuais[6] criada a partir das facilidades trazidas por ele, como a rápida comunicação e conexão entre dados. É certo que, o momento atual está marcado pela digitalização de serviços, coleta e tratamento massivo de dados.

Nesse contexto, surgiram novos desafios, tais como, normas para coleta, limites para o tratamento, garantia da privacidade e transparência, além da responsabilização dos agentes que gerem danos a partir dessas atividades. Diante disso, o Direito Digital[7] se propõe a solucionar essas questões, buscando acompanhar a inovação tecnológica e ao mesmo tempo proteger as garantias fundamentais, utilizando-se de legislações como a Lei Geral de Proteção de Dados – Lei nº 13.709/2018 e a Lei de Acesso à Informação – Lei nº 12.527 para isso.

Em especial, quanto às políticas públicas, este ramo em ascensão têm um papel fundamental. Considerando que para o planejamento e execução destas se faz

[6] O virtual permite a existência legítima do estar "não-presente". Do manifestar-se por intermédio de sistemas de comunicação telemática através de encontros móveis e transitórios de mensagens, com a desconexão em relação a um meio particular, com diversos meios de registro e transmissão oral, escrita e audiovisual em redes digitais. (PECK, Patrícia, 2009, p 17).

[7] O Direito Digital possui todas as características para ser considerado uma disciplina autônoma, justificando a sua posição através de três argumentos: possui um objeto delimitado, qual seja a própria tecnologia, dividido em duas partes, sendo a primeira o objeto mediato, ou seja, a informação, e o segundo o objeto imediato, ou a tecnologia; a existência de uma metodologia própria, a qual visa possibilitar uma melhor compreensão dos problemas derivados da constante utilização das novas tecnologias da informação (informática) e da comunicação (telemática); tal tarefa se realiza mediante o uso de um conjunto de conceitos e normas que possibilitam a resolução dos problemas emanados da aplicação das novas tecnologias às atividades humanas; a existência de fontes próprias, ou seja, fontes legislativas, jurisprudenciais e doutrinárias; não havendo como negar a existência dessas fontes no âmbito do Direito Digital; foi justamente a existência de ditas fontes que possibilitaram, em um grande número de 8 países, principalmente os mais desenvolvidos, a criação da disciplina do Direito Digital nos meios acadêmicos (ALVES, Marcelo de Camilo Tavares. Direito Digital. Goiânia, 2009. p, 9-10).

necessário o tratamento de dados sensíveis, é imperioso que se imponham medidas de governança de dados à administração pública, a fim de garantir a qualidade dos dados, segurança e os direitos dos titulares.

A LGPD (Lei nº 13.709/2018) é uma das normas que se encarregou de estabelecer as mencionadas medidas de governança, especialmente, por meio de seus princípios dispostos nos incisos de seu art. 6º, *in verbis:*

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
>
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
>
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
>
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
>
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
>
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
>
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
>
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de

> proteção de dados pessoais e, inclusive, da eficácia dessas medidas

Destaca-se os princípios da finalidade, adequação, necessidade, que visam assegurar a segurança e a confiança no tratamento dos dados, já que garante a privacidade de seus titulares.

Em aparente conflito, a LAI (Lei nº 12.527/2011) impõe as obrigações de publicidade e transparência, garantindo o acesso à informação pública, servindo como mecanismo de controle social. Contudo, esse aparente antagonismo entre privacidade e transparência pode ser interpretado como uma oportunidade para reduzir assimetrias informacionais e promover o equilíbrio entre direitos fundamentais. A harmonização entre LGPD e LAI é, portanto, essencial para a construção de uma governança digital ética, eficiente e democrática.

Por fim, esclarece-se que, de acordo com Silva e Oliveira (2020), os dados ambientais são "informações sistematizadas que representam atributos físicos, químicos e biológicos do ambiente natural ou modificado, coletadas com o objetivo de subsidiar ações de gestão ambiental e políticas públicas sustentáveis". Dessa forma, estes também são dados tratáveis, devendo seguir-se o disposto na LGPD e LAI, a fim de promover a segurança e publicização adequada.

2.3 Lei Geral de Proteção de Dados e o papel dos dados ambientais e públicos

A gestão contemporânea do meio ambiente no Brasil depende cada vez mais de grandes volumes de dados ambientais públicos , imagens de satélite, GIS (Geographic Information Systems), mapas de uso do solo, alertas de desmatamento entre outros. Porém, esse uso intensivo desses dados levanta tensões entre dois direitos fundamentais: transparência e acesso à informação e privacidade, proteção de dados pessoais e garantia de direitos de comunidades vulneráveis. A LGPD e a LAI operam como instrumentos legais centrais nesse cenário.

Conforme o art. 5º da LGPD, dados pessoais são informações relativas à pessoa natural identificada ou identificável. São considerados dados pessoais sensíveis aqueles que revelam origem racial ou étnica, convicções religiosas, opinião

política, filiação sindical, dado genético ou biométrico, dados relativos à saúde ou à vida sexual, entre outros (Lei nº 13.709/2018). A LGPD também prevê a figura do dado anonimizado, que não permite a identificação do titular mediante uso de meios técnicos razoáveis (art. 5º, §1º).

Embora os dados ambientais, em si, não sejam dados pessoais, eles frequentemente são associados a informações que permitem a identificação de pessoas, como localização de propriedades, limites de terra e titulares de posses. Nesse sentido, a LGPD se aplica indiretamente quando esses dados ambientais se cruzam com dados pessoais ou territorialidades identificáveis.

Nas comunidades indígenas, quilombolas e ribeirinhas, dados geográficos (coordenadas de aldeias, rotas tradicionais) e culturais podem revelar informações sensíveis e estratégicas. Se esses dados forem tratados sem cuidado, podem ser instrumento de vigilância, perseguição ou discriminação de lideranças e ativistas.

De acordo com levantamento divulgado pelo portal Achados e Pedidos, "em mais de uma ocasião, a Funai admitiu não dispor de dados estruturados a respeito do monitoramento e fiscalização de territórios indígenas" (ACHADOS E PEDIDOS, 2021). Diante dessa omissão institucional, organizações da sociedade civil têm assumido papel fundamental na produção e sistematização de informações. O Conselho Indigenista Missionário (Cimi), por exemplo, reportou 277 casos de violência direta contra pessoas indígenas em 2019, além de um aumento de 135% nos registros de invasões possessórias, exploração ilegal de recursos naturais e danos ao patrimônio no mesmo período (CIMI, 2020).

Esses dados demonstram a relevância da atuação das entidades não estatais na promoção da transparência e na proteção dos direitos socioambientais, especialmente em contextos de omissão ou insuficiência de informações por parte do poder público.

2.4 Lei de Acesso à Informação - LAI

A Lei de Acesso à Informação fundamenta-se em princípios essenciais que orientam sua aplicação:

Transparência ativa: obrigação dos órgãos públicos de divulgar informações de interesse coletivo ou geral, independentemente de solicitações (art. 8º da LAI);Transparência passiva: direito de qualquer pessoa de solicitar informações específicas, que devem ser fornecidas no prazo legal, salvo em casos de sigilo legalmente previsto (art. 10 da LAI); Publicidade: as informações devem ser disponibilizadas de forma acessível, clara e em linguagem de fácil compreensão, promovendo a ampla divulgação (art. 8º da LAI); e Eficiência: os órgãos públicos devem adotar procedimentos objetivos e ágeis para garantir o acesso à informação (art. 5º da LAI).

Esses princípios são fundamentais para a construção de uma gestão pública democrática, permitindo o controle social e a fiscalização das ações governamentais.

O acesso a informações sobre licenciamento ambiental é considerado um direito fundamental, essencial para a proteção do meio ambiente e para a garantia de direitos das comunidades afetadas por empreendimentos. A Lei Complementar nº 140/2011, que estabelece normas para a cooperação entre União, Estados, Municípios e Distrito Federal na proteção do meio ambiente, reforça a necessidade de transparência nos processos de licenciamento ambiental.

Segundo o artigo 2º da LAI, é dever do Estado garantir o direito de acesso à informação, que será franqueado mediante procedimentos objetivos e ágeis, de forma transparente. Isso inclui a divulgação de documentos e informações relativas a políticas, planos, programas e projetos que possam causar impacto ambiental. A redução da transparência dificulta o controle social e aumenta o risco de danos ambientais não mitigáveis.

3 PERSPECTIVA DA ANÁLISE JURÍDICA

3.1 Impactos do PL sobre a transparência digital

Ainda que teoricamente o processo de Licenciamento pareça ser controlado e efetivamente cumprido segundo as normativas vigentes, há uma constante fragilização acerca da transparência, proteção de dados e acesso à informação dos empreendedores impactantes.

Como evidenciado nos acidentes envolvendo as barragens de rejeitos minerais em Brumadinho, que, segundo a CPI (Brasil, 2023), as expansões das barragens da empresa VALE S.A. não possuíam EIA/RIMA para comprovar o estudo dos impactos ambientais, sociais e econômicos, contradizendo todos os princípios da Lei de Acesso à Informação, Lei Geral de Proteção de Dados e principalmente da lei 6.938/81.

Além disso, com o advento do Projeto de Lei 2.159/2021 (Brasil, 2021), há o temor acerca da flexibilização da Legislação Ambiental vigente. Segundo o PL, entre as principais implicações estão a dispensa de licenciamento para atividades de agricultura, pecuária, silvicultura e obras de infraestrutura, consideradas de alto impacto pela Resolução CONAMA 237/1997. Ainda, com o novo PL, pretende-se instituir a Licenças por Adesão e Compromisso (LAC) como forma de "auto-licenciamento" via internet, eliminando análise prévia de órgãos fiscalizadores.

Conforme Parecer Técnico sobre o PL da devastação, elaborado por Luis E. Sánchez (USP) e Alberto Fonseca (UFOP), infere-se que o PL 2.159/2021 não soluciona os problemas do licenciamento ambiental no Brasil e gera maior insegurança jurídica, reduzindo o controle sobre práticas que causam degradação ambiental e ameaçando a efetividade do processo licenciatório.

Segundo o parecer, os redatores do PL desconhecem a base teórica da formulação de políticas públicas no Brasil. Segundo o texto do projeto, destacam-se o artigo 5º, § 2º, que amplia a possibilidade de definição de licenças específicas por atos normativos, verbis:

> § 2º Sem prejuízo das disposições desta Lei, tendo em vista a natureza, as características e as peculiaridades da atividade ou do empreendimento, podem ser definidas licenças específicas por ato normativo dos entes federativos competentes, de acordo com a Lei Complementar nº 140, de 8 de dezembro de 2011.

Tal trecho torna-se contraditório com a proposição do projeto, que pretende flexibilizar normativas com argumentos de agilização dos processos de licenciamento. Todavia, demonstram agravamento da fragmentação entre os entes federativos por falta de normas gerais na própria proposta. Além disso, as regulações do CONAMA já decidem por meio da autoridade licenciadora.

Além disso, nos trechos contidos nos artigos 29 e 31, que discorrem diretamente sobre a base de dados e integração de sistemas de informação, há uma dissonância com esses acessos à informações. Conforme o Parecer Técnico, há limitações quanto ao reaproveitamento de dados provenientes do SISNAMA de empreendimentos existentes, não sendo estabelecidos a quem cabe essa função. Ainda, destaca-se que não há previsão ou menção de recursos humanos e financeiros para organização e manutenção das bases de dados, portanto não é clara a garantia de acesso público e gratuito.

No que concerne ao Artigo 33, o PL discorre que cabe à autoridade licenciadora a disponibilização em sítio eletrônico próprio os pedidos de licenciamento recebidos, posterior aprovação, rejeição ou renovação e estudos ambientais, porém destaca com o Artigo 34 que as informações que integram o Licenciamento são de natureza pública. Outrossim, é importante pontuar que tais dados não abrangem pareceres de órgãos fiscalizadores ou relatórios de monitoramento e acompanhamento, evidenciando ruídos quanto à efetiva transparência nos procedimentos legais.

No âmbito do Direito Digital, torna-se ainda mais preocupante pela proposta de restrição da participação de autarquias ambientais, como a FUNAI e ICMBio e da sociedade civil, ferindo gravemente os princípios instituídos pela LAI e LGPD, presentes nos Artigos 3º e 21º do PL. Sem mais, a proposta fere, também, a soberania alimentar e nutricional, afetando diversas políticas públicas conquistadas com a participação popular, como as Leis nº 12.188/2010 (PNATER) e nº 11.326/2006 (Política Nacional de Agricultura Familiar e Empreendimentos Familiares Rurais).

Adicionalmente, o Supremo Tribunal Federal (STF), na ADI 5014, decidiu que a Licença por Adesão e Compromisso deve ser restrita a atividades de baixo impacto ambiental, incompatível com a ampliação proposta no PL, o que implica sérios riscos para a fiscalização e prevenção de danos ambientais.

Apesar do sancionamento do PL com vetos aos principais trechos lesivos às normativas e políticas públicas vigentes em agosto de 2025, a Bancada Ruralista instituiu uma Medida Provisória (MP 1.308/2025) recuperando os vetos realizados

por meio de uma ação coordenada entre parlamentares, com histórica quantidade de emendas enviadas.

A Bancada Ruralista, principal interessada no PL da Devastação, foi fundada inicialmente como Frente Ampla Ruralista até 1994, de forma informal. A princípio, a Bancada mobilizou-se para garantir aos grandes empreendedores do agronegócio o "direito à propriedade rural", que hoje traduz-se como a garantia de tomada de terras de origem dos povos originários, que nunca foram efetivamente regulamentados de forma abrangente. À exemplo, a Bancada Ruralista foi a principal articuladora política do PL 2.903/2023, tese acerca do Marco Temporal, mesmo após a instituição de inconstitucionalidade pelo Supremo Tribunal Federal, em 2023.

A defesa do "direito à propriedade rural" baseia-se na restrição dos direitos indígenas com uma tese jurídica de que a demarcação sob posse indígena a partir da promulgação da Constituição Federal, em 1988, funcionando como uma estratégia de segurança jurídica e ampliação de terras ao agronegócio, enfraquecendo direitos primários constituintes do artigo. 231 da CF.

Atualmente, a Bancada está intimamente ligada aos interesses da agropecuária exportadora e da mineração, campeões em impacto ambiental, destacando-se por trabalhos de "modernização" da legislação fundiária e tributária e regulamentação da questão indígena e quilombola. Portanto, a PL da Devastação é de grande interesse para a articulação com o lobby empresarial para agravar o neoextrativismo brasileiro, evidenciado pelo histórico de defesa de pautas inconstitucionais e difusas.

Esses fatos e análises acadêmicas reforçam que o PL 2.159/2021 representa não uma solução para o licenciamento ambiental, mas um retrocesso que ameaça não só a proteção ambiental, os direitos socioambientais e a segurança jurídica, como o acesso à transparência e publicidade por parte da sociedade civil e interessados.

3.2 Conflitos entre o PL e a LGPD

Conforme discutido nas seções anteriores, há uma aparente e conflituosa relação entre o PL da Devastação e a LGPD. A divulgação sem critérios claros viola

o direito à autodeterminação e à proteção de dados sensíveis segundo normativa da LGPD, conforme Art. 2º, 5º, 7º e 11º, *in verbis*:

> Art. 2º – Finalidade da LGPD: A disciplina da proteção de dados pessoais tem como fundamentos: I – o respeito à privacidade; II – a autodeterminação informativa; III – a liberdade de expressão, de informação, de comunicação e de opinião; IV – a inviolabilidade da intimidade, da honra e da imagem; V – o desenvolvimento econômico e tecnológico e a inovação; VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.
>
> Art. 5º, II – Definições Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
>
> Art. 7º – Hipóteses de tratamento de dados pessoais: O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I – mediante o fornecimento de consentimento pelo titular; II – para o cumprimento de obrigação legal ou regulatória pelo controlador; (...) §1º O tratamento posterior dos dados pessoais poderá ser realizado para novas finalidades, desde que observados os princípios e as bases legais, e que seja informado ao titular.
>
> Art. 11 – Tratamento de dados sensíveis: O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I – quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; (...) §1º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes a interesses discriminatórios ilícitos ou abusivos.

Conforme interpretação da Lei, o inciso II do artigo 2º expressa de forma clara o poder do titular de controlar o fluxo de suas informações, sendo uma violação a divulgação de dados sem critérios claros ou base legal. Em consonância com os artigos 5º e 7º, os dados pessoais sensíveis, sobretudo quando relacionado ao

contexto ambiental, considerando comunidades impactadas (quilombolas, indígenas e/ou assentados), deve-se manter o nível máximo de proteção se considerarmos a informação constante na Nota Técnica ANPR nº 003/2024-UC (2024). No contexto da PL da Devastação, a relação entre a segurança de dados traz consigo diversas informações acerca do modo de vida, localização territorial, saúde ou vínculos comunitários.

Inclusive por meio do art. 7º em seu §4º, possibilitando a "renovação automática" das licenças, sem análise prévia necessária, bastando somente a autodeclaração do empreendedor. Tal dispositivo torna o pleno acesso à informação como limitado e/ou omisso, fragilizando diversas normativas distintas: o artigo 23 da Constituição Federal (Brasil, 1988), o artigo 4º da PNMA (Brasil, 1981) e principalmente os princípios de boa-fé, qualidade de dados, transparência e responsabilização, presentes na LAI e LGPD.

Ainda, consoante com a Audiência Pública do Conselho Nacional dos Direitos Humanos (CNDH) acerca do PL da Devastação (2025), as medidas propostas violam o direito à consulta prévia, livre e informada e consentimento dos povos e comunidades tradicionais, prevista e assinada pelo Brasil a Convenção 169 da OIT, podendo gerar ruídos no acesso à informação de áreas de conflitos fundiários.

Ao simplificar ou eliminar etapas de consulta pública e manifestação de entes federativos, tem-se uma limitação ao acesso de comunidades tradicionais e comunidades locais que possam ser impactadas por empreendimentos de alto impacto, dificultando novamente a manifestação e fragilizando o controle social, ferindo o art. 2º da LGPD supracitado e expressando ainda mais as desigualdades e conflitos fundiários.

Adicionalmente, A Lei Geral de Proteção de Dados (LGPD), em seu artigo 4º, inciso II, alínea "a" (Brasil, 2018), estabelece que a lei não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de proteção do meio ambiente, quando conduzido por órgãos competentes. No entanto, essa exclusão do escopo do tratamento de dados pessoais pode ser equivocadamente utilizada como justificativa para restringir o acesso a informações de interesse público, sob o

pretexto de proteção de dados pessoais. Tal interpretação distorce o equilíbrio previsto na LGPD, que busca proteger a privacidade sem impedir a transparência e o controle social sobre questões ambientais fundamentais. Portanto, é essencial um entendimento adequado que harmonize a proteção dos dados pessoais com a garantia do acesso à informação ambiental.

3.3 Dados sob ataque: entre a desinformação e a manipulação

Vivemos em uma era em que os dados têm um papel central na forma como entendemos o mundo. Eles orientam decisões, moldam opiniões e influenciam políticas públicas. No entanto, no contexto ambiental, esses mesmos dados também podem ser distorcidos, ocultados ou usados de forma seletiva para justificar interesses econômicos ou políticos. É o que se observa no debate em torno do Projeto de Lei nº 2.159/2021, o chamado "PL da Devastação", onde informações técnicas e científicas são frequentemente apresentadas de forma parcial para sustentar a ideia de que o licenciamento ambiental seria apenas um entrave burocrático ao desenvolvimento.

Esse tipo de manipulação acontece, muitas vezes, por meio do uso de dados incompletos, enviesados ou fora de contexto. Por exemplo, números sobre a demora na concessão de licenças costumam ser destacados, enquanto se omitem dados sobre os impactos ambientais cumulativos, a perda de biodiversidade e os riscos sociais de projetos aprovados sem estudos adequados. Assim, cria-se uma narrativa de eficiência e progresso, que ignora as consequências ambientais e sociais de longo prazo. O resultado é uma espécie de "discurso de aparência técnica", em que dados passam a ser usados não para informar, mas para convencer.

As plataformas digitais amplificam esse problema. Em redes sociais, informações complexas são transformadas em frases curtas, gráficos simplificados ou vídeos virais, muitas vezes sem qualquer rigor técnico. É o terreno fértil da desinformação ambiental, em que estudos científicos são descontextualizados e opiniões ganham o mesmo peso que evidências. Esse fenômeno, conhecido como fake news ambiental, influencia o debate público e enfraquece o papel das instituições científicas, gerando confusão e descrédito em torno da própria ciência.

Nesse cenário, a proteção de dados e o combate à desinformação estão profundamente conectados. A Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI) não tratam apenas de sigilo e privacidade: elas também são instrumentos para garantir que os dados públicos sejam verdadeiros, acessíveis e utilizados de forma ética. A integridade das informações ambientais é fundamental para que o cidadão possa distinguir os dados científicos de narrativas manipuladas, e assim, participar de forma consciente nas decisões que afetam o meio ambiente.

Proteger os dados, portanto, vai muito além da segurança digital. É também proteger a verdade, a ciência e a democracia ambiental. Quando dados são distorcidos, não é apenas a informação que se perde, mas também a capacidade da sociedade de agir de forma justa e sustentável. Em tempos de tanta polarização e de ataques à ciência, cuidar da qualidade e da transparência dos dados é, em última instância, cuidar do próprio meio ambiente.

3.4 Ocultação ou restrição de dados ambientais

A gestão de dados ambientais vem enfrentando restrições e ocultações, justificadas por argumentos políticos ou econômicos que não tomam como princípio basilar a transparência pública, enfraquecendo o controle social. O Projeto de Lei nº 2.159/2021 é um expoente disso, uma vez que propõe a flexibilização do licenciamento ambiental.

Medidas como as propostas no referido projeto colaboram para favorecer interesses econômicos de curto prazo, como o avanço de empreendimentos em áreas sensíveis, em detrimento da proteção ambiental e dos direitos coletivos. Contudo, segundo Ugeda (2024), a má administração ou a supressão deliberada de informações ambientais configura uma forma de necropolítica institucional, na qual o Estado escolhe quais territórios e populações serão expostos à degradação ambiental por meio da invisibilização de dados relevantes.

O relatório da Data Privacy Brasil (2023) corrobora o exposto. Segundo análise, o enfraquecimento da transparência está diretamente ligado à dificuldade de contestar projetos como o PL 2.159/2021. Isso porque, conforme apresentado, esse

projeto pretende reduzir exigências documentais, acarretando a diminuição da qualidade e, portanto, a segurança das informações prestadas. Assim, com a ausência de dados confiáveis e acessíveis a avaliação dos impactos, a possibilidade de propor alternativas e exigir responsabilização fica prejudicada.

Ainda há a necessidade de analisar o "PL da devastação" sob a óptica do preceito fundamental de ao acesso à informação, disposto no art. 5º, inc. XIV da Constituição Federal, bem como da Lei de Acesso à Informação - Lei nº 12.527, que operacionaliza o referido direito ao garantir a publicidade e transparência quanto aos dados públicos.

Em suma, a transparência quanto aos dados ambientais é um direito que permite a análise, questionamento e influência sobre decisões quanto à utilização de territórios e consequências na saúde pública. Dificultar o acesso a eles empobrece a possibilidade de análise e debate público, representa, ainda, um retrocesso à democracia, na medida em que cerceia um preceito fundamental, e uma ameaça à justiça socioambiental e ao direito ao futuro.

4 PERSPECTIVA DA ANÁLISE ECONÔMICA

O intuito de realizar uma análise econômica é mensurar a análise de impacto que uma determinada decisão pode ter a longo prazo. Há no âmbito técnico a diferenciação entre uma análise ex-ante (anterior à medida) e uma análise ex-post (posterior à implementação), no presente artigo, o intuito é realizar uma análise ex-ante, uma vez que o PL ainda não entrou em vigor. A estruturação de uma pesquisa ex-ante tem como base fundamental avaliar as consequências potenciais de alguma medida e facilitar o monitoramento da mesma após um estudo técnico prévio (IPEA, 2022). Neste caso, busca-se compreender qual o possível impacto caso o PL seja aprovado, tendo como lente a proteção dos dados e acesso à informação.

A primeira vertente de análise aqui abordada pode ser em relação à dispensa de licenciamento às propriedades registradas no Cadastro Ambiental Rural e aderentes ao Programa de Regularização Ambiental. A dispensa do licenciamento às propriedades que se encaixem no disposto no Art. 9 do Projeto de Lei em questão

apresenta um risco potencial muito grande de redução ao acesso à informação, uma vez que a necessidade de licenciamento é uma forma de estabelecer vínculos e critérios de monitoramento das propriedades no país. Em 2022, dados mais recentes disponíveis, o Brasil tinha cerca de 6,48 milhões de cadastros no CAR (Brasil, 2022) . Um segundo ponto de atenção é o fato de que o PL abre muito espaço para a subjetividade dizer o que vai ou não ser fiscalizado pelas autoridades, pois determina que serão fiscalizadas de forma ativa, pois para muitos casos, bastará a autodeclaração dos proprietários.

Além do já elencado, a relação entre o PL da Devastação e as leis de informação possui fundamentos muito mais profundos e níveis de consequências potenciais diferentes, assim, para uma análise ex-ante satisfatória, a presente seção se dividirá em duas metodologias de análise ex-ante: Matriz de Riscos e Análise de Impacto Regulatório (AIR). A combinação das duas metodologias permite um panorama completo que envolve aspectos quantitativos e qualitativos da medida.

4.1 Matriz de riscos

A análise de uma matriz de riscos consiste na avaliação de um risco e seu potencial impacto levando em consideração as partes afetadas, a gravidade de sua consequência e a sua probabilidade de acontecimento. A Organização Internacional de Normalização (ISO) elaborou um guia de gestão de riscos que será utilizado como base para esboçar a matriz do presente artigo, assim, seguindo às orientações, a matriz deverá conter: partes afetadas, origem do risco, evento adverso, possíveis consequências, probabilidade e controle do risco. (ISO, 2018)

Assim, conforme as diretrizes, a primeira análise a ser feita é pontuar qual o risco, isto é, o efeito concreto que gera a preocupação. Ao pontuar esse ponto de partida, será possível analisar suas ramificações de forma mais direta e aprofundada para cada tipo de acontecimento. Destaca-se aqui que uma análise de matriz de risco não se restringe a efeitos negativos, no entanto, como o intuito do presente artigo é apresentar as fragilidades e preocupações acerca da proteção de dados com a nova legislação, o documento, por questões de objetividade, se reservará aos impactos negativos previamente pontuados. Assim, para estruturar a matriz em questão, serão

utilizados os riscos apontados na seção denominada análise interdisciplinar, sendo eles diminuição da transparência, violação do direito de autodeterminação, aumento da vulnerabilidade de dados sensíveis, distorção e manipulação de dados e ocultação de dados relevantes (violação direta da LAI). Em seguida, busca-se encontrar quais são as proteções do dispositivo que tentam evitar os riscos apresentados. Em seguida, realiza-se a pesquisa quanto às partes interessadas, chamado no modelo base de stakeholders e, no cenário em que a situação se estabelece, temos dois polos principais a serem afetados por decisões do setor, os produtores que deverão seguir os novos normativos e o agente fiscalizador, que com a nova política deverá reorganizar seus custos de forma a se adequar ao novo modelo regulatório. Após delimitar esses fatos iniciais, aponta-se qual a origem do risco, seja ela uma fragilidade na legislação, algum tipo de manifestação concreta ou outra possível lacuna. Dando prosseguimento, aponta-se qual o evento adverso, isto é, um acontecimento representa a materialização do risco pontuado, complementando essa descrição com as suas consequências e a probabilidade de sua ocorrência. Por fim, encerra-se a matriz de riscos com a elaboração de um controle, isto é, caso esse risco venha a se concretizar, quais são as medidas que poderão ser tomadas para ao menos mitigar seus impactos. Para consultar a versão otimizada, em formato de tabela, vide Anexo I do presente trabalho.

O primeiro risco a ser analisado é a preocupação mais eminente do assunto abordado, isto é, a diminuição na transparência de dados ambientais. Neste caso, a principal ferramenta preventiva é a Lei de Acesso à Informação e os artigos 29, 31, 33 e 34 do próprio PL, que versam acerca do tratamento e natureza das informações envolvidas em seus processos. Os principais stakeholders são as os produtores e empresas sujeitas à mudança de legislação, pela mudança no procedimento, os órgãos fiscalizadores, pela necessidade de adaptação na forma de realizar o monitoramento e organização de dados armazenados e a própria sociedade civil, por estar sujeita aos potenciais riscos aqui pontuados. A principal preocupação reside em 5 pontos principais, em primeiro lugar, a dispensa de licenciamento para determinados tipos de projeto, o que levanta um alerta para projetos de alto potencial lesivo que podem adquirir estas dispensas. Em segundo lugar está a introdução da possibilidade de auto-licenciamento pela modalidade da LAC, já explicada

previamente no presente trabalho. O terceiro risco refere-se à alteração procedimental envolvida no PL, isto é, troca de sistemas de monitoramento e armazenamento, o que implica em um risco de perda informacional se o processo não for devidamente conduzido. Em quarto lugar estão as preocupações referentes à ambiguidade de normativos já citada, acerca da responsabilidade sobre os dados e, por fim, acende-se o alerta acerca da restrição da participação de autarquias ambientais no processo decisório e desenvolvedor dos projetos.

Assim, com os principais desdobramentos associados ao primeiro risco, passa-se a segunda parte da análise, os possíveis eventos adversos relacionados a cada desdobramento, considerando suas consequências, probabilidade de ocorrência e potenciais ferramentas de controle em caso de ocorrência. O primeiro evento adverso avaliado é a impossibilidade de acesso à dados de projetos que deixaram de ser obrigatórios com a dispensa do licenciamento, aqui aponta-se a principal fragilidade, pois tal flexibilização faz parte da estrutura do PL e permite a construção de delimitações de segurança ambiental ambíguas, além da redução da participação popular no desenvolvimento destas obras e da redução de margem de controle público pela redução informacional. Como o PL ainda não entrou em vigor, uma mensuração exata se torna um pouco complexa, entretanto, com o atual nível de fiscalização e exigências, a ocorrência de irregularidades já é expressiva, e essa flexibilização é uma porta de entrada para ainda mais irregularidades, que serão ainda menos fiscalizadas e divulgadas. Conforme estudo apresentado em 2020 pela Diretoria de Proteção Ambiental do Ibama, o Brasil apresenta expressivos números de delitos ambientais, principalmente quanto ao descumprimento de condicionantes de licenciamento, o classificando como um problema de alta prioridade (Brasil, 2020). Assim, tendo em vista dados anteriores, é possível estabelecer uma hipótese cautelosa de que há uma alta probabilidade que a flexibilização servirá como uma legitimação de irregularidades e aumento da ocorrência desses delitos. Nessa mesma linha está o segundo desdobramento, pois o autolicenciamento abre portas para fraudes informacionais que facilitam a ocultação de irregularidades, agora menos fiscalizadas, neste caso, o principal controle envolve a fiscalização e efetiva punição posteriores às autorizações.

O terceiro evento adverso é a possível extinção dos dados, pois a mudança regulatória altera os dados a serem controlados e, aqui já tecendo um paralelo com o quarto evento adverso, há uma insegurança jurídica quanto a responsabilidade sobre esses dados que pode gerar decisões conflitantes no judiciário e no procedimento da LAI. Assim, aqui analisam-se duas consequências principais, primeiramente, a perda de bases de dados por erros na transferências de sistema, que, atualmente por conta dos avanços em tecnologia e integração, possui uma probabilidade relativamente baixa, apesar de seu alto potencial lesivo, por representar uma expressiva redução do acervo histórico muito usado no desenvolvimento de políticas públicas, neste caso, o principal está na reorganização de sistemas e, em caso de perdas de dados, novas avaliações para a reconstrução das bases perdidas. Em segundo lugar está relacionada à insegurança jurídica gerada pelos dispositivos ambíguos, que pode levar a um aumento do contencioso nesta área e, considerando a característica litigante do cenário brasileiro, especialmente na área ambiental e agropecuária, há uma alta probabilidade de que esse risco se concretize, pois, conforme divulgado pelo CNJ, dentre os 5 maiores litigantes, 2 estão diretamente relacionados ao que é regulamentado pelos licenciamentos, sendo eles Confederação da Agricultura e Pecuária do Brasil (CNA), a Federação da Agricultura e Pecuária do Estado de SC (Faesc) (Brasil, 2022). Assim, o principal controle relacionado à esta segunda consequência reside na reformulação por processo legislativo para esclarecer estas ambiguidades ou a construção de uma jurisprudência clara de forma a reduzir o número de casos judicializados. O quinto e último evento adverso relacionado a este primeiro risco é a aprovação de projetos sem a participação de instituições como a Funai e o ICMBIo, assim, há uma redução da preocupação ambiental, além da perda de acesso à informações por fontes confiáveis por parte da população, como essa restrição também é prevista na própria estrutura do PL da Devastação, a probabilidade da redução participativa dessas autarquias é alta e a melhor forma de controle é tentar permitir a consulta posterior desses institutos aos projetos, para ao menos disponibilizar as informações necessárias.

O segundo risco mensurado refere-se à violação do direito de autodeterminação, muito resguardado pelo compromisso firmado pelo Brasil na Convenção 169 da Organização Internacional do Trabalho (OIT). Neste caso, as

principais partes interessadas são os polos comuns entre os riscos, isto é, produtores e órgãos fiscalizadores, mas também figuram como stakeholders aqui as Comunidades Tradicionais que potencialmente serão impactadas pelas mudanças regulatórias previstas. A origem desse risco reside na possibilidade de renovação de licenças sem consulta prévia ou participação das Comunidades Tradicionais no processo e, consequentemente, ausência de consulta pública. Assim, o principal evento adverso aqui é o caso de renovação automática de um projeto que autorize atividade lesiva ao meio ambiente ou comunidades tradicionais existentes no local do projeto, o que pode ocasionar expressivas perdas sociais e ambientais, além de acentuar conflitos fundiários ao colocar essas comunidades em uma posição extremamente vulnerável pela impossibilidade de participação nas decisões. Mais uma vez, a previsão de tais mecanismos na própria estrutura do PL, sob falsa justificativa de celeridade processual representa uma alta chance de concretização desses riscos por sua previsão materialmente expressa. Assim, nos casos desse tipo de violação, a principal saída é a alteração desse dispositivo para que, ao menos seja prevista uma auditoria externa para garantir a consulta desses polos, além de uma maior atenção para averiguar denúncias de violações e disponibilização de amparo às comunidades fragilizadas em caso de aprovação de projeto lesivo.

O terceiro risco reside no aumento da vulnerabilidade de dados sensíveis, protegidos pela LGPD e pela Nota Técnica ANPR nº 003/2024-UC . Aqui, figuram como stakeholders os órgãos fiscalizadores e as comunidades tradicionais, pois a origem principal do risco reside na distorção de dados e exposição de dados pessoais das comunidades tradicionais sem o devido embasamento legal por meio da distorção de normativos como a não aplicabilidade da LGPD a casos relacionados à proteção do meio ambiente para privilegiar interesses privados. Esse acontecimento tem como principal consequência à exposição dessas comunidades à uma situação de vulnerabilidade ao divulgar informações como localização e modo de vida e isso se concretiza pelo aumento da possibilidade de invasões e movimentações irregulares para a expulsão dessas comunidades tendo como objetivo a expansão do agronegócio. Assim, as principais ferramentas de controle em caso de vazamento de dados são medidas de conscientização e interpretação coerente da norma de forma a

conscientizar a todos sobre a sensibilidade dessas informações além de suporte às comunidades vulneráveis de modo a protegê-las de possíveis pressões ilícitas.

Em seguida, analisa-se o quarto risco, caracterizado pela distorção e manipulação de dados. A divulgação parcial e tendenciosa de informações fere a garantia de amplo acesso previsto pela LAI e tem como principais partes interessadas os proprietários de projetos regulamentáveis, os órgãos fiscalizadores e a própria sociedade civil como um todo. O presente evento adverso tem como principal consequência a perda de capacidade de manifestação ampla da sociedade além da formação de ideais incompletos e tendenciosos que, em último caso, podem influenciar em casos com manipulações eleitorais. A preocupação com a integridade dos dados e seu impacto no âmbito eleitoral á é uma pauta relevante no país e não é restrita somente ao cerne do direito ambiental, inclusive, a expressividade desse tipo de risco é tanta que há um Projeto de Lei tramitando com urgência no legislativo, o PL 2630/2020, ou, Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, que busca, justamente regulamentar a divulgação de informações para evitar manipulações eleitorais. Assim, apesar de muitos critérios subjetivos estarem envolvidos, como a capacidade de divulgação e alcance das mídias e o senso crítico do receptor da informação, a velocidade com a qual se acessa informação atualmente e o notório interesse político do assunto tornam esse tipo de manipulação um risco com probabilidade média de incidência. Assim, no caso de distorções amplamente divulgadas, o principal controle a ser feito é a divulgação de contrapartidas, isto é, promoção efetiva das informações completas em busca da segurança da transparência e amplitude de informações previstas na LAI.

Para encerrar, analisa-se o risco de ocultação de dados relevantes, violação direta do instrumento preventivo instituído pela LAI, que tem como stakeholders os órgãos fiscalizadores, as empresas sujeitas ao PL e a própria sociedade civil. Neste caso, o risco se origina na flexibilização na exigência de documentos e informações para obtenção de licenciamentos ambientais, que pode culminar no evento adverso concretizado pela aprovação de um projeto sem o devido rigor técnico. A maior preocupação é quanto à análise deste projeto a longo prazo, pois, com a maior flexibilizaçãode exigências, pode ser que se torne impossível a constatação de informações acerca do projeto aprovado justamente pela inexistência de documentos

comprobatórios, especialmente em relação a conformidade com proteções ambientais. Essa redução na base de consulta é também um importante risco social, pois restringe a possibilidade de inclusão pública em pautas importantes como a proteção de direitos ambientais e sociais de povos afetados. Quanto à probabilidade da ocorrência desse risco, por sua origem ser materialmente prevista, isto é, parte expressa do PL, pode-se deduzir que ela é relativamente alta, pela concretude de sua origem e nesse caso, o melhor controle é a construção de um mecanismo de cobrança plausível para que seja possível preencher essas lacunas mesmo após a aprovação do projeto, em conformidade com a LAI.

4.2 Análise de Impacto Regulatório (AIR)

A AIR é uma metodologia ex-ante muito comum e bem fundamentada no âmbito da análise econômica e serve para elencar potenciais consequências, gastos com políticas e ver se seu custo-benefício é efetivo. Para ser considerada bem sucedida, a AIR deve se iniciar desde a fase de concepção da norma, identificar claramente o problema e os objetivos desejados da proposta, bem como identificar e avaliar todas as soluções alternativas possíveis, incluindo aquelas que não envolvam regulamentação, deve-se sempre buscar avaliar todos os custos e benefícios potenciais, tanto diretos quanto indiretos, baseando-se em todas as evidências disponíveis e no conhecimento científico especializado. Além disso, o processo deve ser desenvolvido de forma transparente junto aos interessados, e os resultados devem ser claramente comunicados. (OCDE, 2020). Assim, conforme as diretrizes da OCDE, esta seção do texto será dedicada à desenvolver uma AIR consistente do PL 2.159/2021.

O primeiro passo para a construção de uma boa AIR é captar os interesses e pontos de vista dos stakeholders. Idealmente, em uma Análise Regulatória realizada pelo próprio governo, isso seria realizado por meio de uma consulta direta, no entanto, no âmbito universitário, esse contato direto não é disponível, portanto, este preparo da análise será realizado com base em posicionamentos públicos acerca do tema. O primeiro posicionamento que auxilia a base do impacto regulatório é o da FUNAI, que explicita os riscos envolvidos com as comunidades tradicionais, em

relação a estes stakeholders evidencia-se um interesse com a preservação dos territórios e a preocupação com a diminuição de sua rede protetiva. Assim, o segundo ponto é o próprio argumento por trás da aprovação do Projeto de Lei estudado no presente artigo (BRASIL, 2025)

O segundo passo de uma AIR, que envolve o segundo e o terceiro passo, é pontuar qual o centro do problema a ser abordado pela solução que está sendo analisada e explicitar qual é o objetivo da política apresentada. Neste caso, o PL surge com o intuito de simplificar procedimentos e gerar celeridade processual sob a justificativa de muitos entraves e atrasos vinculados ao regime até então vigente. A intenção do PL é reduzir o volume de peticionamentos e licenciamentos, que, em 2022 alcançavam a margem média de cerca de seis milhões e meio de projetos cadastrados no Cadastro Ambiental Rural (CAR). Entretanto, a premissa de simplificação deve ser lida com muitas ressalvas especialmente pelos riscos à elas agregados, conforme previamente detalhado na matriz de risco desenvolvida no presente artigo. Nesta segunda etapa, em caso de elaboração por órgãos oficiais, a mensuração é mais minuciosa e se dá de forma mais quantitativa com o levantamento dos dados orçamentários, ou seja valores afetados pela regulação vigente, no entanto, há nível universitário, sem amplo acesso à esse tipo de base, limita-se à análise a um panorama geral do assunto.

Em seguida, apresenta-se a estrutura detalhada da proposta, identificando seu rascunho, neste caso, o próprio PL, o corpo administrativo por ela responsável, algo que, conforme mencionado não está completamente claro, no entanto, extrai-se do texto que os registros permanecem sob responsabilidade pública, por meio do CONAMA. Além disso, é necessário apresentar o regime de implementação e qual a estratégia que será aplicada para garantir compliance. Quanto a essa quarta etapa, defende-se no projeto que ele apenas aprimora os mecanismos vigentes atualmente e, a principal ferramenta está centralizada na obrigatoriedade do licenciamento ambiental para a concessão de crédito, além das repercussões penais e administrativas como forma de incentivo ao cumprimento da legislação, como a aplicação de multa e possível julgamento por crimes ambientais em casos mais sérios.

O quinto passo é levantar as principais alternativas, mesmo que não regulatórias, para solucionar o problema apontado, isto é, neste caso, uma suposta rigidez na legislação vigente e uma lentidão processual devido ao extenso processo burocrático. Assim, ao invés de reduzir as exigências ambientais, realizar reformas somente administrativas, de forma a melhor alocar os recursos, focando em um aumento da velocidade de análise e a otimização dos procedimentos, além disso, a ideia de permitir maior autonomia na renovação de projetos não é de toda ruim, de forma ao inverter o sentido da procura, assim, o empresário deve ir atrás dos órgãos para regularizar sua situação, não o sentido oposto, no entanto, sem reduzir ou flexibilizar exigências de segurança ambiental e de dados. Assim, reformula-se apenas o processo, não a legislação em si. Na sétima etapa, retoma-se essa análise de forma a pontuar o porquê dessa escolha regulatória ser mais vantajosa do que as alternativas apresentadas e, conforme a análise discorrida no presente artigo, sugere-se que não foi realizada uma AIR prévia, especialmente porque diversos riscos foram desconsiderados e não houve transparência pública em relação aos impactos orçamentários da medida, entretanto, na tentativa de cumprir com uma AIR tradicional, realiza-se a abstração de que a medida foi preferível às outras porque o modelo vigente já estava defasado e perpetuá-lo apenas traria mais gastos a longo prazo, assim, a melhor decisão seria de fato reformular todo o processo.

Em sexto lugar, realiza-se a análise quantitativa de custo e benefício, e, conforme previamente mencionado, no âmbito universitário não se tem acesso claro a estas bases de dados, porém é possível realizar uma abstração do que está sendo pontuado, sendo assim, como principais custos elenca-se os custos diretos com ajustes de sistema e metodologias de fiscalização para adequar-se ao novo sistema, isto é, reajustar as plataformas e capacitar os funcionários acerca da nova legislação. Outro custo agregado é o custo de fiscalização, pois, com maior flexibilidade na obtenção de licenciamentos, para manter um mesmo nível de segurança ambiental, a fiscalização à posteriori deverá ser reforçada. Quanto aos benefícios, indica-se supostamente um enxugamento da linha processual e o potencial crescimento econômico pela maior liberdade dos empresários e maior facilidade de instituir um novo projeto.

Por fim, o último passo de uma AIR é delimitar como será analisada a performance da medida adotada a longo prazo e já antecipar quais serão os dados necessários para manter esse controle, neste caso, dois parâmetros devem ser analisados para o PL 2159/2021. Primeiramente, o volume de licenciamentos, para acompanhar se o PL efetivamente contribuiu para o desenvolvimento de novos projetos e, em segundo lugar, deve ser monitorado o número de irregularidades apontadas, bem como casos de violações ambientais, de forma a aferir qual o verdadeiro impacto da nova legislação.

5 CONCLUSÕES

Deste modo, por meio do presente artigo foi possível pontuar como o PL da Devastação se apresenta como um projeto de alto risco para a sociedade brasileira, não só pelo potencial destrutivo em relação ao meio ambiente mas também pelo risco de violação à proteção de dados sensíveis e também ao amplo acesso da população aos dados referentes aos projetos submetidos à essa legislação.

Ao realizar a análise do desenvolvimento histórico do projeto fica claro que há uma pressão de grandes empresários para a flexibilização das normas e não há uma devida preocupação com as consequências que a norma proposta poderá trazer, assim o intuito do artigo foi esclarecer alguns desses pontos de forma a ressaltar a importância de uma análise multidisciplinar ao aprovar uma mudança regulatória tão brusca quanto a proposta pelo PL 2159/2021. Com a perspectiva da análise econômica foi possível compreender de forma mais precisa a origem de cada um desses riscos, que se pautam principalmente na flexibilização de normas ambientais e procedimentos para obtenção de licenciamento sem se preocupar com a consulta ao público e muito menos com as informações de quem será afetado pelas medidas agora aprovadas de forma mais simples, como as comunidades tradicionais.

Assim, por meio deste artigo explicitam-se alguns pontos de atenção que foram desconsiderados no desenvolvimento do PL sugerindo uma precariedade do rigor técnico da nova norma e um grande retrocesso para a transparência e proteção

de dados no país, colocando como prioridade apenas os potenciais interesses econômicos e não considerando os sociais e, como disse a economista Maria da Conceição Tavares, "Uma economia que não se preocupa com justiça social é uma economia que condena os povos […]". Portanto, o intuito do presente artigo foi trazer essa reflexão acerca da preocupação com a proteção dos dados e transparência para o povo, reforçando a importância de um amplo debate com todas as partes envolvidas.

REFERÊNCIAS

ACHADOS E PEDIDOS. Funai admite não ter dados estruturados sobre monitoramento de terras indígenas. São Paulo: Fiquem Sabendo, 2021. Disponível em: https://www.achadosepedidos.org.br. Acesso em: 17 out. 2025.

ALVES, Marcelo de Camilo Tavares. Direito digital. Goiânia, 2009. p. 9-10. Disponível em: http://aldeia3.computacao.net/greenstone/collect/trabalho/import/Direito%20Digital.pdf. Acesso em: 19 out. 2025.

ANDES-SN. Governo sanciona "PL da Devastação" com 63 vetos, mas ameaças continuam. Brasília, DF, 12 ago. 2025. Disponível em: https://www.andes.org.br/conteudos/noticia/governo-sanciona-pL-da-devastacao-com-63-vetos-mas-ameacas-continuam1. Acesso em: 17 out. 2025.

BRASIL. Câmara dos Deputados. Proposição PL 3962/2008. Ficha de tramitação. Brasília, DF, 2008. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=257161. Acesso em: 17 out. 2025.

BRASIL. Congresso Nacional. Comissão Parlamentar de Inquérito da Barragem de Brumadinho. Relatório final da CPI da Barragem de Brumadinho. Brasília, DF: Senado Federal, 2023. 200 p. Disponível em: https://legis.senado.leg.br/atividade/comissoes/comissao/2246/. Acesso em: 16 out. 2025.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 2016. 496 p. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf. Acesso em: 16 out. 2025.

BRASIL. Lei Complementar nº 140, de 8 de dezembro de 2011. Estabelece normas para a cooperação federativa na proteção do meio ambiente. *Diário Oficial da União*, Brasília, DF, 9 dez. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp140.htm. Acesso em: 17 out. 2025.

BRASIL. Lei nº 6.938, de 31 de agosto de 1981. Dispõe sobre a Política Nacional do Meio Ambiente. *Diário Oficial da União*, Brasília, DF, 2 set. 1981. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l6938.htm. Acesso em: 17 out. 2025.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações públicas (Lei de Acesso à Informação – LAI). *Diário Oficial da União*, Brasília, DF, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 17 out. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 out. 2025.

BRASIL. Ministério da Agricultura e Pecuária. Brasil contabiliza 6,48 milhões de cadastros rurais por meio do CAR. Brasília, DF, 10 fev. 2022. Disponível em: https://www.gov.br/pt-br/noticias/agricultura-e-pecuaria/2022/02/brasil-contabiliza-6-48-milhoes-de-cadastros-rurais-por-meio-do-car. Acesso em: 17 out. 2025.

BRASIL. Ministério do Meio Ambiente. Procedimentos para o licenciamento ambiental do Brasil. Brasília, DF, 2016. p. 255-266.

BRASIL. Projeto de Lei nº 2.159, de 2021. Dispõe sobre o licenciamento ambiental. Brasília, DF. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/148785. Acesso em: 16 out. 2025.

BRASIL. Senado Federal. Projeto de Lei nº 2.159, de 2021 (nº 3.729/2004 na Câmara dos Deputados). Dispõe sobre o licenciamento ambiental. Brasília, DF, 2021. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?disposition=inline&dm=8979282. Acesso em: 17 out. 2025.

CÂMARA DOS DEPUTADOS. Lula sanciona novo licenciamento ambiental com 63 vetos. Brasília, DF, 8 ago. 2025. Disponível em: https://www.camara.leg.br/noticias/1186832-lula-sanciona-novo-licenciamento-ambiental-com-63-vetos/. Acesso em: 17 out. 2025.

CIMI – CONSELHO INDIGENISTA MISSIONÁRIO. Violência contra os Povos Indígenas do Brasil – Dados de 2019. Brasília: CIMI, 2020. Disponível em: https://cimi.org.br. Acesso em: 17 out. 2025.

COSTA; ALBUQUERQUE. O licenciamento ambiental no Brasil e os seus desafios. *Revista Saúde e Meio Ambiente*, Três Lagoas, v. 12, n. 2, p. 101-115, jan./jul. 2021.

COSTA; COSTA. A flexibilização do licenciamento ambiental no Brasil. *Brazilian Journal of Development*, Curitiba, v. 8, n. 2, p. 10187-10199, 2022.

DAMA INTERNATIONAL. DAMA-DMBOK: Data Management Body of Knowledge. 2017.

DELOITTE. Cost of Compliance and Regulatory Productivity. Deloitte Consulting, 2017. Disponível em: https://www.deloitte.com/us/en/services/consulting/articles/cost-of-compliance-regulatory-productivity.html. Acesso em: 17 out. 2025.

FGV COMUNICAÇÃO RIO. Debate climático-ambiental e desinformação. Mídia e Democracia, 2023. Disponível em: https://midiademocracia.fgv.br/estudos/debate-climatico-ambiental-pauta-eventos-extremos-mas-e-atravessado-por-desinformacao-e. Acesso em: 17 out. 2025.

FIÚZA, Patrícia; GLOBO NOTÍCIAS. Controladoria-Geral do Estado aponta fragilidades no licenciamento e fiscalização de barragens em MG. 2019. Disponível em: https://g1.globo.com/mg/minas-gerais/noticia/2019/07/19/relatorio-inedito-da-cge-aponta-fragilidades-no-sistema-de-licenciamento-e-fiscalizacao-de-barragens-em-mg.ghtml. Acesso em: 10 out. 2025.

FUNAI – FUNDAÇÃO NACIONAL DOS POVOS INDÍGENAS. Funai alerta para impactos irreversíveis sobre os povos indígenas com o PL do Licenciamento Ambiental. 2025. Disponível em: https://www.gov.br/funai/pt-br/assuntos/noticias/2025/funai-alerta-para-impactos-irreversiveis-sobre-os-povos-indigenas-e-seus-territorios-com-a-aprovacao-do-pl-do-licenciamento-ambiental-na-camara. Acesso em: 13 nov. 2025.

IPEA – INSTITUTO DE PESQUISA ECONÔMICA APLICADA. Análise "ex ante" de políticas públicas. Brasília, DF: IPEA, 2022. Disponível em: https://repositorio.ipea.gov.br/server/api/core/bitstreams/d5b1418b-278c-4106-9a40-91a4b3cc53e9/content. Acesso em: 17 out. 2025.

ISO – INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 31000:2018 – Risk management – Guidelines. Geneva: ISO, 2018. Disponível em: https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en. Acesso em: 17 out. 2025.

NETO; CHARÃO-MARQUES. Extensão rural: trajetórias e desafios. Porto Alegre: Editora da UFRGS, 2023.

OECD. Regulatory Impact Assessment. OECD Best Practice Principles for Regulatory Policy. Paris: OECD Publishing, 2020. Disponível em: https://doi.org/10.1787/7a9638cb-en. Acesso em: 17 out. 2025.

PAIVA, Mário Antônio Lobato de. Os institutos do direito informático. 2002. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/anexos/30390-31543-1-PB.pdf. Acesso em: 16 out. 2025.

RADIS. O que muda com os vetos de Lula ao "PL da Devastação". Rio de Janeiro, RJ, 2 set. 2025. Disponível em: https://radis.ensp.fiocruz.br/reportagem/meio-ambiente/o-que-muda-com-os-vetos-de-lula-ao-pl-da-devastacao/. Acesso em: 17 out. 2025.

SAVIANI FILHO, Hermógenes. Maria da Conceição Tavares: "A economia que não se preocupa com justiça social condena os povos". Instituto Justiça Fiscal, 17 jun. 2024. Disponível em: https://ijf.org.br/maria-da-conceicao-tavares-a-economia-que-nao-se-preocupa-com-a-justica-social-e-uma-economia-que-condena-os-povos/. Acesso em: 21 nov. 2025.

UGEDA, L. Falta de gestão de dados públicos como necropolítica ambiental brasileira. *Consultor Jurídico*, 21 set. 2024. Disponível em: https://www.conjur.com.br/2024-set-21/falta-de-gestao-de-dados-publicos-como-necropolitica-ambiental-brasileira/. Acesso em: 17 out. 2025.

VERGILI, Gabriela; SALIBA, Pedro. Políticas ambientais, transparência pública e proteção de dados: viabilidade jurídica do compartilhamento de dados pessoais no CAR. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2023.

O USO DA INTELIGÊNCIA ARTIFICIAL NO PODER JUDICIÁRIO

Eduardo Ceolin da Silva Menna Barreto[1]
Lucas Limone[2]

RESUMO

O presente artigo analisa os limites jurídicos e éticos da inserção da Inteligência Artificial (IA) no Poder Judiciário brasileiro, avaliando sua compatibilidade com a busca por eficiência e a preservação dos direitos fundamentais. A pesquisa demonstra que a massiva adoção da IA, embora justificada pela celeridade na prestação jurisdicional, enfrenta desafios inerentes à sua tecnologia. O primeiro reside no "efeito caixa-preta", que gera opacidade no processo decisório e confronta o dever constitucional de motivação das decisões. O segundo desafio decorre do uso de dados históricos, que podem introduzir vieses discriminatórios. Adicionalmente, o texto discute o conflito entre o princípio da publicidade dos atos processuais e as diretrizes de privacidade da Lei Geral de Proteção de Dados (LGPD), destacando a vulnerabilidade gerada pela exposição ostensiva de dados sensíveis em sistemas como o PJe. Conclui-se que, a IA no Judiciário, apesar de promover ganhos em eficiência na atividade-meio, só se justifica mediante o cumprimento rigoroso dos princípios da LGPD (minimização e adequação) e pela manutenção da revisão humana em todas as etapas, atuando esta como o principal mecanismo para mitigação de vieses e garantia da isonomia processual.

Palavras-chave: Poder Judiciário, Inteligência Artificial (IA), Discriminação Algorítmica, Segurança Jurídica, LGPD (Lei Geral de Proteção de Dados)

SUMÁRIO: 1. Introdução; 2. A inteligência artificial no Poder Judiciário aspectos gerais; 3. Limites éticos e morais para o uso da inteligência artificial no poder judiciário brasileiro – ia na tomada de decisões; 4. Proteção dos dados utilizados pela ia no poder judiciário – LGPD; 5. Conclusões; 6. Referências.

1 INTRODUÇÃO

[1] Graduando em Direito do Uniceub – Centro Universitário de Brasília. E-mail: eduardo.ceolin@sempreceub.com
[2] Graduando em Direito do Uniceub – Centro Universitário de Brasília. E-mail: lucas.limone@sempreceub.com

O presente artigo tem por objetivo abordar o uso da inteligência artificial (IA) que tem remodelado o mundo contemporâneo, deixando de ser um mero conceito de ficção científica para se tornar um elemento central na organização social, econômica e política.

O ser humano, ao proporcionar a capacidade de constante aprendizado a inteligência artificial (*machine learning*), possibilitou que ela automatizasse seu aprendizado e adquirisse, em pouco tempo, a aptidão de simular as habilidades humanas de estudo, percepção e tomada de decisão[3], tornando-se, para muitos, um componente essencial das atividades diárias e fazendo com que permeie praticamente todas as áreas da vida.

A quase onipresença da IA na vida humana, contudo, tem levantado questionamentos éticos e jurídicos que transcendem a simples gestão de dados. No âmbito jurídico, essa transformação culminou na intensa aplicação da IA pelo Poder Judiciário brasileiro, como uma resposta institucional à necessidade urgente de garantir a celeridade e a eficiência na prestação jurisdicional.

Assim, foram desenvolvidas ferramentas para classificar processos, identificar precedentes e, em alguns casos, até mesmo sugerir decisões. Essa migração para o digital, vista por alguns sob a ótica da Análise Econômica do Direito (AED) como um imperativo para otimizar recursos e reduzir o tempo de tramitação processual (Berzagui & Silva)[4].

A inserção da IA no espaço de decisão judicial gera diversos questionamentos acerca do risco de desumanização da Justiça. Conforme Laura Schertel Ferreira Mendes[5], o cerne da discussão não reside apenas na eficiência, mas na potencialidade da tecnologia de gerar discriminação algorítmica e vulnerabilidade ampliada, mesmo em ambientes formalmente neutros como o Judiciário. A própria forma como a IA opera a coleta e o tratamento de informações levanta questionamentos fundamentais sobre a justiça material.

---

[3] O que é aprendizado de máquina?, disponível em https://www.ibm.com/br-pt/think/topics/machine-learning . Acesso em 08 de outubro de 2025.

[4] **BERZAGUI, Bruno; SILVA, José Everton da,** A utilização da inteligência artificial para aumento da eficiência do poder judiciário: um estudo a partir da análise econômica do direito

[5] MENDES, Laura Schertel Ferreira, Mattiuzzo, Marcela; Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia;

Dessa forma, presenciamos uma colisão entre a busca por celeridade processual e a necessidade de preservação da imparcialidade e da justiça, assim, emergindo a problemática central deste trabalho: **Quais são os limites jurídicos e éticos do uso da Inteligência Artificial no Poder Judiciário sem comprometer a busca pela eficiência?**

2 A INTELIGÊNCIA ARTIFICIAL NO PODER JUDICIÁRIO ASPECTOS GERAIS

A necessidade de transparência e a preservação dos direitos fundamentais demandam e impõe uma análise aprofundada sobre o funcionamento interno desses sistemas e os possíveis riscos que a inteligência artificial pode ocasionar ao exercício do Poder Judiciário.

É inevitável o choque com o chamado "efeito caixa-preta", que se manifesta na dificuldade em auditar e compreender os critérios que levam o algoritmo a sugerir um determinado desfecho processual. Na literatura especializada, os algoritmos são frequentemente designados como *black boxes* por Frank Pasquale (Mendes e Mattiuzzo, p. 21)[6].

Ficando claro que esta opacidade atenta diretamente contra o dever constitucional de motivação das decisões judiciais (Art. 93, IX, da CF/88), um pilar fundamental para a segurança jurídica e a garantia do direito de defesa.

Além disso, a questão da opacidade se estende e chega a diretamente se relacionar com um ponto supracitado, a fonte de aprendizado da IA. Os sistemas são alimentados por um repositório de dados históricos que, como alertado por Laura Schertel Ferreira Mendes, podem carregar consigo vieses sociais e estruturais, levando o Judiciário a replicar injustiças passadas sob o manto da neutralidade tecnológica.

[6] MENDES, Laura Schertel Ferreira, Mattiuzzo, Marcela; Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia;

Nessa toada, complementa Danilo Doneda[7], a gestão e o tratamento desses dados devem respeitar o princípio da autodeterminação informativa, conferindo ao indivíduo o controle sobre o uso de suas informações.

Tais elementos demonstram que a regulamentação jurídica e a auditoria constante da IA não se configuram como um impedimento à eficiência e celeridade, mas sim como uma premissa indispensável para a tutela dos direitos fundamentais.

Por outro prisma, a problemática tecnológica do Judiciário impõe uma reflexão sobre a recente crítica a disponibilidade ostensiva de informações pessoais nos sistemas eletrônicos dos tribunais. [8]

O princípio constitucional da publicidade dos atos processuais (Art. 93, IX, da CF/88)[9] permitiu que milhões de dados sensíveis, incluindo detalhes de dívidas, histórico de saúde, litígios familiares e outras informações da vida privada, fossem digitalizados.

A facilidade de consulta pública em plataformas como o PJe (Processo Judicial Eletrônico) transformou vastos repositórios de dados judiciais em fontes abertas, passíveis de serem acessadas por qualquer indivíduo através da consulta pública ou, mais perigosamente, por algoritmos de *data mining*.

Essa exposição massiva colide frontalmente com a filosofia trazida pela Lei Geral de Proteção de Dados (LGPD). Embora a lei estabeleça uma base legal para o tratamento de dados pelo Poder Público (Art. 23), ela impõe que esse tratamento deve atender à sua finalidade pública e, crucialmente, ao princípio da necessidade e da minimização dos dados (LGPD, Art. 6º, I e III).

Na perspectiva de Danilo Doneda, mesmo quando há o interesse público, a autodeterminação informativa exige que o indivíduo não perca totalmente o controle

---

[7] DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo:Revista dos Tribunais, 2019.

[8] A PUBLICIDADE DOS ATOS PROCESSUAIS E SEU DIÁLOGO COM A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. https://ceafpesquisa.mpba.mp.br/textos/a-publicidade-dos-atos-processuais-e-seu-dialogo-com-a-lei-geral-de-protecao-de-dados-pessoais/ . Acessado em 11/10/2025.

[9] Art. 93. Lei complementar, de iniciativa do Supremo Tribunal Federal, disporá sobre o Estatuto da Magistratura, observados os seguintes princípios: (...)
IX – todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação;

sobre suas informações. Portanto, a publicidade, que antes era uma garantia democrática, transforma-se em risco à privacidade e à segurança jurídica, pois expõe o cidadão desnecessariamente, abrindo margem para a discriminação algorítmica.

A LGPD, ao estabelecer a necessidade de adequação dos dados (Art. 6º, II), impõe ao Judiciário o dever de adotar mecanismos de segurança e, principalmente, de anonimização e pseudonimização para os dados disponibilizados ao público em geral. Porém, ainda não parece estar efetivamente sendo concretizado pelo Judiciário. A simples divulgação do nome das partes e do objeto da ação, por exemplo, não requer a exposição de documentos pessoais sensíveis.

O problema se acentua com o uso da IA, pois os algoritmos de triagem e predição se alimentam justamente desses dados detalhados. Como visto nas considerações de Laura Schertel Mendes, se a tecnologia não é neutra, a ampla disponibilidade de dados sensíveis para *data mining* cria um ciclo vicioso entre a exposição inicial que facilita a discriminação algorítmica e o próprio Judiciário, que ao usar esses dados para treinar suas IAs (como o Projeto Victor, desenvolvido pelo STF), precisa garantir que o tratamento de informação respeite os direitos fundamentais.

Entretanto, apesar dos diversos riscos éticos e jurídicos que se apresentam ao manejo de dados, é necessário reconhecer que as iniciativas de IA no Brasil já demonstram ganhos consideráveis em eficiência. Conforme disse Luiz Fernando Bandeira de Mello, Conselheiro do CNJ e presidente da Comissão Permanente de TI e encarregado pela proteção de dados do CNJ, em uma entrevista ao CNJ, o panorama do uso da IA pelo Poder Judiciário foi detalhado:

> "LFBM: No último levantamento, identificamos 67 iniciativas de uso de inteligência artificial em 47 tribunais. E desde então, novas iniciativas devem ter surgido. O Supremo usa 3 sistemas: O Victor (para análise de temas de repercussão geral), a Rafa (para classificação de processos relacionados com a Agenda 2030) e, mais recentemente, a VitórIA (identificando processos com o mesmo objeto que permitam tratamento conjunto). O STJ utiliza o Athos, enquanto o TJ de São Paulo conta com cinco sistemas, alguns deles desenvolvidos em parceria com a USP, como o LUCAS, usado para identificação de temas repetitivos, com precedentes vinculados. Recentemente conheci novos projetos de IA no TJPE e no TJMG que são bastante promissores.

> Sem dúvida, estamos em um estágio de desenvolvimento dessa espécie de ferramenta. A IA vem sendo útil, sim, para obter ganhos em eficiência. Mas ainda é um tanto embrionária, temos bastante a evoluir." [10]

Essa demonstração prática, que inclui sistemas como o Victor (STF) e o Athos (STJ), evidencia que a maior parte das iniciativas catalogadas reside na atividade-meio, ou seja, na classificação, triagem e organização do fluxo processual.

Tais estratégias demonstram que o futuro da IA no Judiciário não reside na automatização plena, mas na IA aumentada, onde a máquina atua como um auxiliar do magistrado. Em relação aos problemas discriminatórios que a inteligência artificial possa gerar, o Dr. Luiz Fernando Bandeira de Mello, também responde:

> REVISTA CNJ: COMO PODEMOS COMPATIBILIZAR O USO DE INTELIGÊNCIA ARTI-FICIAL NO PODER JUDICIÁRIO COM OS RISCOS DE VIESES DISCRIMINATÓRIOS?
>
> LFBM: O viés discriminatório é um conhecido problema da inteligência artificial, mas que está profundamente ligado a problemas estruturais na base de dados e ao treinamento que a máquina recebeu. Para resolver esse problema, temos alguns caminhos: o primeiro, é usar aquela base de dados "purificada" que já possuímos hoje na PDPJ; em segundo lugar, é necessário parametrizar a ferramenta de IA para que expressamente processe as informações excluindo determinados vieses; finalmente, a revisão humana continuará a ser a etapa mais importante e não excluo a possibilidade de programar o sistema para que alerte o magistrado sobre algo assim: "a minuta de decisão aparentemente não atende ao protocolo com perspectiva de gênero". E duas opções: confirmar/revisar. Um alerta como esse pode ser mais eficaz para prevenir um determinado viés do que os métodos que utilizamos hoje.

Desse modo, é possível perceber o inegável benefício que a Inteligência Artificial traz para o poder judiciário, reduzindo o tempo para análise de grandes volumes de dados, automatizando tarefas, elaborando decisões e auxiliando o magistrado de forma geral, bem como viabiliza que os processos judiciais avancem de maneira muito mais célere, evitando que algumas causas demorem anos para serem julgadas.

[10] Revista CNJ, v.7, n.2, jul./dez. 2023 p. 10

No entanto, é de extrema importância considerarmos algumas questões éticas e morais na introdução da IA no direito brasileiro, vez que sua introdução na área jurídica exige, antes de tudo, respeito as normas constitucionais e de privacidade, necessitando da vistoria humana em todas as etapas do processo.

3 LIMITES ÉTICOS E MORAIS PARA O USO DA INTELIGÊNCIA ARTIFICIAL NO PODER JUDICIÁRIO BRASILEIRO – IA NA TOMADA DE DECISÕES

Nesse sentido, como mencionado anteriormente, a inserção da Inteligência Artificial no processo judicial exige a participação humana em todos os estágios da automatização, considerando que o direito brasileiro não se remete apenas a aplicação seca da lei, mas sim de ponderação entre valores e a avaliação minuciosa de cada caso, uma vez que nenhum processo é igual.

A utilização de sistemas de IA no auxílio de tomadas de decisões carrega grandes riscos éticos, principalmente quando consideramos que os algoritmos manipulam os dados sem transparência nenhuma e podem refletir a desigualdade brasileira ao analisar os processos ou ao elaborarem decisões (aplicando a lei de forma literal). Tendo isso em vista, se a Inteligência Artificial não passar por uma fiscalização humana, é quase certo que a imparcialidade e a isonomia serão violadas, vez que o sistema de automatização pode refletir os preconceitos/estereótipos existentes em nossa sociedade, além de não analisar cada caso com suas peculiaridades.

Portanto, mesmo que a automação facilite as atividades no ambiente judicial, ainda é essencial que as análises que o sistema de IA geram sejam verificados por alguma mente humana, por meio de validação e compreensão crítica dos dados gerados, evitando que os processos judiciais encontrem-se apenas nas mãos de um robô, o que pode trazer ainda mais prejuízos e insegurança para a população.

3.1 Fundamentos éticos e democráticos da IA no judiciário

A Resolução nº 615, de 11 de março de 2025, do Conselho Nacional de Justiça (CNJ), estabelece o patamar ético para o desenvolvimento e uso da IA no Judiciário brasileiro. O **Artigo 2º** da referida norma delineia os fundamentos que devem nortear toda e qualquer solução tecnológica, atuando como um filtro de legalidade e moralidade. Esses fundamentos reforçam a tese central de que a tecnologia deve servir à Justiça, e não o contrário, com foco na **centralidade da pessoa humana** (inciso IV).

O CNJ deixa claro que o desenvolvimento tecnológico (inciso III) está subordinado ao **respeito aos direitos fundamentais e aos valores democráticos** (inciso I). Este é um ponto crucial, pois impede que a busca por eficiência (celeridade e economia) se torne uma justificativa para violações de garantias processuais.

Além disso, a norma obriga à **promoção da igualdade, da pluralidade e da justiça decisória** (inciso VI), reconhecendo implicitamente o risco de **discriminação algorítmica** inerente aos sistemas treinados com dados históricos enviesados, tal como discutido pela doutrina de Laura Schertel Ferreira Mendes (2022).

A obrigatoriedade da **participação e supervisão humana em todas as etapas** (inciso V) é reforçada, limitando estritamente a automação a "serviços judiciários meramente acessórios ou procedimentais", garantindo que o juízo de valor e a responsabilidade jurídica permaneçam inalienavelmente com o magistrado (Resolução CNJ nº 615/2025, Art. 2º, V).

No âmbito da **proteção de dados**, o CNJ exige a **curadoria dos dados** (inciso IX), demandando que as fontes de dados sejam "seguras, rastreáveis e auditáveis". Este requisito impõe um dever ético de limpeza e neutralização dos *datasets*, buscando prevenir que a IA aprenda e amplifique injustiças históricas.

A transparência é consolidada através da exigência de **transparência dos relatórios de auditoria e de avaliação de impacto algorítmico** (inciso XII), pavimentando o caminho para a responsabilização (*accountability*).

Complementando os fundamentos, o **Artigo 3º** da Resolução CNJ nº 615/2025 estabelece os princípios práticos que regerão a governança e o uso da IA nos tribunais, estendendo a proteção do devido processo legal para o ambiente algorítmico. Em termos simples, se o Artigo 2º diz *o que* a IA deve respeitar (direitos humanos e democracia), o Artigo 3º define como ela deve ser usada para garantir esses respeitos, estendendo a proteção do devido processo legal para o mundo digital.

O primeiro princípio (inciso I) estabelecido é o da **justiça, equidade, inclusão e não-discriminação abusiva ou ilícita** (Art. 3º, I). Este ponto reforça que a IA deve ser uma ferramenta ativa na promoção da Justiça Material. Isso significa que a tecnologia não pode se limitar a replicar a lei friamente, mas deve ser configurada para combater e não perpetuar as desigualdades e os preconceitos que historicamente se manifestam na sociedade e nos dados processuais.

Para garantir essa justiça, o CNJ lista um conjunto de princípios instrumentais que visam desmantelar o problema da opacidade algorítmica (o famoso "efeito caixa-preta"). O inciso II exige **transparência, explicabilidade, contestabilidade, auditabilidade e confiabilidade**.

- **Explicabilidade**: É o direito de a parte entender a lógica, mesmo que simplificada, que levou o algoritmo a sugerir um resultado ou classificar o processo de uma determinada forma.
- **Contestabilidade:** Garante que a parte possa, de fato, impugnar a sugestão da IA. Não basta saber a explicação; é preciso ter a ferramenta processual para discordar dela, reforçando a Ampla Defesa.
- **Auditabilidade:** Permite que o sistema seja constantemente inspecionado e rastreado, garantindo que ele não mude seu comportamento sem que ninguém perceba, mantendo a confiança no sistema.

O princípio da Segurança Jurídica (Art. 3º, III) é firmemente ligado à Segurança da Informação. O CNJ reconhece que um sistema de IA que não é seguro

contra-ataques, vazamentos ou falhas de programação é uma ameaça à própria estabilidade das decisões judiciais.

Além disso, a Resolução reafirma a observância integral do Devido Processo Legal, da Ampla Defesa e do Contraditório. O princípio da identidade física do juiz (Art. 3º, V) é mantido como salvaguarda final e como um limite ético insuperável, garantindo que o magistrado, o ser humano responsável pela decisão, seja quem conduziu o processo e não apenas um endossante de uma sugestão robótica.

Por fim, o CNJ adota uma postura de cautela e prevenção (Art. 3º, VI). Isso significa que, antes de implementar uma nova IA, os tribunais devem realizar uma avaliação rigorosa dos riscos e ter planos claros para mitigá-los.

A supervisão humana (Art. 3º, VII), que é a principal linha de defesa ética, deve ser efetiva, periódica e adequada ao nível de risco da solução. Quanto maior o risco de a IA causar um dano, mais intensa deve ser a supervisão do ser humano sobre ela.

Para que essa supervisão funcione, o CNJ exige a capacitação contínua (Art. 3º, VIII) de magistrados e servidores. Não se espera que juízes se tornem programadores, mas sim que desenvolvam uma análise crítica sobre os resultados da IA, entendendo seus vieses e limitações, para evitar o viés de conformidade (simplesmente aceitar a sugestão da máquina).

Em conclusão, os Artigos 2º e 3º da Resolução CNJ nº 615/2025 demonstram o esforço normativo do Judiciário brasileiro em casar a eficiência da IA com a ética constitucional, transformando a transparência, o direito de contestação e a supervisão humana nas condições de validade essenciais para a inovação tecnológica no sistema de justiça.

4 PROTEÇÃO DOS DADOS UTILIZADOS PELA IA NO PODER JUDICIÁRIO - LGPD

Além disso, é inegável que a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, afeta diretamente a utilização da Inteligência Artificial no direito brasileiro, sobretudo se considerarmos que há o tratamento de dados das partes, advogados e servidores. Com a própria LGPD estabelecendo critérios para a

utilização de dados sensíveis e pessoais, observando os princípios da finalidade, adequação, necessidade, segurança e transparência.

Nessa toada, ao utilizar a Inteligência Artificial no poder judiciário e aplicar a LGPD, é de extrema importância que se tenha a minimização dos dados utilizados, vez que operar esse grande volume de dados vai completamente contra ao que estabelece a LGPD, a qual determina a utilização do mínimo possível de informações pessoais para atingir o objetivo legítimo do tratamento. Podendo esse se tornar um ponto de fragilidade no âmbito judicial se não nos atentarmos à administração adequada dos dados e à sua proteção.

A automação irresponsável pode afetar diretamente o direito dos cidadãos brasileiros, principalmente considerando que, se os dados pessoais não forem tratados adequadamente, pode-se gerar um ambiente de insegurança fora da área judicial, vez que, se os dados das partes forem vazados, as pessoas estarão mais propensas a serem alvos de golpes.

Diante do exposto, a adoção da Inteligência Artificial no poder judiciário só se justifica quando atrelada ao cumprimento rigoroso da LGPD e ancorada com um tratamento sólido e responsável dos dados pessoais. Visto que, ausentes esses cuidados ao tratar as informações, a automação vai potencializar vulnerabilidades, expor cidadãos a riscos indevidos e corroer a confiança social na Justiça.

Assim, o caminho correto é o da inovação responsável, implementando a IA com transparência e melhoria contínua, sob coordenação institucional e com participação plural da mente humana, garantindo que o avanço tecnológico sirva ao interesse público e à proteção efetiva dos dados pessoais.

5 CONCLUSÕES

A aplicação da Inteligência Artificial no Poder Judiciário brasileiro, conforme falado no decorrer deste artigo, apresenta um cenário complexo e diversificado, no qual a expectativa de agilidade e eficácia está intrinsecamente ligada a sérios desafios éticos e jurídicos. A presença constante da IA na sociedade atual, bem como sua habilidade de aprendizado contínuo e automação, incentiva a sua implementação

no judiciário como uma resposta à necessidade de uma prestação jurisdicional mais eficiente e ágil.

Entretanto, alimentar esses sistemas de IA com dados históricos apresenta o risco de replicar e perpetuar preconceitos sociais e estruturais, essa perpetuação de injustiças históricas sob a aparência de objetividade algorítmica representa uma grave ameaça à imparcialidade e equidade da justiça, com isso se tornado ainda mais evidente com o fácil acesso de dados pessoais nos sistemas eletrônicos dos tribunais, fato esse que agrava ainda mais a vulnerabilidade da população.

No contexto digital, o princípio constitucional da publicidade dos atos processuais, que anteriormente funcionava como uma garantia democrática, tornou-se um meio de exposição em massa de informações sensíveis, entrando em conflito direto com as disposições da LGPD.

Por isso, a incorporação da IA no direito brasileiro requer um cumprimento rigoroso das normas constitucionais e dos direitos de privacidade, exigindo a supervisão humana em todas as fases do processo, pois a legislação brasileira não se limita à aplicação estrita e literal, mas requer a consideração de valores e a análise cuidadosa de cada caso em sua particularidade. A automação irresponsável, sem supervisão humana e sem conformidade rigorosa com a LGPD, não só comprometeria a imparcialidade e a equidade, reproduzindo preconceitos e estereótipos sociais, como também iria desgastar a confiança da sociedade no sistema judicial.

Assim, a aplicação da Inteligência Artificial no Poder Judiciário só será justificada quando em conformidade com o disposto na LGPD, obtendo-se um tratamento sólido, responsável e transparente dos dados pessoais. Garantindo que a automação atenda aos interesses públicos e proteja os direitos fundamentais, em vez de se transformar em um novo risco para a já delicada área jurídica em nosso país.

REFERÊNCIAS

BERZAGUI, Bruno; SILVA, José Everton da. A utilização da inteligência artificial para aumento da eficiência do poder judiciário: um estudo a partir da análise econômica do direito. Disponível em:

https://periodicos.uesc.br/index.php/dike/article/download/3518/2302. Acesso em: 8 out. 2025.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 11 out. 2025.

BRASIL. Conselho Nacional de Justiça. Resolução nº 615, de 11 de março de 2025.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019. Disponível em: https://revista.uemg.br/index.php/inovajur/article/download/7088/4316. Acesso em: 11 out. 2025.

GOMES, Eduardo Biacchi; VAZ, Andréa Arruda; DIAS, Sandra Mara de Oliveira. Limites éticos para o uso da inteligência artificial no sistema de justiça brasileiro, de acordo com a Lei 13.709/2018 (LGPD) e Resoluções 331 e 332 do CNJ. *Revista Internacional CONSINTER de Direito*, Vila Nova de Gaia, n. 13, p. 107-124, dez. 2021. Disponível em: http://scielo.pt/scielo.php?script=sci_arttext&pid=S2183-95222021000200107&lng=pt&nrm=iso. Acesso em: 16 out. 2025. Epub 8 set. 2022.

IBM. O que é aprendizado de máquina? Disponível em: https://www.ibm.com/br-pt/think/topics/machine-learning. Acesso em: 8 out. 2025.

KOSINSKI, Matthew. What is black box artificial intelligence (AI)? Disponível em: https://www.ibm.com/think/topics/black-box-ai. Acesso em: 11 out. 2025.

MACHADO, Fernanda de Vargas; COLOMBO, Cristiano. Inteligência artificial aplicada à atividade jurisdicional: desafios e perspectivas para sua implementação no Judiciário. *Revista da Escola Judicial do TRT4*, v. 3, n. 5, p. 117–141, 2021. DOI: 10.70940/rejud4.2021.113. Disponível em: https://periodicos.trt4.jus.br/revistaejud4/article/view/113. Acesso em: 16 out. 2025.

MATHUR, Arunesh et al. Dark patterns at scale: findings from a crawl of 11,000 shopping websites. *Proceedings of the ACM on Human-Computer Interaction*, v. 3, n. CSCW, p. 1–32, 2019.

MENDES, Laura Schertel Ferreira; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766/Schertel%20Mendes%3B%20Mattiuzzo%2C%202019. Acesso em: 11 out. 2025.

REVISTA CNJ. v. 7, n. 2, jul./dez. 2023, p. 10. Disponível em: https://www.cnj.jus.br/ojs/revista-cnj/issue/view/16. Acesso em: 11 out. 2025.

SANTOS, Aline da Conceição. A publicidade dos atos processuais e seu diálogo com a Lei Geral de Proteção de Dados Pessoais. Disponível em: https://ceafpesquisa.mpba.mp.br/textos/a-publicidade-dos-atos-processuais-e-seu-dialogo-com-a-lei-geral-de-protecao-de-dados-pessoais/. Acesso em: 11 out. 2025.

TEIGÃO, Rafael Coninck; FOGAÇA, Leonardo de Andrade Ferraz. O uso ético e responsável da inteligência artificial no Judiciário brasileiro: impactos para o jurisdicionado e balizas regulatórias. *Revista Jurídica Gralha Azul – TJPR*, v. 1, n. 28, 2025. DOI: 10.62248/w1y8bv17. Disponível em: https://revista.tjpr.jus.br/gralhaazul/article/view/189. Acesso em: 16 out. 2025.

TORRECILLAS, A. C. P.; SANTOS, M. C.; ROCHA, S. R. G. Os desafios éticos e legais do uso da inteligência artificial no poder judiciário brasileiro. *Refas – Revista Fatec Zona Sul*, v. 11, n. 5, p. 1–12, 2025. DOI: 10.26853/Refas_ISSN-2359-182X_v11n05_01. Disponível em: https://www.revistarefas.com.br/RevFATECZS/article/view/784. Acesso em: 16 out. 2025.

DIREITO ELEITORAL E DIGITAL NO COMBATE À DESINFORMAÇÃO

Maria Luísa de Castro Queiroz[1]
João Francisco Santana Madella[2]

RESUMO

O presente artigo analisa de que forma o Direito Eleitoral e o Direito Digital podem atuar de maneira conjunta no enfrentamento das fake news e da desinformação durante o período eleitoral. O estudo busca compreender como o ordenamento jurídico brasileiro tem se adaptado às transformações tecnológicas que impactam a democracia, especialmente diante do uso de deepfakes, inteligência artificial e outras ferramentas digitais. São analisadas as normas que regulam a propaganda eleitoral na internet, com destaque para as Resoluções do Tribunal Superior Eleitoral nº 23.610/2019 e nº 23.732/2024, identificando seus avanços e limitações práticas. A partir dessa análise, o artigo propõe uma reflexão sobre a necessidade de uma regulação mais clara e eficaz, que consiga equilibrar a liberdade de expressão, fundamental para a democracia, com a proteção da integridade do processo eleitoral.

Palavras-chave: Fake news; Direito Digital; Direito Eleitoral; Processo eleitoral; Desinformação; Regulação digital; TSE; Eleições 2026.

SUMÁRIO: 1. Introdução; 2.Fake News e o Direito Digital; 3. O Lucro das Big Tech; 4. Regulação eleitoral no ambiente digital; 5. Desinformação eleitoral e os novos desafios normativos para as eleições de 2026; 6. Conclusão; Referências.

1 INTRODUÇÃO

O avanço tecnológico e a popularização da internet transformaram significativamente a forma como as pessoas se informam, se comunicam e participam da vida pública. O ambiente digital tornou-se, nas últimas décadas, o principal espaço de debate político, substituindo em grande parte os meios tradicionais de comunicação, como rádio, televisão e imprensa escrita. Atualmente,

[1] Graduanda em Direito no UniCeub - Centro Universitário de Brasília - E-mail: malucqueiroz@sempreceub.com.
[2] Graduando em Direito no UniCeub - Centro Universitário de Brasília - E-mail: joaomadella@sempreceub.com.

discussões políticas se desenvolvem em redes sociais, aplicativos de mensagens e plataformas de vídeo, onde o acesso à informação é rápido e amplamente acessível. Esse cenário representa, ao mesmo tempo, um grande avanço para a democracia e um desafio inédito para as instituições jurídicas e políticas.

De um lado, a internet possibilitou a ampliação do diálogo entre as pessoas, permitindo que diferentes vozes e grupos sociais pudessem se manifestar de maneira mais direta e horizontal. O cidadão comum, que antes ocupava um papel mais passivo na esfera política, passou a ter meios de expressar suas opiniões, organizar movimentos e influenciar debates de grande alcance. De outro lado, esse mesmo ambiente abriu espaço para a circulação desenfreada de informações sem qualquer tipo de verificação, muitas delas criadas com o propósito deliberado de enganar, manipular ou atacar adversários políticos. Diante desse cenário, as fake news passou a representar uma ameaça à legitimidade dos processos eleitorais.

O impacto das fake news digitais nas eleições é um problema complexo e de difícil controle. Mensagens falsas se espalham rapidamente em redes sociais e aplicativos de mensagens, explorando algoritmos que priorizam conteúdos sensacionalistas e de grande engajamento. Consequência disso é uma grande distorção na formação da opinião pública, já que muitos eleitores acabam tomando decisões com base em informações falsas. Além disso, o ambiente digital, com seu anonimato, torna difícil responsabilizar os responsáveis e remover conteúdos prejudiciais a tempo de evitar danos ao processo eleitoral.

Esse cenário exige uma análise detalhada do ponto de vista jurídico, especialmente onde se cruzam o Direito Eleitoral e o Direito Digital. O primeiro, que tem como função garantir a legitimidade das eleições e a igualdade entre os candidatos, precisa se adaptar a um contexto em que as campanhas e a propaganda eleitoral acontecem, em grande parte, no ambiente virtual. O segundo, por ser um campo recente e em constante evolução, busca criar ferramentas jurídicas para enfrentar os novos desafios trazidos pelas tecnologias, como a desinformação, a violação de dados e os ataques à reputação.

2 FAKE NEWS E O DIREITO DIGITAL

O termo fake news ganhou ampla difusão nos últimos anos e passou a ocupar um papel central nas discussões sobre democracia, comunicação e regulação do ambiente digital. Embora o conceito não possua uma definição jurídica única, ele pode ser compreendido como a divulgação intencional de informações falsas ou enganosas, com o objetivo de manipular a opinião pública, causar danos à reputação de pessoas ou instituições, ou influenciar decisões políticas e eleitorais. No ambiente digital, a propagação dessas notícias é potencializada pela estrutura das redes sociais, que privilegia conteúdos de alto engajamento, independentemente de sua veracidade.

Nesse contexto, o Direito Digital aparece como o ramo jurídico responsável por regular as interações que ocorrem no ambiente virtual, procurando conciliar o exercício da liberdade de expressão com a necessidade de garantir responsabilidade e segurança nas informações compartilhadas. No Brasil, um dos principais marcos normativos dessa área é o Marco Civil da Internet (Lei nº 12.965/2014), que estabelece princípios, garantias e deveres para o uso da rede. A lei consagra princípios essenciais, como a neutralidade da rede, a proteção da privacidade, a liberdade de expressão e a responsabilidade proporcional dos usuários e provedores. Conforme o artigo 3º, a utilização da internet deve seguir esses valores, assegurando um espaço digital democrático e livre. No entanto, a própria legislação impõe que o exercício dessas liberdades respeite a dignidade da pessoa humana e a veracidade das informações, especialmente quando o conteúdo afeta o interesse coletivo.

Outro instrumento jurídico relevante no enfrentamento das fake news é a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), conhecida como LGPD. Embora seu objetivo principal seja a proteção da privacidade e dos dados pessoais, a lei também se mostra fundamental para conter práticas de manipulação de informações. Isso porque a coleta e o uso indevido de dados de usuários são frequentemente utilizados para direcionar conteúdos falsos de forma segmentada, fenômeno conhecido como microtargeting político. A LGPD, ao exigir transparência e consentimento no tratamento de dados, contribui indiretamente para o combate à desinformação, uma vez que limita a possibilidade de uso abusivo das informações pessoais para fins de manipulação eleitoral ou comercial. Assim, a proteção de dados torna-se um instrumento importante para reforçar a integridade do ambiente digital e preservar a autonomia do cidadão diante das campanhas de desinformação.

Um dos maiores desafios atuais, está relacionado à responsabilidade das plataformas digitais, as chamadas big techs. Empresas como Meta (Facebook, Instagram), Google, X (antigo Twitter) e TikTok desempenham papel central na difusão de informações e, consequentemente, na propagação das fake news. A discussão jurídica gira em torno de até que ponto essas plataformas devem ser responsabilizadas pelo conteúdo publicado por seus usuários. O Marco Civil da Internet adota, como regra, o princípio da responsabilidade subjetiva, segundo o qual as plataformas digitais só respondem caso deixem de remover um conteúdo ilícito após determinação judicial. Contudo, diante da rapidez com que as fake news se propagam nas redes, esse modelo tem se mostrado, em muitos casos, insuficiente para conter os prejuízos causados à opinião pública e à integridade do processo eleitoral.

Por isso, cresce o debate sobre a necessidade de uma regulação mais clara e efetiva sobre o papel das plataformas na moderação de conteúdo. Projetos como o PL das Fake News (PL nº 2.630/2020) buscam estabelecer deveres de transparência e cooperação entre as plataformas e o poder público, sem comprometer a liberdade de expressão. Ainda que a discussão seja recente e complexa, há consenso de que as big techs não podem se eximir totalmente da responsabilidade por um ecossistema informacional que elas mesmas estruturam e monetizam. O desafio é encontrar um equilíbrio entre a liberdade de comunicação e a necessidade de impedir que a desinformação continue a comprometer o funcionamento das instituições democráticas.

Em síntese, o enfrentamento das fake news no ambiente digital exige uma atuação coordenada entre diferentes instrumentos jurídicos — o Marco Civil da Internet, a LGPD e futuras legislações específicas —, além de uma postura mais ativa das plataformas digitais. Nesse sentido, o Direito Digital desempenha um papel essencial na construção de um espaço virtual que garanta não apenas a livre circulação de ideias, mas também a responsabilidade, a veracidade e a integridade da informação, elementos indispensáveis para o fortalecimento da democracia.

3 O LUCRO DAS BIG TECH

Um dos principais fatores que impulsionam a disseminação de fake news é o próprio modelo de negócio das Big Techs. Essas empresas, movidas pelo lucro, priorizam engajamento, cliques e visualizações, deixando em segundo plano a veracidade e o impacto social do que é divulgado. Como aponta a matéria "Fake news e operacionalidade das big techs: chamado à regulação necessária" (JOTA, 2025), as grandes plataformas atuam de forma pouco transparente, tratando seus algoritmos como verdadeiras "caixas-pretas". Na prática, isso significa que seus sistemas de recomendação acabam privilegiando conteúdos sensacionalistas, polarizadores e emocionalmente apelativos, justamente os que mantêm o usuário por mais tempo na plataforma e geram maior retorno financeiro por meio de anúncios.

Essa lógica cria um ciclo problemático: quanto mais um conteúdo desperta reações intensas, mais ele é impulsionado, independentemente de ser verdadeiro ou não. Assim, informações falsas ou distorcidas acabam sendo promovidas, não por seu valor informativo, mas porque atraem atenção e engajamento. O advogado-geral da União, Jorge Messias, destacou que muitos desses algoritmos operam sem qualquer tipo de escrutínio público, o que abre espaço para práticas que beneficiam não apenas o lucro, mas também interesses políticos específicos, sem que as empresas assumam responsabilidade pelos danos gerados.

Diante disso, a regulação das plataformas não é mais apenas uma medida desejável, mas uma urgência. Sem regras que garantam transparência nos algoritmos, deveres de prestação de contas e responsabilização por negligência ou conivência na propagação de desinformação, as Big Techs continuam atuando em um cenário em que os lucros permanecem privados, enquanto os custos sociais, políticos e éticos são repassados à sociedade.

Além disso, esse modelo mercadológico atinge de forma ainda mais severa grupos vulneráveis, como os idosos, que muitas vezes não dominam os mecanismos digitais de checagem e navegação. Quando as plataformas privilegiam alcance e viralização sem considerar a veracidade, essas pessoas acabam mais expostas à desinformação, reproduzindo-a sem perceber. Com isso, o problema vai além do campo econômico: trata-se também de um desafio democrático e social. Por isso, é essencial que o Direito Digital, a LGPD, o TSE e demais órgãos regulatórios adotem

uma postura mais firme diante de um modelo de negócios que se sustenta, prioritariamente, no retorno financeiro, em detrimento do bem coletivo.

4 REGULAÇÃO ELEITORAL NO AMBIENTE DIGITAL

O avanço das tecnologias de comunicação transformou de maneira profunda a dinâmica das campanhas eleitorais e a atuação da Justiça Eleitoral. Se antes a propaganda política se concentrava em meios tradicionais, como rádio, televisão e panfletos, hoje ela se desenvolve majoritariamente nas plataformas digitais. Esse novo contexto exigiu do Tribunal Superior Eleitoral (TSE) a constante atualização de suas normas para compatibilizar o ambiente virtual com os princípios que regem o processo eleitoral, como a isonomia entre candidatos, a transparência e a lisura do pleito.

A Resolução nº 23.610/2019, por exemplo, regulamenta a propaganda eleitoral na internet e estabelece parâmetros para o uso das redes sociais e de impulsionamento de conteúdo. Ela determina que a propaganda paga só pode ocorrer mediante identificação do contratante e comprovação de CNPJ ou CPF, buscando evitar práticas de manipulação e disseminação de desinformação por perfis inautênticos. Além disso, a norma prevê mecanismos de responsabilização para casos de violação à honra, divulgação de fatos sabidamente inverídicos e impulsionamento irregular de postagens.

Apesar desses avanços, a aplicação das regras eleitorais no ambiente digital enfrenta desafios consideráveis. A natureza descentralizada da internet, a velocidade de propagação das informações e o anonimato dos usuários dificultam o exercício do poder de polícia da Justiça Eleitoral. A remoção de conteúdos falsos, por exemplo, muitas vezes ocorre tarde demais, quando os danos à imagem dos candidatos e à formação da opinião pública já se consolidaram. Como aponta o TSE, notícias falsas circulam até 70% mais rápido do que as verdadeiras, o que torna praticamente impossível neutralizar completamente seus efeitos durante o período eleitoral.

Nesse cenário, o Direito Eleitoral passa a dialogar de forma cada vez mais próxima com o Direito Digital, em busca de soluções que preservem tanto a

liberdade de expressão quanto a integridade do processo democrático. A regulação da desinformação, portanto, não deve ser vista como uma forma de censura, mas como um instrumento de proteção da verdade e da confiança pública, elementos essenciais para o exercício livre e consciente do voto.

Superada a análise do marco regulatório vigente, é possível avançar para uma reflexão sobre os novos desafios normativos que se impõem ao Brasil diante das transformações tecnológicas recentes, especialmente no contexto das eleições de 2026.

5 DESINFORMAÇÃO ELEITORAL E OS NOVOS DESAFIOS NORMATIVOS PARA AS ELEIÇÕES DE 2026.

Com a proximidade das eleições de 2026, o Brasil enfrenta um cenário difícil no enfrentamento da desinformação eleitoral. A experiência recente da última eleição municipal demonstrou que as notícias falsas continuam exercendo influência determinante no processo democrático, agora com um grau de sofisticação tecnológica que desafia os mecanismos tradicionais de identificação e repressão.

Dados do Tribunal Superior Eleitoral indicam o registro de mais de 37 mil representações por propaganda irregular, sendo cerca de cinco mil diretamente relacionadas a ilícitos digitais. As demais, embora não diretamente tecnológicas, envolveram dificuldades de verificação decorrentes do uso de ferramentas de inteligência artificial, deepfakes, disparos em massa e contas falsas.

O problema não é apenas de quantidade. A natureza acerca da qualidade da desinformação atual exige uma atuação judicial mais técnica e célere. O que antes se restringia a montagens grosseiras evoluiu para conteúdos muito realistas, por vezes indetectáveis sem perícia digital.

Ferramentas como o VEO, capazes de gerar vídeos inteiramente novos e verossímeis, desafiam conceitos jurídicos clássicos e impõem revisão urgente das normas, pois a fronteira entre ficção e falsificação se torna cada vez mais próxima.

Entre os desafios que virão, destaca-se a necessidade de diferenciar tecnicamente e juridicamente os deepfakes, que manipulam vídeos reais dos

conteúdos criados integralmente por inteligência artificial generativa, que não derivam de material já existente.

Essa diferença é essencial, pois reflete na tipificação das condutas e na aplicação da Resolução TSE nº 23.610/2019, atualizada pela Res. nº 23.732/2024, que proíbe a veiculação de conteúdo sintético manipulado digitalmente com finalidade eleitoral.

A norma, contudo, não esclarece se a referida vedação alcança os vídeos totalmente gerados por IA, sem referência a material real. O art. 9º-B da mesma resolução admite o uso de IA desde que identificado com aviso expresso, o que cria uma zona cinzenta entre o permitido e o proibido.

Diante dessa dualidade, mostra-se urgente uma atualização legislativa que defina com clareza o uso ilícito da IA nas campanhas políticas, trazendo segurança jurídica e equilíbrio entre liberdade de comunicação e integridade eleitoral.

A rastreabilidade das informações também se apresenta como uma problemática. Embora o anonimato seja vedado pela Lei das Eleições (art. 57-D da Lei nº 9.504/97), a multiplicação de perfis falsos, o uso de VPNs e de plataformas estrangeiras dificultam a identificação dos responsáveis por conteúdos ilícitos.

O procedimento atual de rastreamento, baseado em ordens judiciais sucessivas a provedores, é moroso e frequentemente ineficaz diante da velocidade de propagação da desinformação.

6 CONCLUSÃO

Diante do exposto, propõe-se a criação de mecanismos mínimos de identificação digital, como a exigência de canais verificáveis de contato (telefone ou e-mail autenticado) e a previsão de suspensão temporária de contas que se recusem a cumprir ordens judiciais de verificação.

Essa medida preserva a liberdade de expressão e também impõe responsabilidade proporcional, evitando que o anonimato seja instrumentalizado para fins ilícitos.

Outro ponto importante diz respeito à distribuição do ônus da prova em ilícitos digitais eleitorais. Diante da complexidade técnica desses conteúdos, a comprovação de falsidade pode se tornar praticamente inviável para a parte ofendida.

Com base nos princípios da vulnerabilidade, seria razoável admitir, em situações específicas, a inversão do ônus probatório — instituto previsto no art. 6º, VIII, do Código de Defesa do Consumidor e no art. 373, §1º, do Código de Processo Civil.

Assim, quando existirem indícios suficientes de manipulação ou uso indevido de tecnologia direcionada à desinformação, deve-se atribuir ao divulgador o dever de comprovar a autenticidade do material.

Veja bem, essa solução não implica presunção de culpa, mas busca restabelecer o equilíbrio processual diante da dificuldade técnica entre o cidadão comum e as grandes estruturas de comunicação digital.

Dessa forma, o enfrentamento da desinformação eleitoral impõe uma abordagem normativa moderna, que una rigor técnico, celeridade e proporcionalidade.

As eleições de 2026 certamente testarão a capacidade do Estado e dos operadores do Direito em se adaptar-se a um novo modelo informacional.

O combate à desinformação, portanto, não se limita à repressão, mas envolve também a prevenção, a clareza regulatória e a responsabilização efetiva. A preservação da integridade eleitoral dependerá da precisão das normas, da cooperação entre autoridades e plataformas digitais e do compromisso ético dos agentes públicos e privados com a verdade como valor democrático essencial.

REFERÊNCIAS

JOTA. **Fake news e operacionalidade das big techs: chamado à regulação necessária**. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/fake-news-e-operacionalidade-das-big-techs-chamado-a-regulacao-necessaria

USP. **Como identificar e combater as fake news no Brasil.** Jornal USP, [S.l.], s.d. Disponível em: https://jornal.usp.br/atualidades/como-identificar-e-combater-as-fake-news-no-brasil/

TRIBUNAL SUPERIOR ELEITORAL. Pílulas contra a desinformação: notícias falsas circulam 70% mais rápido do que as verdadeiras. Brasília: TSE, 6 jun. 2022. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2022/Junho/pilulas-contra-a-desinformacao-noticias-falsas-circulam-70-mais-rapido-do-que-as-verdadeiras

SENADO FEDERAL. DataSenado: 80% dos brasileiros temem impacto de fake news nas eleições. Rádio Senado, Brasília, 26 ago. 2024. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2024/08/26/datasenado-80-dos-brasileiros-temem-impacto-de-fake-news-nas-eleicoes

ADVOCACIA-GERAL DA UNIÃO. Jorge Messias defende regulação das plataformas de redes sociais. Brasília: AGU, 2024. Disponível em: https://www.gov.br/agu/pt-br/comunicacao/noticias/jorge-messias-defende-regulacao-das-plataformas-de-redes-sociais

SENADO FEDERAL. Para brasileiros, notícias falsas impactam eleições, revela DataSenado. Brasília, 23 ago. 2024. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/08/23/para-brasileiros-noticias-falsas-impactam-eleicoes-revela-datasenado

TRIBUNAL SUPERIOR ELEITORAL. Programa de enfrentamento à desinformação do TSE tem mais de 150 parcerias. Brasília: TSE, jul. 2022. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2022/Julho/programa-de-enfrentamento-a-desinformacao-do-tse-tem-mais-de-150-parcerias-659181

SECRETARIA DE COMUNICAÇÃO SOCIAL DA PRESIDÊNCIA DA REPÚBLICA. As ameaças da desinformação eleitoral na era da “dromocracia”. Brasília: SECOM, set. 2024. Disponível em: https://www.gov.br/secom/pt-br/fatos/brasil-contra-fake/noticias/2024/09/as-ameacas-da-desinformacao-eleitoral-na-era-da-201cdromocracia201d

UNIVERSIDADE FEDERAL DE SANTA CATARINA. Os impactos das Fake News nas eleições. Trabalho de Conclusão de Curso (Graduação em Direito) – UFSC, Florianópolis, 2023. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/255750/Os%20impactos%20das%20Fake%20News%20nas%20elei%C3%A7%C3%B5es%20-%20TCC.pdf?sequence=1&isAllowed=y

G1. TSE proíbe envio em massa de propaganda por aplicativos nas eleições de 2022. G1 – Jornal Nacional, Rio de Janeiro, 15 dez. 2021. Disponível em: https://g1.globo.com/jornal-nacional/noticia/2021/12/15/tse-proibe-envio-em-massa-de-propaganda-por-aplicativos-nas-eleicoes-de-2022.ghtml

SENADO FEDERAL. Notícias falsas na internet preocupam especialistas e autoridades em ano eleitoral. Disponível em: https://www12.senado.leg.br/noticias/videos/2024/04/noticias-falsas-na-internet-preocupam-especialistas-e-autoridades-em-ano-eleitoral

TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO. TRE-ES promove palestra com o tema "Aspectos práticos do Direito Eleitoral Digital: os desafios da desinformação". Disponível em: https://www.tre-es.jus.br/comunicacao/noticias/2024/Agosto/tre-es-promove-palestra-com-o-tema-aspectos-praticos-do-direito-eleitoral-digital-os-desafios-da-desinformacao

PARTE V – ECONOMIA DIGITAL, CONSUMO E COMÉRCIO ELETRÔNICO

LGPD E COMÉR CIO ELETRÔNICO: PROTEÇÃO DO CONSUMIDOR EM AMBIENTE DIGITAL

Ana Beatriz Soares Lima[1]
Bruno Vinicius Carvalho[2]
Gustavo Gonçalves de Castro Marques[3]

RESUMO

O crescimento do e-commerce gerou uma economia de dados que expõe consumidores à hipervulnerabilidade informacional. Baseado na tese de Danilo Doneda, o artigo defende que o foco deve ser a proteção de dados pessoais como direito fundamental, garantindo a autodeterminação informativa. A LGPD é o instrumento para equilibrar essa relação, impondo princípios (Finalidade, Transparência) e bases legais. Contudo, critica-se o "mito do consentimento" no e-commerce devido à assimetria de poder e alerta-se para o risco do legítimo interesse como justificativa para o profiling sem controle. A adequação da lei exige que as empresas adotem a Accountability e a Abordagem Baseada em Risco (como o DPIA), indo além de um mero "check list". Práticas como precificação dinâmica e Dark Patterns são vistas como ilícitos duplos, que violam tanto o CDC quanto a LGPD, sabotando a autonomia do consumidor. A efetividade da LGPD depende, crucialmente, da fiscalização rigorosa e da conscientização dos cidadãos.

Palavras-chave: LGPD (Lei Geral de Proteção de Dados); Comércio Eletrônico (E-commerce); Proteção de Dados Pessoais; Autodeterminação Informativa; Hipervulnerabilidade Informacional; Direito do Consumidor; Diálogo das Fontes; Assimetria de Poder; Mito do Consentimento; Legítimo Interesse; Accountability (Prestação de Contas); Dark Patterns; Precificação Dinâmica.

Sumário: Introdução. 1. O consumidor na era digital e a ascensão do comércio eletrônico. 2. A lei geral de proteção de dados (LGPD) como instrumento de proteção ao consumidor. 3.Impactos e desafios da adequação da LGPD no comércio eletrônico. 4. O diálogo das fontes e a hipervulnerabilidade informacional. Considerações finais. Referências.

[1] Graduando em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: ana.beatrizl@sempreceub.com
[2] Graduando em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: bruno.cfranca@sempreceub.com
[3] Graduando em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: gustavo.goncalves@sempreceub.com

1 INTRODUÇÃO

O comércio eletrônico no Brasil vem crescendo rapidamente, impulsionado pelo aumento do acesso à internet e pelas mudanças de comportamento aceleradas desde a pandemia do COVID-19. Essa transformação modificou profundamente a forma como as pessoas compram e se relacionam com as empresas. Se por um lado, as plataformas digitais facilitaram o acesso a produtos e serviços, oferecendo mais opções e comodidade, por outro, também trouxeram novas vulnerabilidades ligadas ao ambiente virtual.

Hoje as transações comerciais são, acima de tudo, trocas de dados. Informações pessoais, hábitos de navegação e preferências de consumo se tornaram informações valiosas para as empresas, que os utilizam para melhorar a logística, personalizar experiências e basear-se para campanhas de marketing de forma cada vez mais precisa. No entanto, essa coleta e uso intenso de dados criam desequilíbrios entre empresas e consumidores, abrindo espaço para riscos como vazamentos de informações, fraudes, roubo de identidade, e manipulação por meio de publicidade direcionada.

Com isso, a Lei nº 13.709/2018, Lei Geral de Proteção de Dados (LGPD) surge como um marco essencial na defesa dos direitos dos cidadãos no ambiente digital. Inspirada na legislação europeia, ela define regras claras sobre como empresas e órgãos públicos podem coletar, armazenar e utilizar dados pessoais, buscando garantir mais transparência e segurança.

Este artigo pretende analisar como a LGPD se relaciona com o comércio eletrônico, especialmente no que diz respeito à proteção do consumidor online. O objetivo é entender de que forma os princípios, as bases legais e os direitos previstos na lei influenciam as práticas do mercado digital e ajudam a equilibrar essa relação. A importância do estudo está em mostrar que a LGPD vai além do simples cumprimento de regras por parte das empresas — ela representa uma nova forma de garantir direitos do consumidor na era da informação.

2 O CONSUMIDOR NA ERA DIGITAL E A ASCENSÃO DO COMÉRCIO ELETRÔNICO

O crescimento do comércio eletrônico no Brasil transformou de forma definitiva a maneira como consumimos. Hoje, comprar pela internet faz parte da rotina de milhões de pessoas, e quase toda transação comercial envolve algum tipo de troca de dados. O consumidor atual, totalmente conectado, deixa rastros digitais a cada clique, pesquisa ou produto visualizado. Essas informações, coletadas e analisadas constantemente, são o combustível da chamada “economia dos dados”, que movimenta o mercado digital.

É exatamente neste ponto que a tese de Danilo Doneda, em "Da Privacidade à Proteção de Dados Pessoais", se torna central. O autor demonstra que o conceito clássico de privacidade, historicamente entendido como o "direito de ser deixado em paz" (right to be let alone) ou a proteção da vida íntima, tornou-se insuficiente para lidar com a economia digital. O problema no e-commerce não é (apenas) a intrusão indevida na esfera privada do consumidor, mas a utilização e o fluxo constante de seus dados pessoais, que são tratados como matéria-prima (commodity).

O consumidor, ao navegar, não está sendo "espionado" em sua casa, mas está tendo seu comportamento publicamente registrado, analisado e monetizado. Doneda (2023) argumenta que essa nova realidade exige um direito de nova geração: a proteção de dados pessoais como um direito fundamental autônomo. O foco muda da defesa contra intrusões para o controle sobre o uso das informações. Este direito é fundamentado na ideia de autodeterminação informativa, ou seja, o direito de cada indivíduo de decidir quem, quando e como pode tratar seus dados pessoais (DONEDA, 2023).

As empresas utilizam diversas tecnologias para coletar esses dados. Sendo elas: 1. Dados cadastrais: são as informações que o próprio consumidor fornece nome, CPF, endereço, e-mail e telefone, ao criar uma conta ou finalizar uma compra. São necessários para emitir nota fiscal e entregar o produto, mas também servem de base para formar perfis de consumo. 2. Dados de comportamento e navegação: coletados de forma mais discreta, por meio de ferramentas como cookies e pixels. Os cookies “lembram” as preferências do usuário, enquanto os pixels monitoram ações

específicas, como a inclusão de um produto no carrinho ou a conclusão de uma compra. Essas ferramentas permitem às empresas entender o comportamento do consumidor e direcionar ofertas personalizadas. 3. Dados de localização: obtidos, em geral, via GPS de celulares, ajudam a oferecer promoções próximas ao local do cliente. Contudo, também podem revelar hábitos diários e nível de renda, o que aumenta os riscos de uso indevido.

Apesar de tornarem a experiência de compra mais conveniente e personalizada, esses mecanismos expõem o consumidor a riscos. Vazamentos de dados, por exemplo, podem resultar em fraudes, roubo de identidade e chantagens virtuais. Outro perigo é a discriminação algorítmica, em que o preço de um produto varia conforme o perfil do cliente. Assim, quem acessa um site a partir de um bairro mais caro ou de um celular de última geração pode pagar mais pelo mesmo item, o que fere o princípio da igualdade previsto no Código de Defesa do Consumidor. Essa prática exemplifica a perda da autodeterminação informativa, criando uma profunda assimetria de poder: a empresa detém um conhecimento profundo sobre o consumidor, enquanto este muitas vezes nem sabe que está sendo analisado (DONEDA, 2023).

Além disso, há a manipulação comportamental, em que o marketing digital explora fragilidades psicológicas, como o medo de perder uma oportunidade, por meio de avisos de “últimas unidades” ou contadores regressivos. O resultado é o consumo por impulso e a perda de controle sobre as próprias decisões.

3 A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) COMO INSTRUMENTO DE PROTEÇÃO AO CONSUMIDOR

Diante disso, surgiu a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados, como uma resposta à crescente exposição de dados pessoais. Inspirada na legislação europeia (GDPR), a LGPD é a materialização jurídica, no Brasil, desse direito à autodeterminação informativa que Doneda e outros acadêmicos defendiam (DONEDA, 2023), e parte de uma ideia essencial: o dado pessoal não pertence à empresa, mas sim à pessoa a quem ele se refere. Logo, os dados fazem parte da própria identidade do indivíduo.

A lei apresenta dez princípios (art. 6º LGPD), mas três são especialmente importantes para o comércio eletrônico: Finalidade: Os dados só podem ser coletados para um objetivo específico, legítimo e informado ao consumidor. Uma loja online, por exemplo, não pode usar o histórico de navegação de um cliente para vender a terceiros sem avisá-lo claramente. Necessidade: A empresa deve pedir apenas os dados realmente necessários. Se a compra exige apenas nome e endereço, não há motivo para solicitar profissão ou estado civil. Transparência: O consumidor tem direito a informações claras e acessíveis sobre como seus dados são tratados. As políticas de privacidade, portanto, devem ser escritas em linguagem simples, indicando quais dados são coletados, para que servem e por quanto tempo são armazenados.

Além dos princípios, a LGPD determina que todo tratamento de dados deve ter uma base legal. As mais comuns no comércio eletrônico são: Execução de contrato (art. 7º, V): permite o uso dos dados necessários para completar uma compra, como CPF e endereço. Consentimento (art. 7º, I): é exigido para finalidades que vão além da compra, como o envio de e-mails promocionais ou o uso de cookies de publicidade. Esse consentimento deve ser livre e explícito o consumidor precisa marcar ativamente a opção de aceitar. Aqui, a obra de Doneda (2023) oferece uma perspectiva crítica essencial: o "mito do consentimento". No comércio eletrônico, o consumidor que clica em "Aceito" para finalizar a compra não está, de fato, exercendo sua autonomia, mas sim aderindo a uma política de "pegar ou largar" (take it or leave it). Nesses casos de clara assimetria de poder, o consentimento perde sua função, e é por isso que a lei valoriza outros princípios, como a Necessidade e a Finalidade, para limitar o poder das empresas (DONEDA, 2023).

Legítimo interesse (art. 7º, IX): Esta é, talvez, a base legal mais controversa e complexa no comércio eletrônico. Se o consentimento é falho por ser assimétrico, o legítimo interesse é perigoso por ser unilateral. A sua análise superficial limita seu uso a "prevenir fraudes", mas, na prática, é sob esta base que as empresas justificam a maioria das operações de profiling, marketing comportamental e analytics que sustentam seus modelos de negócio, tudo sem pedir autorização ao consumidor. A obra de Doneda (2023) adverte que o LI não é um "cheque em branco". A lei (Art. 10) exige que a empresa realize um "teste de ponderação" (LIA), balanceando seu

interesse comercial contra os "direitos e liberdades fundamentais do titular". O problema, que Doneda (2023) aponta, é que esta ponderação é feita pela própria empresa, de forma opaca, gerando um risco enorme de que o LI sirva apenas para legitimar o abuso que o "mito do consentimento" já não conseguia cobrir.

Por fim, o art. 18 da LGPD, assegura ao consumidor direitos concretos sobre seus dados: ele pode confirmar se há tratamento, pedir acesso às informações, corrigir erros, excluir dados desnecessários e revogar consentimentos quando desejar.

4 IMPACTOS E DESAFIOS DA ADEQUAÇÃO DA LGPD NO COMÉRCIO ELETRÔNICO

Ademais, a adequação à Lei nº 13.709/2018 (LGPD) no comércio eletrônico impõe a necessidade de que as empresas não apenas adaptem processos operacionais, mas internalizem uma cultura organizacional de privacidade. Doneda (2023) ressalta que a proteção de dados pessoais exige uma abordagem sistêmica, que vá além do “check-list” de conformidade e envolva a revisão crítica de modelos de negócio baseados em dados massivos (DONEDA, 2023). Esta crítica ao "checklist" é, na verdade, a crítica à falha em adotar a filosofia central da lei: a Accountability (prestação de contas, Art. 6º, X) e a Abordagem Baseada em Risco (Risk-Based Approach).

A Accountability, como explica Doneda (2023), inverte o ônus: não cabe ao consumidor provar o abuso; cabe à empresa de e-commerce comprovar proativamente que suas operações são legais e seguras. Essa comprovação é feita pela gestão de riscos. A LGPD não é uma lei de "pode ou não pode", mas uma lei que exige que a empresa avalie "qual o risco e como você o mitiga". No ambiente digital, isso significa que varejistas eletrônicos devem mapear não somente os pontos de coleta de dados, mas entender os fluxos subsequentes (anonimização, reidentificação, compartilhamento com terceiros) e os riscos correlatos à vida privada dos consumidores. A falta dessa visão estratégica acarreta vulnerabilidades que vão desde vazamentos até responsabilidade administrativa e civil.

Logo, entre os principais desafios, destaca-se o ajuste às novas exigências de governança de dados. Estas exigências não são tarefas burocráticas, mas os instrumentos práticos da Abordagem Baseada em Risco: a exigência de designação de encarregado (art. 41 da LGPD) e a realização de avaliações de impacto à proteção de dados (art. 38). O DPIA (art. 38), em particular, é a materialização da abordagem de risco. Como Doneda (2023) evidencia, não é apenas um documento formal; é a obrigação do e-commerce de avaliar o risco de discriminação de seus algoritmos e mitigá-lo antes que ele afete o consumidor.

Doneda (2023) evidencia que, no Brasil, muitas empresas ainda operam com estruturas hierárquicas tradicionais e não estão preparadas para operar com processos de governança que envolvam a privacidade desde a concepção (privacy by design) e desde a implementação (privacy by default) (DONEDA, 2023). Estes não são apenas processos técnicos, mas a internalização da gestão de risco, forçando a empresa a desenhar sistemas que sejam seguros por padrão, em vez de corrigir falhas depois. No comércio eletrônico, esse desafio se agrava pela alta rotatividade de dados, pela terceirização de serviços de marketing digital e pela globalização de fluxos, fatores que exigem integração de controles, auditoria contínua e treinamento de colaboradores. A ausência desses mecanismos compromete a efetividade da LGPD e expõe os consumidores a riscos que a própria legislação buscou mitigar.

Por fim, o ecossistema regulatório brasileiro revela-se insuficiente se considerado apenas sob o prisma normativo; a real eficácia da LGPD depende da educação dos consumidores e da fiscalização robusta pela Autoridade Nacional de Proteção de Dados (ANPD). Segundo o Instituto Brasileiro de Defesa do Consumidor (IDEC, 2021), muitos titulares de dados desconhecem a extensão de seus direitos previstos no art. 18 da LGPD (acesso, correção, eliminação e portabilidade) e, assim, não exercem ativamente suas prerrogativas (IDEC, 2021). Doneda (2023) complementa que, sem uma cultura cidadã de proteção de dados, a aplicação prática da norma fica fragilizada, especialmente no comércio eletrônico, onde o usuário muitas vezes aceita termos complexos e pouco claros (DONEDA, 2023). Dessa forma, o verdadeiro impacto da adequação está condicionado não apenas à adoção de medidas internas pelas empresas, mas à construção de um ambiente digital em que os dados pessoais sejam tratados com respeito,

responsabilidade e transparência, assegurando, de fato, a proteção do consumidor em ambiente digital.

5 O DIÁLOGO DAS FONTES E A HIPERVULNERABILIDADE INFORMACIONAL

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) não atua em um vácuo jurídico, nem substitui as legislações anteriores. No contexto do comércio eletrônico, sua aplicação é sinérgica e complementar ao Código de Defesa do Consumidor (Lei nº 8.078/1990). Esta interação é doutrinariamente conhecida como Diálogo das Fontes, teoria consagrada por Cláudia Lima Marques, que postula a aplicação conjunta das normas, buscando sempre a maior proteção ao indivíduo.

O CDC, em seu Art. 4º, I, já reconhecia a vulnerabilidade do consumidor. Contudo, essa vulnerabilidade era classicamente entendida como técnica, jurídica ou econômica. A obra de Danilo Doneda é fundamental para compreender que a sociedade da informação, impulsionada pelo e-commerce, criou uma nova e mais profunda camada: a hipervulnerabilidade informacional.

Como Doneda argumenta, o problema central da era digital é a assimetria de poder radical entre o controlador (a plataforma de e-commerce) e o titular (o consumidor). O consumidor não tem como saber quais dados são coletados, como são processados, com quem são compartilhados ou, mais importante, como esse processamento é usado para influenciar seu comportamento. A vulnerabilidade, portanto, deixa de ser apenas sobre o produto e passa a ser sobre a própria autonomia de escolha do indivíduo, que é minada por mecanismos de dados que ele não pode ver nem controlar.

Neste cenário de diálogo das fontes, práticas abusivas que já eram combatidas pelo CDC ganham uma nova dimensão de ilicitude sob a ótica da LGPD. Um dos exemplos mais claros dessa dupla violação é a discriminação algorítmica, manifestada no e-commerce através da precificação dinâmica (dynamic pricing). Trata-se da prática de cobrar valores diferentes pelo mesmo produto ou serviço, com base no perfil comportamental, localização (inferida por GPS ou CEP) ou até mesmo

no dispositivo de acesso do consumidor (um celular de última geração pode sinalizar maior poder aquisitivo e, assim, receber preços mais altos).

Sob a ótica do CDC, tal prática já fere o princípio da boa-fé objetiva (Art. 4º, III) e é vedada por elevar, sem justa causa, o preço de produtos (Art. 39, X), além de ferir a isonomia entre os consumidores. Contudo, é a análise de Doneda (2023) sobre a perfilização (profiling) que revela a gravidade do ato. A precificação dinâmica não é aleatória; ela é o resultado direto da capacidade tecnológica de criar perfis detalhados, categorizando e "pontuando" consumidores. Doneda (2023) explica que a ameaça central da perfilização é a perda da autodeterminação informativa, onde o indivíduo é "congelado" em um perfil que ele não controla e que passa a ditar as oportunidades que lhe são oferecidas. Quando uma plataforma de e-commerce usa esse perfil para cobrar mais caro, ela não está apenas lesando o consumidor financeiramente (violando o CDC); ela está violando o direito do titular de não ser submetido a decisões automatizadas que afetem seus interesses sem seu conhecimento e sem transparência (violando o Princípio da Transparência e o Art. 20 da LGPD).

O segundo exemplo são os chamados Dark Patterns (Padrões Sombrios). São elementos de design em interfaces de sites e aplicativos (UI/UX) deliberadamente projetados para enganar, coagir ou manipular o usuário a tomar decisões que não são do seu interesse, como realizar uma compra por impulso, assinar um serviço sem perceber ou, crucialmente, fornecer mais dados do que o necessário. No âmbito do CDC, os Dark Patterns são evidentes práticas abusivas, enquadrando-se perfeitamente no Art. 39, IV: "prevalece-se da fraqueza ou ignorância do consumidor, tendo em vista sua idade, saúde, conhecimento ou condição social, para impingir-lhe seus produtos ou serviços".

Mas é na intersecção com a tese de Doneda (2023) que sua gravidade é totalmente exposta. Se, como vimos no Capítulo II, o consentimento no e-commerce já sofre do "mito do consentimento" devido à assimetria de poder (a política do "pegar ou largar"), os Dark Patterns são a ferramenta prática dessa assimetria. Eles são a materialização da má-fé. Doneda (2023) defende a autodeterminação informativa como o direito do indivíduo de ter controle sobre o fluxo de seus dados.

Os Dark Patterns (como caixas de "aceito" pré-marcadas, botões "recusar" escondidos ou a dificuldade imposta para cancelar um newsletter) são projetados especificamente para retirar esse controle, induzindo o consumidor a "consentir" de forma não-livre, não-informada e não-inequívoca. Eles são a prova de que a plataforma não está buscando o consentimento, mas apenas a legitimação formal para uma coleta de dados que já era abusiva em sua origem.

6 CONSIDERAÇÕES FINAIS

Este artigo teve como objetivo analisar os desafios e os instrumentos de proteção do consumidor na era do comércio eletrônico, um ambiente marcado pela economia dos dados. A investigação partiu da constatação de que o conceito clássico de privacidade, focado no "direito de ser deixado em paz", mostrou-se insuficiente para lidar com os riscos da coleta e processamento massivo de informações pessoais.

Conclui-se, em linha com a tese central de Danilo Doneda (2023), que a proteção de dados pessoais emergiu como um direito fundamental autônomo, focado na autodeterminação informativa. O problema central do e-commerce não é a intrusão, mas a perda de controle do consumidor sobre o fluxo de seus próprios dados, que são tratados como matéria-prima.

O estudo das bases legais da LGPD (Capítulo II) revelou a complexidade dessa proteção. Demonstrou-se que o "mito do consentimento", em um cenário de profunda assimetria de poder, serve frequentemente como mera formalidade para legitimar abusos. Mais importante, identificou-se o legítimo interesse (Art. 7º, IX) como o verdadeiro e mais perigoso campo de tensão, onde a ausência de um teste de ponderação (LIA) transparente e fiscalizado o transforma em um "cheque em branco" para práticas de profiling e marketing invasivo.

Diante da fragilidade das bases legais, a pesquisa avançou para a implementação prática da lei (Capítulo III). Verificou-se que a eficácia da LGPD não reside no cumprimento de um mero "checklist". A verdadeira adequação, conforme a tese de Doneda (2023), exige a internalização da Accountability (prestação de contas) e da Abordagem Baseada em Risco. Ferramentas como o

Relatório de Impacto (DPIA) e o Privacy by Design não são tarefas burocráticas, mas os instrumentos pelos quais a empresa de e-commerce deve proativamente gerenciar os riscos que seus algoritmos de discriminação e manipulação criam.

Por fim, o Capítulo IV consolidou o argumento ao aplicar a teoria do Diálogo das Fontes. Ao conectar a LGPD ao Código de Defesa do Consumidor, foi possível definir o consumidor digital como um sujeito em estado de hipervulnerabilidade informacional. Práticas como a precificação dinâmica e o uso de Dark Patterns não são apenas estratégias de venda: são atos duplamente ilícitos. Elas violam simultaneamente o CDC (ao explorar a fraqueza e ferir a boa-fé) e a LGPD (ao sabotar a autodeterminação informativa e viciar o consentimento).

Portanto, a LGPD é, de fato, o instrumento jurídico essencial para a proteção do consumidor na era digital. Contudo, sua efetividade não é automática. Ela está condicionada a três fatores cruciais que representam os desafios futuros: 1) a superação da cultura do "checklist" pelas empresas, em favor de uma real governança de riscos; 2) uma fiscalização robusta da Autoridade Nacional de Proteção de Dados (ANPD), especialmente na auditoria dos testes de legítimo interesse; e 3) o fomento de uma "cultura cidadã de proteção de dados", que capacite os consumidores a exercerem ativamente os direitos que a lei lhes assegura.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia orientativo cookies e proteção de dados pessoais. Brasília, DF: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf. Acesso em: 20 nov. 2025.

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

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 20 nov. 2025.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República. Disponível em:

http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 20 nov. 2025.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Código de Defesa do Consumidor (CDC).** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L8078compilado.htm. Acesso em: 20 nov. 2025.

BRASIL. "LEI Nº 13.709, de 14 de AGOSTO de 2018." *Planalto.gov.br*, 2022, www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** 3. ed. São Paulo: Thomson Reuters Brasil, 2023.

GUIAS DE BOAS PRÁTICAS LEI GERAL DE PROTEÇÃO DE DADOS (LGPD). Brasília, DF: Ministério da Economia, Secretaria de Governo Digital, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. Acesso em: 20 nov. 2025.

INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR (IDEC). São Paulo: IDEC, [2025]. Disponível em: https://idec.org.br/. Acesso em: 20 nov. 2025.

E-COMMERCE E SEUS DESAFIOS NA COLETA E ARMAZENAMENTO DE DADOS DE CLIENTES

Emilly de Alcântara Cordeiro[1]

RESUMO

O presente artigo tem como objetivo analisar os desafios enfrentados pelo comércio eletrônico diante da aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD), com ênfase no estudo da plataforma Mercado Livre. O avanço da economia digital trouxe benefícios inegáveis à sociedade, permitindo maior comodidade, rapidez nas transações e ampliação das oportunidades de negócios. No entanto, esse crescimento também ampliou os riscos relacionados à privacidade, à segurança das informações e ao uso indevido de dados pessoais. Nesse contexto, torna-se essencial compreender como as empresas do setor vêm se adaptando à legislação e quais medidas podem ser adotadas para garantir a conformidade com os princípios da LGPD. O artigo apresenta uma abordagem qualitativa e exploratória, fundamentada em revisão bibliográfica e análise documental de práticas empresariais, buscando compreender o impacto jurídico, técnico e ético da proteção de dados no ambiente digital. A Lei nº 13.709, de 14 de agosto de 2018, dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), estabelecendo regras claras sobre coleta, armazenamento e compartilhamento de informações. Nesse sentido, a pesquisa demonstra que a adequação à LGPD requer não apenas investimentos em infraestrutura tecnológica e políticas de segurança da informação, mas também o desenvolvimento de uma cultura organizacional voltada à ética, à transparência e ao respeito à privacidade dos usuários. Conclui-se que a conformidade com a LGPD é um desafio contínuo, que demanda capacitação dos colaboradores, revisão de processos internos e comprometimento institucional. Além de atender às exigências legais, a adequação fortalece a confiança dos consumidores, tornando-se um diferencial competitivo e um fator essencial para a consolidação de um ambiente digital mais seguro, responsável e sustentável.

Palavras-chave: Plataformas Digitais; Documentos; Segurança; Internet; Empresas.

Sumário: Introdução; fundamentos Jurídicos; o marco civil da LGPD; Desafios e Prática de adequação; Comércio eletrônico e o uso de dados pessoais; Garantias da LGPD, Jurisprudência, Infraestrutura Tecnológica Necessária; Ética na Coleta de Dados; Integração entre Sistemas e Fontes de Dados; Conclusão e Referências.

[1] Graduando em Direito e Administração no Uniceub - Centro Universitário de Brasília, Formada em Inglês pela Casa Thomas Jefferson. E-mail: emillyalcantara069@gmail.com.

1 INTRODUÇÃO

O comércio eletrônico já faz parte da nossa rotina, com poucos cliques, compramos o que precisamos sem sair de casa, aproveitando a praticidade, a rapidez e a enorme variedade que a internet oferece. Mas, enquanto tudo isso parece simples para o usuário, existe um desafio importante por trás das telas: o cuidado com os dados pessoais dos clientes. Informações como nome, endereço, CPF e até dados de pagamento são essenciais para que a compra aconteça, e justamente por isso precisam ser tratadas com muita responsabilidade. Qualquer descuido pode colocar a privacidade das pessoas em risco. Por isso, as empresas de e-commerce precisam investir cada vez mais em tecnologia, transparência e práticas seguras para proteger seus usuários. Diante desse cenário, discutir como essas plataformas lidam com esses desafios se torna fundamental para construir um ambiente digital mais confiável e seguro para todos.

2 O IMPACTO DA LGPD NA PROTEÇÃO DE DADOS E NOS DESAFIOS DO COMÉRCIO ELETRÔNICO NO BRASIL

O crescimento exponencial do comércio eletrônico nas últimas décadas transformou profundamente as relações de consumo e a forma como empresas e clientes interagem no ambiente digital. Plataformas como o Mercado Livre tornaram-se parte essencial da economia brasileira, conectando milhões de vendedores e compradores em transações diárias que envolvem um volume expressivo de dados pessoais e financeiros. Contudo, esse cenário também intensificou os riscos relacionados ao vazamento de informações, fraudes virtuais e uso indevido de dados para fins comerciais.

Diante desse contexto, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), surgiu como uma resposta normativa e ética à crescente preocupação com a privacidade. A legislação estabelece princípios, direitos e deveres para o tratamento de informações, exigindo das empresas maior responsabilidade e transparência em suas operações. No entanto, a implementação

efetiva da LGPD representa um desafio complexo, especialmente para o setor de e-commerce, que lida com grandes bases de dados e múltiplos agentes de tratamento.

2.1 A LGPD e seus fundamentos jurídicos

A LGPD foi inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e representa um marco para o ordenamento jurídico brasileiro. A lei define dado pessoal como toda informação relacionada a pessoa natural identificada e estabelece princípios como finalidade, adequação, necessidade, livre acesso, qualidade, segurança e responsabilização. Esses princípios visam assegurar que o tratamento de dados ocorra de forma ética e proporcional aos objetivos declarados pelas empresas.

Além disso, a LGPD criou a Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar e orientar o cumprimento da legislação. O papel da ANPD é essencial para promover uma cultura de proteção de dados e garantir que o tratamento das informações respeite os direitos fundamentais dos titulares.

2.2 O comércio eletrônico e o uso de dados pessoais

O e-commerce depende fortemente do uso de dados pessoais para oferecer serviços personalizados e eficientes. As plataformas coletam informações como nome, CPF, endereço, histórico de navegação e preferências de consumo, utilizando-as para recomendar produtos, calcular fretes e aprimorar a experiência do usuário. Entretanto, esse tratamento massivo de dados eleva o risco de incidentes de segurança, exigindo medidas técnicas e organizacionais adequadas.

No contexto brasileiro, o crescimento das vendas online durante a pandemia de COVID-19 intensificou o volume de dados tratados diariamente. Segundo dados da Associação Brasileira de Comércio Eletrônico (ABCOMM), o setor cresceu mais de 70% entre 2020 e 2022, o que evidencia a urgência de políticas de proteção compatíveis com o novo cenário digital. Assim, compreender o funcionamento do e-commerce à luz da LGPD é fundamental para equilibrar o desenvolvimento econômico e a proteção do consumidor.

2.3 O caso do Mercado Livre: desafios e práticas de adequação

O Mercado Livre é uma das maiores plataformas de comércio eletrônico da América Latina, processando milhões de transações diariamente. Seu modelo de negócios envolve o uso intensivo de dados para fins de autenticação, personalização de ofertas, análise de crédito e prevenção de fraudes. Tais operações demandam alto grau de segurança da informação e conformidade com a legislação vigente.

Entre os principais desafios enfrentados pela empresa estão o gerenciamento de consentimentos, a atualização constante das políticas de privacidade e a integração de sistemas com terceiros, como transportadoras e processadores de pagamento. A LGPD exige que o usuário seja informado de maneira clara sobre o uso de seus dados e tenha a possibilidade de revogar o consentimento a qualquer momento. Além disso, a plataforma precisa assegurar que os parceiros comerciais também estejam em conformidade, evitando a responsabilização solidária por eventuais vazamentos.

O Mercado Livre implementou uma série de medidas de adequação, incluindo políticas internas de governança de dados, criptografia avançada e auditorias de segurança. A empresa também disponibiliza um Encarregado de Proteção de Dados (DPO), responsável por intermediar o contato com os titulares e com a ANPD. Apesar dos avanços, ainda existem dificuldades na padronização de práticas entre os diversos países em que a companhia atua, o que reforça a complexidade da gestão de dados em escala global.

2.4 Desafios técnicos e jurídicos na aplicação da LGPD ao E-commerce

A aplicação da LGPD no e-commerce envolve desafios que transcendem a simples adequação documental. É necessário implementar soluções tecnológicas capazes de garantir a integridade e confidencialidade das informações, como firewalls, backups seguros, monitoramento de acessos e eliminação de identidade. Do ponto de vista jurídico, as empresas precisam revisar contratos com

fornecedores, atualizar termos de uso e definir critérios de responsabilização em casos de incidentes de segurança.

Outro ponto relevante é a capacitação das equipes. A conformidade com a LGPD depende do comprometimento de todos os colaboradores, desde o atendimento ao cliente até o setor de TI. A ausência de cultura organizacional voltada à privacidade é um dos principais obstáculos para o cumprimento efetivo da legislação. Nesse sentido, o investimento em educação digital é uma estratégia indispensável para o sucesso da implementação.

2.5 A importância da conscientização dos usuários sobre a proteção de dados

Além das responsabilidades atribuídas às empresas, é fundamental reconhecer o papel dos próprios usuários na construção de um ambiente digital mais seguro. A proteção de dados pessoais não depende apenas de políticas corporativas e mecanismos tecnológicos, mas também da conscientização dos consumidores quanto ao uso responsável das plataformas online. Muitos incidentes de segurança ocorrem devido ao compartilhamento inadvertido de informações em sites ou aplicativos, à falta de verificação de autenticidade de páginas e à ausência de boas práticas de navegação.

Nesse sentido, campanhas educativas e ações de sensibilização são essenciais para que os usuários compreendam seus direitos garantidos pela LGPD, como o acesso, a correção, a portabilidade e a exclusão de dados. Além disso, é necessário que as plataformas invistam em interfaces mais acessíveis e transparentes, permitindo que o titular de dados exerça o controle efetivo sobre suas informações. A combinação entre educação digital e responsabilidade compartilhada fortalece o ecossistema de proteção de dados e contribui para a criação de uma cultura de privacidade mais sólida no ambiente virtual.

2.6 O papel da governança corporativa na efetividade da LGPD

A implementação da LGPD nas empresas vai além da adoção de ferramentas de segurança; ela requer uma estrutura organizacional pautada em governança e gestão de riscos. A governança corporativa, nesse contexto, assume um papel estratégico, pois define políticas, responsabilidades e fluxos de decisão relacionados ao tratamento de dados pessoais. As empresas que incorporam boas práticas de governança conseguem identificar vulnerabilidades com maior rapidez, prevenir falhas e demonstrar transparência diante de órgãos reguladores e consumidores.

Além disso, a governança favorece a criação de comitês internos de proteção de dados, que atuam de forma interdisciplinar, envolvendo áreas como tecnologia da informação, jurídico e recursos humanos. Essa integração assegura que a proteção de dados seja tratada como uma prioridade institucional e não apenas como uma obrigação legal. Assim, o fortalecimento da governança corporativa contribui para a efetividade da LGPD, reduzindo riscos, promovendo a confiança dos clientes e consolidando uma imagem empresarial alinhada à ética digital e à sustentabilidade das relações comerciais no ambiente online.

2.7 Infraestrutura tecnológica necessária

Para que uma empresa consiga coletar e usar dados de forma inteligente, ela precisa ter uma boa base tecnológica, como os “bastidores” que fazem tudo funcionar. Isso envolve servidores confiáveis, armazenamento seguro (geralmente na nuvem), sistemas que organizam as informações e ferramentas que ajudam os dados a circularem sem se perder pelo caminho.

Com a chegada da LGPD, essa necessidade ficou ainda mais evidente. A lei deixou claro que não basta ter dados é preciso protegê-los. Isso significa que a empresa deve cuidar dessas informações como se fossem um patrimônio valioso, garantindo que não caiam em mãos erradas e que sejam usadas de forma correta e transparente.

Para isso, a infraestrutura tecnológica precisa incluir:

I. **Criptografia**: para que dados importantes fiquem ilegíveis em caso de acesso indevido;

II. **Controles de acesso**: garantindo que só pessoas autorizadas enxerguem certas informações;

III. **Monitoramento constante**: para detectar qualquer ameaça rapidamente;

IV. **Backups**, para evitar perda de dados;

V. **Ferramentas de governança**: ajudam a acompanhar todo o caminho dos dados dentro da empresa.

No fim das contas, a LGPD faz com que tecnologia e responsabilidade andem juntas. As empresas precisam não apenas de sistemas modernos, mas também de uma postura ética e cuidadosa.

2.8 Ética na coleta de dados

Quando uma empresa coleta dados, ela está lidando com algo que pertence ás pessoas, ou seja, informações que dizem quem elas são, o que gostam, o que fazem. Por isso, a ética se torna essencial. Não é só uma questão de seguir leis, como a LGPD, mas de agir com respeito.

Ser ético na coleta de dados significa ser honesto e transparente: avisar claramente o que está sendo coletado, para que será usado e dar às pessoas a chance de escolher. Também envolve não exagerar e coletar apenas o que realmente é necessário, sem invadir a privacidade de ninguém.

Além disso, a empresa deve cuidar desses dados como se fossem algo frágil e valioso, garantindo segurança e evitando qualquer uso abusivo. No fundo, ética em dados é sobre confiança, a empresa mostra que valoriza as pessoas e que usa as informações delas com responsabilidade, empatia e bom senso.

2.9 Integração entre sistemas e fontes de dados

Para que uma empresa realmente aproveite seus dados, não basta só juntar informações de vários sistemas. É claro que integrar tudo, como registros de vendas,

atendimentos, redes sociais e ferramentas internas, ajuda muito, porque dá uma visão mais completa do negócio. É como colocar todas as peças da informação em uma mesma mesa.

Mas existe outro ponto importante, as pessoas dentro da empresa precisam querer e saber usar esses dados. Sem uma cultura data-driven, onde decisões são feitas com base em informações reais e não apenas na intuição, toda essa integração perde valor. Às vezes, a empresa até tem tecnologia, mas falta hábito, confiança ou preparo para transformar dados em ação.

No fundo, integração de sistemas e cultura de dados caminham juntas. Não adianta ter dados bem organizados se ninguém os usa, e também não adianta querer ter data-driven sem ter acesso às informações certas. Quando esses dois lados se conectam, a empresa passa a entender melhor seus clientes, resolver problemas com mais precisão e tomar decisões mais inteligentes.

3 O MARCO CIVIL DA INTERNET E SUAS GARANTIAS NA LGPD

O Marco Civil da Internet, instituído pela Lei nº 12.965/2014, é considerado o marco regulatório fundamental da internet no Brasil, pois estabelece princípios, garantias, direitos e deveres para o uso da rede no país. Essa legislação surgiu da necessidade de equilibrar a liberdade de expressão, a privacidade dos usuários e a neutralidade da rede, assegurando que o ambiente digital fosse regido por normas claras e voltadas à proteção dos direitos fundamentais. Entre seus pilares estão a preservação da intimidade, a inviolabilidade das comunicações e o direito à indenização em casos de danos decorrentes de violação de dados. Dessa forma, o Marco Civil da Internet criou a base jurídica para a construção de uma internet mais segura e responsável.

Com o avanço da tecnologia e a intensificação do uso de dados pessoais em larga escala, tornou-se evidente a necessidade de uma legislação mais específica sobre o tratamento dessas informações. Nesse cenário, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) foi elaborada para complementar o Marco Civil da Internet, trazendo regras detalhadas sobre coleta, armazenamento,

compartilhamento e eliminação de dados pessoais. Enquanto o Marco Civil define princípios gerais de uso da rede, a LGPD estabelece mecanismos concretos de proteção e responsabilização, garantindo que o tratamento de informações seja feito de forma ética, transparente e consentida. Assim, as duas leis se complementam e formam o arcabouço jurídico essencial da privacidade digital no Brasil.

As garantias asseguradas por essas legislações reforçam o direito constitucional à privacidade e à proteção da vida privada, previsto no artigo 5º, inciso X, da Constituição Federal. O cidadão passou a ter mais controle sobre suas informações, podendo exigir das empresas a correção, exclusão ou portabilidade de seus dados. Além disso, tanto o Marco Civil quanto a LGPD reforçam a importância da responsabilização das empresas e da transparência nas relações digitais, estimulando uma cultura de respeito e segurança no ambiente virtual. Em conjunto, essas normas representam um avanço significativo na defesa dos direitos digitais, contribuindo para o fortalecimento da confiança entre usuários, provedores e instituições que atuam no ecossistema digital brasileiro.

Hoje em dia, os dados dos clientes são um dos bens mais valiosos que uma empresa pode ter. Eles mostram quem são as pessoas que confiam na marca, o que compram, como usam os serviços e até informações pessoais sensíveis. Por isso, guardar esses dados com cuidado não é apenas uma obrigação legal, mas também uma forma de respeito e compromisso com o consumidor.

Quando uma empresa coleta informações, ela assume a responsabilidade de mantê-las seguras, protegidas contra acessos indevidos e bem armazenadas. É como se estivesse recebendo algo precioso, que não pode ser deixado exposto ou tratado de qualquer jeito. Além de ser uma questão moral, essa proteção é exigida por leis como a LGPD, que reforçam que o cliente tem direito à privacidade e à segurança.

E quando esses dados são vazados, seja por falha de segurança, descuido ou violação dos sistemas, o cliente não fica desamparado. Ele pode recorrer judicialmente para buscar seus direitos, pedir a responsabilização da empresa e, quando for o caso, solicitar indenização pelos prejuízos sofridos. Isso vale tanto para danos financeiros quanto para situações que coloquem em risco a tranquilidade e a privacidade do consumidor.

3.1 Análise da Jurisprudência TJDFT – Processo nº 0701695-39.2025.8.07.0021

Poder judiciário da União Tribunal de Justiça do Distrito Federal e dos territórios gabinete da juiza de direito Marília de Ávila e Silva Sampaio número do processo: 0701695-39.2025.8.07.0021 classe judicial: embargos de declaração cível (1689) embargante: NU financeira s.a. - sociedade de credito, financiamento e investimento embargado: Adriana da Conceicão Rodrigues da Silva despacho. Nos termos do artigo 1023, § 2º, CPC, colha-se manifestação do embargado, no prazo legal. Brasília/DF, 23 de outubro de 2025. Marília de Ávila e Silva Sampaio Relatora.

A decisão proferida pela Segunda Turma Recursal do Tribunal de Justiça do Distrito Federal e Territórios traz uma análise relevante e bastante atual sobre golpes praticados contra consumidores mediante uso indevido de dados pessoais, questão que tem se tornado cada vez mais frequente diante da crescente digitalização das relações bancárias. O caso trata de uma consumidora que, após receber uma ligação de alguém que se passou por funcionário do banco, acabou sendo vítima de fraude. O ponto central da controvérsia gira em torno de como o suposto fraudador obteve dados pessoais sigilosos da autora, o que reforçou a credibilidade da ligação e contribuiu diretamente para a concretização do golpe.

A consumidora buscou a Justiça pretendendo a declaração de nulidade das operações bancárias realizadas por terceiros e a condenação do banco ao pagamento de indenização por danos morais. Em primeira instância, porém, o pedido foi rejeitado, sob o argumento de que não teria havido falha do banco e que a fraude teria sido possível por culpa exclusiva da vítima. Inconformada, a autora recorreu à Turma Recursal.

Ao analisar o caso, o colegiado adotou uma postura diferente. A Turma Recursal observou que o fraudador possuía informações sensíveis e específicas da cliente dados que, em circunstâncias normais, deveriam estar protegidos pelos mecanismos de segurança da instituição financeira. Esse ponto foi determinante para

que o Tribunal, o simples fato de o criminoso ter tido acesso a informações internas do banco indica que houve falha na guarda, na segurança ou no sigilo dessas informações. Em outras palavras, ainda que a fraude não tenha ocorrido dentro do aplicativo ou do sistema bancário, houve um vazamento de dados, e isso caracteriza falha no serviço prestado.

Com base nesse entendimento, o julgamento aplicou o artigo 14 do Código de Defesa do Consumidor, que estabelece a responsabilidade objetiva dos fornecedores de serviços, isto é, eles respondem independentemente de culpa quando há defeito na prestação do serviço. Além disso, foram utilizados como fundamento os artigos 42 e 43 da Lei Geral de Proteção de Dados (LGPD), que tratam, respectivamente, da responsabilidade do agente de tratamento por danos decorrentes de violação à segurança dos dados e do dever de transparência quanto ao tratamento dessas informações.

Outro ponto relevante foi a aplicação da Súmula 479 do Superior Tribunal de Justiça (STJ), que dispõe que as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito das operações bancárias. Ou seja, mesmo que um terceiro tenha praticado o golpe, se esse ato encontra relação com a atividade bancária e ocorre em seu contexto, o banco deve assumir a responsabilidade.

Com base nessa construção jurídica, a Turma Recursal reconheceu que as operações contestadas não poderiam ser atribuídas à consumidora e, portanto, declarou sua nulidade. Esse entendimento reforça a proteção do consumidor frente à crescente sofisticação de golpes que exploram vulnerabilidades nos sistemas de informação das instituições financeiras.

Por outro lado, ao analisar o pedido de indenização por danos morais, o Tribunal adotou um posicionamento mais moderado. Embora tenha reconhecido a falha de segurança, considerou que o caso não ultrapassou o limite do mero aborrecimento. Para a Turma, não houve prova suficiente de que a consumidora tenha experimentado abalo significativo à sua dignidade, desgaste psicológico relevante ou exposição vexatória. Assim, decidiu que o episódio não configurou dano moral indenizável, sendo insuficiente para gerar compensação financeira.

O recurso da autora, portanto, foi conhecido e parcialmente provido e já as operações foram anuladas, mas não houve condenação em danos morais. A decisão também afastou o pagamento de honorários, por se tratar de julgamento em sede de Juizado Especial, onde não há sucumbência recursal.

No conjunto, essa jurisprudência reforça a compreensão de que os bancos têm o dever de adotar medidas eficazes para proteger os dados de seus clientes, inclusive contra ameaças externas. Ao mesmo tempo, evidencia o rigor adotado pelos tribunais na análise de pedidos de danos morais, exigindo comprovação de prejuízo efetivo além do simples incômodo.

3.2 Jurisprudência Processo nº 0701391-10.2024.8.07.0010

Juizado especial cível. Recurso inominado. Direito do consumidor. Golpe praticado via telefone. Análise casuística. Fragilização de dados cadastrais. Lgpd art. 43 dever de segurança. Compra com cartão de crédito. Falha na prestação do serviço. Devolução em dobro. Devida. Recurso conhecido e não provido. 1. Na origem, trata-se de pretensão indenizatória por danos materiais, em decorrência de compra feita no cartão de crédito da autora, além de compensação por danos morais. O recurso do banco réu visa a reforma da sentença para que sejam julgados improcedentes os pedidos formulados na inicial, por se tratar de culpa exclusiva da requerente, ante a ausência do dever de cautela na guarda do plástico, e que não houve comunicação dos fatos à autoridade policial. 2. Recurso próprio, tempestivo e com preparo regular (ID 62273486). Contrarrazões apresentadas, id 62273493.

O caso trata de uma consumidora que sofreu golpe por telefone, no qual terceiros realizaram compra indevida utilizando seu cartão de crédito. A sentença reconheceu a responsabilidade do banco e determinou a devolução em dobro do valor cobrado. O banco recorreu, alegando culpa exclusiva da cliente por falta de cuidado e ausência de boletim de ocorrência.

A Turma Recursal destacou que a relação é de consumo, regida pelo CDC, que presume a vulnerabilidade do consumidor. Em operações digitais essa vulnerabilidade é ainda maior, pois o cliente depende totalmente dos sistemas e da

segurança do fornecedor. O acórdão reconhece que houve fragilização dos dados pessoais, violando o dever de segurança previsto na LGPD, especialmente o art. 43.

O Tribunal explicou que as instituições financeiras respondem objetivamente por fraudes praticadas por terceiros, conforme a Súmula 479 do STJ, pois esses riscos fazem parte da própria atividade bancária. Com a expansão das operações digitais, aumentaram também os golpes, e os bancos devem investir em mecanismos capazes de proteger seus clientes.

A análise de fraudes deve ser feita caso a caso, mas neste processo ficou claro que os estelionatários possuíam dados sigilosos da consumidora, o que deu credibilidade ao golpe. Assim, o banco não conseguiu provar que a fraude ocorreu por culpa exclusiva da cliente. Ao contrário, verificou-se falha no sistema de segurança e violação à proteção dos dados pessoais. Á decisão também aplicou a teoria da aparência, pois a fraude simulava de forma convincente um contato legítimo do banco. A consumidora, portanto, não tinha meios razoáveis de identificar o golpe.

Reconhecida a cobrança indevida e inexistindo engano justificável, o Tribunal determinou a devolução em dobro, conforme art. 42, parágrafo único, do CDC. Não se exige má-fé do fornecedor, apenas erro injustificável, o que ficou caracterizado.

O recurso do banco foi conhecido, mas não provido, mantendo-se integralmente a sentença que condenou o banco à restituição dobrada e ao pagamento de honorários. A decisão foi unânime.

4 CONCLUSÃO

A adequação à LGPD é fundamental para uma economia digital ética e segura. No e-commerce, empresas como o Mercado Livre enfrentam desafios na coleta e proteção de dados pessoais. A adaptação envolve não apenas tecnologias avançadas, mas também uma mudança cultural, com todos os colaboradores comprometidos com a privacidade e a transparência.

Os desafios enfrentados pelo e-commerce são múltiplos e interligados, além de garantir a segurança das informações, é necessário obter consentimento claro dos usuários, gerenciar de forma adequada os dados compartilhados com parceiros e fornecedores, e atualizar constantemente políticas internas e externas para acompanhar a evolução da legislação. A conformidade com a LGPD, portanto, não é um esforço pontual, mas uma responsabilidade contínua que exige investimento constante, alinhamento estratégico e comprometimento institucional em todas as áreas da empresa.

Do ponto de vista jurídico, o entendimento dos tribunais superiores, como o STJ e o STF, reforça que a responsabilidade das plataformas digitais varia conforme o nível de intermediação nas transações e o tratamento de dados realizados. Plataformas que atuam apenas como intermediárias ou facilitadoras de anúncios têm sua responsabilidade limitada, mas isso não exime a obrigação de cumprir integralmente a LGPD. Esse posicionamento evidencia a necessidade de cada empresa avaliar cuidadosamente seu modelo de operação, garantindo que todas as práticas estejam alinhadas com a legislação e com os direitos dos consumidores.

Além dos aspectos legais, a proteção de dados tornou-se um diferencial competitivo no mercado digital. Empresas que priorizam a segurança, a transparência e o respeito à privacidade fortalecem a confiança dos clientes, aumentam sua credibilidade e consolidam uma reputação sólida frente à concorrência. Em um ambiente de constantes ataques cibernéticos, fraudes online e vazamento de informações, a confiança do consumidor é um ativo estratégico que impacta diretamente a sustentabilidade do negócio e a sua capacidade de crescimento no longo prazo.

A adequação à LGPD vai além do cumprimento legal, sendo uma oportunidade de transformação cultural e tecnológica no e-commerce. Boas práticas de governança de dados e transparência fortalecem a confiança do consumidor e o posicionamento das empresas. A privacidade passa a ser um pilar da inovação responsável e do sucesso sustentável no mercado digital. No fim, proteger dados não é apenas uma tarefa técnica, é um ato de confiança. Quanto melhor a empresa cuida dessas informações, mais segura a relação com o cliente se torna.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, 2018.

ANPD – Autoridade Nacional de Proteção de Dados. Guia de boas práticas para o tratamento de dados pessoais. Brasília, 2023.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. São Paulo: Revista dos Tribunais, 2019.

MERCADO LIVRE. Política de privacidade. Disponível em: https://www.mercadolivre.com.br/privacidade. Acesso em: 13 out. 2025.

ABCOMM – Associação Brasileira de Comércio Eletrônico. Relatório de crescimento do setor 2022. São Paulo, 2023.

BRASIL ESCOLA. Lei Geral de Proteção de Dados (LGPD): o que é e quais seus objetivos. Disponível em: https://brasilescola.uol.com.br/. Acesso em: 24 nov. 2025.

PORTAL GOV.BR. Entenda a LGPD e como ela protege seus dados pessoais. Disponível em: https://www.gov.br/anpd. Acesso em: 24 nov. 2025.

SEBRAE. Panorama do comércio eletrônico no Brasil (2024). Disponível em: https://www.sebrae.com.br/. Acesso em: 24 nov. 2025.

ECOMMERCE BRASIL. Tendências do e-commerce brasileiro em 2025. Disponível em: https://www.ecommercebrasil.com.br/. Acesso em: 24 nov. 2025.

JURISPRUDÊNCIA – 0701695-39.2025.8.07.0021. *Acórdão 2054253, 0701695-39.2025.8.07.0021*. Relator(a): MARÍLIA DE ÁVILA E SILVA SAMPAIO, Segunda Turma Recursal, data de julgamento: 08/10/2025, publicado no DJe: 17/10/2025.

JURISPRUDÊNCIA – 0701391-10.2024.8.07.0010. *Acórdão 1908313, 0701391-10.2024.8.07.0010*. Relator(a): MARÍLIA DE ÁVILA E SILVA SAMPAIO, Segunda Turma Recursal, data de julgamento: 19/08/2024, publicado no DJe: 26/08/2024.

EXCLUSÃO DIGITAL: A NOVA FACE DA DESIGUALDADE SOCIAL NO BRASIL

Ágatha Ruiz Pinheiro Torres de Florambel[1]
Alana Karoline Andrade[2]
Giovana Andressa Leite Alves[3]

RESUMO

O presente artigo analisa a exclusão digital como componente da desigualdade social no Brasil, evidenciando como o acesso limitado às tecnologias da informação intensifica as vulnerabilidades históricas e compromete a efetivação de direitos fundamentais. Primeiramente, discute-se a expansão do conceito de desigualdade social, que começa a incluir a dimensão tecnológica devido à importância da internet na vida diária. Em seguida, analisa-se a digitalização do Poder Judiciário, ressaltando os progressos do processo eletrônico, mas também os obstáculos decorrentes da falta de uma infraestrutura adequada. O artigo também demonstra que a desigualdade digital repercute diretamente na educação, expondo a precariedade do acesso à internet entre estudantes de baixa renda, restringindo oportunidades de aprendizagem. Além disso, se torna evidente o caráter regional da exclusão digital, pois as regiões Norte e Nordeste apresentam os piores índices de conectividade e menor acesso à banda larga de qualidade, o que limita o uso de serviços públicos digitais, a inserção no mercado de trabalho e o desenvolvimento de competências tecnológicas. A exclusão digital, ao perpetuar e intensificar as desigualdades sociais, educacionais e econômicas, representa um obstáculo significativo à plena cidadania.

Palavras-Chave: Desigualdade social; Internet; Exclusão digital; Informação; Digital; Acesso à Justiça; Processos; Educação; Desigualdade regional.

SUMÁRIO: 1. Introdução; 2. A mudança dos autos físicos para o processo digital e as barreiras da internet; 3. Acesso à Internet como Fator de Exclusão Educacional; 4. Impacto regional e social no acesso à internet; 5. Conclusão.

1 INTRODUÇÃO

[1] Graduanda em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: agatha.florambel@sempreceub.com
[2] Graduanda em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: alana.andrade@sempreceub.com
[3] Graduanda em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: giovana.aalves@sempreceub.com

O desenvolvimento acelerado das tecnologias digitais têm redefinido profundamente a estrutura social contemporânea, revelando que o acesso, ou a falta dele, aos recursos tecnológicos se tornou um fator central na produção de novas formas de desigualdade. Nesse contexto, compreender os impactos da era digital exige analisar como as transformações tecnológicas se articulam às desigualdades já existentes, ampliando ou agravando vulnerabilidades históricas.

A desigualdade social é um fenômeno complexo e multifacetado, como explica Marcelo Ferreira Trezza Knop em sua tese Desigualdade digital e desigualdade social no Brasil. Segundo o autor:

> a desigualdade social é um fenômeno complexo e multifacetado. Multifacetado, pois é influenciado por diversos e complementares fatores, seja pelos mais elementares, como o direito à saúde, à vida e à existência, seja a partir da posse e usufruto de bens materiais, posições e habilidades escassas. Complexo, pois envolve a diversidade presente nas ciências humanas, sociais e sociais aplicadas, e suas implicações teóricas e metodológicas direcionadas à compreensão do fenômeno. (Knop, 2020, p.14)

Portanto, a desigualdade social é afetada por diversos fatores, abrangendo também o acesso à informação, e as tecnologias. Nesse sentido, o acesso à internet tornou-se um novo elemento determinante para a desigualdade social. Contudo, diversos brasileiros ainda vivem à margem dessa realidade digital, o que aprofunda as desigualdades e cria novas barreiras para a vida em sociedade e exercício de diversos direitos, como o acesso à justiça e a educação de qualidade.

Os avanços tecnológicos transformaram de maneira profunda a sociedade e hoje a tecnologia é vista como algo indispensável. Nesse contexto, a internet se faz cada dia mais presente e necessária no cotidiano dos brasileiros, não se pode mais sair de casa sem o celular, pois ele é necessário para ter acesso ao cardápio de um restaurante, para pagar uma conta, e para diversos serviços básicos. Sendo assim, se faz necessária a discussão acerca do que acontece quando não se tem acesso à internet, sendo essa uma forma de exclusão social, que impacta diretamente na desigualdade social.

Como explicam Karen Kohn e Cláudia Herte de Moraes em seu estudo “O impacto das novas tecnologias na sociedade: conceitos e características da Sociedade

da Informação e da Sociedade Digital", os computadores hoje têm um papel fundamental na sociedade, o que altera o cenário social. A tecnologia facilitou diversos serviços, e além disso criou um espaço público virtual para comunicação, o que permite ligar pessoas não só de um mesmo país, como do mundo, e propicia um espaço para debates políticos, econômicos e acesso a informações. No entanto, também explicam que o Brasil é um país marcado pela desigualdade e por isso parcela da sociedade é excluída do fenômeno da globalização, perdendo a participação nesse ambiente digital que é tão rico. (Kohn e Moraes, 2007)

Em "O retrato da exclusão digital na sociedade brasileira" escrito por Lília Bilati de Almeida; Luiza Gonçalves de Paula; Flávio Campos Carelli; Tito Lívio Gomes Osório e Marcelo Genestra" os autores explicam que a exclusão digital também possui um impacto na chance dessas pessoas que não tem acesso às tecnologias de entrarem no mercado de trabalho, citando que nos dias atuais é muito comum o conhecimento em informática ser um requisito para uma vaga de emprego (Almeida, Paula, Carelli, Osório e Genestra, 2011). Além disso, hoje diversos processos de seleção para vagas de emprego acontecem 100% online, então tanto para ter conhecimento dessas vagas, quanto para participar do processo seletivo é preciso ter acesso a internet. Isso, cria mais uma barreira para as pessoas que já estão em situação de vulnerabilidade, pois perdem oportunidades de se inserirem no mercado de trabalho, o que as mantém nessa posição de desvantagem, e dificuldade de mudar de classe social.

Ademais, as tecnologias da informação hoje são também uma ferramenta poderosa para uma educação de qualidade, existem diversos cursos online, que inclusive podem ser gratuitos, além disso dentro da plataforma YouTube existem diversos "vídeos aula" disponíveis, e ainda existem diversas outras ferramentas disponíveis na internet que auxiliam vários estudantes em todos os níveis de ensino. No entanto, isso gera mais um nível de desigualdade, pois os estudantes que não tem acesso à internet podem ficar em desvantagem por não terem acesso a essas ferramentas que facilitam a vida e agregam ao estudo desses alunos.

Ainda, é possível perceber que a desigualdade de acesso às tecnologias possui um recorte regional, ou seja, o acesso às tecnologias é maior em algumas regiões do

Brasil, é menor em outras, devido a desigualdade social entre as regiões do país. Em áreas mais desenvolvidas a infraestrutura da internet é mais ampla e estável, permitindo que a população tenha maior acesso às tecnologias da informação, enquanto em áreas menos desenvolvidas a população enfrenta desafios para acessar a internet no cotidiano.

Além disso, a desigualdade de acesso às tecnologias afeta até mesmo o acesso à justiça, que é um direito fundamental, visto que hoje os processos judiciais tramitam por meio de sistemas digitais. Essa mudança dos autos físicos para o processo digital tende a afastar a população mais vulnerável, que não tem acesso à internet, ou não são capacitados para utilizá-la, do acompanhamento dos seus processos, isso muitas vezes faz com que essas pessoas que não tem conhecimento na área acreditem que não podem recorrer ao poder judiciário.

Nesse contexto, a desigualdade de acesso às tecnologias e a internet é um sério problema no país, pois o Brasil é um país onde 20,5 milhões de pessoas ainda não têm acesso à internet, segundo pesquisa do IBGE de 2024. Vale ressaltar, que para além do acesso à internet, também é essencial a qualidade da rede, para que seja possível realizar um bom uso dessas ferramentas, e o acesso à internet de qualidade é um problema persistente principalmente em regiões mais carentes. Ainda, outro problema é a falta de capacitação para o uso dessas tecnologias, que é necessário para que elas sejam usadas de maneira produtiva.

Portanto, a desigualdade digital ainda é um desafio, e deve ser enfrentada, pois ela contribui aprofundando outras formas de exclusão social, já que quem não tem acesso às tecnologias passa por dificuldades para acompanhar as informações e usufruir de serviços essenciais. Essa exclusão aumenta a desigualdade social e afeta o exercício da cidadania plena, principalmente para a população de baixa renda, que já está em posição de vulnerabilidade e com dificuldade de acesso à internet.

2 A MUDANÇA DOS AUTOS FÍSICOS PARA O PROCESSO DIGITAL E AS BARREIRAS DA INTERNET

No meio de tantos avanços tecnológicos, o poder judiciário também se modernizou, e em 2006 foi editada a Lei n. 11.419, de 19 de dezembro de 2006, que

trata da informatização do processo judicial, e instituiu o processo eletrônico. Tiago Carneiro Rabelo em seu estudo "O PROCESSO JUDICIAL ELETRÔNICO E A EXPERIÊNCIA BRASILEIRA" explica que a partir da edição da Lei n. 11.419, de 19 de dezembro de 2006 o poder judiciário passou por um momento de transformação em diversos âmbitos, inclusive no âmbito dos autos do processo que deixaram de ser físicos e passaram a ser digitais e disponíveis na internet (Rabelo, 2019).

Alessandra Duncke, Camila Cristina Paumann e Leonardo Segatti Colombo em seu artigo "A IMPLEMENTAÇÃO DE UMA CULTURA DE JUSTIÇA DIGITAL" explicam que a transformação do processo físico em digital possui diversas vantagens como "a desnecessidade do uso de papel ou deslocamento até o Fórum da Comarca, bem como a possibilidade de realizar o envio de petições até as 24 (vinte e quatro) horas do dia" (Kuncke, Paumann e Colombo, 2019, p.9 e 10). Os autores também expõem que essa transformação possibilita uma tramitação mais rápida e econômica, além da sustentabilidade por abandonar o uso do papel (Kuncke, Paumann e Colombo, 2019).

No entanto, essa transformação também enfrenta desafios como a desigualdade no acesso às tecnologias, como explicam Germano Pontes Carvalho e Henrique Rodrigues Lelis em seu artigo "A DIGITALIZAÇÃO DOS PROCESSOS JUDICIAIS E A CELERIDADE PROCESSUAL: UMA ANÁLISE À LUZ DO PRINCÍPIO CONSTITUCIONAL DA DURAÇÃO RAZOÁVEL DO PROCESSO." Segundo os autores "A digitalização dos processos judiciais, embora carregue o potencial de democratizar o acesso à justiça, evidencia barreiras que aprofundam as desigualdades sociais" (Carvalho e Lelis, p. 160). Como explicam Carvalho e Lelis, a falta de infraestrutura afeta principalmente a população de regiões afastadas e em situação de vulnerabilidade, além disso expõe outro fator que contribui para essa exclusão digital, que é a falta de acesso à educação e a capacitação dessas pessoas para manejar os aparelhos tecnológicos. Os autores explicam ainda outro problema, que é o alto custo que esses aparelhos possuem e ainda o preço da internet, valores esses que "representam um ônus adicional para famílias de baixa renda, o que acaba restringindo ainda mais o acesso." (Carvalho e Lelis, p. 162).

A Constituição Brasileira, em seu artigo 5°, inciso XXXV prevê que "a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito", deste artigo decorre o direito fundamental de acesso à justiça. O acesso à justiça é um pilar do estado democrático de direito, sobre isso Ana Francisca Figueiredo Dias Bittar, Jannaina Patrícia Pereira e Lara Lemos de Castro Carneiro explicam em seu texto "O direito fundamental de acesso à justiça como pilar do estado democrático de direito"

> O Estado Democrático de Direito é um modelo de governo em que os direitos e as liberdades dos cidadãos são garantidos e protegidos por normas jurídicas. E, para que esses direitos sejam efetivamente realizados, é imprescindível que o sistema de justiça seja acessível a todos os cidadãos, sem distinções, permitindo que estes possam reivindicar seus direitos e proteger-se contra abusos de poder. A acessibilidade à justiça é, portanto, um dos pilares fundamentais do Estado de Direito, pois garante a cidadania plena. (Bittar, Pereira e Carneiro, 2025, p. 8).

Portanto, o acesso à justiça é um direito fundamental, que deve ser garantido a todos os cidadãos, e a instituição do processo eletrônico representa um avanço e promete maior inclusão, acessibilidade, celeridade e economia. No entanto, o Brasil enfrenta um desafio com essa justiça digital, que é garantir o acesso a toda a população, tendo em vista que a exclusão digital é uma realidade na sociedade brasileira. Em virtude da transição dos processos físicos para o meio digital, diversas pessoas que não tem conhecimento na área de tecnologia acreditam que não tem acesso ao seu processo, e ainda, que não tem o direito de acesso à justiça, seja por falta de acesso às informações, por falta dos aparelhos de tecnologia, ou por não saber como utilizá-los.

Diante do exposto, resta claro que a digitalização dos autos judiciais é um avanço irreversível e necessário. Mas, se não vier acompanhada de políticas inclusivas, pode reforçar as desigualdades sociais e devido a dificuldade de uma inclusão digital verdadeira. É notório que o acesso à justiça é afetado por essas novas tecnologias e é preciso combater a desigualdade digital para garantir que todas as pessoas tenham acesso aos seus processos e não se afastem de seus direitos.

3 ACESSO À INTERNET COMO FATOR DE EXCLUSÃO EDUCACIONAL

Como exposto, as tecnologias da informação afetam as mais diversas áreas do cotidiano, criando novas possibilidades e barreiras, e a educação no Brasil, também está passando por transformações devido aos avanços tecnológicos, e esse processo foi acelerado por conta da pandemia de COVID-19. Durante esse período as aulas foram suspensas em razão do isolamento necessário para combater esse vírus, por isso as aulas precisaram ser realizadas de forma remota, sendo transmitidas através das tecnologias disponíveis no meio digital. Essa situação mostra como as tecnologias podem ser aplicadas para beneficiar o ambiente escolar, no entanto também cria barreiras, principalmente devido a desigualdade de acesso à internet.

Durante a pandemia de COVID-19 o problema da desigualdade no acesso à internet foi escancarado, nesse sentido, o artigo "Desigualdades digitais e educação", publicado pela revista Ciência Hoje, discute como a pandemia de COVID-19 ampliou as desigualdades já existentes na educação brasileira, principalmente no acesso às tecnologias digitais. Antes mesmo da pandemia, o acesso à internet e a equipamentos como computadores já era muito desigual entre as classes sociais. Enquanto as famílias de maior renda possuíam boa conectividade e infraestrutura, as de menor renda enfrentam grande dificuldade para acessar recursos tecnológicos. Com o ensino remoto, essas diferenças ficaram ainda mais evidentes, já que muitos alunos das classes mais baixas não tinham computador, internet estável ou apoio para acompanhar as aulas, ficando sem acesso às matérias ministradas.

O texto também destaca que a exclusão digital não se resume à falta de acesso, mas envolve o domínio digital, ou seja, a habilidade de empregar de forma crítica os recursos tecnológicos, interpretar dados, diferenciar informações confiáveis e envolver-se de maneira ativa no espaço virtual. Essa habilidade varia entre diferentes classes sociais e áreas do país, o que acentua as desigualdades na educação e restringe a independência dos estudantes. De acordo com a matéria, diversos jovens de 6 a 14 anos não puderam participar de atividades educacionais durante os tempos de medidas sanitárias, sendo que as que mais sofreram foram aquelas que vêm de lares de menor renda.

A matéria da CNTE "Desigualdade no acesso à internet impacta qualidade da educação" de 2023, expõe que a falta de acesso à internet de qualidade aumenta as desigualdades na educação brasileira. De acordo com pesquisa conduzida pelo centro regional de estudos para o desenvolvimento da sociedade da informação, menos da metade dos estudantes de 9 a 17 anos têm internet na escola, e os mais pobres enfrentam conexões ruins e falta de equipamentos, isso é um reflexo das desigualdades sociais já existentes, e também da desvalorização da educação, que é um problema no país. Durante a pandemia, muitos não conseguiram acompanhar as aulas remotas, o que prejudicou o aprendizado e aumentou as chances de evasão escolar.

Ademais, o direito à educação é um direito social previsto no artigo 6° da Constituição Federal, no entanto a efetivação desse direito para todos, enfrenta diversos desafios, sendo um deles a falta de infraestrutura. Resta demonstrado que as novas tecnologias são muito benéficas em diversas áreas, no entanto o acesso desigual a essas tecnologias cria um problema, pois representam uma barreira para a população de baixa renda ter acesso a diversos serviços, inclusive a educação de qualidade. No âmbito da educação a população mais vulnerável, que tem maior dificuldade de acesso à internet, perde diversas oportunidades, materiais de estudo e inclusive aulas. Em escolas públicas, especialmente nas zonas rurais e periferias urbanas, o acesso a laboratórios de informática, redes Wi-Fi e plataformas educacionais também é limitado. Essa desigualdade no acesso às tecnologias se transforma em uma desigualdade no acesso à educação de qualidade, o que afeta diretamente a vida dessas pessoas em diversas áreas, como no mercado de trabalho e renda. Hoje, o acesso, domínio e o uso crítico das tecnologias são condições essenciais para participação plena na vida escolar e para o desenvolvimento integral dos estudantes.

Em resumo, a batalha contra a desigualdade digital é, na verdade, uma defesa da concretização do direito à educação em seu sentido mais amplo: o direito de adquirir conhecimento, de se engajar e de se desenvolver integralmente na sociedade da informação. Assegurar que todos tenham acesso equitativo à internet, treinamento em tecnologia e um ambiente de estudo adequado representa realizar o conceito

definido na Constituição de uma educação pública, sem custos, acessível e de excelente qualidade para todos os cidadãos brasileiros.

4 IMPACTO REGIONAL E SOCIAL NO ACESSO À INTERNET:

Inicialmente, ao analisar o impacto regional e social no acesso à internet, evidencia-se a importância de compreender como as desigualdades tecnológicas se distribuem pelo território brasileiro. Vale ressaltar que o Brasil é um país profundamente desigual, e tais disparidades também se manifestam entre suas regiões, o que reforça a importância de avaliar como esses fatores influenciam o acesso à conectividade. Nesse panorama, torna-se essencial avaliar os obstáculos significativos e a vulnerabilidade estrutural que dificultam uma inclusão digital eficaz, especialmente nas regiões Norte e Nordeste do país.

Conforme demonstra Eduardo Gomes Mendonça, em seu estudo "DA MARGINALIZAÇÃO À INCLUSÃO DIGITAL: DESAFIOS E OPORTUNIDADES PARA FAVELAS E COMUNIDADES URBANAS BRASILEIRAS", no que diz respeito à infraestrutura e ao acesso, as regiões Norte e Nordeste apresentam a menor cobertura de rede no país, com o Norte registrando 85,3% e o Nordeste, 84,2%, números abaixo da média nacional de 88%. No mesmo estudo, observa-se ainda que o Norte tem o menor percentual de residências com acesso à internet (90,4%), contrastando com 95,4% no Centro-Oeste.

Posto isso, a qualidade do serviço é outra barreira essencial: os altos custos de conexão e a baixa estabilidade da rede comprometem a experiência dos usuários, sobretudo na região Norte do país. Ademais, essa região possui a maior proporção de domicílios cuja conexão principal ocorre via redes móveis 3G ou 4G (27%), enquanto o Sul apresenta maior dependência da fibra óptica. Consequentemente, a predominância do acesso exclusivamente pelo celular, especialmente entre as classes sociais mais baixas, limita de forma significativa o uso da internet para atividades mais robustas, como estudos, trabalho remoto e acesso a serviços públicos (Mendonça, 2024).

Nesse sentido, tais limitações intensificam a desigualdade social, sobretudo porque a falta de acesso à internet e a carência de habilidades digitais, mais evidentes nas regiões Norte e Nordeste, constituem barreiras significativas ao uso pleno de serviços públicos online, como a plataforma Gov.br, por exemplo (Mendonça, 2024).

Conforme observa Mendonça (2024), nas regiões Norte e Nordeste, as famílias de menor renda convivem com uma conectividade restrita, seja pela insuficiência de recursos para a aquisição de computadores, seja pela dificuldade em acessar serviços de internet que ofereçam qualidade adequada. Assim, o autor destaca ainda que, durante a pandemia de Covid-19, essa exclusão digital tornou-se ainda mais evidente, dificultando o acesso a benefícios sociais essenciais, como o auxílio emergencial, agravando vulnerabilidades pré-existentes.

Além disso, a dificuldade de acesso à internet nessas regiões também significa dificuldade de acesso a processos judiciais por meio de sistemas digitais, ao acesso a uma educação de qualidade e ao uso de diversas ferramentas digitais essenciais no cotidiano.

Diante dessas disparidades, o governo federal tem implementado iniciativas e programas estratégicos destinados a mitigar a desigualdade regional no acesso digital, promovendo uma inclusão digital mais ampla no país. Entre as ações previstas na Estratégia Brasileira para a Transformação Digital (E-Digital), destacam-se aquelas direcionadas especialmente às regiões Norte e Nordeste, que, como já demonstrado, apresentam déficits mais acentuados de infraestrutura e conectividade.

Nesse contexto, Mendonça (2024) explica que a E-Digital foi instituída justamente para acelerar a digitalização da sociedade brasileira e ampliar o acesso às Tecnologias da Informação e Comunicação, reunindo programas que buscam fortalecer a infraestrutura de rede em áreas mais vulneráveis.

Entre essas iniciativas, destaca-se o Programa Norte Conectado, que tem como propósito enfrentar os obstáculos geográficos da Amazônia mediante a implantação de cabos de fibra óptica subfluviais no leito dos rios. A medida busca interligar municípios da região e ampliar o acesso à internet de alta velocidade,

beneficiando mais de 9 milhões de habitantes. Embora apresente grande potencial de transformação regional, o programa enfrenta desafios técnicos significativos e elevados custos de manutenção a longo prazo, o que pode comprometer sua sustentabilidade (Mendonça, 2024).

Além do Programa Norte Conectado, outra iniciativa destacada por Mendonça (2024) é o Programa Nordeste Conectado. O autor explica que essa política utiliza a infraestrutura de fibra óptica da CHESF (Companhia Hidrelétrica do São Francisco) para disponibilizar acesso de alta velocidade a cidades-polo e a instituições públicas, especialmente escolas e universidades. Contudo, destaque que por depender majoritariamente da rede já existente, o programa enfrenta limitações para alcançar localidades mais isoladas da região,restringindo o alcance da inclusão digital almejada.

Concomitante a isso, o autor destaca que as regiões Sul e Sudeste do país apresentam uma qualidade de acesso à internet significativamente superior, alcançando cerca de 87% da população conectada, em contraste com os aproximadamente 78% registrados na região Norte. O autor observa, ainda, que a concentração dos projetos de Pesquisa, Desenvolvimento e Inovação (PD&I) do Programa Recursos Humanos em Áreas Estratégicas (RHAE) também se dá majoritariamente nessas duas regiões, o que limita a difusão dos avanços tecnológicos e amplia as desigualdades estruturais no restante do território nacional.

Posto isso, verifica-se, a partir da análise desenvolvida, que, apesar da infraestrutura mais robusta, essas regiões ainda concentram desigualdades internas, particularmente evidentes em comunidades urbanas e favelas, onde a exclusão digital permanece significativa. Nesse sentido, mesmo diante de um contexto geral de melhor conectividade, as classes sociais mais baixas continuam sendo as mais afetadas nas regiões Sul e Sudeste do país, evidenciando que a desigualdade de acesso persiste mesmo nos espaços considerados mais conectados.

Outrossim, a pesquisa TIC Domicílios 2024 demonstra que, embora o acesso à internet esteja se aproximando da universalização, a qualidade do acesso, medida pelo conceito de Conectividade Significativa (CS), varia drasticamente entre as macrorregiões do país. Nesse contexto, a conectividade significativa não se limita ao

simples acesso à internet, pois trata-se da articulação entre infraestrutura de boa qualidade, dispositivos apropriados, competências digitais, oferta de conteúdos úteis e condições socioeconômicas que permitam utilizar a tecnologia de forma plena.

Segundo a pesquisa TIC Domicílios 2024, a análise regional indica que a desigualdade digital permanece profundamente enraizada no Brasil, afetando a capacidade dos indivíduos de aproveitar plenamente as oportunidades oferecidas pelo ambiente online. No que se refere às macrorregiões, o estudo aponta que os maiores níveis de Conectividade Significativa (CS) concentram-se nas regiões Sul e Sudeste, abrangendo 33% e 28% da população, respectivamente, enquanto os menores índices são encontrados no Nordeste e Norte, com 11% e 12%.

Esses dados evidenciam que a inclusão digital no Brasil vai além do simples acesso à internet, dependendo de infraestrutura, capacitação e condições socioeconômicas, ainda desigualmente distribuídas. A concentração de conectividade significativa no Sul e Sudeste reforça desigualdades históricas, deixando Nordeste e Norte em vulnerabilidade e dificultando o aproveitamento das oportunidades digitais.

Sendo assim, embora ainda não se tenha alcançado o cenário ideal, os dados mais recentes da União Internacional de Telecomunicações (UIT) indicam que o Brasil avançou de maneira consistente em suas políticas públicas de inclusão digital. Em 2025, o país atingiu 84,4 pontos no Índice de Desenvolvimento das TICs (IDI), superando os resultados de 2024 (82,0) e 2023 (81,9), além de se situar acima da média global, da média das Américas e dos países de renda média-alta. Esses números refletem a elevação do nível de conectividade significativa no país e evidenciam um progresso rumo a um acesso digital mais amplo, estável e de melhor qualidade para toda a população.

Com isso, no que diz respeito ao impacto das desigualdades de conectividade nas oportunidades digitais, observa-se que o comércio eletrônico também apresenta forte variação regional, uma vez que é muito mais frequente nas regiões Sul (55%) e Sudeste (54%), enquanto no Nordeste (34%), Norte (36%) e Centro-Oeste (36%) essa prática é consideravelmente menos comum, ainda de acordo com a pesquisa TIC Domicílios 2024.

Além disso, o estudo observou que o uso de serviços de governo eletrônico (e-Gov) revela uma relação direta com o nível de instrução e, sobretudo, com os graus de Conectividade Significativa (CS), pois usuários que possuem o nível mais alto de CS acessam plataformas governamentais em 88% dos casos, enquanto aqueles com o nível mais baixo realizam esse acesso em apenas 38%.

Dessa forma, as análises apresentadas evidenciam que a desigualdade digital no Brasil permanece fortemente marcada por disparidades regionais, com as regiões Norte e Nordeste apresentando os níveis mais baixos de conectividade significativa. Nesses locais, o acesso à internet ocorre majoritariamente por meio de celulares, muitas vezes o único dispositivo disponível, o que limita o desenvolvimento de habilidades digitais avançadas e restringe o uso produtivo da rede. Esse cenário mostra que a desigualdade digital vai além da mera falta de conectividade, refletindo um problema social complexo, ligado a desigualdades estruturais históricas. Superar essas barreiras exige não apenas ampliar a infraestrutura, mas também promover capacitação, acesso a dispositivos adequados e políticas adaptadas às especificidades de cada região, sob pena de a expansão tecnológica reproduzir e intensificar desigualdades já existentes.

5 CONCLUSÃO

Diante da análise desenvolvida, nota-se que a desigualdade digital está longe de ser um aspecto isolado, isto é, constitui uma dimensão estrutural da desigualdade social brasileira. O acesso à internet e às tecnologias da informação tornou-se um requisito básico para o exercício pleno da cidadania, impactando diretamente direitos essenciais, como educação, acesso à justiça, participação política, inserção no mercado de trabalho e usufruto de serviços públicos. Nesse contexto, a exclusão digital atua como mecanismo contemporâneo de reprodução de vulnerabilidades históricas, aprofundando assimetrias econômicas, regionais e sociais.

Posto isso, no âmbito do Poder Judiciário, a transição do processo físico para o processo digital representa um avanço inegável em termos de eficiência, sustentabilidade e celeridade. Contudo, também trouxe consigo novos desafios, sobretudo no que se refere ao acesso à justiça. Milhões de brasileiros ainda carecem

de infraestrutura tecnológica básica, desconhecem o uso de ferramentas digitais ou enfrentam limitações econômicas que tornam inviável o acompanhamento de seus processos, e esses brasileiros muitas vezes pensam que perderam seu acesso à justiça. Assim, a digitalização processual, apesar de seu caráter modernizador, demanda a adoção de políticas públicas que assegurem condições mínimas de conectividade e alfabetização digital, sem as quais o acesso à justiça permanece comprometido.

Já ao observar o cenário educacional, evidencia-se que a falta de acesso adequado à internet compromete a aprendizagem, limita oportunidades acadêmicas e intensifica a desigualdade entre estudantes de diferentes classes sociais e regiões do país. A experiência da pandemia de COVID-19 expôs, de maneira incontornável, os efeitos da privação digital sobre o acompanhamento das atividades escolares, revelando que a ausência de conectividade e de competência digital impede o desenvolvimento pleno do direito à educação.

Concomitante a isso, a dimensão regional da desigualdade digital revela disparidades profundas entre Norte, Nordeste e as demais regiões do país. Enquanto Sul e Sudeste concentram os maiores índices de Conectividade Significativa e melhores condições de infraestrutura, Norte e Nordeste enfrentam limitações estruturais, custos elevados, instabilidade de conexão e dependência acentuada do acesso exclusivamente por dispositivos móveis. Essas disparidades regionais afetam o acesso a serviços públicos, a justiça, a participação econômica, a educação de qualidade e a própria capacidade das populações locais de integrarem-se à sociedade da informação. Com isso, ainda que programas governamentais como Norte Conectado e Nordeste Conectado sejam avanços importantes, persistem desafios quanto à sua implementação, manutenção e alcance real nas áreas mais remotas.

Não obstante, apesar das desigualdades ainda evidentes, o Brasil apresenta avanços significativos, contudo, esses progressos não eliminam a urgência de políticas públicas robustas, contínuas e territorialmente sensíveis, que integrem infraestrutura, capacitação digital, redução de custos, estímulo à inovação e ampliação do acesso a equipamentos adequados.

Diante de todo o exposto, conclui-se que a superação da desigualdade digital exige uma abordagem multidimensional e integrada, que compreenda tecnologia como direito social e elemento essencial à cidadania contemporânea. Garantir conectividade universal, significativa e de qualidade não é apenas modernizar o país, mas assegurar que todos os brasileiros, independentemente de classe, região ou condição social, possam exercer plenamente seus direitos e participar de forma efetiva da vida social, econômica e política. Desse modo, somente com inclusão digital ampla e efetiva será possível reduzir desigualdades históricas, fortalecer a democracia e promover um desenvolvimento verdadeiramente justo e democrático.

REFERÊNCIAS

ALMEIDA, Lília Bilati de; PAULA, Luiza Gonçalves de; CARELLI, Flávio Campos; OSÓRIO, Tito Lívio Gomes; GENESTRA, Marcelo. O retrato da exclusão digital na sociedade brasileira. **JISTM Journal of Information Systems & Technology Management**, v. 2, n. 1, p. 55-67, 2005. Disponível em: https://www.scielo.br/j/jistm/a/7BZxyCX73JT9tJbBmsbfZ8w/?lang=pt#back. Acesso em: 11 nov. 2025.

BITTAR, A. F. F. D.; PEREIRA, J. P.; CARNEIRO, L. L. de C. O direito fundamental de acesso à justiça como pilar do estado democrático de direito. **CONTRIBUCIONES A LAS CIENCIAS SOCIALES,** [S. l.], v. 18, n. 5, p. e18032, 2025. DOI: 10.55905/revconv.18n.5-280. Disponível em: https://ojs.revistacontribuciones.com/ojs/index.php/clcs/article/view/18032. Acesso em: 20 nov. 2025.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 out. 2025.

BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial. Diário Oficial da União: seção 1, Brasília, DF, 19 dez. 2006. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm. Acesso em: 20 nov. 2025

CARVALHO, Germano Pontes; LELIS, Henrique Rodrigues. A DIGITALIZAÇÃO DOS PROCESSOS JUDICIAIS E A CELERIDADE PROCESSUAL: UMA ANÁLISE À LUZ DO PRINCÍPIO CONSTITUCIONAL DA DURAÇÃO RAZOÁVEL DO PROCESSO. **Revista Ibero-Americana de Humanidades, Ciências e Educação,** [S. l.], p. 25–307, 2025. Disponível em: https://periodicorease.pro.br/rease/article/view/18655. Acesso em: 20 nov. 2025.

CNTE - CONFEDERAÇÃO NACIONAL DOS TRABALHADORES EM EDUCAÇÃO. Desigualdade no acesso à internet impacta qualidade da educação. Brasília, DF, 2023. Disponível em: https://cnte.org.br/noticias/desigualdade-no-acesso-a-internet-impacta-qualidade-da-educacao-c1bf. Acesso em: 10 out. 2025.

DUNCKE, Alessandra; PAUMANN, Camila Cristina; COLOMBO, Leonardo Segatti. A implementação de uma cultura de justiça digital, **Anais do 5º Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede**, Santa Maria, RS, 2 e 3 setembro, 2019. Santa Maria: UFSM, 2019. Disponível em: https://www.ufsm.br/app/uploads/sites/563/2019/09/7.7.pdf. Acesso em: 17 nov. 2025.

GOMES MENDONÇA, Eduardo. Da marginalização à inclusão digital: desafios e oportunidades para favelas e comunidades urbanas brasileiras. 2024. Disponível em: https://www.lacnic.net/innovaportal/file/7215/1/versao-final-gomes-mendonca.pdf Acesso em: 12 out. 2025.

KOHN, Karen; MORAES, Cláudia Herte de. **O impacto das novas tecnologias na sociedade: conceitos e características da Sociedade da Informação e da Sociedade Digital**. 2007. Trabalho apresentado no III Intercom Júnior – Jornada de Iniciação Científica em Comunicação, na subárea Cibercultura e tecnologias da comunicação. Curso de Jornalismo do Centro de Educação Superior Norte do RS/UFSM, Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação XXX Congresso Brasileiro de Ciências da Comunicação, Santos, 29 de agosto a 2 de setembro de 2007. Disponível em: http://www.intercom.org.br/papers/nacionais/2007/resumos/R1533-1.pdf. Acesso em: 11 nov. 2025.

KNOP, Marcelo Ferreira Trezza, **Desigualdade digital e desigualdade social no Brasil**, 2020, Tese. Programa de Pós-graduação em Ciências Sociais - Universidade Federal de Juiz de Fora (UFJF). Disponível em: https://repositorio.ufjf.br/jspui/handle/ufjf/11695

MACEDO, Renata Mourão; PARREIRAS, Carolina. Desigualdades digitais e educação. **Ciência Hoje**, Rio de Janeiro, Dezembro 2021. Disponível em: https://cienciahoje.org.br/artigo/desigualdades-digitais-e-educacao/. Acesso em: 10 out. 2025.

MOURA, Bruno de Freitas. Pesquisa identifica 20,5 milhões de brasileiros sem acesso à internet. **Agência Brasil,** 24 julho, 2025. Disponível em: https://agenciabrasil.ebc.com.br/direitos-humanos/noticia/2025-07/pesquisa-identifica-205-milhoes-de-brasileiros-sem-acesso-internet. Acesso em: 17 nov. 2025.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros**: TIC Domicílios 2024. São Paulo: Comitê Gestor da Internet no Brasil, 2025. Disponível em:

https://cetic.br/media/docs/publicacoes/2/20250512120132/tic_domicilios_2024_livro_eletronico.pdf Acesso em: 12 out. 2025.

RABELO, Tiago Carneiro. O processo judicial eletrônico e a experiência brasileira. In: ENAJUS, **Encontro de Administradores da Justiça**, 2019, Brasília, 2019. p. 1-17. Disponível em: https://enajus.org.br/anais/assets/papers/2019/275.pdf. Acesso em: 17 nov. 2025.

TELESÍNTESE. UIT: Brasil supera média global em conectividade significativa. **Telesíntese**, 2025. Disponível em: https://telesintese.com.br/uit-brasil-supera-media-global-em-conectividade-significativa/ Acesso em: 16 nov. 2025.

PARTE VI – APOSTAS ESPORTIVAS, TECNOLOGIA E REGULAÇÃO

APOSTAS ESPORTIVAS, MANIPULAÇÃO DE RESULTADOS E RESPONSABILIDADE PENAL: UMA ANÁLISE À LUZ DOS CASOS PAQUETÁ E BRUNO HENRIQUE E OS DESAFIOS JURÍDICOS DIANTE DA INOVAÇÃO TECNOLÓGICA NAS "BETS"

Amanda Muniz Godoy Modesto[1]
Cibely Maria Pires de Oliveira[2]
Gustavo Cauã Alves de Oliveira[3]
João Henrique Escobar Costa[4]
Kauann Gabriel Silva Alves[5]
Marcus Vinícius de Oliveira Bastos Goulart Cruz[6]
Vinicius Augusto de Oliveira Feitoza e Leite de Oliveira[7]

RESUMO

O progresso tecnológico e o crescimento do mercado de apostas esportivas introduziram novos desafios legais ao sistema brasileiro, principalmente no que diz respeito à manipulação de resultados e à responsabilidade penal de atletas e outros profissionais do esporte. Os casos recentes de Lucas Paquetá e Bruno Henrique reacenderam a discussão sobre a linha tênue entre o comportamento legal e a infração no contexto das "bets". Este artigo visa examinar a responsabilidade penal nesses casos, considerando a legislação brasileira e as inovações tecnológicas que expandiram o alcance e a complexidade das apostas. O estudo, de natureza qualitativa e bibliográfica, aborda a função do Direito Penal frente ao aumento da

[1] Amanda Godoy - Graduanda em Direito do UniCEUB – Centro Universitário de Brasília- Email: amanda.munizm@sempreceub.com
[2] Cibely Maria - Graduanda em Direito do UniCEUB – Centro Universitário de Brasília, formada em inglês na Wizard - Email: cibely.pires@sempreceub.com
[3] Gustavo Cauã Alves - Graduando em Direito do UniCEUB – Centro Universitário de Brasília. Email: gustavo.caua@sempreceub.com
[4] João Henrique Costa - Graduando em Direito do UniCEUB – Centro Universitário de Brasília. Email: joao.hc@sempreceub.com
[5] Kauann Gabriel Silva Alves - Graduando em Direito do UniCEUB – Centro Universitário de Brasília. Email: kauann.alves@sempreceub.com
[6] Marcus Vinícius Goulart - Graduando em Direito do UniCEUB – Centro Universitário de Brasília, LinkedIn: linkedin.com/in/marcusvsk. Email: marcus.cruz@sempreceub.com
[7] Vinícius Augusto Feitoza - Graduando em Direito do UniCEUB – Centro Universitário de Brasília. Email: feitozav68@sempreceub.com

influência das plataformas digitais e sugere reflexões sobre a demanda por uma regulamentação mais transparente e eficiente.

Palavras-chave: Apostas Esportivas; Manipulação de Resultados; Responsabilidade Penal; Tecnologia; Direito Penal.

Sumário: Introdução. 1. Contextualização das apostas esportivas no Brasil. 1.1. O Contraste Histórico: Do Jogo do Bicho à Lei das Bets. 1.2. A Lei das "Bets" (Lei nº 14.790/2023) e o Papel do Ministério da Fazenda. 1.3. A Dinâmica do Mercado e a Ascensão de Plataformas como a BET.BR. 2. Manipulação de resultados e responsabilidade penal dos atletas. 3. Casos Paquetá e Bruno Henrique: reflexões sobre a imputação penal. 4. Desafios jurídicos diante da inovação tecnológica nas "bets". Considerações finais. Referências.

1 INTRODUÇÃO

Nos últimos anos, o setor de apostas esportivas no Brasil teve um crescimento significativo, impulsionado pela digitalização e pelo aumento da popularidade das plataformas conhecidas como bets. A combinação do fácil acesso a essas plataformas com a falta de regulamentação específica até pouco tempo atrás favoreceu o aumento de práticas arriscadas e, em certas situações, levou à ocorrência de crimes, como a manipulação de resultados.

Casos famosos, como os de Lucas Paquetá e Bruno Henrique, ambos investigados por suposto envolvimento em esquemas de apostas, evidenciam a necessidade de entender os aspectos jurídicos desse fenômeno. A questão principal é estabelecer até que grau a conduta do atleta pode caracterizar responsabilidade penal e como o Direito deve se ajustar às novas maneiras de interação entre esporte, tecnologia e economia digital.

O artigo tem como objetivo analisar o enquadramento jurídico da manipulação de resultados, avaliar a responsabilidade penal dos atletas com base na legislação atual e debater os obstáculos que o sistema jurídico brasileiro enfrenta em relação às inovações tecnológicas nas apostas esportivas.

2 CONTEXTUALIZAÇÃO DAS APOSTAS ESPORTIVAS NO BRASIL

A Lei n.º 13.756/2018 autorizou a legalização das apostas esportivas de quota fixa no Brasil, sendo regulamentada de forma parcial apenas em 2023. O texto legal possibilitou a operação de empresas estrangeiras e nacionais no país, autorizando apostas em eventos esportivos reais. Contudo, a falta de um marco regulatório abrangente e eficaz contribuiu para o surgimento de um cenário de incertezas, principalmente em relação à supervisão e à integridade das competições.

A situação no Brasil espelha uma tendência mundial. As apostas se tornaram um mercado digitalizado graças à tecnologia, permitindo que o apostador participe de jogos de diversas modalidades e países com apenas um clique. Embora tenha sido um progresso positivo do ponto de vista econômico, ele trouxe vulnerabilidades jurídicas e éticas, especialmente quando há envolvimento direto ou indireto de atletas e dirigentes.

A manipulação de resultados, definida como qualquer ação destinada a modificar fraudulentamente o resultado de uma partida, tornou-se uma preocupação primordial tanto para as entidades esportivas quanto para os órgãos de persecução penal. No entanto, a questão não é nova: práticas semelhantes existem desde o século XX, mas ganharam novas dimensões com a internet e os algoritmos das plataformas de apostas.

2.1 O contraste histórico: do jogo do bicho à Lei das Bets

Historicamente, a prática de jogos de azar no Brasil sempre gerou controvérsias. Um exemplo bastante notável é o Jogo do Bicho, que foi criado no Rio de Janeiro em 1892. Apesar de não ser uma aposta esportiva de quota fixa, ele se tornou uma loteria bastante popular, funcionando de maneira informal por mais de cem anos e sendo classificado como uma contravenção penal. Esse contexto de jogos não regulamentados contrasta com a recente liberação das apostas esportivas digitais, que visam à formalização e à arrecadação.

Outrossim, o percurso entre o Jogo do Bicho e as atuais plataformas digitais revela uma mudança profunda na relação do Estado com as apostas. Se antes a repressão era baseada quase exclusivamente no combate policial a estruturas

clandestinas, hoje o foco desloca-se para a criação de mecanismos de controle econômico e tecnológico. Esse movimento evidencia que, enquanto o Jogo do Bicho se desenvolveu à margem da lei, as bets surgem em um contexto de institucionalização e tentativa de integração ao sistema jurídico formal.

2.2 A Lei das "Bets" (Lei Nº 14.790/2023) e o papel do Ministério da Fazenda

A Lei n.º 13.756/2018 foi a primeira a permitir a legalização das apostas esportivas de quota fixa no Brasil. Contudo, a regulamentação integral e a criação de um marco regulatório eficaz só ocorreram com a aprovação da Lei n.º 14.790/2023. A principal legislação em vigor atualmente é a "Lei das Bets", aprovada em 2023, que estabelece a regulamentação e a tributação dessas apostas, abrangendo eventos esportivos e virtuais.

Uma das principais disposições da nova lei é a atribuição ao Ministério da Fazenda (ou ao órgão que o substituir) para autorizar, regulamentar e supervisionar o mercado de apostas. Desse modo, o Ministério desempenha o papel de principal guardião da integridade das apostas e da coleta de impostos proveniente do setor.

2.3 A dinâmica do mercado e a ascensão de plataformas como a BET.BR

O progresso tecnológico converteu as apostas em um setor digital. A facilidade de acesso incentivou a entrada de várias operadoras, nacionais e estrangeiras, como a BET.BR, no mercado brasileiro.

Após o primeiro marco legal (Lei n.º 13.756/2018), essas plataformas conhecidas como "bets" surgiram de forma exponencial no Brasil, aproveitando a ausência de um regulamento completo e a popularidade do esporte. Elas usam a internet e algoritmos para possibilitar que o apostador participe de jogos de diversas modalidades e países com apenas um "clique".

No entanto, esse crescimento, apesar de ser economicamente positivo, trouxe vulnerabilidades jurídicas e éticas, como a manipulação de resultados. Essa questão

se tornou uma preocupação central para as entidades esportivas e órgãos de persecução penal.

3 MANIPULAÇÃO DE RESULTADOS E RESPONSABILIDADE PENAL DOS ATLETAS

No ordenamento jurídico brasileiro, a manipulação de resultados pode caracterizar diversas infrações penais, dependendo das circunstâncias de cada caso. Os possíveis enquadramentos incluem: (i) Estelionato (art. 171 do Código Penal), no qual ocorre fraude para obter vantagem ilícita; (ii) Corrupção passiva (art. 317 do Código Penal), caso o atleta ou dirigente peça ou aceite vantagem indevida para alterar resultados; (iii) Associação criminosa (art. 288 do Código Penal), quando há uma atuação organizada para manipulação sistemática; e até mesmo fraude em competição esportiva, conforme o art. 41-C do Estatuto do Torcedor (Lei n.º 10.671/2003), adicionado pela Lei n.º 12.299/2010.

O artigo 41-C estabelece que é crime "promover, constituir, financiar ou participar de ato destinado a alterar o resultado de competição esportiva", com pena de reclusão de dois a seis anos e multa. Portanto, o atleta que aposta em jogos nos quais está envolvido ou que induz outros a fazê-lo pode enfrentar consequências legais.

No cenário atual, a tecnologia das plataformas de apostas aumentou a probabilidade de tais comportamentos, uma vez que facilita o acesso e esconde a identidade dos participantes. Além disso, muitos jovens atletas ou atletas de categorias de base ignoram as implicações legais das apostas, tornando-se alvos fáceis para aliciadores.

4 CASOS PAQUETÁ E BRUNO HENRIQUE: REFLEXÕES SOBRE A IMPUTAÇÃO PENAL

O caso do atleta Lucas Paquetá, sob investigação da Federação Inglesa de Futebol (FA) e das autoridades britânicas, tornou-se representativo. Suspeita-se que o jogador tenha recebido cartões amarelos intencionalmente para favorecer

apostadores. Mesmo sem uma condenação, a investigação suscita questões importantes relacionadas ao dolo, à prova e à territorialidade da jurisdição penal, considerando que o ato teria ocorrido em território estrangeiro, mas com impacto global.

O caso de Bruno Henrique no Brasil, que também está sob investigação por suposta manipulação de resultados em apostas, trouxe de volta a discussão sobre a responsabilização de jogadores que, embora não estejam diretamente envolvidos nas fraudes, possam ter conhecimento de esquemas de manipulação. Em ambos os casos, ressalta-se o desafio de demonstrar o animus fraudulento e a relação direta do atleta com o resultado.

O princípio da presunção de inocência é essencial em casos como os de Lucas Paquetá e Bruno Henrique, pois determina que os jogadores sejam considerados inocentes até que exista uma evidência sólida e legalmente adquirida que comprove sua culpabilidade. Sua implementação exige que a acusação (seja da Justiça Desportiva ou Penal) tenha a responsabilidade de comprovar o delito, e não o jogador de demonstrar sua inocência. Este princípio atua como uma proteção contra condenações fundamentadas apenas em suspeitas, devido à complexidade em demonstrar o animus fraudandi (intenção de fraudar) e à ausência de uma influência direta do atleta no resultado ou evento específico da aposta. Dessa forma, ele assegura que, mesmo frente à intensa demanda por moralidade esportiva para manter a integridade da competição, os direitos fundamentais do acusado.

Esses casos também evidenciam uma falha na regulamentação: a falta de políticas de integridade esportiva e de programas de compliance obrigatórios nas instituições, os quais poderiam evitar ocorrências semelhantes.

5 DESAFIOS JURÍDICOS DIANTE DA INOVAÇÃO TECNOLÓGICA NAS “BETS”

A revolução tecnológica nas apostas esportivas demanda uma resposta legal adequada. O sistema penal convencional, projetado para delitos físicos e concretos, encontra dificuldades ao tratar de crimes digitais e de difícil rastreamento. A

identificação de usuários, a criptografia e o uso de carteiras virtuais em apostas internacionais complicam a ação penal.

Ademais, a inteligência artificial utilizada nas apostas gera mercados automatizados e dinâmicos, em que os preços oscilam em tempo real. Essa instabilidade pode ser aproveitada por grupos organizados que, ao alterar informações ou resultados, conseguem ganhos significativos em pouco tempo.

O Direito Penal brasileiro deve harmonizar dois princípios essenciais: a segurança jurídica e a eficácia da punição. Isso significa que é necessário atualizar as leis, criar mecanismos de cooperação internacional e intensificar o diálogo entre o Direito Penal, o Direito Digital e o Direito Desportivo.

Outro obstáculo é de natureza ética e social: as apostas são amplamente promovidas por influenciadores, clubes e emissoras, o que normaliza a atividade e atrai um público jovem. Logo, a ausência de instrução digital e financeira eleva a probabilidade de dependência e participação em atividades ilegais.

6 CONCLUSÕES

A relação entre apostas esportivas, manipulação de resultados e responsabilidade penal evidencia a necessidade de diálogo constante entre o Direito Penal, o Direito Desportivo e o Direito Digital. Nesse sentido, os casos envolvendo Lucas Paquetá e Bruno Henrique mostram como o sistema jurídico ainda encontra dificuldades para lidar com condutas potencialmente ilícitas em um ambiente marcado pela tecnologia e pela rapidez das operações.

Diante desse cenário, o Brasil vive um momento decisivo: o crescimento das plataformas de apostas representa uma oportunidade de desenvolvimento econômico; por outro lado, impõe desafios significativos à preservação da integridade esportiva. Combater a manipulação de resultados exige não apenas repressão penal, mas também políticas de prevenção, educação ética e regulamentação eficiente, capazes de antecipar riscos e orientar condutas.

Destarte, o futuro desse setor depende diretamente da capacidade das instituições de acompanhar o ritmo das inovações tecnológicas. Normas claras só se

tornam efetivas quando acompanhadas de fiscalização contínua, mecanismos sólidos de governança e estratégias de integridade compatíveis com a dinâmica digital das apostas. Caso contrário, abrem-se espaços propícios para práticas ilícitas e para o enfraquecimento da confiança no esporte.

Por essa razão, o Direito Penal deve ser acionado com prudência, sempre como última medida. A criminalização isolada não resolve as causas do problema e tampouco impede que novas ocorrências surjam. Assim, compreender o fenômeno das apostas como parte de um ecossistema complexo, influenciado por fatores sociais, econômicos e tecnológicos, torna-se indispensável para uma resposta jurídica consistente.

Infere-se, portanto, que a consolidação de um modelo regulatório equilibrado depende da soma entre legislação atualizada, fiscalização efetiva e atuação ética das instituições esportivas. Somente dessa forma será possível garantir um ambiente competitivo transparente, protegido contra manipulações e alinhado com as demandas contemporâneas do esporte profissional.

REFERÊNCIAS

BRASIL. **Código Penal.** Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Diário Oficial da União, Rio de Janeiro, DF, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 20 de Outubro. 2025.

BRASIL. Lei nº 10.671, de 15 de maio de 2003. **Dispõe sobre o Estatuto de Defesa do Torcedor**. Diário Oficial da União, Brasília, DF, 16 maio de 2003. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/10671.htm. Acesso em: 20 de Outubro. 2025.

BRASIL. Lei nº 12.299, de 27 de julho de 2010. **Dispõe sobre medidas de prevenção e repressão aos fenômenos de violência por ocasião de competições esportivas**; altera a Lei nº 10.671, de 15 de maio de 2003 (Estatuto de Defesa do Torcedor); e dá outras providências. Diário Oficial da União, Brasília, DF, 28 jul. 2010. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/lei/l12299.htm. Acesso em: 20 de Outubro. 2025.

BRASIL. Lei nº 14.790, de 29 de dezembro de 2023. **Dispõe sobre a modalidade lotérica denominada apostas de quota fixa, inclusive em eventos esportivos e virtuais**. Diário Oficial da União, Brasília, DF, 29 dez. 2023. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14790.htm. Acesso em: 20 de Outubro. 2025.

FREITAS, Júlio César de. **Direito Penal Desportivo: aspectos criminais das apostas e manipulação de resultados**. São Paulo: RT, 2022.

OLIVEIRA, Lucas. **Apostas esportivas e responsabilidade penal: o impacto das novas tecnologias no esporte.** Revista Brasileira de Direito Penal, v. 10, n. 2, 2024.

SUPERIOR TRIBUNAL DE JUSTIÇA DESPORTIVA (STJD). **Bruno Henrique punido com 12 jogos de suspensão e multa.** Rio de Janeiro: STJD, [s.d.]. Disponível em: https://www.stjd.org.br/comunicacao/noticias/article-21. Acesso em: 20 de Outubro. 2025.

REGULAÇÃO, VÍCIO E IMPACTOS SOCIAIS: APOSTAS ESPORTIVAS DIGITAIS NO BRASIL

Carlos Abraão Zimmerman Araújo B.[1]
Maira Heloísa Amarante Silveira[2]
Jussey Marcos Vargas Monterio[3]

RESUMO

As apostas esportivas digitais tornaram-se um fenômeno de massa no Brasil, impulsionadas pela tecnologia, redes sociais e marketing com influenciadores. Antes em uma zona cinzenta legal, movimentam bilhões e usam algoritmos de odds e publicidade intensa. Com a Lei 14.790/2023, o país avança na regulamentação da modalidade de quota fixa, buscando tributar e controlar o setor. Contudo, persistem desafios como a fiscalização de sites não licenciados e a adoção de tecnologias de segurança e verificação dos usuários. O principal problema envolve os impactos sociais e éticos. A facilidade de acesso e a publicidade persuasiva aumentam os casos de vício, especialmente entre jovens, levando a endividamento, sofrimento psicológico e conflitos familiares. Conclui-se que a regulamentação deve ir além da arrecadação, funcionando como política pública preventiva. Propõe-se restringir a publicidade, fortalecer ações de prevenção e tratamento, aprimorar a fiscalização e proteger os valores éticos do esporte, equilibrando o potencial econômico com a dignidade e o bem-estar social.

Palavras-chave: Apostas Esportivas (Bet's); Regulamentação; Vício em Apostas; Impacto Social; Desafios Éticos; Lavagem de Dinheiro (PLD/CFT).

Sumário: Introdução; 1. Contexto e funcionamento das bets no Brasil; 2. Vício e Impacto Social; 3. A Problemática das Bet's; 4. Desafios Jurídicos e Tecnológicos da Regulamentação das Bets; 5. Propostas e Soluções para um Uso Responsável e Ético das Bets; 6. Conclusão; 7. Referências.

1 INTRODUÇÃO

1 Graduando em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: Zimmermanabraao@gmail.com/Carloscarisma@gmailcom. LinkedIn: https://bit.ly/3K5YUD0

2 Graduanda em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: maiirasilveira@hotmail.com Gmail: maiirasilveira11@gmail.com; LinkedIn: https://bit.ly/48qJJxq Lattes:https://bit.ly/4pqwQJF;

3 Graduando em Direito do UniCEUB – Centro Universitário de Brasília. E-mail: marcos.jussey@sempreceub.com Gmail: marquinhosjussey@gmail.com LinkedIn: https://bit.ly/3K5YUD0

Nos últimos anos, as apostas esportivas, conhecidas popularmente como *bets*, passaram de uma prática marginal para um fenômeno de massa no Brasil. O crescimento desse mercado está diretamente ligado à expansão da internet, dos meios de pagamento digitais e das plataformas de entretenimento online. Hoje, apostar em um jogo de futebol, ou até em esportes eletrônicos tornou-se uma atividade comum entre milhões de brasileiros, refletindo uma transformação cultural que mistura lazer, emoção e a promessa de lucro rápido. O que antes era restrito a cassinos clandestinos ou loterias físicas ganhou um novo formato digital, acessível a qualquer pessoa com um celular e conexão à rede.

2 CONTEXTO E FUNCIONAMENTOS DAS BETS NO BRASIL

O surgimento das *bets* está relacionado ao avanço tecnológico e à globalização do mercado de apostas. A internet possibilitou que empresas estrangeiras, sediadas em países onde o jogo é legalizado, oferecessem seus serviços a usuários brasileiros sem precisar ter uma estrutura física no país. Com isso, essas plataformas se tornaram parte de uma economia digital transnacional, operando em larga escala e movimentando bilhões de reais. A popularização dos meios de pagamento eletrônicos, como carteiras digitais e criptomoedas, também facilitou as transações e contribuiu para o crescimento do setor. O marketing agressivo, aliado ao patrocínio de clubes e competições esportivas, fez com que o nome de grandes *bets* se tornasse familiar até mesmo para quem nunca apostou.

Do ponto de vista jurídico, a situação das *bets* no Brasil é complexa e marcada por um processo de regulamentação ainda em andamento. Durante muito tempo, as apostas esportivas foram enquadradas como jogos de azar e, portanto, proibidas pelo Decreto-Lei nº 3.688/1941 (Lei das Contravenções Penais). No entanto, em 2018, a Lei nº 13.756 introduziu a modalidade de apostas de quota fixa, permitindo que o governo regulamentasse esse tipo de atividade. Apesar disso, a regulamentação prática só começou a avançar recentemente, com debates no Congresso Nacional e a edição de medidas provisórias que buscam organizar o setor, definir regras de tributação e garantir a proteção do consumidor. Enquanto isso, as

plataformas estrangeiras continuam operando em uma espécie de "zona cinzenta" legal: não são exatamente ilegais, mas tampouco totalmente regularizadas.

O funcionamento das *bets* é baseado em sistemas automatizados e algoritmos que calculam as probabilidades de determinados resultados esportivos. O usuário cria uma conta, deposita um valor e escolhe os eventos em que deseja apostar. Cada aposta é associada a uma *odd*, que representa a chance de o resultado ocorrer. Quanto menor a probabilidade, maior o retorno potencial. Essa lógica é o que atrai muitos apostadores, já que o risco e a recompensa caminham juntos. As plataformas registram todas as apostas em tempo real e utilizam tecnologias avançadas para garantir rapidez nas operações e nos pagamentos. Do ponto de vista tecnológico, é um setor altamente sofisticado, com uso de inteligência artificial para ajustar as *odds* e prever o comportamento dos apostadores. Entretanto, essa inovação tecnológica vem acompanhada de diversos problemas sociais e econômicos.

A facilidade de acesso às *bets*, combinada com a forte presença nas redes sociais e nos esportes, tem levado ao aumento de comportamentos compulsivos e de endividamento entre jovens e adultos. A ilusão de ganhos fáceis e a repetição constante das apostas podem gerar dependência, semelhante ao vício em jogos de azar tradicionais. Além disso, a ausência de controle estatal e de políticas de conscientização agrava a vulnerabilidade dos usuários, que muitas vezes desconhecem os riscos financeiros e psicológicos envolvidos nesse tipo de entretenimento.

Outro aspecto preocupante é o econômico. A falta de regulamentação clara faz com que boa parte do dinheiro movimentado pelas *bets* não seja tributado no Brasil, gerando perda de arrecadação pública e dificultando a fiscalização de eventuais práticas ilícitas, como lavagem de dinheiro. Esse cenário evidencia a necessidade de o Estado atuar de maneira efetiva para equilibrar os interesses econômicos e sociais. A regulamentação das apostas pode representar uma importante fonte de receita e, ao mesmo tempo, permitir a criação de mecanismos de controle, prevenção ao vício e promoção do jogo responsável.

Além disso, há uma dimensão ética e cultural a ser considerada. As *bets* transformaram a relação dos torcedores com o esporte, muitas vezes deslocando o

foco da paixão pelo jogo para o interesse financeiro. Essa mudança de comportamento impacta diretamente o valor simbólico do esporte, que passa a ser visto como uma oportunidade de lucro, e não apenas como lazer ou competição. Por outro lado, defensores do setor afirmam que a regulamentação pode tornar as apostas uma forma legítima de entretenimento, desde que acompanhada de transparência, responsabilidade e limites bem definidos.

Em síntese, as *bets* representam um fenômeno multifacetado que envolve tecnologia, economia, direito e comportamento social. O Brasil vive um momento de transição entre a informalidade e a busca por um modelo regulatório que garanta segurança jurídica e proteção aos cidadãos. O desafio é equilibrar o potencial econômico do setor com os riscos que ele apresenta, reconhecendo que a inovação tecnológica, quando mal regulada, pode gerar consequências sociais graves. Portanto, compreender o contexto e o funcionamento das *bets* é essencial para discutir o futuro das apostas esportivas no país, dentro de um cenário em que o Direito precisa acompanhar o ritmo acelerado das transformações digitais.

Além de todos esses aspectos, é importante destacar o papel do Direito na construção de uma regulação moderna e eficiente para o setor das apostas. A atuação estatal deve ir além da mera arrecadação de tributos, buscando também proteger o consumidor e garantir a integridade das competições esportivas. O desafio jurídico está em elaborar normas que acompanhem o avanço tecnológico sem sufocar a inovação, conciliando o interesse econômico com a preservação de valores sociais e éticos. Nesse sentido, o estudo das *bets* dentro da disciplina de Direito, Tecnologia e Inovação revela-se essencial, pois demonstra como o ordenamento jurídico precisa se adaptar a novas realidades digitais, assegurando que o progresso ocorra de forma justa, transparente e responsável.

3 VÍCIO E IMPACTO SOCIAL

O crescimento das apostas esportivas no Brasil trouxe não apenas uma nova forma de entretenimento, mas também um conjunto de problemas sociais, e econômicos, que têm chamado a atenção de vários especialistas e autoridades. O vício em apostas é impulsionado pela facilidade de acesso às plataformas digitais e

pela grande exposição em formas de propaganda, de modo que se tornou uma preocupação cada vez maior. As bets se apresentam como um programa inofensivo de entretenimento e diversão, que, de uma forma muito perigosa, mascaram uma dependência semelhante à de outros jogos de aposta que são proibidos no Brasil, capazes de comprometer a saúde mental, o equilíbrio financeiro e as relações sociais de quem aposta.

O ambiente digital em que as bets se desenvolvem potencializa comportamentos compulsivos. De uma forma muito fácil e rápida é possível realizar novas apostas, o que torna o controle pessoal mais difícil e a exposição ao risco constante. Além do mais, a promessa de ganhos rápidos estimula a liberação de dopamina, um neurotransmissor associado à sensação de prazer e recompensa, criando um ciclo viciante que estimula vontade e necessidade de apostar novamente. Essa dinâmica é conhecida como "reforço intermitente", um mecanismo psicológico comum em vícios comportamentais, como o uso excessivo de redes sociais e jogos eletrônicos. O apostador, mesmo após perdas sucessivas, tende a continuar acreditando que o próximo palpite trará o "grande acerto", o que o mantém preso em um padrão de comportamento repetitivo e autodestrutivo.

Outro fator agravante é a forma como o marketing das casas de apostas é direcionado. As campanhas publicitárias utilizam influenciadores, atletas e celebridades para associar as bets à ideia de sucesso, riqueza e status. Nas redes sociais e transmissões esportivas, o ato de apostar é apresentado como algo moderno, empolgante e socialmente aceito, o que reforça o desejo de pertencimento entre os jovens. Esse tipo de publicidade, muitas vezes sem regulação adequada, contribui para a banalização do jogo e atinge principalmente um público em formação, mais vulnerável à impulsividade e à busca por recompensas instantâneas.

Os impactos sociais das bets vão além de quem aposta. O endividamento é uma das consequências mais frequentes entre apostadores compulsivos, afetando famílias inteiras e gerando tensões financeiras e emocionais. E há um fator preocupante: boa parte dos apostadores pertence às classes populares, que vêem nas apostas uma chance de mudar de vida rapidamente. Só que isso cria um ciclo

vicioso, em que a esperança de lucro imediato substitui o investimento em educação e trabalho, reforçando a vulnerabilidade socioeconômica.

Do ponto de vista psicológico, as consequências também são sérias. A frustração pelas perdas pode gerar culpa, ansiedade, depressão e até pensamentos suicidas. E, infelizmente, o Brasil ainda não oferece políticas públicas eficazes para lidar com isso. As leis que tratam do tema não trazem medidas voltadas à prevenção e ao tratamento da dependência, o que mostra uma falha grave no enfrentamento do problema.

Diante desse cenário, torna-se evidente que a discussão sobre as Bet's precisa ir além da dimensão jurídica ou econômica. É fundamental compreender as implicações humanas desse fenômeno e adotar uma perspectiva ética e social sobre o tema. A regulamentação das apostas, apesar de ser muito necessária, deve vir acompanhada de campanhas de conscientização sobre jogo responsável, programas de prevenção ao vício e mecanismos de apoio psicológico.

Em suma, o crescimento desenfreado das bets revela um dilema contemporâneo: o mesmo avanço tecnológico que democratizou o acesso ao entretenimento também criou novas formas de dependência e vulnerabilidade. O desafio está em equilibrar liberdade individual e responsabilidade coletiva, reconhecendo que o vício em apostas não é apenas um problema pessoal, mas um fenômeno social que exige reflexão, empatia e ação concreta. Entender a problemática das bets é, portanto, compreender os limites éticos do consumo digital e a necessidade urgente de políticas que protejam o cidadão em meio à lógica e perigosa do lucro fácil, sem esforço.

4 A PROBLEMÁTICA DAS BETS

Nos últimos anos, as plataformas de apostas esportivas, conhecidas popularmente como bets, consolidaram-se como um fenômeno social, econômico e cultural no Brasil. O que antes era uma prática restrita a ambientes físicos, hoje se desenvolve de forma massiva em plataformas digitais acessíveis a qualquer pessoa com um celular e uma conta bancária. O apelo visual, a promessa de lucros rápidos e

a presença constante de influenciadores e atletas como divulgadores criaram um ambiente favorável à expansão do setor, muitas vezes sem que o público compreenda integralmente os riscos envolvidos.

A ausência inicial de regulamentação adequada fez com que o mercado das bets se estruturasse à margem de um controle jurídico efetivo, gerando insegurança e favorecendo práticas questionáveis, como evasão de divisas e sonegação fiscal. Além disso, a falta de transparência sobre os mecanismos de definição de odds e resultados aumenta a vulnerabilidade dos apostadores e a possibilidade de manipulação esportiva, comprometendo a integridade das competições e a credibilidade do esporte.

Nos últimos anos, o Estado brasileiro passou a reconhecer a urgência de regular o setor, editando normas voltadas à concessão de licenças e ao recolhimento de tributos. O objetivo é garantir que as empresas operem de maneira lícita e sob supervisão, de modo a proteger o consumidor e assegurar retorno financeiro à sociedade. Contudo, a simples criação de leis não é suficiente: é indispensável que haja fiscalização efetiva, integração entre órgãos de controle e políticas públicas de conscientização sobre o jogo responsável, sobretudo entre os jovens, que compõem a maioria do público apostador.

Do ponto de vista jurídico e ético, as bets desafiam o equilíbrio entre a liberdade econômica e a proteção do interesse coletivo. Embora a Constituição Federal assegure o direito à livre iniciativa, ela também impõe ao Estado o dever de intervir sempre que a exploração econômica coloque em risco a ordem pública ou o bem-estar social. Assim, a regulamentação das apostas esportivas deve transcender a arrecadação fiscal e assumir um caráter de política pública preventiva, capaz de minimizar danos sociais e promover o uso consciente das plataformas digitais.

Conclui-se que a problemática das bets ultrapassa o debate sobre legalidade ou proibição: trata-se de um tema que exige reflexão jurídica, ética e social. A regulamentação é necessária e positiva, mas deve ser acompanhada de mecanismos de proteção, educação financeira e controle estatal. Somente assim será possível equilibrar o entretenimento legítimo com a preservação da integridade econômica e psicológica do cidadão. Visa-se, portanto, não apenas o lucro e o bem-estar

socioeconômico da sociedade, mas também a compreensão, a partir de princípios éticos, de que o verdadeiro valor moral dessa regulamentação está na proteção da população contra possíveis vícios, enganos ou propostas de ganhos milagrosos, sem qualquer embasamento lógico ou científico. Busca-se, por meio da informação e da conscientização, educar e adotar estratégias em que o lucro não seja apenas econômico, mas também cultural, moral e ético.

5 DESAFIOS JURÍDICOS E TECNOLÓGICOS DA REGULAMENTAÇÃO DAS BETS

A regulamentação das plataformas de apostas esportivas no Brasil envolve uma combinação de desafios jurídicos e tecnológicos que tornam o processo mais complexo do que parece. Do ponto de vista legal, o país ainda atravessa uma fase de transição: embora as apostas de quota fixa tenham sido autorizadas pela Lei nº 13.756/2018, a efetiva regulamentação só começou a avançar com o Marco Legal das Bets em 2023, com a Lei 14.790/2023. Esse cenário cria um vácuo normativo que dificulta o controle do setor, especialmente porque muitas casas de apostas já atuavam no Brasil antes do estabelecimento de regras claras.

Entre os principais desafios jurídicos, destaca-se a necessidade de definir responsabilidades entre operadores, apostadores e o Estado. Questões como transparência das odds, mecanismos de prevenção ao vício, políticas de proteção a menores de idade e garantias de pagamento ainda estão em processo de padronização. Além disso, há o problema da atuação de sites não licenciados, que continuam acessíveis aos usuários e podem driblar órgãos fiscalizadores. Para as autoridades, bloquear e monitorar essas plataformas é um processo complexo, especialmente porque muitos sites operam em servidores fora do país.

No aspecto tecnológico, o setor exige sistemas de rastreamento de operações, verificação de identidade, prevenção à lavagem de dinheiro e proteção de dados. Nesse ponto, a experiência de instituições financeiras internacionais, como o Bank of Communications (BOCOM), um dos maiores bancos da China, ajuda a ilustrar o nível de rigor que o mercado de apostas também necessita adotar. O BOCOM segue políticas robustas de Prevenção à Lavagem de Dinheiro e Combate ao

Financiamento do Terrorismo (PLD/CFT), estruturadas com base em três etapas clássicas de lavagem de dinheiro: colocação, ocultação e integração, e reforçadas por procedimentos rígidos de identificação e monitoramento de clientes (KYC).

No banco, o processo de "Conheça Seu Cliente" envolve a verificação detalhada da identidade, da origem dos recursos e da compatibilidade entre renda, movimentação e perfil financeiro, com atualizações periódicas e análise de risco contínua. Esse mesmo tipo de controle tende a ser exigido das casas de apostas regulamentadas no Brasil, já que o setor é frequentemente explorado para ocultar recursos ilícitos por meio de apostas de alto volume, manipulação de premiações ou utilização de terceiros ("laranjas"). Assim como ocorre nas instituições financeiras, as bets teriam de implementar sistemas capazes de identificar padrões suspeitos, rastrear transações e impedir que plataformas não licenciadas funcionem como canais de lavagem de dinheiro. A nova regulamentação prevê exigências como KYC ("Know Your Customer"), auditorias técnicas e integração com sistemas governamentais. Porém, a implementação prática desses controles envolve custos elevados e demanda tecnologias robustas, o que pode afastar empresas menores e fortalecer monopólios digitais. Além disso, com a velocidade das inovações (criptomoedas, inteligência artificial, uso de bots), os mecanismos de fiscalização precisam ser constantemente atualizados para evitar fraudes, manipulação de resultados e uso de plataformas ilícitas.

Assim, os desafios jurídicos e tecnológicos caminham juntos. Essa falta de normas claras fragiliza a atuação estatal, enquanto o avanço das tecnologias cria novas formas de risco. Para que o setor funcione de maneira segura, será preciso combinar legislação eficiente, fiscalização ativa e ferramentas tecnológicas capazes de acompanhar o ritmo do mercado.

6 PROPOSTAS E SOLUÇÕES PARA UM USO RESPONSÁVEL E ÉTICO DAS BETS

Ao observar todos os impactos negativos causados pela expansão desenfreada que as apostas esportivas vêm tendo no Brasil, torna-se evidente que qualquer proposta de regulamentação deve ter como prioridade a contenção dos danos sociais

e psicológicos, e não o incentivo à prática. O discurso geralmente adotado pelas próprias empresas do setor de "uso responsável" das bets, não pode servir de pretexto para camuflar a gravidade dos problemas que elas geram, como o endividamento, a deterioração das relações sociais e familiares e principalmente o vício (RODRIGUES, 2023). Mais do que criar um mercado lucrativo e formal, é necessário questionar até que ponto a sociedade deve normalizar e aceitar uma atividade que se alimenta da fragilidade emocional e financeira das pessoas (HAN,2017).

Nesse contexto, a primeira proposta deve ser restringir fortemente a publicidade das apostas esportivas, especialmente em horários e meios de grande alcance entre jovens. É inaceitável que atletas, celebridades e influenciadores promovam as bets como algo divertido e sem riscos, quando se sabe que muitos usuários acabam desenvolvendo vícios e prejuízos severos (SANTOS; LIMA, 2022). Dessa forma, como ocorreu com o controle da propaganda de cigarro e bebidas alcoólicas, é fundamental impor limites rigorosos, exigindo avisos claros sobre os perigos do vício e penalidades para a publicidade enganosa.

A criação de políticas públicas voltadas à prevenção e tratamento do vício em apostas é outra medida urgente, reconhecendo o problema como uma questão de saúde mental e social (OMS, 2021). O Estado deve oferecer apoio psicológico gratuito, campanhas de conscientização e canais de denúncia para casos de abusos ou manipulação das plataformas. É essencial que o foco da regulamentação não seja a arrecadação de impostos, mas sim a proteção do cidadão e preservação da integridade social.

Do ponto de vista jurídico, é necessário criar uma legislação mais transparente e rígida, que limite o alcance das empresas estrangeiras e fiscalize de forma efetiva suas operações. As bets devem estar sujeitas a regras claras e regras que a imponham limites, incluindo bloqueios ou suspensão de plataforma que descumpre normas éticas e legais. Legalizar, porém sem fiscalizar, é o mesmo que legitimar a exploração de milhares de brasileiros, principalmente os jovens e os mais vulneráveis economicamente.

Também é necessário ser reavaliado o papel do esporte, que vem sendo corrompido pela associação com as casas de apostas. Essa relação transforma o esporte em um produto comercial, afastando-o de seus valores educativos e culturais (PRONI, 2019). A ética esportiva deve prevalecer sobre o lucro, impedindo que clubes e atletas sirvam apenas como ferramentas de marketing ou até marionete das bets.

Por fim, as propostas e soluções para as bets no Brasil devem ou deveriam nascer de uma postura vigilante e ética, voltada à preservação da saúde mental, da integridade e da dignidade humana. adaptar a sociedade lógica das apostas, mais do que qualquer outra coisa, é preciso limitar seus danos e reafirmar valores que não podem ser negociados em nome do lucro.

7 CONCLUSÃO

A análise crítica sobre a expansão das apostas esportivas no Brasil revela que o fenômeno das bets não pode ser compreendido apenas como uma inovação tecnológica ou uma nova modalidade de entretenimento. Trata-se, antes, de um sintoma contemporâneo da sociedade do desempenho, descrita por Byung-Chul Han, em que tudo se torna mercadoria; Inclusive a esperança, o lazer e a emoção humana. A promessa de lucro rápido, reforçada por mecanismos psicológicos de dependência, demonstra que o setor se alimenta mais da vulnerabilidade emocional do que da racionalidade econômica do apostador, aprofundando desigualdades e fragilizando estruturas familiares e sociais.

Ao longo do trabalho, fica evidente que o crescimento do mercado das bets não ocorreu de maneira espontânea, mas foi impulsionado por um ambiente digital desenhado para capturar atenção e extrair comportamento. Os sistemas de odds, de reforço intermitente e os algoritmos preditivos utilizados pelas plataformas operam como verdadeiras engrenagens de estímulo, premiando o apostador aleatoriamente para mantê-lo engajado. Assim como apontam Adorno e Horkheimer na crítica à indústria cultural, o entretenimento deixa de ser simples diversão e passa a exercer uma função disciplinadora, moldando o comportamento coletivo e adaptando o

indivíduo às lógicas de mercado. Neste caso, à lógica do risco contínuo travestido de sucesso e liberdade econômica.

Sob a perspectiva jurídica, percebe-se que o Estado brasileiro demorou a compreender a dimensão do problema, permitindo que as bets crescessem em uma zona cinzenta regulatória. A Lei 14.790/2023 representa um avanço, mas a regulamentação, isoladamente, não resolve os desafios estruturais. Sem fiscalização tecnológica robusta, sem integração entre órgãos de controle e sem políticas públicas consistentes, qualquer marco regulatório corre o risco de se tornar letra morta, servindo apenas como mecanismo de arrecadação tributária. A experiência internacional e as práticas de instituições como o BOCOM deixam claro que mercados sensíveis, sobretudo aqueles suscetíveis à lavagem de dinheiro e manipulações informacionais exigem padrões elevados de monitoramento, KYC, PLD/FT e governança.

Contudo, o ponto central desta conclusão não é defender uma regulamentação meramente técnica, mas sim afirmar que a questão das bets é, antes de tudo, um problema social, ético e humano. Quando milhares de jovens passam a enxergar o esporte não como cultura, identidade ou expressão comunitária, mas como janela para ganhos instantâneos, perde-se parte do valor simbólico que o esporte sempre representou. O futebol, patrimônio afetivo nacional é reconfigurado em produto financeiro, mediado por odds, palpites e algoritmos. O risco aqui não é apenas econômico, mas moral.

Por isso, a regulamentação deve adotar uma abordagem integral e preventiva, que articule controle estatal, responsabilidade das empresas e proteção das camadas mais vulneráveis da população. É necessário administrar com rigor e sabedoria a publicidade, sobretudo aquela que utiliza influenciadores e atletas para seduzir jovens. Também é urgente que o Estado implemente programas de tratamento psicológico, campanhas de conscientização e mecanismos de apoio ao apostador compulsivo. A discussão sobre as bets deve ser inserida dentro da política pública de saúde mental, e não apenas dentro da esfera econômica ou tributária.

Se a sociedade brasileira deseja lidar de forma madura com a realidade das apostas esportivas, deve reconhecer que existe uma assimetria clara entre as

plataformas e os indivíduos. De um lado, empresas altamente tecnológicas, com estruturas sofisticadas de análise comportamental. Do outro, cidadãos vulneráveis, emocionalmente expostos e muitas vezes iludidos pela ideia de que o lucro pode substituir o esforço, o estudo e o trabalho. A ética exige que o Direito intervenha justamente onde a vulnerabilidade humana encontra mecanismos de exploração econômica.

Portanto, conclui-se que a regulamentação das bets no Brasil deve buscar não apenas organizar o mercado, mas proteger a dignidade intrínseca humana, valor que não pode ser negociado em nome do lucro. O desafio contemporâneo é equilibrar liberdade econômica e responsabilidade social, reconhecendo que o entretenimento não pode, e não deve, custar sofrimento psíquico, endividamento e destruição familiar. A tecnologia não é neutra e, quando usada sem limites, transforma-se em instrumento de fragilização coletiva.

Em última análise, compreender e regular as bets significa reafirmar que o Direito existe para servir à sociedade, e não para legitimar estruturas que aprofundam desigualdades. A verdadeira modernidade jurídica não está em permitir tudo, mas em proteger o essencial: a integridade, a saúde mental e a dignidade de cada cidadão brasileiro.

REFERÊNCIAS

ADORNO, Theodor; HORKHEIMER, Max. *Dialética do Esclarecimento.* Rio de Janeiro: Zahar, 1985.

BRASIL. *Constituição da República Federativa do Brasil de 1988.* Brasília, DF: Senado Federal, 1988.

BRASIL. *Lei nº 9.294, de 15 de julho de 1996.* Dispõe sobre restrições à propaganda BANK OF COMMUNICATIONS BBM S.A. *Política de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo.* Rio de Janeiro, 2025.

BRASIL. Lei nº 9.294, de 15 de julho de 1996. Dispõe sobre as restrições ao uso e à propaganda de produtos fumígeros, bebidas alcoólicas e medicamentos. Brasília, DF: Planalto, 2000. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9294.htm. Acesso em: 10 de nov. de 2025.

GONÇALVES, Mariana. *Regulação e impactos sociais das apostas esportivas no Brasil.* São Paulo: Revista de Direito e Sociedade, 2024.

HAN, Byung-Chul. *A Sociedade do Cansaço.* Petrópolis, RJ: Vozes, 2017.

MACHADO, Rafael. *Aspectos jurídicos da regulamentação das apostas online no Brasil.* Revista Brasileira de Direito Digital, 2023.

OMS – Organização Mundial da Saúde. *Relatório sobre Transtornos Relacionados a Jogos de Aposta.* Genebra: OMS, 2021.

PRONI, Marcelo Weishaupt. *Esporte e Capitalismo: novas formas de mercantilização.* Campinas, SP: Autores Associados, 2019.

RODRIGUES, Ana Paula. *Aposta, vício e vulnerabilidade social: um olhar crítico sobre o mercado das bets.* Belo Horizonte, MG: Fórum, 2023.

SANTOS, Júlia; LIMA, Pedro. *Publicidade, influência digital e vício: a nova face das apostas esportivas.* Revista Comunicação e Sociedade, 2022.

ADVICE COMPLIANCE. *Mercado de jogos e apostas no Brasil: avanços, regulamentações e os desafios do compliance.* 2024. Disponível em: https://advicecompliance.com.br/mercado-de-jogos-e-apostas-no-brasil-avancos-regulamentacoes-e-os-desafios-do-compliance/. Acesso em: 10 nov. 2025.

TAXGROUP. *Tributação das bets no Brasil: regras, desafios e as bets regulamentadas.* 2024. Disponível em: https://www.taxgroup.com.br/intelligence/tributacao-das-bets-no-brasil-regras-desafios-e-as-bets-regulamentadas/. Acesso em: 10 de nov. de 2025.

LICKS ADVOGADOS. *Lei das Bets: a Lei nº 14.740/2023 e o novo paradigma da regulação de jogos e apostas.* 2024. Disponível em: https://www.lickslegal.com/post/lei-das-bets-a-lei-no-14-740-2023-e-o-novo-paradigma-da-regulacao-de-jogos-e-apostas. Acesso em: 10 de nov. de 2025.

A MENTE É MARAVILHOSA. *O que é reforço intermitente e como isso nos afeta.* 2024. Disponível em: https://amenteemaravilhosa.com.br/o-que-e-reforco-intermitente-e-como-isso-nos-afeta/. Acesso em: 10 de nov. de 2025.

UOL VIVA BEM. *Para que serve a dopamina: saiba como a substância do vício é produzida.* 2024. Disponível em: https://www.uol.com.br/vivabem/faq/para-que-serve-a-dopamina-saiba-como-substancia-do-vicio-e-produzida.htm. Acesso em: 10 de nov. de 2025.

MIGALHAS. *Jogos e apostas: a influência de famosos.* 2024. Disponível em: https://www.migalhas.com.br/depeso/440495/jogos-e-apostas-tem-influencia-de-famosos. Acesso em: 10 de nov. de 2025.

A REGULAMENTAÇÃO DAS APOSTAS ESPORTIVAS ONLINE E A RESPONSABILIDADE DOS INFLUENCIADORES DIGITAIS NO BRASIL: UMA ANÁLISE LEGAL E PUBLICITÁRIA

Joelson Araujo Silva dos Santos[1]

RESUMO

O rápido crescimento das apostas esportivas online, conhecidas como "bets", no Brasil, impulsionado pela popularidade das redes sociais e a atuação de influenciadores digitais, gerou um cenário complexo que demanda análise sob a ótica da legalidade e da ética publicitária. Este artigo examina a evolução desse mercado, o marco normativo aplicável, à relação entre autorregulação e legislação estatal, a responsabilidade civil e administrativa dos influenciadores, os direitos do consumidor e as comparações com outros setores regulados, além de propor caminhos para uma regulamentação eficaz. Utilizando o método dedutivo-dialético e com base em estudos doutrinários, legislação brasileira e casos concretos, conclui-se que os influenciadores digitais, ao atuarem como fornecedores por equiparação, possuem responsabilidade objetiva e solidária pelos produtos e serviços que divulgam, exigindo maior transparência e regulação para proteger os consumidores e mitigar os riscos sociais.

Palavras-chave: Apostas esportivas online. Influenciadores digitais. Responsabilidade civil. Código de Defesa do Consumidor. CONAR. Regulamentação.

SUMÁRIO: Introdução. 1.Contextualização das apostas no Brasil. 2. Marco normativo aplicável. 3. Autorregulação vs. Legislação obrigatória. 4. Responsabilidade civil e administrativa dos influenciadores. 5. Direitos do consumidor e transparência; 5.1 Comparativo com restrições em propagandas de cigarros e bebidas alcoólicas. Conclusões e recomendações. Referências.

1 INTRODUÇÃO

[1] Bacharel em Comunicação Social: Publicidade e Propaganda, Graduando em Direito do UniCEUB – Centro Universitário de Brasília.

A ascensão das plataformas de apostas esportivas online, comumente chamadas de "bets", transformou o panorama do entretenimento e do comércio digital no Brasil. Esse fenômeno é notório nos maiores campeonatos de futebol, shows e, de forma massiva, nas redes sociais, por meio de milhares de influenciadores digitais. A expansão do setor é expressiva, de acordo com uma pesquisa realizada pela empresa BigDataCorp, especialista em datatech, o número de empresas atuantes passou de 840 em 2021 para aproximadamente 2.100 em 2024, com uma movimentação de até R$ 30 bilhões por mês no primeiro trimestre de 2024. Contudo, esse crescimento gera impactos significativos, um estudo do Banco Santander indicou que, em 2024, brasileiros perderam até R$ 36 bilhões em apostas online, o que equivale a 0,3% do PIB nacional. Os impactos são ainda mais severos nas camadas mais pobres da população, que gastam quatro vezes mais em sites de apostas, com dados do Banco Central mostrando R$ 10 bilhões recebidos de beneficiários do Bolsa Família, e 26% desses cadastrados alegando endividamento por conta das apostas.

Historicamente, as apostas foram introduzidas no Brasil pelos europeus no século XVI, com jogos de cartas e dados, e permaneceram em um limbo legal de proibições e legalizações intermitentes ao longo dos anos, desde o Império até a era Vargas e Dutra. A Loteria Federal, sob monopólio da Caixa Econômica Federal, surgiu para regulamentar algumas modalidades. No entanto, a verdadeira revolução veio com a internet, a partir do final dos anos 1990 e início dos 2000, que possibilitou o surgimento das casas de apostas online.

O marco legal mais recente para as apostas de quota fixa é a Lei nº 14.790, de 29 de dezembro de 2023, que regulamenta a modalidade, estabelecendo diretrizes para sua exploração, tributação e publicidade. Antes disso, a Lei nº 13.756/2018 já havia legalizado as apostas esportivas de quota fixa no país. Em meio a esse cenário, em 2024, o Senado Federal instalou uma Comissão Parlamentar de Inquérito (CPI) para investigar a atuação dos sites de apostas online no Brasil, e um projeto de lei (PL 2234/2022) ainda tramita para regulamentar o funcionamento de cassinos e outros jogos de azar.

2 MARCO NORMATIVO APLICÁVEL

A publicidade das apostas online no Brasil é regida por um conjunto de normas que abrange desde a Constituição Federal até leis específicas, códigos de autorregulação e doutrina jurídica.

A Constituição Federal de 1988 estabelece a livre expressão da atividade intelectual, artística, científica e de comunicação (Art. 5º, IX), além de determinar que o Estado deve promover a defesa do consumidor (Art. 5º, XXXII). A livre iniciativa (Art. 1º, IV) deve ser harmonizada com a proteção dos interesses do consumidor.

O Código de Defesa do Consumidor (Lei nº 8.078/1990) é fundamental nesse contexto, definindo consumidor como toda pessoa, física ou jurídica, que adquire ou utiliza produto ou serviço como destinatário final (Art. 2º). Fornecedor, por sua vez, é quem desenvolve atividades como produção, criação, distribuição ou comercialização de produtos ou prestação de serviços (Art. 3º). O CDC assegura o direito à informação adequada e clara sobre produtos e serviços (Art. 6º, III), exigindo que a publicidade seja clara, precisa, ostensiva e em língua portuguesa (Art. 31), e facilmente identificável como tal (Art. 36). Mais importante, o CDC proíbe a publicidade enganosa (falsa ou que induza o consumidor ao erro) e abusiva (discriminatória, que explore o medo, a superstição, incita a violência, desrespeita o meio ambiente ou induz comportamento prejudicial). A responsabilidade por danos é solidária entre todos os membros da cadeia de consumo (Art. 7º, parágrafo único; Art. 12, caput; e Art. 18, §1º, II).

O Código Civil (Lei nº 10.406/2002) estabelece que aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, comete ato ilícito (Art. 186) e fica obrigado a repará-lo (Art. 927).

A Lei nº 14.790/2023, que regulamenta as apostas de quota fixa, prevê especificamente restrições à publicidade. Ela exige avisos de desestímulo ao jogo e advertência sobre seus malefícios, além de proibir publicidade direcionada a menores de 18 anos. Também veda afirmações infundadas sobre probabilidades de ganhar, a apresentação da aposta como socialmente atraente, como forma de êxito

pessoal, solução para problemas financeiros, fonte de renda adicional ou investimento financeiro. Além disso, estabelece a necessidade de aviso de classificação etária e a responsabilidade solidária das empresas divulgadoras, incluindo provedores de aplicação de internet, pelo conteúdo veiculado após notificação do Ministério da Fazenda.

O Código Brasileiro de Autorregulamentação Publicitária (CBAP) do CONAR (Conselho Nacional de Autorregulamentação Publicitária) classifica a atividade de influenciadores digitais como anúncio publicitário (Art. 18). O CBAP exige que o anúncio seja claramente distinguido como tal (Art. 28), combatendo a publicidade invisível. Para influenciadores, o Guia de Publicidade por Influenciadores Digitais do CONAR recomenda o uso de termos como "publicidade", "publi", "parceria paga" ou hashtags como #ad ou #publi.

Outras normas incluem o Marco Civil da Internet (Lei nº 12.965/2014), que reforça a responsabilidade nas interações online, e o Decreto-Lei nº 3.688/1941, que tipifica a divulgação de jogos de azar não autorizados como contravenção penal (Art. 50). Todas as normativas citadas criam o cenário que regula a publicidade no âmbito das apostas online no país, assim contribuindo para a interpretação da responsabilidade dos influenciadores digitais na divulgação de “bets” no ambiente online.

3 AUTORREGULAÇÃO VS. LEGISLAÇÃO OBRIGATÓRIA

No Brasil, o controle da publicidade adota uma modalidade mista, exercida tanto pelo Estado quanto por instituições não-governamentais como o CONAR. Este, é denominado como uma associação de direito privado e sem fins lucrativos, tem como objetivo zelar pela comunicação social e atuar como órgão judicante em litígios éticos relacionados a conteúdos publicitários. Suas sanções são de natureza administrativa, como advertência, recomendação de alteração/correção do anúncio, sustação da divulgação e divulgação da posição do CONAR. Embora a instituição não tenha poder de aplicar multas, suas decisões são consideradas fonte subsidiária para a caracterização de abusos.

Contudo, a atuação do CONAR é frequentemente vista como "mais branda" e pode não repreender de forma efetiva e proporcional os influenciadores pelos danos causados. Casos como os envolvendo Ana Clara e O Boticário, Gabriela Pugliesi e Desinchá, e mais recentemente a Blaze.com com diversos influenciadores (Bruna Biancardi, Gabriela Martins, Rayanne Florentino, etc.) ilustram a aplicação de sanções como alteração de anúncios e advertências devido à falta de clareza na identificação publicitária ou ausência de avisos de restrição etária e sobre os riscos do jogo. Houve um aumento significativo nos processos julgados pelo CONAR envolvendo influenciadores, totalizando 73 representações em 2021, correspondendo a 27% dos casos, e 39,1% das denúncias na internet em 2019 relacionadas a redes sociais.

Por outro lado, a legislação estatal, como o CDC e o Código Civil, possui força coercitiva, com a possibilidade de multas (Procons), indenizações (civil) e até sanções criminais. A Lei nº 14.790/2023, ao regulamentar as bets, estabelece proibições e deveres claros para a publicidade, visando coibir práticas lesivas.

Uma lacuna regulatória reside na profissão de influenciador digital, que ainda não é regulamentada por lei específica, gerando discussões sobre a aplicabilidade de diversas legislações. O entendimento da jurisprudência, notadamente do Superior Tribunal de Justiça (STJ), tem se inclinado a responsabilizar primariamente o anunciante, não a agência publicitária ou o veículo, onde se enquadraria o influenciador. Contudo, doutrinadores como Tartuce e Neves (2025) argumentam que essa visão não é a mais adequada, pois contraria princípios do sistema consumerista, como a presunção de solidariedade e a boa-fé objetiva, e defende a responsabilização de toda a cadeia publicitária. A falta de uma regulamentação mais rígida pode facilitar o aumento dos casos de vícios em apostas, como alertam especialistas.

4 RESPONSABILIDADE CIVIL E ADMINISTRATIVA DOS INFLUENCIADORES

A responsabilidade civil dos influenciadores digitais decorre da posição de garantidores que assumem ao indicar um produto ou serviço. A confiança que os seguidores depositam no influenciador confere um poder persuasivo que incentiva o consumidor a adquirir o que é promovido.

A responsabilidade civil, definida pelos artigos 186 e 927 do Código Civil, exige uma conduta (ação ou omissão), um dano e o nexo causal entre eles. No contexto da publicidade digital de apostas, uma conduta irresponsável do influenciador, como omitir riscos, induzir ao erro ou direcionar conteúdo a públicos vulneráveis, pode configurar o elemento subjetivo da culpa ou até dolo.

A doutrina e a jurisprudência debatem a natureza dessa responsabilidade (objetiva ou subjetiva). Contudo, a linha que exploraremos no presente trabalho segue o entendimento de que a responsabilidade é, via de regra, objetiva no âmbito do CDC. Essa perspectiva baseia-se na Teoria do Risco, que dispensa a comprovação de dolo ou culpa, bastando a existência da ação ou omissão e o resultado danoso. Os influenciadores são enquadrados como fornecedores por equiparação, conceito desenvolvido por Leonardo Bessa, pois atuam como intermediários na relação de consumo, apresentando-se ao consumidor como se fossem os próprios fornecedores. Eles não são considerados profissionais liberais, pois sua contratação se dá pela fama e prestígio, não por qualidades técnicas ou intelectuais, e são "impostos" aos consumidores pelos anunciantes, não escolhidos intuitu personae. A quebra dos princípios da boa-fé objetiva e da confiança, que são de ordem pública, fundamenta essa responsabilidade objetiva.

A responsabilidade é também solidária entre o anunciante, a agência e o veículo (influenciador). Caso o influenciador seja responsabilizado, ele tem o direito de regresso contra o anunciante se a culpa pelo dano não for sua, com base no Art. 934 do Código Civil e no parágrafo único do Art. 13 do CDC. No entanto, por vedação da denunciação à lide em processos consumeristas (Art. 88 do CDC), a ação de regresso deve ser ajuizada em processo autônomo.

Na esfera administrativa, os influenciadores e empresas podem ser alvo de multas aplicadas pelos Procons estaduais, suspensão da veiculação da publicidade, advertências e recomendações do CONAR. Exemplos recentes incluem a

condenação de uma influenciadora pelo TJ-SP por publicidade enganosa de um curso online, resultando em reembolso e indenização por danos morais, e o caso da influenciadora Virgínia Fonseca, condenada a ressarcir uma consumidora que não recebeu um óculos de sol comprado de uma loja recomendada.

A responsabilidade penal também é possível. O Art. 66 do CDC penaliza quem faz afirmação falsa ou enganosa, ou omite informações relevantes sobre produtos/serviços. Além disso, a divulgação de jogos de azar não autorizados, como cassinos e jogo do bicho, é considerada contravenção penal (Art. 50 do Decreto-Lei nº 3.688/1941), enquanto a promoção de apostas de quota fixa, se feita em desconformidade com a Lei nº 14.790/2023, também pode gerar responsabilidade.

5 DIREITOS DO CONSUMIDOR E TRANSPARÊNCIA

A aplicação do CDC é crucial para a proteção dos seguidores que, ao serem diretamente afetados pelos anúncios publicitários dos influenciadores, são considerados consumidores. Os influenciadores, por sua vez, são enquadrados como fornecedores por equiparação, integrando a cadeia de fornecimento.

A publicidade invisível, na qual o conteúdo comercial não se distingue claramente do editorial, é uma prática ilícita por violar o princípio da identificação publicitária. O CONAR e o CDC (Art. 36) repreendem essa prática, levando à criação de mecanismos como a sinalização obrigatória de "propaganda paga" em plataformas digitais, que torna explícito ao consumidor quando a análise ou recomendação de um produto ou serviço possui natureza comercial. Além disso, o CDC coíbe a publicidade enganosa (falsa ou que induz a erro) e a publicidade abusiva (discriminatória, que explora o medo, a superstição, a inexperiência ou induz a comportamentos perigosos). A ausência de clareza nas postagens, mesmo que não intencional, pode levar à responsabilização.

5.1 Comparativo com restrições em propagandas de cigarros e bebidas alcoólicas:

O Brasil possui um histórico de sucesso na implementação de políticas restritivas à publicidade em setores considerados de risco. A política antitabagista, por exemplo, resultou na proibição total da propaganda de produtos fumígenos desde 2011, permitindo apenas a exposição em pontos de venda com advertências sanitárias obrigatórias, o que contribuiu para uma redução de cerca de 40% no número de fumantes, segundo relatório da Organização Mundial de Saúde (OMS). No passado, a indústria do tabaco também utilizou celebridades para associar o ato de fumar a estilo e sofisticação, ocultando os riscos.

Para as bebidas alcoólicas, o Código do CONAR (Anexos "A", "P" e "T") estabelece regras rigorosas. É proibida a participação de crianças e adolescentes em anúncios, modelos devem parecer ter mais de 25 anos, não se pode associar o consumo a sucesso pessoal ou maior poder de sedução, e é obrigatória a inclusão de "cláusulas de advertência" como "Beba com moderação" ou "Venda e consumo proibidos para menores". A veiculação em rádio e TV possui horários restritos.

No caso das apostas, a Lei nº 14.790/2023 já incorpora proibições semelhantes às de álcool e tabaco, vedando a publicidade que prometa ganhos irrealistas ou que associe apostas a êxito pessoal e soluções financeiras, além de proibir o direcionamento a menores de 18 anos e exigir avisos de desestímulo ao jogo. Recentemente, o Senado aprovou restrições adicionais a publicidade nas apostas de quota fixa acrescendo ao projeto de lei n° 2985, de 2023, que atualizam a Lei nº 13.756, de 12 de dezembro de 2018, proibindo anúncios com atletas, artistas, comunicadores e influenciadores, com algumas exceções para patrocínios específicos e horários delimitados. Porém, essas obrigações ainda não foram positivadas no ordenamento, necessitando do cumprimento do devido processo legislativo para que entrem em vigor.

6 CONCLUSÕES E RECOMENDAÇÕES

Os influenciadores digitais, que de meros formadores de opinião se tornaram instrumentos essenciais de publicidade, enfrentam uma crescente onda de responsabilidades legais e éticas. O rápido avanço do marketing de influência nas

redes sociais tem superado a capacidade da legislação e da autorregulação de acompanhá-lo, gerando lacunas e desafios significativos.

A análise jurídica demonstra que, sob a ótica do Código de Defesa do Consumidor e do Código de Autorregulamentação Publicitária do CONAR, os influenciadores digitais podem ser enquadrados como fornecedores por equiparação. Essa classificação implica em responsabilidade objetiva e solidária pelos produtos e serviços divulgados em seus "publiposts", independentemente de dolo ou culpa, desde que haja ação ou omissão que cause dano ao consumidor. Embora o Superior Tribunal de Justiça ainda tenda a responsabilizar principalmente o anunciante, a doutrina moderna e a jurisprudência incipiente apontam para a responsabilização de toda a cadeia publicitária, incluindo os influenciadores.

As práticas de publicidade enganosa, abusiva e, em particular, a falta de identificação publicitária (publicidade invisível) são amplamente repreendidas pelos órgãos de controle, como o CONAR, que tem registrado um aumento substancial de casos envolvendo influenciadores. A Lei nº 14.790/2023 e as recentes propostas aprovadas no Senado (PL 2.985/2023) estabelecem restrições importantes à publicidade de bets, exigindo transparência, avisos de riscos e proibindo o direcionamento a menores de idade ou a associação do jogo a soluções financeiras.

Para garantir a proteção integral ao consumidor e mitigar os graves riscos sociais e de saúde pública associados às apostas online, as seguintes recomendações são essenciais: regulamentação abrangente e fiscalização efetiva, sendo crucial que a legislação se adapte rapidamente para cobrir todas as modalidades de jogos de azar online, com um órgão regulador estatal independente e bem equipado para fiscalizar a conformidade das empresas e influenciadores; responsabilização dos influenciadores, reforçando o entendimento da responsabilidade objetiva e solidária dos influenciadores digitais como fornecedores por equiparação, garantindo que respondam pelos danos causados por publicidade irregular ou enganosa; transparência obrigatória, exigindo a identificação clara e ostensiva de todo conteúdo publicitário nas redes sociais, utilizando ferramentas e termos inequívocos, bem como a inclusão de mensagens de advertência sobre os riscos inerentes às apostas; proteção de públicos vulneráveis, implementando medidas rigorosas para proteger

crianças, adolescentes e indivíduos socioeconomicamente desfavorecidos da publicidade de apostas, coibindo qualquer direcionamento ou apelo a esses grupos; e políticas de prevenção e tratamento, reconhecendo o vício em jogos como um problema de saúde pública e investindo em políticas populacionais de prevenção, educação e tratamento da ludopatia, inspirando-se no sucesso das campanhas antitabagismo no Brasil.

Somente por meio de um esforço conjunto entre governos, empresas, órgãos de autorregulação e a sociedade civil será possível estabelecer um equilíbrio saudável entre o desenvolvimento do mercado de apostas online e a proteção dos consumidores, garantindo um ambiente digital mais ético e responsável.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE AGÊNCIAS DE PUBLICIDADE. Código de boas práticas em publicidade digital. 2021. Disponível em:https://www.abap.com.br/wp-content/uploads/2021/09/iab-brasilcodigo-de-boas-pratica agosto-2021.pdf. Acesso em: 24 ago. 2025.

AZEVEDO, Marina Barbosa; MAGALHÃES, Vanessa de Pádua Rios. A responsabilidade civil dos influenciadores digitais pelos produtos e serviços divulgados nas redes sociais. Âmbito Jurídico, 1 nov. 2020. Disponível em: https://ambitojuridico.com.br/a-responsabilidade-civil-dos-influenciadores-digitais-pelos-produtos-e-servicos-divulgados-nas-redes-sociais/. Acesso em: 22 ago. 2025.

BIANCHI, Mônica. Brasileiros perderam até R$ 3,6 bi com bets e podem tirar 0,3% do PIB, diz Santander. Veja, 25 out. 2024. Economia. Disponível em: https://veja.abril.com.br/economia/brasileiros-perderam-ate-r-36-bi-com-bets-e-podem-tirar-03-do-pib-diz-santander/. Acesso em: 25 ago. 2025.

BRASIL. Lei nº 14.790, de 29 de dezembro de 2023. Dispõe sobre a modalidade lotérica denominada apostas de quota fixa [...]. Diário Oficial da União: seção 1, Brasília, DF, ano 160, n. 246-A, p. 1, 30 dez. 2023. Edição extra. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/L14790.htm. Acesso em: 8 out. 2025.

BRASIL. Senado Federal. Projeto de Lei nº 2.234, de 2022. Institui o marco legal para a exploração de jogos e apostas em todo o território nacional e dá outras providências. Brasília, DF: Senado Federal, 2022. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/154401. Acesso em: 21 ago. 2025.

BRASIL. Senado Federal. Projeto de Lei nº 2.985, de 2023. Altera a Lei nº 13.756, de 12 de dezembro de 2018, que dispõe sobre a modalidade lotérica denominada apostas de quota fixa, para vedar ações de comunicação, publicidade e propaganda. Brasília, DF: Senado Federal, 2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/158047. Acesso em: 21 ago. 2025.

CAMPOS, Sílvio Tadeu de. A transparência nas redes sociais: A importância da clareza nas postagens publicitárias. Migalhas, 24 out. 2024. Disponível em: https://www.migalhas.com.br/depeso/418193/a-importancia-da-clareza-nas-postagens-publicitarias-nas-redes-sociais. Acesso em: 29 ago. 2025.

CIRILO, Giovanna. Responsabilidade dos influenciadores digitais: desafios legais na publicidade moderna. Jusbrasil, 30 jun. 2025. Disponível em: https://www.jusbrasil.com.br/artigos/responsabilidade-dos-influenciadores-digitais-desafios-legais-na-publicidade-moderna/4091696003. Acesso em: 22 ago. 2025.

CONSELHO NACIONAL DE AUTORREGULAMENTAÇÃO PUBLICITÁRIA. Anexo X - Publicidade de Apostas. dez. 2023. Disponível em: http://www.conar.org.br/pdf/CONAR-ANEXO-X-PUBLICIDADE-APOSTAS-dezembro-2023.pdf. Acesso em: 21 ago. 2025.

CONSELHO NACIONAL DE AUTORREGULAMENTAÇÃO PUBLICITÁRIA. Código Brasileiro de Autorregulamentação Publicitária. Edição 2021/2022. Disponível em: http://www.conar.org.br/pdf/codigo-conar-2021_6pv.pdf. Acesso em: 22 ago. 2025.

CONSELHO NACIONAL DE AUTORREGULAMENTAÇÃO PUBLICITÁRIA. Decisões. Disponível em: http://www.conar.org.br/. Acesso em: 21 ago. 2025.

CONSELHO NACIONAL DE AUTORREGULAMENTAÇÃO PUBLICITÁRIA. Guia de Orientação: Publicidade por Influenciadores Digitais. 2021. Disponível em: http://conar.org.br/pdf/CONAR_Guia-de-Publicidade-Influenciadores_2021-03-11.pdf. Acesso em: 22 ago. 2025.

FERRARI, Leon. Bets e Tigrinho: quase 450 milhões no mundo sofrem danos relacionados a jogos de azar. Instituto de Psiquiatria IPq, 29 out. 2024. Disponível em: https://ipqhc.org.br/2024/10/29/14696/. Acesso em: 21 ago. 2025.

GASPARATTO, Ana Paula Gilio; FREITAS, Cinthia Obladen de Almendra; EFING, Antônio Carlos. Responsabilidade civil dos influenciadores digitais. Revista Jurídica Cesumar Mestrado, v. 19, n. 1, p. 65-87, jan./abr. 2019. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/6493. Acesso em: 22 ago. 2025.

INFLUENCIADORES e o Direito: quando a publicidade vira infração?. Blog da Livraria RT, 17 jun. 2025. Disponível em:

https://blog.livrariart.com.br/artigos/influenciadores-direito-publicidade/. Acesso em: 22 ago. 2025.

MARINHO, Paulo Henrique Sousa; GOMES, Mateus Pereira. Regulamentação dos Cassinos e Casas de Apostas Online no Brasil. Revista Ibero- Americana de Humanidades, Ciências e Educação- REASE, v. 10, n. 6, p. 2001-2015, 2024. Disponível em: https://periodicorease.pro.br/rease/article/view/14504. Acesso em: 29 ago. 2025.

PEDRA, João Marcos de Carvalho. Influenciadores e propaganda de bets: quando há responsabilidade civil?. Blog do Direito IDP, 23 mai. 2025. Disponível em: https://blog.idp.edu.br/influenciadores-e-propaganda-de-bets-quando-ha-responsabilidade-civil/. Acesso em: 21 ago. 2025.

REDAÇÃO VEJA. Tabagismo: Brasil reduz em 40% o número de fumantes, revela OMS. Veja, 16 jan. 2024. Saúde. Disponível em: https://veja.abril.com.br/saude/tabagismo-brasil-reduz-em-40-o-numero-de-fumantes-revela-oms/. Acesso em: 25 ago. 2025.

RICARTE, Caroline. Responsabilidade civil dos influenciadores digitais sobre os danos causados pelas apostas. Migalhas, 22 maio 2025. Disponível em: https://www.migalhas.com.br/depeso/430843/responsabilidade-de-influenciadores-digitais-sobre-danos-das-apostas. Acesso em: 29 ago. 2025.

TARTUCE, Flávio; NEVES, Daniel Amorim Assumpção. Manual de direito do consumidor: volume único. 14. ed. Rio de Janeiro: Método, 2025. E-book. ISBN 9788530996963. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788530996963/. Acesso em: 10 set. 2025.