REVISTA DA
Escola Superior da Procuradoria-Geral do Estado de São Paulo

Journal of the State of São Paulo Legal Office's School

Volume 16

Jan. / Dez. 2025

ISSN 2966-1897

GOVERNO DO ESTADO DE SÃO PAULO

TARCÍSIO DE FREITAS
GOVERNADOR DO ESTADO

PROCURADORIA-GERAL DO ESTADO

INÊS MARIA DOS SANTOS COIMBRA
Procuradora-Geral do Estado

MARIANA BEATRIZ TADEU DE OLIVEIRA
Procuradora do Estado
Chefe do Centro de Estudos

CENTRO DE ESTUDOS E ESCOLA SUPERIOR
DA PROCURADORIA-GERAL DO ESTADO

REVISTA DA ESCOLA SUPERIOR DA PROCURADORIA-GERAL DO ESTADO DE SÃO PAULO

JOURNAL OF THE STATE OF SÃO PAULO LEGAL OFFICE'S SCHOOL

v. 16 • janeiro / dezembro 2025
ISSN 2966-1897

CENTRO DE ESTUDOS E ESCOLA SUPERIOR
DA PROCURADORIA-GERAL DO ESTADO

©2025

A Revista da Escola Superior da Procuradoria-Geral do Estado de São Paulo (RESPGE-SP) é uma publicação anual da Escola Superior da Procuradoria-Geral do Estado de São Paulo. É permitida a reprodução de trechos dos artigos, desde que mencionada a fonte original de publicação.

Tiragem: Revista eletrônica

Editor Científico / Scientific Editor

André Luiz dos Santos Nakamura

Conselho Editorial / Editorial Board

Alvaro Bereijo, Universidad Autónoma de Madrid, Madrid, Espanha

Carlos Ari Vieira Sundfeld, Fundação Getúlio Vargas, São Paulo/SP, Brasil

Carlos Blanco de Morais, Universidade de Lisboa, Lisboa, Portugal

Celso Antônio Bandeira de Mello, Pontifícia Universidade Católica de São Paulo, São Paulo/SP, Brasil

Consuelo Yatsuda Moromizato Yoshida, Pontifícia Universidade Católica de São Paulo, São Paulo/SP, Brasil

Daniel Antônio de Moraes Sarmento, Universidade do Estado do Rio de Janeiro, Rio de Janeiro/RJ, Brasil

Dinorá Adelaide Musetti Grotti, Pontifícia Universidade Católica de São Paulo, São Paulo/SP, Brasil

Elival da Silva Ramos, Universidade de São Paulo, São Paulo/SP, Brasil

Fernando Facury Scaff, Universidade de São Paulo, São Paulo/SP, Brasil

Giselda Maria Fernandes Novaes Hironaka, Universidade de São Paulo, São Paulo/SP, Brasil

Gustavo Binenbojm, Universidade do Estado do Rio de Janeiro, Centro de Ciências Sociais, Faculdade de Direito, Rio de Janeiro/RJ, Brasil

Humberto Theodoro Júnior, Universidade Federal de Minas Gerais, Belo Horizonte/MG, Brasil

Jorge Miranda, Universidade de Lisboa, Lisboa, Portugal

José Reinaldo de Lima Lopes, Universidade de São Paulo, São Paulo/SP, Brasil

Juan Zornoza Péres, Universidad Carlos III de Madrid, Madrid, Espanha

Juvêncio Borges da Silva, Associação de Ensino de Ribeirão Preto, Ribeirão Preto/SP, Brasil

Luiz Alberto David Araújo, Pontifícia Universidade Católica de São Paulo, São Paulo/SP, Brasil

Manoel Gonçalves Ferreira Filho, Universidade de São Paulo, São Paulo/SP, Brasil

Margerete Gresse, University of Washington, Seattle, EUA

Maria Garcia, Pontifícia Universidade Católica de São Paulo, São Paulo/SP, Brasil

Maria Helena Diniz, Pontifícia Universidade Católica de São Paulo, São Paulo/SP, Brasil

Nina Beatriz Stocco Ranieri, Universidade de São Paulo, São Paulo/SP, Brasil

Paulo Affonso Leme Machado, Universidade Metodista de Piracicaba, Piracicaba/SP, Brasil

Sueli Dallari, Universidade de São Paulo, São Paulo/SP, Brasil

Corpo Editorial / Publishers

Alexandre Coutinho da Silveira, Faculdade FACI, Belém/PA, Brasil

André Luiz dos Santos Nakamura, Universidade Paulista (Unip), São Paulo/SP, Brasil

André Petzhold Dias, Universidade do Estado do Amazonas (UEA), Boca do Acre/AM, Brasil

Anselmo Prieto Alvares, Pontifícia Universidade Católica de São Paulo, São Paulo/SP, Brasil

Arlindo Philippi Junior, Universidade de São Paulo/SP, Brasil

Carlos Marden Cabral Coutinho, Centro Universitário Christus (UNICHRISTUS), Fortaleza/CE, Brasil

Eduardo Carlos Bianca Bittar, Universidade de São Paulo, São Paulo/SP, Brasil

Érika Bechara, Pontifícia Universidade Católica de São Paulo, São Paulo/SP, Brasil

Fabio André Uema, Academia de Polícia Militar do Barro Branco (APMBB), São Paulo/SP

Fernando Dias Menezes de Almeida, Universidade de São Paulo, São Paulo/SP, Brasil

Fernando Gomes Favacho, Faculdade FACI, Belém/PA, Brasil

Guilherme Assis de Almeida, Universidade de São Paulo, São Paulo/SP, Brasil

Ilton Garcia da Costa, Universidade Estadual do Norte do Paraná, Jacarezinho/PR, Brasil

José Levi Mello do Amaral Júnior, Universidade de São Paulo, São Paulo/SP, Brasil

José Mauricio Conti, Universidade de São Paulo, São Paulo/SP, Brasil

Luciana de Toledo Temer Castelo Branco, Pontifícia Universidade Católica de São Paulo, São Paulo/SP, Brasil

Luis Claudio Ferreira Catanhêde, Escola Superior da Procuradoria-Geral do Estado de São Paulo, São Paulo/SP, Brasil

Luiz Henrique Volpe Camargo, Universidade Federal do Mato Grosso do Sul (UFMS), Campo Grande/MS, Brasil

Márcio Pugliesi, Pontifícia Universidade Católica de São Paulo, São Paulo/SP, Brasil

Marco Antonio dos Santos Rodrigues, Universidade do Estado do Rio de Janeiro, Centro de Ciências Sociais, Faculdade de Direito, Rio de Janeiro/RJ, Brasil

Marcos Antônio Rios da Nóbrega, Universidade Federal de Pernambuco (UFPE), Recife/PE, Brasil

Maria Paula Dallari Bucci, Universidade de São Paulo, São Paulo/SP, Brasil

Mônica Cristina Queiroz, Centro Universitário Unihorizontes, Belo Horizonte/MG, Brasil

Olavo de Oliveira Neto, Universidade Federal do Mato Grosso do Sul, Campo Grande/MS, Brasil

Onofre Alves Batista Júnior, Universidade Federal de Minas Gerais (UFMG), Belo Horizonte/MG, Brasil

Patrícia Ulson Pizarro Werner, Escola Superior da Procuradoria-Geral do Estado de São Paulo, São Paulo/SP, Brasil

Pietro de Jesús Lora Alarcón, Pontifícia Universidade Católica de São Paulo, São Paulo/SP, Brasil

Roberto Wagner Marquesi, Universidade Estadual de Londrina, Londrina/PR, Brasil

Rodrigo Borges Valadão, Escola Superior de Advocacia Pública do Estado (ESAP-PGE/RJ), Rio de Janeiro/RJ, Brasil

Vidal Serrano Nunes Júnior, Pontifícia Universidade Católica de São Paulo, São Paulo/SP, Brasil

Welder Queiroz dos Santos, Universidade Federal de Mato Grosso, Faculdade de Direito, Cuiabá/MT, Brasil

A *RESPGE-SP* conta com um grupo permanente de pareceristas, formado pelos integrantes do Conselho e do Corpo Editoriais da publicação, bem como por professores e pesquisadores da ESPGE. Além disso, a *RESPGE-SP* pode convidar especialistas *ad hoc* para análise dos manuscritos.

***Pareceristas colaboradores* – 2025**

Alexandre Lucas Veltroni – Doutor em Direito do Estado pela Pontifícia Universidade Católica de São Paulo - PUC-SP

Anselmo Prieto Alvarez – Prof. Dr. na Pontifícia Universidade Católica de São Paulo, PUCCAMP, Mackenzie-Campinas e Universidade Estadual de Londrina

Carlos Jose Teixeira de Toledo – Mestre e Doutor em Direito pela Universidade de São Paulo

Christiane Mina Falsarella - Doutora em Direito pela Universidade de São Paulo

Fabio André Uema Oliveira – Doutor em Direito pela Pontifícia Universidade Católica de São Paulo

Lucas Soares de Oliveira – Mestre em Efetividade do Direito pela Pontifícia Universidade Católica de São Paulo

Mônica Cristina Queiroz – Doutora em Direito Privado pela Pontifícia Universidade Católica de Minas Gerais

Nelson Finotti Silva – Doutor em Direito Processual Civil pela Pontifícia Universidade Católica de São Paulo

Patrícia Ulson Pizarro Werner – Doutora em Direito pela Pontifícia Universidade Católica de São Paulo

Romualdo Baptista dos Santos - Doutor em Direito pela Universidade de São Paulo

Secretaria-executiva

Bárbara de Sousa Castilho (BK)
Deise Aparecida Santiago
Eric Rodolfo Gaspar Krauniski (BK)
Fernando Augusto dos Santos
Igor Rodrigues Quadrado
Paulo Severo dos Santos
Rafael de Lima Nobre
Thiago Blumer Marangone
E-mail: espge-secretaria@sp.gov.br

Serviço de Divulgação
Juliana Aguilera do Nascimento Silva Guedes
Glauciane Pontes Helena Franco
Luciene de Cássia de Santana
Maisa Maciel Rodrigues

Revisão de Texto e Editoração
Giovanna Macedo | Tikinet
Reinaldo Rodrigues | Tikinet

Projeto Gráfico
Tikinet

Diagramação
Jonathan Leandro | Tikinet

Correspondência
Pedidos de permuta devem ser endereçados à ESPGE.
Exchange orders should be addressed to ESPGE.

Normas editoriais disponíveis em:
www.pge.sp.gov.br/ESPGE_2016/AcessoHome/estatuto_respge.html

Endereço / Address
Rua Pamplona, 227 – 2º andar
Bela Vista – São Paulo/SP – Brasil
CEP 01405-100
Tel.: +55 11 3286-7020/7005
E-mail: espge-secretaria@sp.gov.br
Endereço eletrônico: www.pge.sp.gov.br/ESPGE_2016/homeESPGE.aspx

Revista da Escola Superior da Procuradoria-Geral do Estado de São Paulo – Journal of the State of São Paulo Legal Office's School / Escola Superior da Procuradoria-Geral do Estado de São Paulo. – V. 16, nº1 (2025) – São Paulo : Procuradoria-Geral do Estado de São Paulo, Escola Superior, 2025.

Anual.
Textos multilíngues.
Resumos em português e inglês.

ISSN 2966-1897
2010 (V. 1) (1), 2011 (V. 2) (1), 2012 (V. 3) (1), 2013 (V. 4) (1), 2014 (V. 5) (1), 2015 (V. 6) (1), 2016 (V. 7) (1), 2017 (V. 8) (1), 2018 (V.9) (1), 2019 (V.10) (1), 2020 (V.11) (1), 2021 (V.12) (1), 2022 (V.13) (1), 2023 (V.14) (1), 2024 (V.15) (1)

1. Direito – Periódicos. I. São Paulo (Estado). Procuradoria-Geral. Escola Superior. II. Journal of the State of São Paulo Legal Office's School.

CDD 340.006.3
CDU 34:007

ESCOLA SUPERIOR DA PROCURADORIA-GERAL DO ESTADO DE SÃO PAULO

EQUIPE 2025

Diretoria

Cintia Byczkowski (de 07/07/2023 a 02/06/2025) e Mariana Beatriz Tadeu de Oliveira (a partir de 03/06/2025) (Procuradora do Estado-Chefe do Centro de Estudos e Diretora da ESPGE, membro nato)

Coordenador-Geral da ESPGE

Valter Antonio Farid Junior (até 02/06/2025)
Caio Gentil Ribeiro (a partir de 01/07/2025)

Conselho Curador 2025

Mariana Beatriz Tadeu de Oliveira (Procuradora do Estado-Chefe do Centro de Estudos e Diretora da ESPGE, membro nato); Carlos José Teixeira de Toledo; Carolina Zancaner Zockun, Diana Loureiro Paiva de Castro, Felipe Gonçalves Fernandes, Fernanda Ghiuro Valentini Fritoli, Joyciane Carvalho Borges, Marcus Vinícius Armani Alves, Paulo Alves Netto de Araújo, Fernanda Ghiuro Valentini Fritoli.

EQUIPE DE COORDENADORES E MONITORES

Direito Digital

Coordenadores de Direito Digital

Caio Gentil Ribeiro; Diana Loureiro Paiva de Castro; Rafael Carvalho de Fassio.

Professores-Assistentes de Direito Digital

Christiane Mina Falsarella; Cláudia Mara Arantes da Silva, Guilherme Cavalcanti; Iago Oliveira Ferreira, Lucas Soares de Oliveira; Mateus Camilo Ribeiro da Silveira, Patrícia Ulson Pizarro Werner, Pedro Henrique Lacerda Barbosa Ladeia, Rafael Santos de Jesus, Renan Raulino Santiago.

Funcionários da ESPGE

Deise Aparecida Santiago, Bárbara de Sousa Castilho (BK), Eric Rodolfo Gaspar Krauniski (BK), Fernando Augusto dos Santos, Igor Rodrigues Quadrado, Paulo Severo dos Santos, Rafael de Lima Nobre, Thiago Blumer Marangone.

SUMÁRIO

Editorial
Caio Gentil Ribeiro

Direito Digital e Inovação Tecnológica

Responsabilidade por Danos Gerados por Inteligência Artificial

A aplicação da inteligência artificial generativa na criação de imagens ultrarrealistas de crianças e adolescentes em situações de exploração e abuso sexual **17**
Eliza Bastos Silveira

A responsabilidade civil de danos causados por *deepfakes*: imagens falsas criadas por inteligência artificial generativa **51**
Natália Fernanda Marques Carvalhanas

Responsabilidade civil por danos causados por sistemas de inteligência artificial **73**
Fábio Trabold Gastaldo

Direitos de Personalidade

O pensamento humano no contexto da infância e adolescência: reflexões jurídicas e tecnológicas **99**
Fernanda Papassoni dos Santos

A "ressurreição digital" e o Projeto de Lei nº 3.592/2023, do Senado Federal: a autorização familiar e a manifestação de vontade do artista quando vivo **121**
Henrique José de Agostinho Cintra

Proteção de Dados Pessoais

Tecnologia e Saúde: A proteção de dados no Sistema Único de Saúde e a Telemedicina **135**
Izadora Rodrigues Normando Simões

Uso de bases de dados em saúde e a privacidade e proteção de dados pessoais **167**
Néa Miwa Kashiwagi e Zillá Oliva Roma

Análise facial e proteção de dados pessoais 183
Murilo Arakaki

Políticas de Inovação

Políticas de inovação das ICTs: percepção dos pesquisadores e das estruturas dos núcleos de inovação tecnológica.....219
Maria Paula de Oliveira Valadares

EDITORIAL

Esta edição da Revista da Escola Superior da Procuradoria-Geral do Estado de São Paulo traz artigos elaborados por alunos da primeira turma da Pós-Graduação em Direito Digital e Inovação, oferecida entre os anos de 2022 e 2023. Tratou-se de curso inédito em escolas de governo. Seu objetivo foi trazer o estado da arte de discussões em ramos emergentes do Direito ligados a novas tecnologias, o que não é necessariamente novo, mas com foco especial no papel do Estado e, consequentemente, da advocacia pública frente a essas emergências. Aqui, houve novidade, e muito consequente. Se grandes empresas de tecnologia são os novos Leviathans, seus irmãos mais velhos ainda estão por aqui e continuam sendo centrais.

O grupo de alunos era formado por Procuradores do Estado, servidores da PGE-SP e de outras secretarias e, de modo inédito na nossa Escola, também por público externo. Tivemos, com isso, grupo com formações acadêmicas e experiências profissionais diversas, algo muito pertinente para um curso em que as questões estavam, ainda que centralizadas no Direito, frequentemente no limiar entre o jurídico e outros ramos do conhecimento.

Escrevo esta apresentação como coordenador da Escola Superior, mas tive a felicidade de ter sido também um dos coordenadores dessa pós-graduação. Estiveram ao meu lado nessa empreitada Rafael Fassio e Diana Castro. Tivemos também a valorosa contribuição de Lucas de Faria Rodrigues.

A ideia veio do Rafael, que, é justo dizer, é um dos maiores conhecedores da área de inovação no Direito brasileiro. A partir disso, percebeu tanto que havia muito a explorar quanto que a Escola Superior da PGE-SP era o melhor lugar para isso. A Diana, civilista de primeira, soube acrescentar o que estava acontecendo naquele que, ao que parece, é o ramo mais antigo do que hoje chamamos de Direito. Ficou responsável, ainda, por um programa a respeito de Proteção de Dados ao mesmo tempo abrangente e atento às especificidades da Administração Pública. Meus dois centavos – o que aqui não é tanto assim uma figura de linguagem – ficou em trazer alguns debates em Filosofia do Direito para o contexto das novas tecnologias, em especial no módulo de Tecnologia e Direitos Fundamentais, bem como em formatar o curso de metodologia. Além disso, todos nos ajudamos muito; foi um curso, de fato, construído – e colocado em prática – em conjunto.

Neste momento em que uma segunda edição do curso começa a ser oferecida, é uma alegria poder apresentar aqui parte dos resultados daquela primeira edição. Digo "parte" porque tenho certeza que, pela qualidade dos professores e dos debates que tivemos ao longo desses dois anos, o maior impacto virá do que essa experiência deixou para cada um de nossos alunos. São servidores públicos – Procuradores ou não – e advogados que, nas suas trajetórias profissionais, se aproximarão

de forma mais crítica e qualificada dos problemas que viram em sala de aula. Educação não muda o mundo, mas muda as pessoas, e sabemos do que as pessoas são capazes. Mas se esses trabalhos não são tudo que essa pós deixa, eles são, ainda assim, bastante coisa, e gostaria de falar um pouco sobre cada um deles.

Três artigos tratam de questões de responsabilidade civil por danos gerados por inteligência artificial (IA). Em um momento em que a IA generativa ainda estava longe de ser o que é hoje, Eliza Bastos Silveira, no artigo "A aplicação da inteligência artificial generativa na criação de imagens ultrarrealistas de crianças e adolescentes em situações de exploração e abuso sexual", escrevia sobre os desafios que o uso dessa tecnologia coloca para a responsabilização em relação à exploração sexual de menores. Propôs reflexão a respeito de como tais condutas poderiam ser qualificadas no Direito Brasileiro – *crime impossível*, quando há conhecimento de se tratar de IA, ou algo semelhante a *erro sobre a pessoa*, quando não há tal conhecimento? – e, concluindo pela insuficiência da proteção pelo nosso direito, analisou projetos de lei em tramitação.

Também antecipando o que logo se tornaria um problema maior, Natália Fernanda Marques Carvalhanas tratou em *A responsabilidade civil de danos causados por deepfakes* da responsabilização por imagens criadas por inteligência artificial generativa. Sua abordagem foi, porém, de responsabilização *civil*. A autora considerou o regime do Código Civil, do Marco Civil da Internet, da Lei Geral de Proteção de Dados e do sistema de Direito do Consumidor para defender a responsabilização objetiva do fornecedor da ferramenta de inteligência artificial.

Fábio Trabold Gastaldo escreveu sobre responsabilidade civil de inteligência artificial a partir de uma perspectiva mais abstrata. Sua questão foi se nosso sistema de responsabilização objetiva é suficiente para fazer frente às novas situações que a inteligência artificial cria, ou se seria necessária mudança legislativa. Considerando uma série de exemplos pré-inteligência artificial, ele conclui que não há por que diferenciá-los da responsabilização (objetiva) por danos gerados por inteligência artificial. As vítimas de danos causados por IA já estão protegidas por nosso ordenamento.

Dois artigos trataram do que podemos chamar de direitos de personalidade, em sentido amplo. Em *O Pensamento Humano no Contexto da Infância e Adolescência*, Fernanda Mascarenhas aborda o tema emergente dos *neurodireitos*, isto é, os direitos à proteção da mente humana. Baseia-se em princípios instituídos pela *Organização dos Estados Americanos* e defende a incorporação da proteção a esses direitos no Brasil como forma de concretizar a proteção prioritária e integral a crianças e adolescentes.

Henrique José de Agostinho Cintra analisou como fica a proteção de direitos de personalidade e direitos autorais de artistas falecidos, quando passa a ser tecnicamente possível criar novas obras com suas imagens e vozes. Em *A "ressurreição digital" e o Projeto de Lei nº 3.592/2023*, o autor aborda como esse projeto busca responder a tal novidade. Argumenta, então, que deve ser privilegiada a manifestação de vontade do artista.

Três artigos tratam de proteção de dados pessoais. Izadora Rodrigues Normando Simões escreve em *Tecnologia e Saúde* a respeito do regime de proteção de dados na telemedicina. A autora faz análise da legislação brasileira e comparada e destrincha o conceito de "dados pessoais sensíveis de saúde". Em *Análise Facial e Proteção de Dados Pessoais*, Murilo Arakaki analisa os problemas jurídicos que surgem não apenas do *reconhecimento* facial, mas propriamente da análise automatizada que classifica indivíduos por características como gênero, idade e humor. Em especial, enfrenta os problemas que essa nova tecnologia gera em termos de discriminação algorítmica e de neurodireitos.

Em *Uso de bases de dados em saúde e a privacidade e proteção de dados pessoais*, as autoras Néa Miwa Kashiwagi e Zillá Oliva Ramos enfrentam o problema da compatibilização entre o uso de grandes bancos de dados em saúde para pesquisa e as garantias de proteção de dados. As autoras repassam os dispositivos vigentes sobre a matéria e destacam a necessidade de protocolos efetivos de anonimização, bem como a pertinência de constituição de centros de dados orientados para pesquisa.

Finalmente, agora a respeito de políticas de inovação, Maria Paula de Oliveira Tavares apresenta, em *Políticas de Inovação das ICTs*, além de revisão de literatura, também resultado de aplicação de questionários semiestruturados a pesquisadores de instituições científicas e tecnológicas. Traz, com isso, achados sobre suas percepções sobre as políticas de inovação em vigor.

Essa revista oferece, assim, uma boa amostra do que foi discutido ao longo da pós-graduação em Direito Digital e Inovação. Traz questões novas e interessantes e são um convite para novos desenvolvimentos doutrinários e legais. Boa leitura.

São Paulo, 19 de março de 2026

Caio Gentil Ribeiro
Procurador do Estado Coordenador da Escola Superior da
Procuradoria-Geral do Estado de São Paulo

A APLICAÇÃO DA INTELIGÊNCIA ARTIFICIAL GENERATIVA NA CRIAÇÃO DE IMAGENS ULTRARREALISTAS DE CRIANÇAS E ADOLESCENTES EM SITUAÇÕES DE EXPLORAÇÃO E ABUSO SEXUAL

The Application of Generative Artificial Intelligence in the Creation of Ultra-Realistic Images of Children and Adolescents in Situations of Sexual Exploitation and Abuse

Eliza Bastos Silveira[1]

SUMÁRIO 1. Introdução; 2. O uso da inteligência artificial para a criação de imagens; 3. Estudo comparado e análise da legislação brasileira vigente; 3.1. Resultados da análise comparativa; 4. Alternativas e providências possíveis; 5. Conclusão; Referências Bibliográficas.

RESUMO O presente artigo aborda o crescente emprego da inteligência artificial generativa para a produção de representações visuais extremamente realistas de crianças e adolescentes em situações de exploração e abuso sexual. A velocidade com que avançam as tecnologias de IA suscita preocupações éticas e legais, uma vez que a criação de imagens desta natureza não só pode ser utilizada para perpetuar a exploração e o abuso sexual de menores, como também dificulta a identificação e punição dos responsáveis. A partir da adoção de pesquisa documental e da realização de estudo comparado, buscou-se esclarecer alguns conceitos técnicos, explicar a forma de funcionamento dos sistemas de geração de imagens, fixar a dimensão do problema por intermédio de informações estatísticas e examinar, comparativamente, a forma como diferentes países tratam sobre a questão em suas legislações, contribuindo com a identificação de estratégias para a prevenção e repressão desse tipo de conduta. Objetivou-se, também, o exame do ordenamento jurídico pátrio e a possibilidade de sua aplicação, bem como a apresentação de possíveis alternativas para a mitigação do problema proposto, destacando a urgente necessidade de criação de políticas e medidas eficazes para lidar com o uso indevido da inteligência artificial generativa nesse contexto, visando proteger os direitos de tão vulnerável parcela da população.

Palavras-chave: Inteligência Artificial Generativa. Imagens Ultrarrealistas. Crianças e Adolescentes. Exploração e Abuso Sexual. Pornografia Infantil.

ABSTRACT This article addresses the growing use of generative artificial intelligence to produce highly realistic visual representations of children and adolescents in situations of sexual exploitation and abuse. The rapid advancement of AI technologies raises ethical and legal concerns, as the creation of such images can not only be used to perpetuate the sexual exploitation and abuse of minors but also complicates the identification and prosecution of those responsible. By adopting documentary research and conducting a comparative study, the article seeks to clarify some technical concepts, explain how image generation systems work, outline the scope of the problem through statistical information, and examine, in a comparative manner, how different countries address this issue in their legislation, contributing to the identification of strategies for the prevention and suppression of such conduct.

[1] Especialista em Direito Penal e Processual Penal e em Direito Público pelo Instituto Damásio de Educação e em Direito Digital e Inovação pela Escola Superior da Procuradoria Geral do Estado de São Paulo. Advogada e Assessora Técnica da Secretaria de Desenvolvimento Econômico e do Núcleo de Inovação e Propriedade Intelectual (NIPI) da Procuradoria Geral do Estado de São Paulo.

DOI: 10.22491/*respge*.v16i1.1730

The article also aims to examine the national legal framework and the possibility of its application, as well as present potential alternatives for mitigating the proposed problem, emphasizing the urgent need to create effective policies and measures to deal with the misuse of generative artificial intelligence in this context, with the goal of protecting the rights of this highly vulnerable segment of the population.

Keywords: Generative Artificial Intelligence. Ultra-realistic Images. Children and Adolescents. Sexual Exploitation and Abuse. Child Pornography.

1. INTRODUÇÃO

Em 22 de dezembro de 2022, o jornal *Estadão* publicou uma matéria online intitulada "Homem é preso na Espanha por criar pornografia infantil[2] usando IA". Conforme noticiado, depois de identificar uma conexão em Valladolid, que mantinha relação com usuários de outros países para a troca de materiais de pornografia infantil, foi iniciada investigação que, após três meses, resultou na prisão de um suspeito e apreensão de grande quantidade de arquivos. A análise dos dois computadores e dos três discos rígidos encontrados fomentou surpreendente conclusão: parte do material apreendido consistia em imagens e vídeos sintetizados por ferramenta de inteligência artificial de código aberto que criava imagens por meio de ampla base de dados. De acordo com o jornal, aquela era a primeira vez que se tinha notícia do uso de IA para esses fins.

Já no dia 8 de novembro de 2023, o *Correio Braziliense* divulgou uma reportagem de autoria do jornalista do *Estado de Minas*, Bruno Luís Barros, denominada "Pornografia infantil com uso de IA em escola de BH é investigada pela polícia", informando que a Polícia Civil de Minas Gerais identificara um adolescente de 15 anos como o responsável por utilizar inteligência artificial para, por meio de fotos reais, produzir falsas imagens de cunho pornográfico e pejorativo de pelo menos 10 estudantes. A investigação teve início com base em denúncias realizadas pelas mães das vítimas à Delegacia Especializada de Apuração de Ato Infracional (DEAI), e o respectivo procedimento de apuração foi encaminhado à Justiça da Infância e Juventude da capital[3].

[2] O termo "pornografia infantil" é considerado inadequado em razão de a palavra "pornografia" remeter a uma prática legalizada e pressupor a participação livre e voluntária dos atores ou de pessoas maiores de idade filmadas ou fotografadas em atos sexuais consensuais (BARRETO; BRESSAN, 2023). Todavia, por ainda constar expressamente em dispositivos legais, o presente artigo o utiliza como sinônimo para designar fotografias e vídeos em que aparecem crianças e adolescentes em situação de exploração e violência sexual ou de nudez.

[3] Os exemplos relacionados evidenciam facetas distintas de um mesmo problema; embora também se defenda a criminalização do uso da inteligência artificial para a modificação de imagens verdadeiras com vistas à produção de materiais de cunho pornográfico, a chamada "nudificação de IA" não constitui objeto do presente artigo, que tem como ponto focal a análise das situações em que as pessoas retratadas não são reais.

Por sua vez, em 17 de maio de 2024, foi publicada a reportagem "Suspeito de pornografia infantil no ES usava inteligência artificial para produzir imagens", de autoria de Carol Poleze, pela Redação *Folha Vitória*. Segundo consta, a Polícia Federal realizou a prisão em flagrante de um homem de 38 anos, no litoral sul do Espírito Santo, em posse de vídeos e imagens contendo abuso sexual infantil, na maioria envolvendo crianças menores de 7 anos. Houve a apreensão de dois celulares, dois HDs, dois *pendrives* e um cartão de memória, nos quais foram encontradas, além de imagens de pessoas reais, outras produzidas com inteligência artificial, em formato 3D realístico.

Em 22 de maio de 2024, o site *Olhar Digital* destacou um caso ainda mais grave. Com a chamada "Homem é preso por criar material com conteúdo sexual infantil usando IA", o jornalista Leandro Costa Criscuolo reportou a prisão de um engenheiro de *software* de 42 anos, no estado de Wisconsin, nos Estados Unidos, sob a acusação de criar e distribuir milhares de imagens de abuso sexual infantil geradas por inteligência artificial. Além de ter diversos arquivos em seu Telegram, o acusado estabeleceu contato via mensagem direta no Instagram com um menino de 15 anos, encaminhando-lhe fotografias realistas de menores nus e explicando-lhe sobre o modo como criava imagens sexualmente explícitas com IA. A reportagem indicou que o material foi produzido no Stable Diffusion, uma ferramenta que gera imagem a partir de *prompts* de texto criada pela Stability AI e na qual o referido engenheiro utilizou comandos extremamente específicos e explícitos para dar origem às imagens.

Mais recentemente, em 2 de abril de 2025, o *Núcleo Jornalismo* publicou uma reportagem de autoria de Sofia Schurig, Leonardo Coelho e Tatiana Azevedo intitulada "Esquema no Instagram espalha imagens de exploração sexual infantil feitas por IA", relatando que, por meio da realização de uma investigação conjunta com a AI Accountability Network, do Pulitzer Center, para avaliar o impacto da flexibilização de algumas das políticas de moderação de conteúdos da Meta nos Estados Unidos, foram identificados 14 perfis no Instagram que publicaram imagens sexualizadas de menores geradas por inteligência artificial e que, em quase todos os casos, os usuários eram direcionados a plataformas de conteúdo por assinatura, como Patreon e Fanvue, nas quais poderiam adquirir materiais personalizados.

Apesar de as referidas notícias causarem grande dose de repugnância, colocam em foco um problema que, há alguns anos, não aparentava ser possível. Trata-se da utilização criminosa das mais modernas inovações de cunho tecnológico para a criação de materiais em que crianças e adolescentes irreais aparecem em cenas de nudez ou contexto de exploração e violência sexual.

A Internet Watch Foundation (IWF) é uma organização sem fins lucrativos que, em outubro de 2023, elaborou importante relatório sobre como a inteligência artificial está sendo usada para a criação de imagens de abuso sexual infantil. De 20.254 imagens geradas por IA e postadas no período de um mês em um fórum da Dark Web, 11.108 foram selecionadas e examinadas pelos analistas da IWF em

razão da elevada probabilidade de serem consideradas criminosas à luz da legislação do Reino Unido (Protection of Children Act 1978 e Coroners and Justice Act 2009). Após dedicarem um total de 87,5 horas para a análise desse material, constatou-se a existência de 2.562 imagens classificadas como pseudofotografias criminais e 416 avaliadas como imagens criminais proibidas[4].

Foram também realizadas outras descobertas: (i) o conteúdo de abuso sexual de menores gerado por IA ainda ocupa apenas uma pequena parcela do que é postado na internet em termos de pornografia infantil, mas a rapidez com que a tecnologia tem avançado deixa clara a sua capacidade de crescimento; (ii) são várias as ferramentas que podem ser utilizadas e todas de difícil detecção, pois os perpetradores podem baixar legalmente tudo o que precisam e, em seguida, produzirem quantas imagens quiserem *off-line*; (iii) mesmo para profissionais altamente treinados, a maior parte das imagens geradas é suficientemente realista e visualmente indistinguível das reais; (iv) foram encontradas muitas imagens que representavam vítimas de abuso sexual conhecidas e crianças famosas, salientando seu potencial de revitimização; (v) a tecnologia permitiu que a capacidade de comercialização e obtenção de lucro decorrentes desses materiais fossem ampliadas; e (vi) embora não sejam proibidos, os manuais para geração de imagens de natureza sexual por IA contribuem consideravelmente com o agravamento do problema em pauta[5].

As informações do relatório parecem ir ao encontro daquelas divulgadas pela organização não governamental brasileira "SaferNet Brasil", existente desde o ano de 2005 e atuante no combate a crimes cibernéticos contra os Direitos Humanos, no acolhimento de vítimas de violência on-line e em programas de educação, prevenção e conscientização, que apontou crescimento de 77,13% das denúncias de imagens de abuso e exploração sexual infantil de 2022 para 2023, o que o seu fundador e diretor-presidente, Thiago Tavares, atribuiu a uma combinação de fatores: introdução da IA generativa para a criação desse tipo de conteúdo, proliferação da venda de pacotes com imagens de nudez e sexo autogeradas por adolescentes e demissões em massa anunciadas pelas *big techs*, que atingiram as equipes de segurança, integridade e moderação de conteúdo de algumas plataformas[6].

Por meio da Nota Técnica nº 02/2025, a referida organização também indicou um avanço preocupante no uso indevido das ferramentas de inteligência artificial

[4] INTERNET WATCH FOUNDATION. Atualização de 2024: Compreendendo a rápida evolução das imagens de abuso infantil geradas por IA. **IWF**, jul. 2024. Tradução livre, realizada com o uso da ferramenta "Google Tradutor". Disponível em: https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/. Acesso em: 17 out. 2025.

[5] Ibidem.

[6] OLIVEIRA, Marcelo. Safernet recebe recorde histórico de novas denúncias de imagens de abuso e exploração sexual infantil na internet. **Safernet**, 6 fev. 2024. Disponível em: https://new.safernet.org.br/content/safernet-recebe-recorde-historico-de-novas-denuncias-de-imagens-de-abuso-e-exploracao-sexual#mobile. Acesso em 28 mai. 2024.

generativa para a produção de conteúdos sintéticos ilegais por meio de imagens reais de crianças e para a criação de representações totalmente artificiais de crianças e adolescentes no ano de 2025[7].

Diante das estatísticas trazidas, mas sem qualquer pretensão de esgotar o assunto, pretende-se estudar tal fenômeno a partir da esfera do direito digital, analisando-se aspectos técnicos e teóricos acerca da criação por inteligência artificial de representações de menores em contexto de violência e exploração sexual e tecendo considerações quanto às suas potenciais consequências jurídicas.

2. O USO DA INTELIGÊNCIA ARTIFICIAL PARA A CRIAÇÃO DE IMAGENS

A inteligência artificial é um campo da ciência da computação que se dedica ao desenvolvimento de sistemas e máquinas capazes de realizar tarefas que, tradicionalmente, demandam inteligência humana e são projetados para aprender, raciocinar, perceber o ambiente e tomar decisões com base em dados e experiências anteriores.

Nas palavras de Veridiana Domingos Cordeiro:

> A Inteligência Artificial, portanto, é um software programado para, ao ser executado, tomar decisões corretas. Decompondo-a a nível unitário, chegamos aos "algoritmos". Um algoritmo é "um procedimento computacional bem definido que toma certo valor ou conjunto de valores como input e produz certo valor, ou conjunto de valores, como output" (CORMEN et al., 2009, p. 5). Ou seja, são códigos de comando que instruem como o computador deve proceder de uma maneira ótima, são procedimentos que solucionam problemas a partir de um número de passos sem mobilizar quaisquer tipos de criatividade ou contemplar qualquer tipo de ambiguidade. Embora seja a peça-chave da Inteligência Artificial, os algoritmos não abstraem, não pensam e nem conhecem; apenas calculam; "algoritmos não raciocinam como nós para fazer o que fazemos com a razão", por exemplo, no caso da tradução automática, "eles processam e escrevem texto de uma forma informativa e útil sem entender nada em relação ao seu significado" (ESPOSITO, 2017, p. 6)[8].

[7] SAFERNET BRASIL. Nota Técnica nº 02/2025. **Safernet**, Salvador: 19 ago. 2025. Disponível em: https://arquivos.safernet.org.br/notas/Nota+Tecnica+02_2025+%5BSaferNet+Brasil%5D.pdf. Acesso em: 17 out. 2025.

[8] CORDEIRO, Veridiana Domingos. Novas questões para a sociologia contemporânea: os impactos da Inteligência Artificial e dos algoritmos nas relações sociais. *In*: COZMAN, Fabio; PLONSKI, Guilherme Ary; NERI, Hugo (Orgs.). **Inteligência Artificial**: avanços e tendências. São Paulo: Instituto de Estudos Avançados, 2021, p. 206-226. Disponível em: https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/BibliotecaDigital/BibDigitalLivros/TodosOsLivros/Inteligencia-artificial=avancos-e-tendencias.pdf. Acesso em: 22 abr. 2024.

Ludermir[9] explica a existência de três subdivisões da inteligência artificial: a "IA Focada", também denominada de "IA Fraca", consistente em algoritmos especializados na resolução de problemas específicos, que podem executar tarefas complexas, mas sempre com foco no objetivo para o qual foram desenvolvidos; a "IA Generalizada", conhecida como "IA Forte", em que os algoritmos tornam-se tão capazes quanto os seres humanos na realização de várias tarefas, adquirindo tal expertise a partir de técnicas de aprendizado de máquina; e, por último, a "IA Superinteligente", que, teoricamente, superariam as capacidades humanas em praticamente todas as áreas, mas, no momento, só aparecem em obras literárias e cinematográficas de ficção científica, não se sabendo ao certo se um dia realmente virão a existir.

O citado aprendizado de máquina é um subcampo da inteligência artificial que se concentra no desenvolvimento de algoritmos e modelos computacionais capazes de aprender padrões e realizar tarefas específicas a partir de dados, sem uma programação explícita para cada tarefa, permitindo que os sistemas melhorem seu desempenho ao longo do tempo e à medida que são expostos a mais dados e experiências[10]. Pode ser realizado de forma supervisionada, não supervisionada e por reforço:

> No Aprendizado Supervisionado, para cada exemplo apresentado ao algoritmo de aprendizado é necessário apresentar a resposta desejada (ou seja, um rótulo informando a que classe o exemplo pertence, no caso de um problema de classificação de imagens, por exemplo, como distinguir imagens de gatos e de cachorros). Cada exemplo é descrito por um vetor de valores (atributos) e pelo rótulo da classe associada. O objetivo do algoritmo é construir um classificador que possa determinar corretamente a classe de novos exemplos ainda não rotulados. Para rótulos de classe discretos, esse problema é chamado de classificação e para valores contínuos como regressão. Esse método de aprendizado é o mais utilizado. No Aprendizado Não Supervisionado, os exemplos são fornecidos ao algoritmo sem rótulos. O algoritmo agrupa os exemplos pelas similaridades dos seus atributos. O algoritmo analisa os exemplos fornecidos e tenta determinar se alguns deles podem ser agrupados de alguma maneira, formando agrupamentos ou clusters. Após a determinação dos agrupamentos, em geral, é necessária uma análise para determinar o que cada agrupamento significa no contexto do problema que está sendo analisado. No Aprendizado por Reforço, o algoritmo não recebe a resposta correta, mas recebe um sinal de reforço, de recompensa ou punição. O algoritmo faz uma hipótese baseado nos exemplos e determina se essa hipótese foi boa ou ruim. Aprendizado

[9] LUDERMIR, Teresa Bernarda. Inteligência Artificial e Aprendizado de Máquina: estado atual e tendências. **Instituto de Estudos Avançados da Universidade de São Paulo**, v. 35, n. 101, jan-abr. 2021. Disponível em: https://doi.org/10.1590/s0103-4014.2021.35101.007. Acesso em: 22 abr. 2024.

[10] Ibidem, p. 88-89.

> por Reforço é bastante utilizado em jogos e robótica, e foi a técnica utilizada no AlphaGo[11].

A aplicação do aprendizado de máquina para resolver desafios nem sempre é simples e requer certos requisitos prévios. É fundamental possuir robusto conjunto de exemplos, muitas vezes exigindo atualizações contínuas, pois a qualidade dos dados geralmente não é a ideal. Além disso, é crucial selecionar composições de algoritmos apropriadas para cada problema específico, sendo necessário que, após o treinamento, haja a verificação da efetiva solução do problema e do seu nível de precisão. Outrossim, a frequente manutenção do sistema é essencial, visto que mudanças nos dados podem impactar no funcionamento dos sistemas ao longo do tempo[12].

A Inteligência Artificial Generativa, por sua vez, é uma aplicação específica do aprendizado de máquina na qual os modelos são treinados para gerar novos exemplos que se assemelham aos dados originais. Isso pode ser feito em diferentes áreas, como geração de imagens realistas e criação de textos e músicas.

Segundo relatório da IWF (2023):

> Existem vários tipos de modelos de texto para imagem, incluindo redes adversárias generativas (GANs) e autoencoders variacionais (VAEs), mas todos os atuais geradores de imagens de IA de última geração – incluindo Midjourney, Stable Diffusion e DALL-E, são modelos de difusão. Treinar um modelo de difusão em grande escala requer um vasto conjunto de dados de imagens que são extraídas da Internet e depois rotuladas com palavras ou frases descritivas – o tipo de texto que mais tarde será usado para alertar as novas gerações. Geralmente, a coleta e a marcação necessária dessas imagens são terceirizadas para outras organizações:
>
> • Midjourney e DALL-E usam um modelo de difusão condicionado a incorporações contrastivas de imagens de pré-treinamento de linguagem-imagem (CLIP). O CLIP é treinado em 400 milhões de pares de imagens, extraídas da internet, com legendas.
>
> • O Stable Diffusion usa um conjunto de dados chamado LAION, desenvolvido por um grupo de pesquisadores europeus, que possui 2,6 bilhões de imagens marcadas no idioma inglês em um conjunto de dados de 6 bilhões de imagens. Várias versões do Stable Diffusion foram treinadas em amostras de milhões de imagens tiradas deste vasto conjunto de dados.
>
> Os modelos de difusão funcionam adicionando ruído gaussiano aleatório (ou simplesmente "ruído") às imagens e, em seguida, executando o processo inverso, "removendo o ruído" passo a passo para reconstruir cada imagem. "Novas" imagens são geradas alterando o ruído antes de executar

[11] Ibidem, idem.

[12] Ibidem.

> novamente o processo reverso de remoção de ruído aprendido. Durante o processo reverso de eliminação de ruído, camadas de ruído são removidas para gerar uma imagem. Um modelo de difusão pode ser interrompido em qualquer ponto ao longo deste processo inverso, mas produziria uma imagem barulhenta e "confusa" se interrompido muito cedo. Uma característica fundamental dos modelos de difusão é que eles são interpolativos. Eles traçam conexões dentro do conjunto de dados de treinamento e podem gerar novas imagens dentro dos limites semânticos desse conjunto de dados. Os modelos de difusão são de grande escala e podem gerar imagens detalhadas e de alta qualidade[13] .

De modo geral, a inteligência artificial tem desempenhado um papel cada vez mais relevante na sociedade atual. Com suas capacidades de processamento de dados e aprendizado contínuo, tem desencadeado avanços em diversas áreas, contribuindo para a otimização de processos, a criação de soluções inovadoras e o desenvolvimento de sistemas cada vez mais eficientes.

Um exemplo concreto que se pode mencionar é a sua aplicação na área da saúde. Com o uso de algoritmos, os médicos e demais profissionais da saúde podem analisar, concomitantemente, grandes quantidades de informações dos pacientes, identificando padrões e prevendo diagnósticos com maior precisão. Isso sem falar que a IA tem sido adotada também no desenvolvimento de novos medicamentos e na interpretação de exames laboratoriais, corroborando com a melhoria dos cuidados de saúde e aprimoramento de tratamentos eficazes.

Não obstante seus benefícios, o surgimento de tão relevante tecnologia trouxe consigo diversos desafios. A IA generativa permitiu o aparecimento de imagens ultrarrealistas de crianças e adolescentes envolvidos em contexto de exploração e violência sexual e, o que já era bastante complicado, tornou-se ainda pior. É imprescindível esclarecer que a disseminação de pornografia infantil está longe de ser um problema exclusivo da atualidade, mas, por certo, intensificou-se com a hiperssexualização infantil nas mídias sociais, a atual disponibilidade de grandes bancos de dados e a sua inadequada e criminosa utilização.

A rede global de computadores, conhecida como "Internet", permite a troca de informações e comunicações em escala mundial e compõe-se de uma infinidade de redes públicas e privadas que utilizam protocolos de comunicação padrão para interagirem entre si. De acordo com Ramalho, pode-se dividir em "Surface Web" e "Deep Web":

> A Surface Web pode ser definida como a parte da Internet que é geralmente acessível através dos motores de busca, como o Google, o Bing ou o Yahoo!, isto é, será o conjunto de páginas detectadas e escolhidas pelos motores

[13] IWF, op. cit., p. 12-13.

> de busca para integrarem os resultados de uma pesquisa. Por outro lado, a Deep Web será aquela área da Internet que não é acessível através dos motores de busca e que é composta, entre outras, por páginas que poderão ter sido propositadamente excluídas dos resultados de pesquisas efetuadas em motores de busca; por páginas cifradas ou cujo acesso depende da introdução de uma palavra-passe, como webmails ou páginas de Instant Messaging, por páginas para as quais nenhum link exterior remete (e que, portanto, não são detectadas pelos crawlers dos motores de busca), bem como por páginas geradas de forma dinâmica ou simplesmente invisíveis para um motor de busca, designadamente por serem compostas por ficheiros em formato script (como JavaScript ou Flash) ou em formato não-HTML (alguns ficheiros PDF, imagens, etc.). Apesar de inexistirem dados recentes que permitam, com algum rigor, conhecer a exata e atual dimensão de ambas as Webs, sabemos que, em 2001, a Deep Web tinha uma dimensão que se estimava ser entre 400 e 550 vezes superior à da Surface Web (sem contar com webmails e Instant Messaging) e continuava a crescer a um ritmo superior a esta[14] .

Diante do potencial de anonimato trazido pela Deep Web, ferramentas que inicialmente foram elaboradas para salvaguardar a liberdade de expressão e informação de seus utilizadores passaram a ser adotadas por perpetradores de ilícitos on-line como meio de eliminação do rastro digital, dando origem à Dark Web: conjuntos de páginas exclusivamente acessíveis a partir de recursos de software especificamente desenvolvidos para o ocultamento de informações durante a navegação on-line e dedicadas à "prática, divulgação, aconselhamento para a prática, incitamento ou publicitação de crimes ou à difusão de material de origem criminosa"[15].

> Daí que, imediatamente após a sua divulgação, o Freenet tenha passado a incluir várias páginas dedicadas à difusão de pornografia infantil e de material protegido por direito de autor, bem como ao ensino de técnicas de fabrico de explosivos e à proliferação de grupos terroristas. Contudo, foi o Tor o programa cuja exploração teve mais impacto na evolução da criminalidade na Deep Web, facto que se deveu desde logo à sua significativa superioridade em termos de rapidez face ao Freenet (não obstante seja, ainda assim, consideravelmente mais lento do que um browser normal), bem como à possibilidade que o Tor confere aos seus utilizadores de navegação num ambiente mais vasto da Internet e, em particular, da Deep Web. Assim, pouco tempo após a sua disponibilização, o Tor viu surgir diversos websites secretos, designados de hidden services, dedicados a todo o tipo de criminalidade. Começaram, então, a aparecer verdadeiros mercados de

[14] RAMALHO, David Silva. A investigação criminal na Dark Web. **Revista de Concorrência e Regulação**, ano IV, número 14/15, abr.-set. 2013.

[15] Ibidem, p. 393.

> droga, documentos falsos e outros materiais ilícitos, como o célebre The Silk Road no qual as transações são feitas com recurso a bitcoins, ou o mercado de drogas, armas e explosivos chamado Black Market Reloaded. Adicionalmente, surgiram mercados online dedicados à venda de pornografia infantil ou mesmo de espécies em vias de extinção, bem como inúmeras páginas e fóruns de pornografia infantil e/ou violenta, bem como fóruns dedicados ao canibalismo, fóruns jihadistas e páginas que comercializavam dados relativos a cartões de crédito obtidos através de esquemas de phishing.[16]

Então, se a divulgação de imagens de crianças e adolescentes em situação de violência e exploração sexual já constitui parte da cibercriminalidade, por qual razão a utilização de sistemas de inteligência artificial para a criação de imagens de mesma natureza e com os mesmos fins é tão diferente do problema que já se enfrenta há anos? Conforme citado, em função do seu alcance, do potencial de comercialização e da rapidez com que se desenvolve.

> O que é diferente no que diz respeito à IA, no entanto, é a velocidade de desenvolvimento e melhoria: quando os nossos analistas viram as primeiras representações de material de abuso sexual infantil gerado por IA (AI CSAM) na primavera deste ano (2023), havia claro indício de que este material foi gerado artificialmente; os fundos não estavam alinhados, as proporções das partes do corpo estavam erradas, ausentes ou desajeitadas. Meio ano depois, estamos agora numa posição em que as imagens são tão realistas que apresentam dificuldades reais de distinção, mesmo para os nossos analistas altamente treinados. O testemunho dos próprios perpetradores em fóruns da dark web também diz o que você quer saber; há júbilo porque as fantasias podem ser feitas sob encomenda. Tudo que você precisa é do idioma para informar ao software o que você deseja ver.[17]

Como bem apontado no Relatório da IWF de 2023, em meio a "todo o foco no realismo, fotorrealismo e hiper-realismo, e debates complexos sobre a legalidade – dito de forma simples – esta tecnologia permite que os perpetradores gerem dezenas, até mesmo centenas de imagens de abuso sexual infantil com o clique de um botão"; o indivíduo é capaz de fazer o *download* da tecnologia de IA com apenas alguns *gigabytes* e de executá-la no modo *off-line*, podendo "gerar quantas imagens de abuso sexual infantil quiser – 'no escuro', com pouco ou nenhum risco de detecção"[18].

Neste caso, a criação destas imagens poderá ser realizada a partir de treinamento algorítmico que tenha como base os registros reais de vítimas de violência sexual ou decorrer de específicas e detalhadas instruções escritas para a conversão do texto em representações visuais.

---

[16] Ibidem, p. 392-393.

[17] IWF, op. cit., p. 4.

[18] Ibidem, p. 7

> O ajuste fino do CSAM geralmente usa conjuntos de dados que apresentam uma criança específica – geralmente uma vítima conhecida de abuso sexual infantil ou uma criança famosa. Isso ocorre porque, para ambas as categorias, existem conjuntos de imagens grandes o suficiente para treinar modelos de IA. A primeira categoria tem a vantagem adicional de conter imagens pornográficas, de modo que o modelo de saída pode não precisar ser combinado com outros modelos ajustados para pornografia. A IWF está ciente há muito tempo da tendência entre as comunidades de perpetradores de "coletar" conteúdo apresentando suas vítimas preferidas de abuso sexual infantil. [...] Agora, os perpetradores podem treinar um modelo para gerar quantas imagens novas da vítima quiserem. Estes modelos são comparáveis aos modelos 3D na medida em que visam reproduzir a semelhança da vítima o mais fielmente possível, mas mantêm a flexibilidade para transpor o(s) personagem(s) gerado(s) para qualquer cenário; qualquer tipo de atividade.[19]

Embora a segunda situação pareça ser "menos pior" por, à primeira vista, não envolver qualquer revitimização infantojuvenil, não se pode olvidar que, em essência, como já explicado, para que exista correspondência entre o *prompt* de comando e a imagem criada, ao longo do treinamento de máquina, em algum momento, a ferramenta precisa ter sido submetida a bancos de dados de vítimas verdadeiras.

Logo, é possível dizer que:

> [...] Prejudica vítimas conhecidas de abuso sexual infantil, cujas imagens estão a ser utilizadas para gerar mais imagens delas em novos cenários. Prejudica novas vítimas de abuso sexual infantil, cujos potenciais investigadores podem gastar tempo e recursos no resgate de crianças que se revelam personagens virtuais. Estas imagens proporcionam novas possibilidades para os perpetradores utilizarem para preparar e coagir crianças. Eles até permitem que os perpetradores mais competentes tecnicamente ganhem dinheiro com abusos. E isso é o pior em termos de qualidade de produção que a tecnologia de IA jamais será. Só tem potencial para melhorar: para produzir imagens mais realistas; para melhor permitir o aliciamento e o abuso de crianças.[20]

Também é necessário mencionar que, além da quantidade e da velocidade com que as representações são criadas, o fato de os criminosos conseguirem facilmente manuais de instruções sobre a otimização e o aperfeiçoamento do conteúdo advindo da IA e poderem discutir e aprender uns com os outros sem que isso resulte para eles quaisquer consequências, contribui, e muito, com o agravamento da situação.

[19] Ibidem, p. 22.

[20] Ibidem, p. 8.

> Vale ressaltar que o AI CSAM compreende uma pequena parte dos fóruns da dark web. A grande maioria desses fóruns está repleta de CSAM reais (embora alguns sejam apenas para discussão e proíbam a postagem de CSAM). No entanto, vários fóruns de longa data adicionaram este ano novas seções de IA aos seus sites – e essas seções estão crescendo em popularidade. Nessas áreas, os perpetradores compartilham conselhos sobre como gerar AI CSAM; solicitar imagens ou modelos sob medida; compartilhar seu trabalho e oferecer feedback sobre o trabalho de outras pessoas. Essas discussões ocorrem abertamente enquanto os usuários se sentem anônimos, acreditando que as autoridades não querem ou não podem descobri-los. Os usuários compartilham conselhos sobre como se conectar a esses fóruns de maneira segura e não rastreável. Onde os usuários compartilham imagens AI CSAM em massa nesses fóruns, esses arquivos às vezes são hospedados na dark web e, outras vezes, hospedados na web aberta, de acordo com uma lista pré-aprovada de hosts de arquivos da web transparentes, anônimos e seguros.[21]

Para que essa prejudicialidade fique muito clara, destacam-se as principais atualizações do relatório da IWF, que avaliou as mudanças ocorridas entre outubro de 2023 e julho de 2024 em relação às imagens de abuso sexual infantil por IA e à tecnologia utilizada para criá-las:

> Principais atualizações do relatório de julho de 2024
>
> 1. Aumento de material de abuso sexual infantil gerado por IA: as últimas descobertas mostram que mais de 3.500 novas imagens de abuso sexual infantil geradas por IA foram carregadas no mesmo fórum da dark web analisado anteriormente em outubro de 2023.
>
> 2. Imagens mais graves: Das imagens geradas por IA confirmadas como abuso sexual infantil no fórum, mais imagens retrataram o abuso mais grave da Categoria A, indicando que os perpetradores são mais capazes de gerar cenários complexos e "hardcore".
>
> 3. Surgimento de vídeos de abuso sexual infantil gerados por IA: vídeos de abuso sexual infantil gerados por IA, principalmente deepfakes, começaram a circular, destacando os rápidos avanços tecnológicos em modelos/geradores de IA. Cada vez mais, vídeos deepfakes compartilhados em fóruns da dark web pegam vídeos pornográficos adultos e adicionam o rosto de uma criança usando ferramentas de IA.
>
> 4. Aumento na Clear Web: Há um aumento notável em imagens de abuso sexual infantil geradas por IA na clear web, inclusive em sites comerciais.

[21] Ibidem, p. 25.

> 5. Abuso sexual infantil por IA com vítimas conhecidas e crianças famosas: os agressores usam cada vez mais modelos de IA aprimorados para gerar novas imagens de vítimas conhecidas de abuso sexual infantil ou crianças famosas.[22]

O que se percebe é que muito se discute sobre os riscos hipotéticos da criação de uma "superinteligência", do surgimento de vírus sintéticos ou ataques cibernéticos, mas, ao contrário desses, as imagens originadas dos algoritmos que, consoante informado pela IWF, mostram "estupro de bebês e crianças pequenas; crianças pré-adolescentes famosas sendo abusadas sexualmente; conteúdo BDSM (escravidão e disciplina, domínio e submissão e sadomasoquismo) apresentando pré-adolescentes e adolescentes"[23], constituem um problema real que está acontecendo agora e requer atenção.

3. ESTUDO COMPARADO E ANÁLISE DA LEGISLAÇÃO BRASILEIRA VIGENTE

A necessidade de proteção à infância e à juventude parece ser uma constante entre a maioria dos países, o que é de fácil percepção diante da elevada quantidade de instrumentos jurídicos internacionais que versam a esse respeito.

A Convenção sobre os Direitos da Criança, promulgada no Brasil por intermédio do Decreto nº 99.710, de 21 de novembro de 1990, previu, em seu artigo 34, expresso comprometimento dos Estados partes em relação à proteção de todas as formas de abuso e exploração sexual a partir da adoção de medidas de caráter nacional, bilateral e multilateral necessárias para impedir quaisquer ofensas ao maior interesse da criança.

Também a título exemplificativo, o Protocolo Facultativo à Convenção sobre os Direitos da Criança, referente à venda de crianças, à prostituição infantil e à pornografia infantil, promulgado por meio do Decreto nº 5.007, de 8 de março de 2004, determinou a proibição de pornografia infantil, definindo-a como "qualquer representação, por qualquer meio, de uma criança envolvida em atividades sexuais explícitas reais ou simuladas, ou qualquer representação dos órgãos sexuais de uma criança para fins primordialmente sexuais" (artigo 2º, "c").

A efetivação dessa tutela se deu a partir da Lei nº 8.069, de 13 de julho de 1990, que dispõe sobre a proteção integral à criança e ao adolescente, tendo a Lei nº 11.829, de 25 de novembro de 2008, conferido nova redação aos artigos 240, 241, 241-A, 241-B, 241-C, 241-D e 241-E, a fim de "aprimorar o combate à produção,

[22] INTERNET WATCH FOUNDATION. Atualização de 2024: Compreendendo a rápida evolução das imagens de abuso infantil geradas por IA. **IWF**, jul. 2024. Tradução livre, realizada com o uso da ferramenta "Google Tradutor". Disponível em: https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/. Acesso em: 17 out. 2025.

[23] IWF, Op. cit, p. 7.

venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet".

Referidos dispositivos reforçaram a criminalização da produção, comercialização, transmissão, publicação e posse de imagens e representações de cenas de sexo explícito ou pornográficas envolvendo criança ou adolescente, bem como o aliciamento, assédio e instigação de criança para a prática de atos libidinosos e, ainda, a exploração da prostituição infantojuvenil.

Todavia, seria possível dizer que as citadas condutas são igualmente reprováveis quando a imagem retratada decorre de uma ferramenta de inteligência artificial que produz, de modo realista, crianças e adolescentes que não existem?

Conforme apontado, o Reino Unido possui duas legislações – Protection of Children Act 1978 e Coroners and Justice Act 2009 – que sancionam a obtenção, distribuição e posse de "fotografia indecente ou pseudofotografia de criança" e de "imagem proibida de uma criança", o que inclui, no primeiro caso, uma imagem, adquirida por meio de computação gráfica ou de outra forma, que pareça ser uma fotografia, e, no segundo, registros não fotográficos, como desenhos, animações e similares.

Já o Código Penal Português, em seu artigo 176, nº 4, preconiza a aplicação de pena para aqueles que praticarem determinados delitos "utilizando material pornográfico com representação realista de menor".

De igual modo prevê a Convenção sobre o Crime Cibernético, firmada em Budapeste em 23 de novembro de 2001 e promulgada no Brasil a partir do Decreto nº 11.491, de 12 de abril de 2023, que ampliou o conceito de pornografia infantil, passando a abranger representações visuais de "imagens realísticas retratando um menor envolvido em conduta sexual explícita".

Não obstante, o tema é polêmico mesmo entre os países em que a possibilidade de punição da pornografia infantil gerada por IA, ainda que de forma implícita, já se encontra codificada.

Contrariamente à tipificação, argumenta-se no sentido de que a inutilização de fotos e vídeos do mundo real tornaria a conduta mais ética e que, a partir de um efeito catártico, serviria como meio para desencorajar a ocorrência de delitos sexuais, o que significa dizer que a visualização dessas imagens geraria, em tese, suficiente e temporária satisfação dos impulsos sexuais pedófilos do seu consumidor, evitando a concretização de ações mais gravosas, refutando entendimentos em sentido contrário[24]. Além disso, alega-se que a sua penalização consistiria em intolerável limitação à liberdade de expressão e absoluta censura moral, uma vez que, nesta

[24] SILVA, João Miguel Almeida da. **Cibercrime**: o crime de pornografia infantil na internet. Dissertação em Ciências Jurídico-Forenses. Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2º Ciclo de Estudos em Direito (conducente ao grau de Mestre), na Área de Especialização em Ciências Jurídico-Forenses. UC, jan. 2016. Disponível em: https://estudogeral.sib.uc.pt/handle/10316/34801. Acesso em: 22 maio 2024.

hipótese, não haveria bem jurídico que justificasse tão ampla tutela penal [25]. A esse respeito, é possível mencionar o caso Aschcroft et al. v. Free Speech Coalition et. al., de 16 de abril de 2002, analisado pelo Supremo Tribunal norte-americano:

> O Supremo Tribunal norte-americano, no caso Aschcroft et al. v. Free Speech Coalition et. al., de 16 de Abril de 2002, considerou a criminalização da pornografia infantil virtual (não só a que usa imagens reais de crianças, mas a que usa imagens que «parecem ser de crianças» ou «dão a impressão» de que se trata de crianças), decorrente do Child Pornography Prevention Act de 1996, inconstitucional por reduzir em medida substancial a liberdade de expressão garantida pela Primeira Emenda à Constituição. De acordo com a argumentação do Governo norte-americano, as imagens de pornografia virtual, embora não resultem em si mesmas de abuso sexual de crianças, poderão incitar ou conduzir à prática desse tipo de crimes. O Supremo Tribunal, na sentença proferida nesse caso, responde a esse argumento dizendo que essa ligação é casual e indirecta e que o dano não decorre necessariamente da forma de expressão ("speech") em causa, mas depende de uma potencialidade não quantificável para a prática de actos criminosos. A mera tendência de uma forma de expressão ("speech") para encorajar actos ilícitos não é razão suficiente para a proibir. Ao argumento do Governo de que, face ao aperfeiçoamento tecnológico, poderá ser impossível distinguir imagens reais e imagens virtuais, e de que será, por isso, fácil para um acusado invocar sempre que se tratam de imagens virtuais mesmo que não o sejam, responde o Supremo Tribunal que não pode ser proibida uma forma de expressão não protegida pela tutela da liberdade de expressão decorrente da Primeira Emenda ("unprotected speech") se dessa forma também se proíbem, em medida substancial, formas de expressão abrangidas por essa tutela ("protected speech"). O Governo não pode suprimir uma forma de expressão lícita ("protected speech") como meio para suprimir uma forma de expressão ilícita ("unprotected speech").[26]

Por outro lado, seus defensores sustentam que, independentemente de se tratar de imagens com pessoas reais ou não, a pornografia infantil virtual é utilizada para normalizar e estimular crianças e adolescentes a participarem de atos sexuais, não sendo de fácil vislumbre a distinção entre o que é ou não real ou, ainda, entre os consumidores de um ou outro tipo de material. Aponta-se, também, o fato de que a sua proliferação promoveria o agravamento de tendências pedófilas preexistentes nos indivíduos[27], desencadeando, em processos de imitação patológica, episódios

[25] PATTO, Pedro Maria Godinho Vaz. Pornografia infantil virtual. **Julgar**, n. 12, set-dez. 2010 (Especial: crimes no seio da família e sobre menores). Disponível em: https://julgar.pt/julgar_em_papel/julgar-n-o-12/. Acesso em: 17 maio 2024.

[26] PATTO, op. cit., p. 3.

[27] SILVA, op. cit., p. 28.

de verdadeiros crimes sexuais contra menores[28]. Nesse sentido, destaca-se o caso R. v. Sharpe, examinado pelo Supremo Tribunal do Canadá:

> [...] pronunciou-se o Supremo Tribunal do Canadá, numa sua sentença de 26 de Abril de 2001, no caso R. v. Sharpe. Nessa sentença afirma-se que qualquer tipo de pornografia infantil, independentemente da utilização efectiva de crianças na sua produção, produz efeitos que a ordem jurídica deve legitimamente contrariar: consolida e reforça nas pessoas com tendências pedófilas a noção de que as relações sexuais entre adultos e crianças são aceitáveis, contribuindo para nelas enfraquecer a natural inibição que impediria essas relações; é, por definição, destinada a estimular esse tipo de comportamento; é, muitas vezes, utilizada como instrumento na prática dessas relações, para levar a criança a aceitá-las. [...] O facto de não haver dados empíricos quantificáveis a respeito da relação entre o consumo de pornografia infantil e a prática de crimes sexuais contra crianças (até porque razões éticas obstam ao uso de métodos experimentais neste campo) não é, por si só, obstáculo à legitimidade da incriminação. Basta que se verifique uma «apreensão racional» dessa ligação. Por outro lado, o dano inerente à pornografia infantil resulta, desde logo, da mensagem que veicula (tal como nos crimes de incitamento à discriminação ou ao ódio racial), e não apenas do modo como é produzida. Essa mensagem — a de que crianças são parceiros sexuais apropriados para adultos — traduz-se na desumanização, "degradação" e "coisificação" das crianças.[29]

Nota-se que a existência ou não de relação entre o consumo de imagens de exploração sexual infantil e a prática de crimes de mesma natureza parece ser importante tema de discussão, haja vista que é ponto comum de debate entre defensores e críticos da criminalização em tela.

Em fala durante o Seminário da Comissão de Segurança Pública e Combate ao Crime Organizado da Câmara dos Deputados, Rufino[30] apontou que "pelo menos 80% dos estupradores de crianças confessam que seus crimes foram estimulados pela pornografia" e que "82% dos presos por crimes sexuais contra crianças e adolescentes

[28] PATTO, op. cit., p. 2.

[29] PATTO, Ibidem, p. 4-5.

[30] RUFINO, Claudio. **A influência da pornografia nos casos de abuso e exploração sexual de crianças e adolescentes**. Câmara dos Deputados. Departamento de Taquigrafia, Revisão e Redação – Núcleo de Redação Final em Comissões. Comissão de Segurança Pública e Combate ao Crime Organizado. Seminário n° 1461/08, 6 nov. 2008. Disponível em: https://www.camara.leg.br/internet/SitaqWeb/TextoHTML.asp?etapa=11&nmComissao=Comiss%C3%A3o%20de%20Seguran%C3%A7a%20P%C3%BAblica%20e%20Combate%20ao%20Crime%20Organizado&tpReuniaoEvento=Semin%C3%A1rio&dtReuniao=06/11/2008&hrInicio=14:18:00&hrFim=17:17:00&origemDiscurso=&nmLocal=Plen%C3%A1rio%20Principal%20-%20CD&nuSessao=1461/08&nuQuarto=0&nuOrador=0&nuInsercao=0&dtHora rioQuarto=14:18&tsgFaseSessao=&Data=06/11/2008&txApelido=&txFaseSessao=&txTipoSessao=Permanente&dtHoraQuarto=14:18&txEtapa=. Acesso em: 28 mai. 2024.

eram consumidores de pornografia ou admitiam que eram viciados em pornografia e que praticaram em suas vítimas as cenas que assistiram por horas, antes ou durante a prática de seus crimes". É verdade que sua credibilidade é posta em xeque, por tratar-se do discurso de um pastor evangélico que, em sua integralidade, mostrou-se polêmico, preconceituoso e sem aparente confirmação científica, ante a falta de menção às fontes das estatísticas referenciadas. Entretanto, fontes mais fidedignas já concluíram pela existência do referido nexo de causalidade.

> Precisamos apenas olhar para o incrível trabalho de Suojellaan Lapsia (Protect Children) e o seu Relatório de Pesquisa de Redirecionamento, onde mais de metade (52%) dos entrevistados sentiram medo de que ver CSAM pudesse levar a atos sexuais contra uma criança; 44% disseram que assistir ao CSAM os fez pensar em procurar contato com uma criança, e mais de um terço (37%) disse ter procurado contato direto com uma criança depois de assistir ao CSAM[31].

Em sentido semelhante:

> Estes estudos conduzem a resultados díspares. Há uns que apontam no sentido de uma diferença pouco significativa (de 32 a 43%) no consumo de pornografia infantil entre pessoas com tendência pedófila agressoras ou não agressoras. Há outros que indicam que de 10 a 25% dos agressores reconhecem que a pornografia influenciou o seu comportamento. Outros apontam para percentagens mais elevadas (53%) de agressores que reconhecem ter a pornografia desempenhado um importante papel na sua conduta. Há agressores que consideram ter a pornografia estimulado a sua conduta, mas também há outros que reconhecem ter a pornografia evitado condutas agressoras através do chamado "efeito catártico". A discrepância entre os dados empíricos da experiência policial, por um lado, e os resultados dos estudos retrospectivos baseados em inquéritos aos agressores, por outro lado, pode ser explicada — afirma-se ainda nesse relatório — precisamente pelo facto de estes estudos se basearem em declarações dos próprios agressores e de estes tenderem a minimizar o alcance e gravidade da sua conduta[32] .

Mesmo assim, tendo em vista a falta de consenso em relação ao quão problemática pode ser a produção de imagens de menores em contexto de violência e exploração sexual por uma IA, é extremamente relevante trazer à baila as considerações dos próprios responsáveis pela conduta, extraídas de um fórum da Dark Web:

> [...] reações contrastantes podem ser encontradas em fóruns onde o AI CSAM é compartilhado. Alguns são desdenhosos: "Posso reconhecer o

[31] HARGREAVES, apud. IWF, op. cit., p. 4.

[32] PATTO, op. cit., p. 7

> trabalho da IA num piscar de olhos". Outros expressam surpresa ou admiração pela qualidade do resultado: "Já se passaram alguns meses desde que verifiquei a IA do garoto. Meu Deus, ficou muito bom!"; "Estes são realmente impressionantes. Parte do realismo delas é cerca de 95% indistinguível das fotos reais"; "Como diabos você consegue esse tipo de imagens? Já vi imagens realistas, mas isso é excelente"; "As imagens geradas por IA estão cada vez melhores"; "O fotorrealismo aqui é impressionante, quero dizer, tenho certeza de que um olho treinado ainda pode ver que é uma imagem gerada, mas não muito". Outros questionam se estão olhando para imagens reais ou imagens fotorrealistas geradas por IA: "Eu simplesmente não consigo entender que esses meninos não são reais!"; "Tem certeza de que são CGI?"; "Parabéns por atingir o fotorrealismo. Isso é uma loucura. Quanto melhor fica a partir daqui?". Exemplos de pessoas perguntando: "quem é?" em resposta às imagens – apenas para serem informados de que as imagens não são de crianças reais – foram encontrados. [...] Um comentário chegou a afirmar que o AI CSAM era superior porque as imagens reais do CSAM costumam ser de baixa qualidade: "A maioria das fotos não chega nem perto da qualidade produzida pela IA. Fotos mal compostas, mal expostas, de baixa resolução e fora de foco são comuns". Outro usuário queria produzir imagens geradas por IA de qualidade inferior para torná-las mais parecidas com CSAM real: "Por padrão, as IAs não ensinavam que a realidade é doentia e suja, porque as pessoas querem imagens bonitas e perfeitas, então as instruem dessa maneira. Mas quando se trata de sexy, falta algo: doente e sujo faz parte! É por isso que não estou satisfeito e tento encontrar maneiras de obter uma renderização mais realista". Como as imagens geradas por IA têm, por padrão, uma aparência "limpa" de alta qualidade, as imagens produzidas de acordo com esse tipo de opinião – imagens que parecem de qualidade inferior, "mais granuladas" ou menos nítidas – podem representar um desafio importante para a futura detecção por IA[33].

O êxtase de muitos criminosos diante das inovações e possibilidades trazidas pela inteligência artificial encerra a discussão e confirma o potencial danoso que circunda a temática em comento, restando saber se a legislação brasileira vigente é suficientemente capaz de lidar com a situação.

O Estatuto da Criança e do Adolescente[34] tipifica os seguintes crimes em espécie:

> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, **envolvendo criança ou adolescente**:

[33] IWF, op. cit., p. 32 e 34

[34] BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial da União**, Brasília, 16 jul. 1990.

Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (Redação dada pela Lei nº 11.829, de 2008)

§1º Incorre nas mesmas penas quem:

I - agência, facilita, recruta, coage ou de qualquer modo intermedeia a participação de **criança ou adolescente** nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena;

II - exibe, transmite, auxilia ou facilita a exibição ou transmissão, em tempo real, pela internet, por aplicativos, por meio de dispositivo informático ou qualquer meio ou ambiente digital, de cena de sexo explícito ou pornográfica com a participação de **criança ou adolescente**.

§2º Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime:

I – no exercício de cargo ou função pública ou a pretexto de exercê-la;

II – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou

III – prevalecendo-se de relações de parentesco consanguíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento. (gn)

Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo **criança ou adolescente**:

Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (gn)

Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo **criança ou adolescente**:

Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.

§1ª Nas mesmas penas incorre quem:

I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;

II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.

§2º As condutas tipificadas nos incisos I e II do §1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo. (gn)

Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo **criança ou adolescente**:

Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

§1º A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.

§2º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:

I – agente público no exercício de suas funções;

II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;

III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.

§3º As pessoas referidas no §2º deste artigo deverão manter sob sigilo o material ilícito referido. (gn)

Art. 241-C. Simular a participação de **criança ou adolescente** em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo. (gn)

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. (gn)

> Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva **criança ou adolescente** em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais. (gn)

Conforme se observa, trata-se de tipos mistos alternativos que se referem a ações especificamente relacionadas a "cena de sexo explícito ou pornográfica envolvendo criança ou adolescente". Ainda que o Superior Tribunal de Justiça (STJ) já tenha afirmado que o disposto no artigo 241-E deve ser interpretado de forma ampla, a fim de garantir que o bem jurídico protegido seja devidamente amparado[35], o mesmo não foi feito em relação ao termo "criança ou adolescente", razão pela qual acredito que a representação de menores criados por IA não corresponde a nenhum dos crimes citados, podendo-se falar na ocorrência de crime impossível, diante da absoluta impropriedade do objeto, nos termos do artigo 17 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal Brasileiro)[36].

Na melhor das hipóteses, caberiam acusações relacionadas aos artigos 286 (Incitação ao Crime) e 287 (Apologia de Crime) do CPB, a depender do caso concreto que estiver sendo considerado, pois, conforme visto na discussão anteriormente mencionada, embora o nexo de causalidade seja o bastante para identificar problemas de ordem ética e moral, pode não ser suficiente para fixar relação direta e incontestável de causa e consequência, o que significa que até mesmo essas infrações de menor potencial ofensivo poderiam não incidir na situação em exame, ante a inexistência de conduta tipificada.

> Incitação ao crime
>
> Art. 286 - Incitar, publicamente, a prática de crime:
>
> Pena - detenção, de três a seis meses, ou multa.
>
> Parágrafo único. Incorre na mesma pena quem incita, publicamente, animosidade entre as Forças Armadas, ou delas contra os poderes constitucionais, as instituições civis ou a sociedade.
>
> Apologia de crime ou criminoso
>
> Art. 287 - Fazer, publicamente, apologia de fato criminoso ou de autor de crime:
>
> Pena - detenção, de três a seis meses, ou multa.

[35] BRASIL. Supremo Tribunal de Justiça. **REsp nº 1.543.267/SC**. Relatora Min. Maria Thereza de Assis Moura, Sexta Turma, julgado em 3 dez. 2015, DJe de 16 fev. 2016. Brasília, DF: STJ, 16 fev. 2016. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=1457585&tipo=0&nreg=201501690431&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20160216&formato=PDF&salvar=false. Acesso em: 23 maio 2024.

[36] BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal Brasileiro. Diário Oficial da União. Rio de Janeiro,1940.

Por outro lado, na hipótese de o indivíduo executar referidas ações acreditando que as imagens representavam crianças e adolescentes reais, entendo que a sua responsabilização seria admissível, visto que o dolo corresponderia àquele que é exigido pelos tipos penais, assemelhando-se ao erro sobre a pessoa, previsto no artigo 20, §3º, do CPB, já que seriam consideradas as condições e qualidades da pessoa contra quem o agente queria praticar o crime.

> Nesta linha, o Supremo Tribunal norte-americano veio a pronunciar-se de novo sobre a questão numa sentença posterior, de 19 de maio de 2008, proferida no caso United States v. Willis, que declarou a constitucionalidade de um outro diploma relativo à punição da pornografia infantil, o Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act, de 2003. Este diploma não pune directamente a pornografia infantil virtual, mas pune a conduta de quem propõe a transacção de material pornográfico na convicção de que esse material representa crianças reais (mesmo que não as represente efectivamente) ou de quem propõe essa transacção com a intenção de criar no adquirente a convicção de que esse material representa crianças reais (mesmo que não as represente efectivamente). No fundo, trata-se de uma punição da simples tentativa. Por esta via, pretende o legislador obviar à impunidade da produção de pornografia infantil pelo facto de o progresso tecnológico, cada vez mais frequentemente, permitir criar a dúvida sobre se as imagens em causa são reais ou virtuais (e a dúvida há-de beneficiar sempre o acusado: *in dubio pro reo*) e de se tornar, assim, um recurso fácil para evitar qualquer condenação alegar que se trata de imagens virtuais[37].

Na verdade, porém, a grande dificuldade de se comprovar a falta de conhecimento quanto ao uso de IA na criação das imagens poderia consolidar tese defensiva capaz de desencadear elevada impunidade em meio aos perpetradores de pornografia infantil, uma vez que o ordenamento jurídico brasileiro prevê a aplicação do princípio *in dubio pro reo*, segundo o qual a dúvida no processo penal, por falta de provas, deve ser interpretada em favor do acusado.

> A impunidade da pornografia infantil virtual pode levar a que, com o aperfeiçoamento tecnológico que torna difícil (senão, mesmo, impossível) distinguir a representação pornográfica de verdadeiras crianças da representação pornográfica virtual realista de crianças, a falsa alegação de que estejam em causa imagens virtuais possa transformar-se em fácil estratagema para evitar quaisquer condenações[38].

[37] PATTO, op. cit., p. 4

[38] PATTO, op. cit., p. 9.

Mesmo que a tipificação em tela pudesse receber interpretação ampliativa e passar a abranger situações como as que se discute neste artigo – o que só se admite em teoria, pois isso violaria a reserva legal, nos termos dos artigos 5º, inciso XXXIX, da Constituição Federal, e 1º do Código Penal Brasileiro (CPB) –, seria viável eventual alegação de erro de proibição, pois o agente poderia carecer de consciência sobre a ilicitude do fato e supor a sua legalidade por não haver pessoas reais envolvidas.

Na prática, as notícias apresentadas na introdução do presente artigo afirmam que o adolescente de 15 anos poderia ser "responsabilizado por até três anos de internação em centro socioeducativo"[39] e que o homem de 48 anos seria "interrogado e encaminhado ao sistema prisional, com prisão preventiva"[40], fazendo supor que não tem existido diferenciações para a responsabilização criminal de pessoas envolvidas com materiais de pornografia infantil, ainda que não se refiram a pessoas verdadeiras. Por outro lado, talvez tal conclusão seja demasiadamente precipitada, uma vez que em todas as situações ocorridas no Brasil foram conjuntamente apreendidas imagens de ambas as espécies. Infelizmente, por se referirem a casos amparados por segredo de justiça, não foi possível identificar os correspondentes processos e tampouco os seus resultados e fundamentos.

3.1 *Resultados da análise comparativa*

Nos ordenamentos estrangeiros analisados, observa-se uma abordagem mais ampla e preventiva do que aquela adotada pelo Brasil. O Reino Unido tipifica expressamente as chamadas *pseudofotografias* e *imagens proibidas de crianças*, abrangendo aquelas geradas digitalmente que aparentam retratar menores reais. De modo semelhante, Portugal, em seu Código Penal (art. 176, nº 4), prevê a punição de quem produza ou detenha *representações realistas de menor*, ainda que inexistente no mundo real. Em ambos os sistemas, o bem jurídico tutelado é a dignidade infantojuvenil em sentido amplo, compreendendo não apenas a proteção da imagem da criança, mas também a prevenção da banalização e do estímulo a práticas pedófilas.

O Brasil, contudo, mantém-se atrelado a uma concepção estritamente ontológica da vítima, o que reduz a eficácia da tutela penal diante da rápida evolução tecnológica. A análise evidenciou que, embora a legislação nacional seja consistente na repressão à pornografia infantil tradicional, não alcança de forma adequada as

[39] BARROS, Bruno Luís. Pornografia infantil com uso de IA em escola de BH é investigada pela polícia. **Correio Braziliense**, 8 nov. 2023. Disponível em: https://www.correio braziliense.com.br/brasil/2023/11/6652353-pornografia-infantil-com-uso-de-ia-em-escola-de-bh-e-investigada-pela-policia.html. Acesso em: 25 maio 2024.

[40] POLEZE, Carol. Suspeito de pornografia infantil no ES usava inteligência artificial para produzir imagens. **Redação Folha Vitória**, 17 maio 2024. Disponível em: https://www.folha vitoria.com.br/policia/noticia/05/2024/pornografia-infantil-preso-no-es-usava-inteligencia-artificial-para-produzir-fotos. Acesso em: 23 mai. 2024.

condutas que envolvem representações virtuais realistas de crianças e adolescentes, criadas por inteligência artificial ou outros meios tecnológicos. Essa limitação gera insegurança jurídica e potencial cenário de impunidade, revelando a necessidade de atualização normativa que acompanhe os novos modos de produção de conteúdo ilícito no ambiente digital.

4. ALTERNATIVAS E PROVIDÊNCIAS POSSÍVEIS

O Projeto de Lei nº 5.694/2023, de autoria do deputado Davys Frederico Teixeira Linhares, do partido Republicanos (DF)[41], apresentado em 24 de novembro de 2023, propôs a criminalização da manipulação ou adulteração de fotos, vídeos ou sons, utilizando-se de sistemas de inteligência artificial, com o intuito de causar constrangimento, humilhação, assédio, ameaça ou qualquer outro tipo de violência contra crianças ou adolescentes. Além disso, aumenta a pena para crimes relacionados à pornografia infantil na hipótese de uso de inteligência artificial, se a cena de sexo explícito ou pornográfica envolvendo criança ou adolescente for manipulada ou adulterada por meio de sistema de inteligência artificial.

Do modo como foi escrito, referido PL parece ter sido pensado especificamente no problema da nudificação de crianças e adolescentes, exemplificado na introdução deste artigo com o caso ocorrido em Minas Gerais, sem dar a devida atenção às situações em que a IA é usada para a criação de material de pornografia infantil de pessoas que não são reais.

Ainda que tal possibilidade possa ser incluída no trecho que versa sobre a manipulação de imagens por sistema de inteligência artificial, em termos de Direito Penal e política criminal, acredito que melhor seria se constasse expressamente na redação do tipo legal a possibilidade de penalização desta espécie de imagem.

O mesmo se pode dizer sobre o Projeto de Lei nº 6.211/2023[42], de autoria da deputada Renata Abreu, do partido Podemos (SP), apresentado em 22 de dezembro de 2023, apenso ao PL nº 5.694/2023, que prevê alterações no Estatuto da Criança e Adolescente (ECA) para "criminalizar a criação de conteúdo erótico e pornográfico, a partir do rosto de crianças e adolescentes, por meio de sistemas de inteligência artificial" e modifica o Código Penal para "criminalizar a criação de conteúdo erótico e pornográfico por meio de sistemas de inteligência artificial, a partir do rosto da vítima, e sem o seu consentimento".

[41] CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.694/2023**. Davys Frederico Linhares – Republicanos/DF, 24/11/2023. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2406508. Acesso em: 30 maio 2024.

[42] CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 6.211/2023**. Renata Abreu – Pode/SP, 22/12/2023. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2416533. Acesso em: 30 maio 2024.

Aqui, houve maior aproximação em relação ao problema em discussão, porém, novamente, a menção ao uso de rosto de criança ou de adolescente exclui a hipótese em que inexiste na representação gráfica alguém real.

Considerando as lacunas identificadas nos referidos Projetos de Lei, talvez o mais adequado, *de lege ferenda*, seria que os tipos penais já previstos no Estatuto da Criança e do Adolescente fossem expressamente aplicáveis também às hipóteses em que as representações de caráter sexual envolvam crianças ou adolescentes inexistentes no mundo real, mas gerados por meio de inteligência artificial ou outros recursos tecnológicos capazes de induzir à crença de veracidade. Essa ampliação garantiria a efetiva tutela da dignidade infantojuvenil diante das novas formas de violência sexual virtual, assegurando que condutas socialmente lesivas, ainda que desprovidas de vítima concreta, não permaneçam impunes. Nesse sentido, uma redação possível para eventual inclusão legislativa seria a do artigo 241-F, nos seguintes termos:

> Artigo 241-F. Para efeito dos crimes previstos nesta Lei, incorre nas mesmas penas previstas nos artigos 240 a 241-E quando a imagem, vídeo ou qualquer outro meio de representação do tipo penal correspondente incluir criança ou adolescente gerado a partir de inteligência artificial ou outro meio tecnológico que seja capaz de induzir, objetivamente, à crença de que se trata de criança ou adolescente real.

Em sentido semelhante à redação ora proposta, recentemente foi apresentado o Projeto de Lei nº 3.066, de 25 de junho de 2025[43], de autoria do deputado Osmar Terra, do partido Movimento Democrático Brasileiro (RS), que

> institui medidas de enfrentamento e repressão aos crimes de pornografia de crianças e adolescentes relacionados ao uso de inteligência artificial e de técnicas de mascaramento de endereço de IP empregadas para viabilizar a prática de crimes relacionados à pornografia infantil na internet, altera a Lei nº 8.069/90 (Estatuto da Criança e do Adolescente), o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), a Lei nº 7.210, de 11 de julho de 1984 (Lei de Execução Penal), a Lei nº 8.072, de 25 de julho de 1990 (Lei dos Crimes Hediondos) e a Lei nº 12.850/2013 (Lei das Organizações Criminosas) para recrudescer o tratamento penal aos criminosos sexuais.

Apesar de também dispor sobre diversos outros assuntos relacionados, no que diz respeito à problemática discutida no presente artigo, se comparado aos demais projetos, o PL nº 3.066/2025 parece ter sido o mais bem pensado. Isso porque, o seu artigo 2º prevê a criação de artigo intitulado "Representação digital fictícia de criança

[43] CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 3.066/2025**. Osmar Terra – MDB/RS, 25 jun. 2025. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2528433. Acesso em: 20 out. 2025.

ou adolescente", segundo o qual considera-se *cena de sexo explícito ou pornográfica* todo e qualquer registro de criança e adolescente, mesmo que não corresponda a situação ou pessoa real e seja integralmente gerada por inteligência artificial generativa ou outro recurso tecnológico:

> Representação digital fictícia de criança ou adolescente
>
> Art. 241-F. Para efeito dos crimes previstos nesta lei, também será considerada "cena de sexo explícito ou pornográfica" toda e qualquer imagem, fotografia, vídeo ou outro registro de criança ou adolescente, mesmo que não corresponda a situação ou pessoa real e seja integralmente gerada por inteligência artificial generativa ou outro recurso tecnológico, desde que produzida com o intuito de exploração sexual, estímulo à pornografia infantojuvenil ou satisfação libidinosa.
>
> Parágrafo único. Não configura crime a representação digital de que trata o caput quando produzida exclusivamente para fins acadêmicos, investigativos ou científicos, desde que ausente qualquer objetivo de estímulo à pornografia infantil, e que haja, quando necessário, prévia autorização judicial.

Como forma de enriquecer a discussão apresentada e reforçar as argumentações trazidas, vale destacar trecho da justificativa do mencionado Projeto de Lei:[44]

> [...] Nesse contexto, o surgimento da pseudopornografia revolucionou o mercado da pornografia infantojuvenil, abrindo novas portas para os criminosos e tornando ainda mais complexo o trabalho de combate a este tipo de conduta. Essas pseudo-imagens pornográficas acabam fazendo com que os consumidores do conteúdo pensem que suas condutas não são criminosas, nem sequer problemáticas, visto que deixam de ver a pornografia infantil em geral como um crime para pensar a conduta apenas como pornografia, algo lícito e cotidiano, apenas para sua satisfação sexual privada. Com isso, a crescente capacidade das tecnologias de criar mídias realistas e convincentes, muitas vezes indistinguíveis de conteúdos reais, impõe desafios significativos para a proteção da dignidade humana e que a ausência de uma legislação ou ao menos um dispositivo específico para lidar com esse fenômeno complexo acaba por abrir brechas legislativas preocupantes, o que exige uma reflexão profunda sobre como adaptar as estruturas legais existentes para abranger essa forma emergente de exploração. A criminalização da pornografia infantil simulada baseia-se na dificuldade de verificação da idade dos envolvidos no material pornográfico, o que acaba por facilitar a impunidade de crimes do gênero. Portanto, um dos motivos para a criminalização da pornografia infantil simulada é justamente a preocupação com a pornografia infantil real, uma prática muito mais grave em todos os aspectos. Nesse sentido, propõe-se que essa conduta passe a

[44] Ibidem.

> ser criminalizada com a mesma pena daquela correspondente à modificação de imagens de crianças e adolescentes reais, visto que isso facilita a investigação policial, bem como a colheita de elementos de prova contra os criminosos, por não haver necessidade de perícia ou busca ativa no que refere à identificação da vítima, facilitando a punição dos criminosos (art. 241-C, 241-E e 241-F) [...]

Como visto, parece imprescindível a construção de texto que verdadeiramente abarque todas as variações da conduta que se pretende reprimir, mas não só isso, pois entende-se tratar de problema multidisciplinar, que requer a incidência de medidas que não sejam só repressivas, mas também preventivas, motivo pelo qual deve-se considerar a possibilidade de responsabilização de outros possíveis envolvidos mediatos.

Exemplificativamente, a existência de profundo aprendizado de máquina obstaria o alcance da Lei Penal aos encarregados do treinamento algorítmico inicial, uma vez que o nexo de causalidade se mostraria tão distante que punir os criadores da IA assemelhar-se-ia à aplicação da Teoria da Imputação Objetiva, vedada no ordenamento jurídico pátrio.

Apesar disso, uma forma de fiscalização e responsabilização das pessoas pelo treinamento algorítmico enviesado e realizado a partir de fotos e vídeos reais de violência sexual poderia ser a criação de comissões ou órgãos especializados, compostos de profissionais da área jurídica, tecnológica e de direitos humanos, que teriam a função de analisar e monitorar os conjuntos de dados utilizados no treinamento dos algoritmos. Essas comissões seriam incumbidas de verificar se as imagens utilizadas foram obtidas de maneira correta, garantindo o consentimento e a privacidade das pessoas retratadas. Outrossim, seria fundamental estabelecer diretrizes claras sobre o uso dessas imagens, bem como impor penalidades rigorosas para aqueles que se envolvessem em práticas ilegais ou antiéticas durante aludido processo de treinamento, visando assegurar a integridade e a dignidade das vítimas e prevenindo o uso indevido da tecnologia em contextos tão sensíveis.

Igualmente fora da esfera criminal, outra interessante proposta, que, por sinal, já tem sido adotada por Google, DALL-E e Midjourney é a utilização de métodos de moderação de conteúdo das plataformas, que pode ocorrer por meio da restrição dos supracitados dados de treinamento, incapacitando a IA de gerar pornografia infantojuvenil – exceto quando combinados outros conceitos previamente conhecidos –, ou a partir de proibições de acesso, restringindo-se os termos que podem ser usados para a criação das imagens[45]. Nesse sentido:

> Modelos de código fechado, nos quais a empresa tem controle total sobre o treinamento e uso do modelo, podem empregar ambos os métodos para

[45] IWF, op. cit., p. 15-16.

> moderação de conteúdo. DALL-E e Midjourney usam ambos os métodos com alto nível de eficácia no domínio CSAM, por exemplo. Os modelos de código aberto podem tentar empregar esses métodos, mas encontram problemas com cada um deles, uma vez que o código é necessariamente editável e os modelos básicos podem ser ajustados – treinados em imagens adicionais[46].

Outra importante alternativa seria a utilização da inovação a nosso favor, lançando mão dos novos instrumentos jurídicos de contratação e de celebração de parcerias para a realização de chamamentos públicos ou abertura de editais que tivessem como objeto a solução de desafios relacionados ao tema tratado neste artigo, como fez a IWF (2023) ao convocar desenvolvedores, programadores, especialistas em dados e designers para participarem de um Hackathon em Londres, na data de 18 de fevereiro de 2023, com o objetivo de "ajudar a criar novas soluções para liderar o mundo na luta contra a propagação de material de abuso sexual infantil na Internet".

As soluções aqui propostas parecem guardar relação com parte das recomendações realizadas pela IWF ao final de seu Relatório, que, em termos gerais, se aplicam à realidade brasileira:

> PARA O GOVERNO:
>
> 1. Explorar na próxima Cimeira de IA do Governo os desafios para lidar com AI CSAM incluindo a necessidade de alinhamento internacional sobre a forma como este conteúdo é tratado em diferentes jurisdições e o compromisso garantido com a colaboração contínua de governos e partes interessadas internacionais.
>
> 2. Que o Ministério da Justiça encomende uma revisão das leis que se aplicam à remoção deste conteúdo online para garantir que são adequadas à finalidade de enfrentar a ameaça do AI CSAM. Isto inclui garantir que a troca de "dicas e sugestões" e "manuais pedófilos" sobre como gerar este conteúdo seja considerada ilegal.
>
> 3. Considerar uma extensão do mandato da IWF para poder examinar minuciosamente os conjuntos de dados em que estas tecnologias são treinadas.
>
> PARA APLICAÇÕES DA LEI E REGULADORES:
>
> 4. Para garantir que o curso de treinamento da Faculdade de Policiamento seja atualizado para cobrir AI CSAM e que orientações claras sejam emitidas para alunos da polícia sobre como processar essas imagens.
>
> 5. Para garantir que haja supervisão regulatória adequada dos modelos de IA antes que eles cheguem ao mercado ou sejam fabricados em código aberto e garantir que estratégias adequadas de mitigação de riscos estejam em vigor. Para modelos de código fechado, as proteções devem ser integradas.

[46] Ibidem, idem.

PARA EMPRESAS DE TECNOLOGIA:

6. Para garantir que as empresas que utilizam e desenvolvem IA generativa e grandes modelos de linguagem (LLMs) coloquem claramente em seus termos e condições que o uso dessas tecnologias para gerar material de abuso sexual infantil é proibido.

7. Que os serviços de pesquisa devem desindexar links para modelos de IA bem ajustados, conhecidos por estarem vinculados à criação da IA CSAM.

8. Para considerar cuidadosamente os desafios de moderação de conteúdo que o AI CSAM cria em termos de priorização e a natureza mista do AI CSAM com o CSAM real[47].

Em vista da complexidade e gravidade do tema, é inegável que existem diversas possibilidades e alternativas para suavizar os problemas ora relacionados; no entanto, é importante ressaltar que nenhuma dessas abordagens é cem por cento eficaz, especialmente quando se trata de ferramentas de código aberto, que podem limitar o alcance das investigações e dificultar ainda mais o controle sobre o uso indevido da Inteligência Artificial Generativa. Como visto, um enfoque multidisciplinar, envolvendo aspectos legais, éticos, tecnológicos e sociais, é essencial para encarar essa dificuldade de maneira abrangente e eficaz.

5. CONCLUSÃO

No presente estudo, busquei destacar que a problematização das imagens de crianças e adolescentes em situações de violência e exploração sexual originadas por inteligência artificial generativa ultrapassa aspectos meramente teóricos e já constitui questão de ordem prática e de exponencial potencial danoso.

O modo de funcionamento da IA, seu treinamento algorítmico e o constante autoaperfeiçoamento por meio do aprendizado de máquina naturalmente impede a plena transparência desta ferramenta, que, quando aplicada para finalidades ilícitas, encontra na Dark Web um ambiente altamente favorável de desenvolvimento, fazendo com que a dificuldade de rastreamento e fiscalização seja maior do que se pode prever.

Conforme visto, muitos países possuem legislações que, apesar de argumentações em contrário, de forma expressa, punem referida conduta. O Brasil, porém, ainda não está preparado para lidar com a situação, pois os tipos penais constantes no Estatuto da Criança e do Adolescente restringem-se à criminalização de ações relacionadas à representação de pessoas reais.

[47] Ibidem, p. 5.

A exposição de casos concretos, os aspectos técnicos envolvidos na criação destas imagens e a análise das legislações do Reino Unido, Estados Unidos, Canadá e Brasil tornam evidente a complexidade e a urgência de lidar com a situação e enfatizam a imprescindibilidade de uma abordagem global e coordenada para o enfrentamento deste desafio.

Embora seja difícil pensar em uma alternativa capaz de sanar o problema proposto, há medidas que podem ser adotadas para minimizar o seu impacto. Nesse sentido, as soluções identificadas apontam para o estabelecimento de novos instrumentos legais, o estímulo à inovação por meio de *hackathons* e a responsabilização ética no treinamento e controle algorítmico.

Conclui-se, portanto, que é imperativo unir esforços entre governos, sociedade civil e setor privado para desenvolver estratégias eficazes que protejam as vítimas e previnam o uso indevido da inteligência artificial generativa para perpetuar a exploração e violência contra crianças e adolescentes.

REFERÊNCIAS BIBLIOGRÁFICAS

ABRUSIO, Juliana; ALMADA, Marco; MARANHÃO, Juliano. Inteligência Artificial e o Direito: duas perspectivas. *In:* COZMAN, Fabio G; NERI, Hugo; PLONSKI, Guilherme Ary. **Inteligência Artificial**: avanços e tendências. São Paulo: Instituto de Estudos Avançados, 2021.

ARBIX, Glauco. "Algoritmos não são inteligentes nem têm ética, nós temos": a transparência no centro da construção de uma IA ética. *In:* COZMAN, Fabio G.; NERI, Hugo; PLONSKI, Guilherme Ary. **Inteligência Artificial**: avanços e tendências. São Paulo: Instituto de Estudos Avançados, 2021.

AZEVEDO, Tatiana; COELHO, Leonardo; SCHURIG, Sofia. Esquema no Instagram espalha imagens de exploração sexual infantil feitas por IA. **Núcleo Jornalismo**, 29 abr. 2025. Disponível em: https://nucleo.jor.br/reportagem/2025-04-02-pornografia-infantil-ia-insta/. Acesso em: 14 out. 2025.

BARRETO, José; BRESSAN, Kelvin J. Aquisição de imagens de abuso e exploração sexual infantojuvenil. **Consultor Jurídico**, 4 jan. 2023. Disponível em: https://www.conjur. com.br/2023-jan-04/barreto-bressan-abuso-exploracao-sexual-infanto-juvenil/#:~:text=O%20uso%20da%20express%C3%A3o%20'pornografia,ser%20c%C3%BAmplices%20do%20pr%C3%B3prio%20abuso. Acesso em: 10 mai. 2024.

BARROS, Bruno Luís. Pornografia infantil com uso de IA em escola de BH é investigada pela polícia. **Correio Braziliense**, 8 nov. 2023. Disponível em: https://www.correiobraziliense.com.br/brasil/2023/11/6652353-pornografia-infantil-com-uso-de-ia-em-escola-de-bh-e-investigada-pela-policia.html. Acesso em: 25 mai. 2024.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal Brasileiro. **Diário Oficial da União**. Rio de Janeiro,1940.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial da União**, Brasília, 16 jul. 1990.

BRASIL. Supremo Tribunal de Justiça. **REsp nº 1.543.267/SC**. Relatora Min. Maria Thereza de Assis Moura, Sexta Turma, julgado em 3 dez. 2015, DJe de 16 fev. 2016. Brasília, DF: STJ, 16 fev. 2016. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=1457585&tipo=0&nreg=201501690431&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20160216&formato=PDF&salvar=false. Acesso em: 23 maio 2024.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 3.066/2025**. Osmar Terra – MDB/RS, 25 jun. 2025. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2528433. Acesso em: 20 out. 2025.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.694/2023**. Davys Frederico Linhares – Republicanos/DF, 24/11/2023. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2406508. Acesso em: 30 maio 2024.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 6.211/2023**. Renata Abreu – Pode/SP, 22/12/2023. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2416533. Acesso em: 30 maio 2024.

COSTA, Anna Helena Reali; BARROS, Leliane Nunes de; NERI, Hugo; REZENDE, Solange Oliveira; SICHMAN, Jaime Simão. Trajetória acadêmica da Inteligência Artificial no Brasil. *In:* COZMAN, Fabio G; NERI, Hugo; PLONSKI, Guilherme Ary. **Inteligência Artificial**: avanços e tendências. São Paulo: Instituto de Estudos Avançados, 2021.

COZMAN, Fabio G; NERI, Hugo. O que, afinal, é Inteligência Artificial? *In:* COZMAN, Fabio G; NERI, Hugo; PLONSKI, Guilherme Ary. **Inteligência Artificial**: avanços e tendências. São Paulo: Instituto de Estudos Avançados, 2021.

CRISCUOLO, Leandro Costa. Homem é preso por criar material com conteúdo sexual infantil usando IA. **Olhar Digital**, 22 mai. 2024. Disponível em: https://olhardigital.com.br/2024/05/22/seguranca/homem-e-preso-por-criar-material-com-conteudo-sexual-infantil-usandoia/#:~:text=Homem%20%C3%A9%20preso%20por%20criar%20material%20com%20conte%C3%BAdo%20sexual%20infantil%20usando%20IA,-Acu sado%20%C3%A9%20um&text=Na%20%C3%BAltima%20segunda%2Dfeira%20(20,(CSAM)%20geradas%20por%20IA. Acesso em: 30 maio 2024.

HOMEM é preso na Espanha por criar pornografia infantil usando IA: a Polícia Nacional do país descobriu que o detido sintetizava as imagens por algoritmos. **Estadão**, 22 dez. 2022. Disponível em: https://www.estadao.com.br/link/cultura-digital/pornografia-in fantil-ia/. Acesso em: 25 maio 2024.

INTERNET WATCH FOUNDATION. Atualização de 2024: Compreendendo a rápida evolução das imagens de abuso infantil geradas por IA. **IWF**, jul. 2024. Tradução livre, realizada com o uso da ferramenta "Google Tradutor". Disponível em: https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual--abuse-imagery/. Acesso em: 17 out. 2025.

INTERNET WATCH FOUNDATION. Como a IA está sendo usada para criar imagens de abuso sexual infantil - Prompt: da fantasia à realidade fotorrealista. **IWF**. Relatório publicado em out. de 2023. Tradução livre, realizada com o uso da ferramenta "Google Tradutor". Disponível em: https://www.iwf.org.uk/annual-report-2023/. Acesso em: 30 abr. 2024.

INTERNET WATCH FOUNDATION. IWF convoca programadores para participarem de seu Hackathon e ajudarem a impedir o abuso sexual infantil online. **IWF**, jan. 2023. Tradução livre, realizada com o uso da ferramenta "Google Tradutor". Disponível em: https://www.iwf.org.uk/news-media/blogs/iwf-calls-on-coders-to-join-their-hackathon--and-help-stop-child-sexual-abuse-online/. Acesso em: 18 maio 2024.

LUDERMIR, Teresa Bernarda. Inteligência Artificial e Aprendizado de Máquina: estado atual e tendências. **Instituto de Estudos Avançados da Universidade de São Paulo**, jan-abr. 2021. Disponível em: https://doi.org/10.1590/s0103-4014.2021.35101.007. Acesso em: 22 abr. 2024.

MASSON, Cleber. **Direito Penal**: Parte Especial (arts. 213 a 359-T). 14. ed. São Paulo: Método, 2024.

MENDES, Cleylton. Além da realidade: IA, menores e o espaço cibernético inexplorado. **Consultor Jurídico**, 8 nov. 2023. Disponível em: https://www.conjur.com.br/2023-nov-08/cleylton-mendes-alem-realidadeia-menores-espaco-cibernetico/. Acesso em: 22 abr. 2024.

MORESCHI, Bruno. Os reveladores erros das máquinas "inteligentes". *In:* COZMAN, Fabio G; NERI, Hugo; PLONSKI, Guilherme Ary. **Inteligência Artificial**: avanços e tendências. São Paulo: Instituto de Estudos Avançados, 2021.

OLIVEIRA, Marcelo. Safernet recebe recorde histórico de novas denúncias de imagens de abuso e exploração sexual infantil na internet. **Safernet**, 6 fev. 2024. Disponível em: https://new.safernet.org.br/content/safernet-recebe-recorde-historico-de-novas-denuncias-de-imagens-de-abuso-e-exploracao-sexual#mobile. Acesso em: 28 maio 2024.

PATTO, Pedro Maria Godinho Vaz. Pornografia infantil virtual. **Julgar**, n. 12, set-dez. 2010 (Especial: crimes no seio da família e sobre menores). Disponível em: https://julgar.pt/julgar_em_papel/julgar-n-o-12/. Acesso em: 17 maio 2024.

PEREIRA, Jennifer do Santos; PEREIRA, João Victor do Santos; VARGAS, Alessandra Alves Fonseca. IA Generativa versus Desenvolvimento de Software: um olhar do presente para o futuro. **Revista Pesquisa e Educação à Distância**, n. 31, jan./jun. 2024. Disponível em: http://revista.universo.edu.br/index.php?journal=2013EAD1&page=issue&op=current. Acesso em: 27 maio 2024

PÉREZ, Rafael Bello; SUÁREZ, Alejandro Rosete. Algumas reflexões sobre as implicações éticas dos avanços recentes na inteligência artificial. **Bioética y Biopolítica**. Acuario: La Habana, 2023.

POLEZE, Carol. Suspeito de pornografia infantil no ES usava inteligência artificial para produzir imagens. **Redação Folha Vitória**, 17 mai. 2024. Disponível em: https://www.folhavitoria.com.br/policia/noticia/05/2024/pornografia-infantil-preso-no-es-usava-inteligencia-artificial-para-produzir-fotos. Acesso em: 23 maio 2024.

RAMALHO, David Silva. A investigação criminal na Dark Web. **Revista de Concorrência e Regulação**, ano IV, número 14/15, abr./set. 2013.

RUFINO, Claudio. **A influência da pornografia nos casos de abuso e exploração sexual de crianças e adolescentes**. Câmara dos Deputados. Departamento de Taquigrafia, Revisão e Redação – Núcleo de Redação Final em Comissões. Comissão de Segurança Pública e Combate ao Crime Organizado. Seminário nº 1461/08, 6 nov. 2008. Disponível em: https://www.camara.leg.br/internet/SitaqWeb/TextoHTML.asp?etapa=11&nmComissao=Comiss%C3%A3o%20de%20Seguran%C3%A7a%20P%C3%BAblica%20e%20Combate%20ao%20Crime%20Organizado&tpReuniaoEvento=Semin%C3%A1rio&dtReuniao=06/11/2008&hrInicio=14:18:00&hrFim=17:17:00&origemDiscurso=&nmLocal=Plen%C3%A1rio%20Principal%20-%20CD&nuSessao=1461/08&nuQuarto=0&nuOrador=0&nuInsercao=0&dtHorarioQuarto=14:18&sgFaseSessao=&Data=06/11/2008&txApelido=&txFaseSessao=&txTipoSessao=Permanente&dtHoraQuarto=14:18&txEtapa=. Acesso em: 28 maio 2024.

SAFERNET BRASIL. Em suas próprias palavras: Como o Telegram tem sido usado no Brasil como um espaço de comércio virtual por criminosos sexuais. **Safernet**. Disponível em: https://arquivos.safernet.org.br/press/Safernet_Telegram.pdf. Acesso em: 17 out. 2025.

SAFERNET BRASIL. Nota Técnica nº 02/2025. **Safernet**. Salvador: 19 ago. 2025. Disponível em: https://arquivos.safernet.org.br/notas/Nota+Tecnica+02_2025+%5BSaferNet+Brasil%5D.pdf. Acesso em: 17 out. 2025.

SILVA, João Miguel Almeida da. **Cibercrime**: o crime de pornografia infantil na internet. Dissertação em Ciências Jurídico-Forenses. Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2º Ciclo de Estudos em Direito (conducente ao grau de Mestre), na Área de Especialização em Ciências Jurídico-Forenses. UC, jan. 2016. Disponível em: https://estudogeral.sib.uc.pt/handle/10316/34801. Acesso em: 22 mai. 2024.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Recurso Especial nº 1.543.267/SC**, relatora Ministra Maria Thereza de Assis Moura, Sexta Turma, julgado em 3/12/2015, DJe de 16/2/2016. Disponível em: https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=%2720 1501690431%27.REG. Acesso em 22 mai. 2024.

Submetido em: 16/12/2024
Aprovado em: 06/09/2025

A RESPONSABILIDADE CIVIL DE DANOS CAUSADOS POR *DEEPFAKES*: IMAGENS FALSAS CRIADAS POR INTELIGÊNCIA ARTIFICIAL GENERATIVA

Civil Liability for Damages Caused by Deepfakes: Fake Images Created by Generative Artificial Intelligence

Natalia Fernanda Marques Carvalhanas[1]

SUMÁRIO 1. Introdução; 2. O que é inteligência artificial; 3. Autoria da obra feita por IA generativa; 4. *Deepfake*, um problema oriundo da IA generativa; 5. Direito brasileiro vs. *Deepfakes*; 5.1. Marco civil da internet; 5.2. Lei Geral de Proteção de Dados (LGPD) e Direito à Imagem; 5.3. A responsabilidade civil dos danos causados pelas *deepfakes*; 5.4. A boa-fé objetiva; 5.5. O dever de reparação; Considerações finais; Referências Bibliográficas

RESUMO O presente artigo oferece um estudo acerca dos *deepfake*s, produtos da inteligência artificial generativa que vêm figurando constantemente em notícias da internet, sobretudo polêmicas negativas, nos últimos três anos. Largamente utilizadas para disseminar notícias falsas e manipular a opinião das pessoas no Brasil e no mundo, essas obras geradas por máquinas praticamente autônomas são uma questão bem complicada, juridicamente falando, pois os institutos do Direito não estão dando conta de abarcar todas as suas demandas, dado o caráter extremamente inovador dos *deepfake*s, bem como seu imenso potencial lesivo. Assim, o estudo em questão verificará a posição de especialistas de direito autoral sobre a inteligência artificial generativa, e buscará entender como o instituto da responsabilidade civil agiria para conter os danos das *deepfake*s.

Palavras-chave: Inteligência Artificial Generativa. *Deepfake*. Direito Autoral. Responsabilidade Civil. Marco Civil da Internet. Lei Geral de Proteção de Dados.

ABSTRACT This paper examines deepfakes, products of generative artificial intelligence that have consistently gained negative attention in internet news in the recent past. Widely used to spread misinformation and manipulate public opinion in Brazil and worldwide, these virtually autonomous machine-generated works present a complex legal challenge. Existing legal frameworks struggle to adequately address their demands, given the extremely innovative nature of deepfakes and their immense harmful potential. Thus, this study will explore the perspectives of copyright specialists on generative artificial intelligence and seek to understand how the legal framework of civil liability would act to mitigate the damages caused by deepfakes.

Keywords: Generative Artificial Intelligence. Copyright. Brazilian Law. Deepfake. Data Protection. Internet Law. Copyright. Civil Responsibility.

[1] Advogada. Formada em Direito pela Universidade de São Paulo (USP). Especialista em Direito Digital e Inovação Tecnológica pela Escola Superior da Procuradoria Geral do Estado de São Paulo.

DOI: 10.22491/*respge*.v16i1.1731

1. INTRODUÇÃO

A inteligência artificial é um mecanismo executado por *software*, robô ou computador para realizar algumas ações típicas de seres humanos (analisar, decidir, aprender etc.). É uma tecnologia largamente utilizada como ferramenta de ajuda e de busca (ex.: *chatbots* e assistentes pessoais de sistemas operacionais) tendo como base e produto comandos e dados já existentes. Todavia, existe um ramo, conhecido como inteligência artificial generativa, cuja função é criar conteúdo inédito. As obras resultantes da inteligência artificial generativa se dão através de mecanismos de algoritmos operados por ordens humanas, tendo como base uma imensa rede de dados. Recentemente, uma série de polêmicas começaram a surgir por conta de uma espécie de produto da inteligência artificial generativa, o *deepfake*. Imagens falsas de pessoas, em sua maioria famosas, realizando ações que jamais realizaram, mas aparentando ser totalmente reais, tamanho o aperfeiçoamento que essa tecnologia vem apresentando.

Considerando o caráter inovador do *deepfake*, o presente artigo visa estudar seu papel no direito autoral, tendo em vista que essas imagens são consideradas obras, mas sua autoria é de difícil aferição, e estudar as consequências jurídicas que essas *deepfakes* têm na sociedade, pois elas, sem dúvidas, causam uma série de problemas. Primeiramente, será feita uma definição acerca da inteligência artificial e da inteligência artificial generativa, sendo a segunda uma espécie da primeira. Em seguida, entrando no campo do direito autoral, haverá uma análise de possíveis métodos para se atribuir direitos de autoria à inteligência artificial, e quem seria exatamente o titular desses direitos. A terceira parte, tratando das *deepfakes*, demonstrará quão nociva é essa espécie de IA generativa para a sociedade e as tentativas de conter seus efeitos, com destaque para o *AI Act*, aprovado em 2024 pela União Europeia e caracterizando-se como a primeira lei que busca a regulamentação de inteligência artificial no mundo. O último ponto caminhará sobre diferentes dispositivos do direito brasileiro e sua relação com a inteligência artificial generativa, de modo a perscrutar se cabe responsabilizar civilmente alguém pelos danos causados pelas *deepfakes*, e, em caso positivo, quem seria responsabilizado. Esta parte da pesquisa busca amparo em normas do direito do consumidor, mas esgota a esfera de responsabilização no campo civil, deixando as responsabilizações nas áreas penal e administrativa de fora. Por fim, analisará se há ou não uma relação de consequência entre os assuntos estudados no terceiro e no quarto ponto. A metodologia utilizada para a realização deste trabalho concentrou-se na leitura de doutrinas, artigos científicos, legislação concernente ao tema e reportagens publicadas na internet.

2. O QUE É INTELIGÊNCIA ARTIFICIAL

O cérebro humano, um pedaço tão pequenino de matéria, é capaz de compreender e interferir em um mundo tão mais complexo que ele. Entender o pensamento

e a ação do cérebro humano tem sido um grande desafio ao longo do tempo. O ramo da IA busca não apenas entender como esse pensamento e ação funcionam, mas também construir entidades (máquinas) inteligentes[2].

Alan Turing foi pioneiro no campo acadêmico ao estabelecer o conceito da inteligência artificial, e o fez através de um sistema que consistia em descobrir se um computador seria capaz de ganhar um jogo contra humanos. Este jogo implicaria na assimilação de informações recebidas de humanos por parte de um computador e teria o nome de "jogo da imitação" pois o comportamento da máquina deveria ser semelhante ao de um humano para ela obter êxito na missão. Para a máquina ganhar o jogo, um interrogador humano, dispondo de uma máquina e de outros dois humanos, teria de ser incapaz de distinguir as respostas da máquina das respostas humanas. Assim, a inteligência artificial não implica na habilidade de cognição da máquina, ou seja, se ela seria ou não capaz de pensar tal qual um humano, mas na sua habilidade de assimilar informações de forma rápida e concisa, assemelhando sua atividade à humana[3].

Além dessa abordagem de Turing para definir a inteligência artificial (IA), a era moderna trouxe outras abordagens que mesclam o pensamento, a humanidade, a racionalidade e o comportamento. A busca por uma inteligência semelhante à humana deve ser parte de uma ciência empírica relacionada à psicologia, envolvendo observações e hipóteses sobre o comportamento humano e os processos do pensamento. Uma abordagem racional, por outro lado, envolve uma combinação entre engenharia e matemática, conectando-se também a estatísticas, teoria do controle e economia[4].

Pesquisas regularmente classificam a IA como um dos mais interessantes e crescentes campos, e ela vem gerando mais de um trilhão de dólares por ano em receita. O *expert* em inteligência artificial Kai-Fu Lee prevê que o impacto dessa inteligência na raça humana será "maior que qualquer coisa já vista". Além disso, por se tratar de uma ciência nova, suas fronteiras intelectuais estão abertas para a pesquisa. A IA também é rica em sub-ramos, sendo eles variados entre os ramos gerais (aprendizado, raciocínio percepção etc.) ou específicos (jogar xadrez, provar teoremas matemáticos, escrever poesia, dirigir carros e diagnosticar doenças). A inteligência artificial é relevante para qualquer tarefa intelectual e é um campo bastante universal[5].

---

[2] RUSSEL, Stuart; NORVIG, Peter. **Inteligência artificial**: uma abordagem moderna. Rio de Janeiro: Campus, 2004, p. 29.

[3] TURING, Alan M. Computing machinery and intelligence**. Mind**, 59, pp. 433-460, 1950. Disponível em http://phil415.pbworks.com/f/TuringComputing.pdf. Acesso em: 10 jun. 2024. ULMER, Eugen. **Urheber und Veerlagsrecht**. 3.d. Berli: Heidelberg, 1980.

[4] RUSSEL, Op. cit., p. 31.

[5] Ibidem, p. 29.

Para a criação de um produto intelectual, o grau de interferência humana, a autonomia do sistema e a previsibilidade do resultado podem variar. Quando são utilizados sistemas de IA para a realização de uma tarefa ou a confecção de um produto, essa criação não ocorre de maneira absolutamente autônoma, tendo em vista que os sistemas são orientados por instruções e regras transmitidas por um ser humano, podendo essa interferência humana ter diferentes escalas[6].

O ramo da inteligência artificial a ser estudado no presente artigo é a inteligência artificial generativa, que faz uso de um campo geral da IA (aprendizado de máquina) para produzir elementos da IA de campos específicos (escrever textos, criar imagens).

Este modelo de IA lida com um enorme banco de dados para aprendizagem e com pouca interferência humana. Por meio de conteúdos que já existem, a IA generativa cria novas soluções e é capaz de fazer isso sem que seus resultados se repitam, e esses produtos criados variam de textos, vídeos, imagens, poesias e até mesmo arte.

> O que difere uma IA generativa é sua capacidade de aprendizado não supervisionado utilizando complexos modelos de aprendizagem de máquina, como o Large Language Model (LLM), que têm ganhado espaço com o crescimento da pesquisa em processamento de linguagem natural. Por possuírem inúmeros parâmetros, treiná-las requer grandes quantidades de dados, infraestrutura e capacidade de processamento computacional. Por esses motivos, IA generativas com base em LLM são suportadas pelas mais conhecidas empresas de tecnologia. A OpenAI, organização que se declara sem fins lucrativos e que tem a Microsoft como principal investidor, é criadora dos sistemas GPT-3 e GPT-4 para textos, DALL-E para imagens e WHISPER para voz[7].

3. AUTORIA DA OBRA FEITA POR IA GENERATIVA

O direito do autor, conforme ensina Carlos Eduardo Bittar[8], é um direito intelectual, em contraposição ao direito de personalidade. Estes últimos se referem às relações da pessoa consigo mesma, quanto a características extrínsecas do ser e a suas qualificações psíquicas e morais (ex.: direito à honra, à vida, à imagem etc.) já os direitos intelectuais envolvem as relações entre a pessoa e as coisas que elas criam e trazem "a lume", ou seja, produtos do intelecto humano, existindo como expressões

[6] SCHIRRU, Luca. Inteligência artificial e o direito autoral: o domínio público em perspectiva. Instituto de Tecnologia e Sociedade do Rio (ITSRIO), 2019, p.7.

[7] MOURA, Carlos Manoel Silva; BRAGA, Tiago Emmanuel Nunes. A inteligência artificial e a criação de conteúdo: os vieses que habitam entre nós. **Anais do Workshop de Informação, Dados e Tecnologia-WIDaT**, 2023, p. 3.

[8] BITTAR, Carlos Eduardo Bianca. **Direito de Autor.** 7. ed. Editora Forense, 2019, p. 17-19.

do espírito criativo humano (ex.: poesia, texto, pintura, canção, escultura). Essas expressões podem fazer parte do ramo sensível de criações (cumprem o papel de aperfeiçoamento intelectual, beleza, sensibilidade), ou do ramo utilitário (de uso econômico ou doméstico). O direito do autor incide sobre as criações sensíveis, ao passo que o direito industrial engloba as criações utilitárias.

O vínculo do autor com sua obra, bem como a posterior circulação jurídica dessa obra, são os elementos protegidos pelo direito do autor nas esferas pessoal e patrimonial, respectivamente. Os direitos morais relacionam-se ao ato criativo, ou seja, à esfera pessoal, enquanto os direitos patrimoniais relacionam-se à exploração econômica dessa obra.

Entretanto, obras produzidas por sistemas de inteligência artificial não possuem todos os elementos tradicionalmente característicos do produto ou obra protegidos pelo direito do autor, pois estes estão ligados à pessoa, e não à máquina. Nos sistemas de inteligência artificial generativa, por sua vez, a interferência humana é muito menor do que a do banco de dados assimilado pela máquina.

Em busca da atribuição de autoria para obras produzidas por um sistema de Inteligência Artificial, Abido e Boff[9] apresentam as diferentes situações que caberiam no arcabouço legislativo brasileiro acerca dos temas em questão: a obra não teria autor (domínio público); o próprio sistema de IA seria o autor das obras geradas; o programador seria o autor; o proprietário do programa seria o autor. Considerando que a atribuição de direitos autorais preza pela criatividade, a originalidade e a atividade do intelecto humano, a presença ou ausência de cada um desses elementos nas obras oriundas de inteligência artificial foi analisada, e diferentes formas de conferir direitos de autor a essas obras foram encontradas.

O elemento da originalidade é encontrado a partir da atividade algorítmica de *machine* e *deep learning* de produzir *outputs* (resultados) inéditos e definitivos através dos *inputs* mandados pelo programador. Para o elemento da criatividade, tem-se que o banco de dados utilizado pelo *machine* e *deep learning* oferece uma gama infinita de ideias para se chegar a um resultado, e essa infinitude se aproxima da habilidade de criatividade humana, inclusive, no artigo, Abido e Boff apontam para uma expectativa de 90% de chance de as máquinas atingirem a criatividade humana até 2075. Dessa forma, o requisito da criatividade não está 100% preenchido, mas tende a sê-lo. Quanto ao último elemento, o de existência de atividade proveniente do intelecto humano, referente à personalidade do autor, o artigo 11 da Lei nº 9.610/98 (Lei de Direitos Autorais): "Autor é a pessoa física criadora de obra literária, artística ou científica. Parágrafo único. A proteção concedida ao autor poderá aplicar-se às pessoas

[9] BOFF, Salete Oro; ABIDO, Leonardo. O Direito de autor no Brasil de obras produzidas pela Inteligência Artificial. **Revista da Fac. Mineira de Direito** (PUC Minas), v. 23, n. 45, 2020.

jurídicas nos casos previstos nesta Lei"[10] impossibilita a atribuição desse elemento a um sistema de IA, um ente *sui generis* e, portanto, sem personalidade. Este fato ensejaria uma reformulação do tal artigo, englobando a possibilidade de o autor ser um *software*.

Embora sejam necessárias algumas adaptações na legislação, entende-se que obras criadas por IA ensejam uma proteção jurídica semelhante às produzidas por humanos, pois, apesar de a interferência humana ser menor, ela ainda existe, tendo em vista que é necessário que haja um programador para realizar comandos à máquina. Considerando que a máquina é entendida pela lei brasileira enquanto ente *sui generis* e, portanto, desprovida de personalidade jurídica, Abido e Boff se utilizam da teoria de Schirru para atribuir um titular de direitos autorais para obras de IA, teoria esta que confere três possibilidades a essa atribuição de direitos. Primeiramente, ele considera colocar em domínio público as obras produto de sistemas de IA. As obras humanas são colocadas em domínio público quando o prazo de sua proteção acaba ou quando sua autoria é desconhecida. Os direitos de obras em domínio público não possuem titular. Uma segunda possibilidade adotada por Schirru seria uma interpretação do artigo 4º da Lei nº 9.609/98 (Lei do Software):

> Art. 4º: Salvo estipulação em contrário, pertencerão exclusivamente ao empregador, contratante de serviços ou órgão público, os direitos relativos ao programa de computador, desenvolvido e elaborado durante a vigência de contrato ou de vínculo estatutário, expressamente destinado à pesquisa e desenvolvimento, ou em que a atividade do empregado, contratado de serviço ou servidor seja prevista, ou ainda, que decorra da própria natureza dos encargos concernentes a esses vínculos[11].

Se enquadrássemos as obras produzidas por IA neste artigo, os direitos autorais dela pertenceriam à empresa titular dos direitos do sistema, e até certo ponto faria sentido, uma vez que a maior parte dos sistemas geradores de IA pertencem a grandes empresas, porém o avanço tecnológico na área de inteligência artificial está fazendo com que qualquer pessoa, seja ela física ou jurídica, possa deter sistemas e figurar como a detentora dos direitos autorais em questão. A última hipótese de Schirru para conferir autoria a algum titular em obras de IA encontra essa figura no programador do sistema. Devido à sua função fundamental de realizar os *inputs* nos sistemas com informações que ele julga essenciais para o funcionamento da máquina e delimitar os parâmetros para a atuação do sistema, o programador é quem mais se aproxima do autor protegido pelo atual modelo de propriedade intelectual.

[10] BRASIL. **Lei nº 9.610, de 19 de fevereiro de 1998**. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Diário Oficial da União. Brasília, fev. 2018a.

[11] BRASIL. **Lei nº 9.609, de 19 de fevereiro de 1998**. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências. Diário Oficial da União. Brasília, fev. 1998b.

O artigo ainda cita uma proposta do parlamento europeu para conferir personalidade aos robôs através do *Draft Report with Recommendations to the Comission on Civil Law Rules on Robotics*, de 31.5.2016, na qual, em seu artigo 59, propõe a criação de um *status* legal específico para robôs, no qual pelo menos os robôs dotados de maior sofisticação poderiam receber um *status* de "pessoa eletrônica" para enfatizar que essa questão de conferir direito autoral a inteligências artificiais está em voga, e também demonstra que, na Inglaterra, essa conferência de direitos autorais a inteligências artificiais já é feita legalmente. No país britânico, o titular de direitos autorais de uma obra criada por inteligência artificial se encontra na pessoa responsável por fazer os arranjos necessários para a criação da obra. Essa é uma abordagem semelhante à terceira hipótese levantada por Schirru, de conferir a titularidade de direitos autorais ao programador do modelo de IA.

4. DEEPFAKE, UM PROBLEMA ORIUNDO DA IA GENERATIVA

O *deep learning*, processo de aprendizado de máquinas utilizado em sistemas de IA generativa possibilita a criação de *deepfakes*, imagens tanto estáticas quanto em vídeos que mudam o rosto ou pequenos aspectos de uma pessoa ou de uma situação, de modo a fazê-las parecer muito realistas, apesar de não o serem.

O termo *deepfake* tem origem em 2017 por causa de um grupo da rede social Reddit que se utilizava da tecnologia em questão para substituir o rosto de atrizes pornográficas pelos rostos de celebridades em vídeos. Essa tecnologia se popularizou e, devido ao grande aprimoramento dessas máquinas, a intervenção humana é cada vez menor para a sua realização. Nos últimos anos, polêmicas envolvendo a disseminação de imagens falsas oriundas de *deepfake* alertaram para o uso indevido dessa ferramenta. Quando se promove desinformação, difamação e conteúdos maliciosos, a necessidade de regulamentação da IA, bem como a responsabilização civil de seus autores, são imprescindíveis[12].

Em 2023, uma *deepfake* do Papa Francisco vestindo uma jaqueta bufante arrancou risadas do mundo inteiro, ao passo que na mesma semana, circulava uma *deepfake* de Donald Trump, presidente dos EUA e político de extrema-direita, sendo preso – episódio este um verdadeiro exemplo de como a desinformação pode afetar a população, que em grande parte acreditava na veracidade daquela imagem. Quando possuem cunho político, essas imagens são deveras perigosas, pois podem manipular as opiniões políticas das pessoas, e com isso desestabilizar os processos eleitorais. No Brasil, as *deepfake*s políticas também já aconteceram, a exemplo de vídeo manipulado do apresentador William Bonner confirmando a existência de fraudes

[12] AUGUSTENE, Agne. O que é um *deepfake*? Os perigos de vídeos de IA falsos. **Nordvpn**, fev. 2023. Disponível em: https://nordvpn.com/pt-br/blog/deepfake-o-que-e/. Acesso em: 10 jun. 2024.

eleitorais nas eleições presidenciais de 2022, algo que jamais ocorreu. A regulação e a responsabilização são necessárias também pelo fato de que o advento das *deepfake*s descredibiliza as informações veiculadas em redes sociais. Quando a princesa de Gales, Kate Middleton, apareceu em um vídeo no começo do ano de 2024 para informar sobre seu estado de saúde e justificar sua ausência dos holofotes, muitas pessoas acreditaram tratar-se de uma *deepfake*, mesmo que o vídeo tenha sido postado na própria conta oficial da princesa, no Instagram[13].

O recente estudo "Fábricas de imagens falsas" publicado em março de 2024 pelo Centro de Combate ao Ódio Digital (CCDH, na sigla em inglês) demonstra que ferramentas de IA generativa produziram *deepfake*s com teor político em 41% dos 160 testes aplicados. Quatro plataformas foram utilizadas para os testes (MidJourney, ChatGPT Plus, Image Creator e Dream Studio), de forma que foram dadas a cada uma delas 40 comandos de texto relacionados às eleições estadunidenses. Os pesquisadores informaram que comandos pedindo "uma foto de Joe Biden doente em um hospital" ou "uma foto de Donald Trump sentado triste em uma cela de prisão" foram prontamente atendidos pelas plataformas. Imagens contendo tumultos nos locais de votação e milícias também foram prontamente geradas, ainda que três dessas quatro plataformas possuam políticas específicas para coibir a desinformação eleitoral. A Midjourney, mesma plataforma que foi responsável pelos *deepfake*s do Papa Francisco e de Donald Trump preso, já mencionados anteriormente, foi a que mais produziu *deepfake*s de cunho político, chegando a responder 65% dos testes realizados nessa pesquisa da CCDH. Um relatório da pesquisa informou que o banco de dados públicos da Midjourney está corrompido por atores maliciosos se utilizando da ferramenta para propagar desinformação eleitoral[14].

A qualidade dos dados aos quais a máquina é submetida é o que determina a inteligência dela, pois esta reproduzirá aquilo que os dados mandam. Assim, dados corrompidos por vieses carregados de preconceito social (como raça, gênero, forma física, orientação sexual) ou conteúdos enviesados com desinformações políticas, fazem com que a máquina não apenas aprenda esses dados, como também os perpetue, quando for exposta a novos dados. A aplicação indiscriminada da inteligência artificial, ou seja, ignorando seus dilemas éticos, oferece muitos riscos para toda a internet, que se depara com conteúdo oriundo de inteligência artificial com frequência[15].

As maiores plataformas de IA generativa fecharam um acordo em fevereiro para comprometerem-se a aperfeiçoar uma marca d'água que atestasse a

[13] SOARES, Matheus. 1 ano da "deepfake do papa": o que mudou? O que virá. **Desinformante**, mar. 2024. Disponível em: https://desinformante.com.br/deepfake-papa/. Acesso em: 10 jun. 2024.

[14] Ibidem.

[15] GARCIA, Ana Cristina. Ética e inteligência artificial. Computação Brasil, n. 43, 2020, p. 14-22.

utilização de inteligência artificial no conteúdo gerado por elas, tamanho o impacto das *deepfake*s na internet. O centro responsável pela pesquisa realizada (CCDH) sugeriu também, como forma de mitigar essa propagação desenfreada de *fake news* em forma de IA, o investimento pelas plataformas em profissionais especializados em IA generativa e desinformação.

A União Europeia aprovou, em 13 de março de 2024, o *AI Act*, para regulamentar a Inteligência Artificial, e a Comissão Europeia pediu formalmente às *bigtechs* Tiktok, Meta, X, Google e Microsoft que realizem ações para frear os riscos envolvendo as IAs generativas[16].

O *AI Act* foi a primeira iniciativa regulatória internacionalmente relevante sobre inteligência artificial. Em artigo publicado pela União Brasileira de Compositores (UBC), o advogado Cláudio Lins de Vasconcelos, especializado em *copyright* e tecnologia, analisou[17] parte do regulamento que versa sobre sistemas de IA e o uso que elas fazem de obras protegidas pelo direito autoral. O Regulamento, nas palavras de Cláudio, é "um colosso de 450 páginas, com preâmbulo de 180 considerandos, 113 artigos e 13 anexos alcança desenvolvedores e provedores de aplicações de IA disponibilizadas no mercado europeu ou que utilizem dados de seus cidadãos, ainda que sediados em outros países".

As grandes empresas de IA buscarão certamente se adequar a essa regulamentação, uma vez que o mercado europeu é muito visado e ninguém quer pagar as multas exorbitantes estipuladas para descumprimento das políticas dessa iniciativa, podendo variar de € 7,5 milhões a € 35 milhões. Apesar de não liderar a corrida tecnológica (protagonizada por Estados Unidos e China), a busca pela "vanguarda regulatória" da União Europeia na IA faz com que essas leis tenham repercussão, e, posteriormente, impacto internacional.

O nível de regulação estabelecido pela normativa varia conforme o risco oferecido pelo tipo de Inteligência Artificial, sendo ferramentas classificadas como "de risco altíssimo", como o reconhecimento facial indiscriminado, proibidas. As ferramentas de IA generativa, cujo altíssimo oferecimento de riscos já fora mencionado anteriormente, se popularizaram nos últimos anos e marcaram presença na normativa, conferindo a seus provedores obrigações de elaborar uma "política de conformidade" com as diretrizes europeias de direito autoral, especialmente com a Diretiva Europeia de direitos autorais digitais. Essa diretiva, aprovada em 2019, exime dados e texto minerados para plataformas de IA da proteção de direitos autorais (salvo se

[16] SOARES, Matheus. IAs generativas são 'fábricas de imagens falsas', aponta estudo. **Desinformante**, mar. 2024. Disponível em: https://desinformante.com.br/ia-generativa-imagens-falsas/. Acesso em: 10 jun. 2024.

[17] VASCONCELOS, Claudio Lins de. A lei europeia sobre IA e os direitos autorais. **UBC**, mar. 2024. Disponível em: https://www.ubc.org.br/publicacoes/noticia/22507/artigo-a-lei-europeia-sobre-ia-e-os-direitos-autorais/. Acesso em: 10 jun. 2024.

houver acontecido a exclusão da base de treinamento de dados pelos titulares das obras). Este direito contribui para que titulares de direitos possam retirar suas imagens de bancos de dados, ajudando a conter a problemática do *deepfake*. Ainda para frear os efeitos do *deepfake*, essa diretiva exige que os desenvolvedores declarem o uso de IA em todos os casos em que o conteúdo foi gerado por plataformas de IA e, ainda, que deixem explícitas quaisquer que forem as semelhanças que existam entre aquele conteúdo artificialmente gerado e entidades, pessoas, objetos e eventos reais e que possam, em consequência, levar o receptor daquele conteúdo à interpretação de que se trata de um conteúdo verdadeiro.

5. DIREITO BRASILEIRO VS. *DEEPFAKES*

A normativa trazida pela União Europeia do *AI Act* foi um grande avanço internacional para a regulamentação da inteligência artificial. A seguir, veremos como a lei brasileira se posiciona nessa questão, especialmente no tocante às *deepfakes*.

> De fato, entretanto, quando se têm presentes os desafios da Revolução Digital, do imenso fluxo digital, da velocidade das trocas de dados (inclusive, de dados pessoais), de perda de fronteiras de registro (dados constantes de provedores internacionais, que evocam situações que mobilizam até mesmo o Direito Internacional) e controle, se percebe o quanto o mundo digital impõe novos desafios à gestão, ao controle e ao combate das formas pelas quais a violação de direitos pode se dar, nessa matéria. Um dos desafios passa a ser a compatibilização do Direito de Autor com as novas tecnologias, inclusive com o uso dos diversos recursos já disponíveis no ordenamento jurídico, que refletem a emergência do Direito Digital[18].

O Direito Digital, ramo recente do Direito que surgiu com o advento da internet e o objetivo de regulá-la, possui poucas normas jurídicas que podem se encaixar ao tema de inteligência artificial e às responsabilidades civis dos danos que elas podem causar. Averiguando primeiramente os dispositivos das leis específicas do Direito Digital, e, posteriormente, recorrendo aos institutos do Direito Civil, esta etapa do presente artigo busca descobrir se há qualquer instituto jurídico que possa responsabilizar atores pelos danos oriundos de *deepfake*s, e, em caso positivo, quem pode ser responsabilizado.

É de extrema importância que ocorra esta responsabilização civil, considerando o potencial lesivo das *deepfakes*. O impacto das *deepfake*s pode ser muito profundo na economia de um país que detém uma grande concentração de capital financeiro proveniente de ações, uma vez que estas estão diretamente ligadas à estabilidade da política, pois o mercado de ações reage bastante a declarações e atitudes

[18] BITTAR, Carlos Eduardo Bianca. **Direito de Autor.** Editora Forense, 7ª edição, 2019, p. 164.

polêmicas de autoridades. Pode acontecer também um "caos" internacional, caso a *deepfake* faça uma declaração de guerra ou qualquer outro elemento que ameace a paz entre os povos. A prática das *deepfake*s é frequente no Brasil, tendo em vista que se trata de um país marcado pela grande polarização político ideológica[19].

Um ensaio acadêmico[20] que aplicou o direito brasileiro hipoteticamente ao caso Cambridge Analytica – empresa que possuía um sistema *deep learning* que, através de uma coleta ilegal de dados (mais precisamente, *big data*) em redes sociais, promovia campanhas políticas enviesadas – iniciou sua pesquisa nas principais leis do Direito Digital para buscar uma solução jurídica para o caso.

O art. 5º, LXXIX da Constituição Federal assegura o direito à proteção dos dados pessoais, inclusive nos meios digitais[21], ao passo que a inclusão da proteção de dados na Constituição Federal ocorreu em 2022 pela Emenda Constitucional nº 115/2022[22].

A segunda lei brasileira que compõe o Direito Digital é a Lei nº 12.737/2012, conhecida por Lei Carolina Dieckmann, que estabeleceu os crimes informáticos alterando dispositivos do Código Penal[23]. Apesar de fazer parte do Direito Digital, tanto o ensaio acadêmico do *Cambridge Analytica* quanto este limitam-se à responsabilização civil e aos danos de ordem civil, fazendo com que o Direito Penal e consequentemente esta lei fiquem fora do escopo da pesquisa.

5.1 *Marco civil da internet*

A terceira lei brasileira pertencente ao Direito Digital é o Marco Civil da Internet, ou Lei nº 12.965/2014[24], estatuto que apresenta princípios, garantias, direitos e deveres para o uso da internet no Brasil nas diferentes unidades federativas.

> O Marco Civil da Internet trouxe grande avanço, especialmente ao delimitar de forma objetiva que o provedor de conexão à internet não será

[19] SOARES, Mariana Falcão; DE ARAÚJO, Denise Maria Teixeira; SANTOS, Thamilles Sousa. Os impactos dos deepfakes sobre a perspectiva do marco civil da internet. **Caderno de Graduação-Ciências Humanas e Sociais-UNIT-ALAGOAS**, v. 7, n. 1, p. 22-22, 2021.

[20] ESPANHA, Marcelo Bueno et al. A Cambridge Analytica, o marco civil da internet e a lei geral de proteção de dados. **Revista Latino-Americana de Gestão, Tecnologia e Sociedade**, v. 1, n. 1, 2024.

[21] BRASIL. **Inciso LXXIX, art. 5º, da Constituição Federal de 1988**. Brasília, DF: Congresso Nacional. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 29 mar. 2026.

[22] Ibidem.

[23] BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informático; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Diário Oficial da União. Brasília, nov. 2012.

[24] BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial da União. Brasília, abr. 2014.

> responsabilizado civilmente por danos gerados por atos e/ou postagens de terceiros que agem como geradores de conteúdo (art. 18 "Ao delimitar que o provedor não é responsável, no entanto, fez a matéria avançar, para que os usuários não se escondam atrás da opacidade gerada pelas redes sociais. Isso permitiu, por outra via, no plano administrativo, caminhar no sentido de estabelecer uma tarefa importante aos provedores, a saber, a de colaborar com a redução das violações e, com isso, operar o desligamento de sites e páginas com conteúdo ofensivo a direitos autorais e a direitos da personalidade[25].

Essa cooperação dos provedores com a redução das violações de direitos está ligada ao artigo seguinte do Marco Civil, que assim dispõe:

> Art. 19: Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de Internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário[26].

Entretanto, responsabilizar o provedor de aplicações acaba sendo por muitas vezes ineficaz, pois a imagem oriunda de *deepfake*, devido ao seu caráter polêmico, é de rápida disseminação, o que torna muito difícil o exercício do controle sobre seu compartilhamento.

5.2. *Lei Geral de Proteção de Dados (LGPD) e Direito à Imagem*

A quarta lei que compõe o Direito Digital Brasileiro é a Lei Geral de Proteção de Dados (LGPD) ou Lei nº 13.709/2018[27], que dispõe "sobre o tratamento de dados pessoais a fim de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural". O disposto no artigo 2º do dispositivo em questão define bem essa proteção:

> Art. 2º: A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I - o respeito à privacidade;
>
> II - a autodeterminação informativa;
>
> III - a liberdade de expressão, de informação, de comunicação e de opinião;

[25] BITTAR, op. cit., p. 165.

[26] Brasil, op. cit.

[27] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União. Brasília, ago. 2018.

> IV - a inviolabilidade da intimidade, da honra e da imagem; (grifos nossos)
>
> V - o desenvolvimento econômico e tecnológico e a inovação;
>
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor;
>
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Com os grifos, percebe-se que a LGPD é bastante neutra quanto à sua proteção, pois o mesmo tratamento que ela confere à liberdade de expressão, confere aos direitos de privacidade e de imagem. Dessa forma, é assegurado que todos podem expressar-se livremente, desde que tomem os devidos cuidados com o conteúdo exposto; todavia, tal expressão não pode conter ódio, violência, injúria ou difamação, pois a existência destes elementos implicaria em uma penalidade de responsabilização pelos atos cometidos.

A proteção à imagem de uma pessoa está salvaguardada tanto pela Constituição Federal de 1988 quanto pelo Código Civil de 2002, enquanto um direito autônomo e inviolável, e, na acepção "imagem", engloba-se os traços da face, corpo, gestos e indumentárias. O Art. 5, X, da Constituição Federal de 1988 assegura o direito à indenização por dano material ou moral quando houver violação a intimidade, vida privada, honra e imagem das pessoas: "Art. 5º, X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação"[28].

O Código Civil, por sua vez, versa sobre o caso de uso da imagem para fins comerciais, sem que haja o consentimento da parte envolvida, mesmo que não tenha atingido a honra, a boa fama ou a respeitabilidade:

> Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se destinarem a fins comerciais[29].

O direito à imagem, conforme já foi dito, faz parte dos direitos da personalidade. Por conta disso, são considerados direitos subjetivos voltados para os bens e valores essenciais da pessoa no aspecto físico, moral e intelectual. Assim, de acordo com seu Art. 11, o Código Civil trata os direitos da imagem como intransmissíveis e irrenunciáveis e, no Art. 12 do mesmo dispositivo, aduz: "Pode-se exigir que cesse a

[28] Ibidem.

[29] BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 10 jan. 2002.

ameaça, ou a lesão, a direito de personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei"[30].

O fato de as imagens utilizadas em sistemas de inteligência artificial generativa serem retiradas de bancos de dados públicos, e por conta de retratarem com muita frequência pessoas públicas, coloca em xeque a questão do consentimento para uso dessas imagens. De acordo com Filipe Medon[31], essa questão de consentimento não é pacificada na doutrina, mas sendo nossa sociedade tão marcada constantemente pela presença da mídia, pelo anseio de exposição pública e dado o alto potencial lesivo de divulgação de imagens, o consentimento inequívoco da pessoa retratada para o uso de sua imagem deve ser sempre a regra, e não a exceção. As *deepfake*s aumentam ainda mais o potencial lesivo dessa divulgação de imagens, pois o retratado tem zero controle sobre a disseminação da sua imagem, além de figurar em uma posição, por vezes, vergonhosa perante a sociedade. A este retratado são, portanto, conferidos os direitos de personalidade.

> Toda expressão formal e sensível da personalidade de um homem é imagem para o Direito. A ideia de imagem não se restringe, assim, à representação do aspecto visual da pessoa pela arte da pintura, da escultura, do desenho, da fotografia, da figuração caricata ou decorativa, da reprodução em manequins e máscaras. Compreende, além imagem sonora da fonografia e da radiodifusão, e os gestos, expressões dinâmicas da personalidade[32].

Nesse contexto, surgem os conceitos de imagem-retrato e imagem-atributo. O primeiro se alinha a expressões formais e sensíveis da personalidade (aparência de uma pessoa; sua voz; sua composição genética etc.) e apenas são atribuídas a pessoas físicas, enquanto o segundo engloba atributos positivos e negativos que são apresentados à sociedade, e podem ser atribuídas tanto a pessoas físicas quanto a pessoas jurídicas[33].

As *deepfakes* podem agir maculando aspectos da imagem-retrato da pessoa, mas ela fere, sobretudo, a imagem-atributo da pessoa ofendida, uma vez que costuma replicar praticamente em perfeição os aspectos da imagem-retrato para que o conteúdo pareça verídico, mas coloca a pessoa em situações que a deixam numa posição negativa perante a sociedade. Percebe-se, dessa forma, que a violação dos direitos de privacidade e de imagem ensejam responsabilização, e as *deepfake*s claramente violam direitos de imagem. Veremos, a seguir, como funciona o instituto da responsabilidade civil e sobre qual agente ela incidiria.

---

[30] Ibidem.

[31] AFFONSO, Filipe José Medon. O direito à imagem na era das deep fakes. **Revista Brasileira de Direito Civil**, v. 27, n. 1, p. 251, 2021.

[32] MORAES, apud MEDON, Ibidem.

[33] Ibidem.

5.3. A *responsabilidade civil dos danos causados pelas deepfakes*

A sensação de anonimato na internet contribui para que muitos usuários disseminem conteúdo inverídico e danoso aos direitos de outrem. Conforme já mencionado anteriormente, a regulamentação da internet ainda é um campo em desenvolvimento, e há muitas lacunas jurídicas a serem preenchidas. Para complicar mais ainda esse panorama, a inteligência artificial vem sendo utilizada como ferramenta para espalhar *deepfake*s em larga escala, que servem de matéria-prima para a produção de *fake news* e mancham a imagem de suas vítimas.

Após verificar a neutralidade da proteção dada pela LGPD, entendemos que o direito à liberdade de expressão, apesar de ser um direito fundamental, não é absoluto, de modo que o exercício abusivo deste direito é tolhido pelo instituto da responsabilidade civil[34].

Para que ocorra a responsabilização civil, são necessários quatro requisitos clássicos: a ocorrência de dano, a conduta, o nexo de causalidade (entre o dano e a conduta) e a ausência de causa excludente de responsabilidade[35]. Como a máquina geradora de inteligência artificial, apesar de possuir uma imensa autonomia, não possui personalidade jurídica própria, e não se pode atribuir a responsabilidade civil a ela. Assim, a conduta é atribuída ao ser humano, a depender do caso concreto, podendo este ser humano figurar como fornecedor ou usuário da máquina[36].

A responsabilidade civil e o dever de reparação a danos causados por sistemas e robôs de inteligência artificial encontram guarida na teoria do risco enquanto sistema de responsabilidade civil, expresso pelo parágrafo único do art. 927 do Código Civil de 2002: "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 atuação da inteligência artificial é imprevisível e por conta disso o responsável por esta IA deve lidar com os riscos resultantes dela[37].

---

[34] JARDIM, Gustavo Tanger. Fake news, deepfake e outras ameaças virtuais: os desafios da responsabilidade civil na rede mundial de computadores. **Revista de Direito da ADVOCEF**, v. 20, n. 36, p. 15-28, 2024.

[35] "Como excludentes de responsabilidade civil devem ser entendidas as circunstâncias que, por atacar um dos elementos ou pressupostos da responsabilidade civil, rompendo o nexo causal, terminam por fulminar qualquer pretensão indenizatória. São elas: o estado de necessidade, a legítima defesa, exercício regular de direito e estrito cumprimento de dever legal, o caso fortuito e a força maior, a culpa exclusiva da vítima e o fato de terceiro." Excludentes da Responsabilidade Civil/ Araújo Júnior, Vital Borba de. – Cabedelo, PB: [s.n], 2014.1.

[36] SILVA, Gabriela Buarque Pereira. **Responsabilidade civil, riscos e inovação tecnológica**: os desafios impostos pela inteligência artificial. Dissertação (Mestrado em Direito) – Universidade Federal de Alagoas, 2020, p.113.

[37] DE TEFFÉ, Chiara Spadaccini; MEDON, Filipe. Responsabilidade civil e regulação de novas tecnologias: questões acerca da utilização de inteligência artificial na tomada de decisões empresariais. **REI-revista estudos institucionais**, v. 6, n. 1, p. 317, 2020.

Tendo por base a responsabilidade civil objetiva, quanto maior o risco envolvido, maior é a gravidade da hipótese, e são subtraídos mais elementos necessários da responsabilidade para que ela exista. Por exemplo quando o risco é considerado inerente à atividade, não é necessária nem a existência de nexo causal, dispensando-se assim a existência de nexo causal na conduta. Caso seja entendida a relação entre a inteligência artificial e seu usuário como uma relação de consumo e com isso possa o dano causado por essa inteligência artificial ser caracterizado como um vício ou fato do produto ou serviço utilizado, devem ser o código de defesa do consumidor e sua responsabilidade civil objetiva aplicados[38].

O polo passivo da imputação de conduta danosa quando a ação provém de uma inteligência artificial, ou seja, sobre qual sujeito essa responsabilidade recairá, é uma questão interessante. Os produtores/programadores de *software/hardware*? Os que inseriram instruções que influenciaram o comportamento do sistema ou os que comercializam as máquinas e lucram com essa venda? Silva[39] coloca uma analogia de responsabilidade entre pais pelos atos de seus filhos e produtores/programadores/usuários pelo treinamento da máquina, porém esta analogia se mostra inviável, uma vez que a máquina, ao contrário dos filhos dos pais utilizados em exemplo, não é uma pessoa. Identificar um responsável efetivo é uma tarefa árdua, mas Silva encontra no fornecedor da máquina uma possível figura para atribuir responsabilidade pelos danos causados por ela, tendo como base a teoria consumerista, de forma a responsabilizar o fornecedor do *software* pelos resultados adversos ao esperado. Em outras palavras, o teórico enseja ao programador do *software* (ora, fornecedor) a responsabilização perante os resultados imprevistos na circulação do conteúdo gerado a partir de IA (ora, produto).

Com fulcro na teoria do risco, conclui-se[40] também que, em muitas situações, não é razoável condicionar a indenização à verificação da existência de um defeito no *software*, uma vez que a máquina poderá apresentar resultados incomuns ou, ainda, comportar-se conforme o esperado e, ainda assim, desencadear danos. Nessa hipótese de comportamento extraordinário ao consumidor, apesar de não estar condicionada à indenização pelo defeito, o fornecedor permanece responsável pelo dano, e a indenização ainda é devida, pois há uma situação de risco inerente, sendo a atividade incomum equiparada ao risco inerente.

Essa situação configura evento fortuito interno que, ao contrário do fortuito externo, não afasta a responsabilidade do fornecedor.

Além do risco inerente existente nessa questão, a hipossuficiência da vítima também é um fator determinante, pois adota-se a relação de consumo para que haja

[38] Ibidem, p. 318.

[39] SILVA, Op. cit., p. 101.

[40] Ibidem, p. 106.

imputação de responsabilidade civil. Mesmo nos casos em que o fornecedor programador é, de fato, considerado responsável pelo dano, a simplificação de reparação do dano da vítima é o foco da questão jurídica, uma vez que a vítima figura no polo hipossuficiente da relação de consumo. Portanto, a hipótese de haver direito de regresso do programador implica na dificuldade de se provar de quem é a culpa: se foi do programador, do designer do programa, do especialista que forneceu o conhecimento, de quem nomeou o especialista etc.[41]

5.4. A *boa-fé objetiva*

A responsabilidade civil é sintetizada pelo Código Civil de 2002 através de três artigos. O art. 927, que exige a reparação do ato ilícito ao sujeito que cometer dano a outrem, o art. 186, que conceitua o ato ilícito: "Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito" e, também o art. 187, que conceitua o abuso de direito, que ocorre quando um sujeito tira proveito de um direito que possui, exercendo-o para além dos limites impostos pela lei, os bons costumes, os fins econômico-sociais originais daquele ato e, principalmente, para além da boa-fé: "Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes."

Destaca-se[42] que tal figura relaciona-se à função de controle da boa-fé objetiva, ainda que se conecte às demais funções desse princípio.

Sob a ótica da *Post Truth*, conceituada como a antítese de *fake news*, o dano social resultante da disseminação de *fake news* é evidente e incontestável, pois ocorre uma manipulação da opinião pública e a boa-fé objetiva é violada em nível social. O nível dessa violação é social, pois a descrença nos meios jornalísticos generalizada fomenta um ciclo vicioso de disseminação de *fake news* através de diferentes veículos de mídia, e a sociedade entra em colapso, principalmente no que diz respeito a assuntos políticos, que acabam por restar todos deturpados. Um exemplo da terrível consequência das *fake news* na vida das pessoas é a suspeita de que a disseminação de *fake news* tenha alterado o resultado das eleições presidenciais dos Estados Unidos da América em 2016[43].

[41] Op. cit.

[42] GUIMARÃES, Glayder Daywerth Pereira; SILVA, Michael César. Fake news à luz da responsabilidade civil digital: o surgimento de um novo dano social. **Revista Jurídica da FA7**, v. 16, n. 2, p. 99-114, 2019.

[43] Ibidem.

A boa-fé objetiva veda que a pessoa viole uma norma jurídica (por exemplo, violar os direitos à imagem de outrem) para tirar proveito dela (por exemplo disseminar inverdades que favoreçam sua opinião política).

De acordo com Menezes Cordeiro[44], "A fórmula *tu quoque* traduz, com generalidade, o aflorar de uma regra pela qual a pessoa que viole uma norma jurídica poderia, sem abuso, exercer a situação jurídica que essa mesma norma lhe tivesse atribuído". Deste modo, essa pretensão caracteriza-se como abusiva, fruto de um relacionamento anterior secreto, violador dos deveres de fidelidade".

5.5. *O dever de reparação*

Conforme já demonstrado anteriormente, os artigos 186 e 927 do Código Civil instituem o dever de reparação jurídica por parte de quem comete ao dano, à vítima dele. Essa restituição é devida, pois o instituto da responsabilidade civil busca a restauração do equilíbrio moral e patrimonial que foi alterado pelo dano causado, devendo a vítima ser restituída ao seu *status quo* de antes do dano.

O dever de reparar o dano deve ser quantificado de acordo com os parâmetros do Código Civil, com destaque para o disposto no artigo 944: "a indenização mede-se pela extensão do dano". Entretanto, este artigo é mais afeito com a reparação do dano patrimonial, cujo volume da perda patrimonial dele decorrente cabe à apuração do magistrado e das partes[45].

O dano moral reside na violação de direitos da personalidade da vítima, e, conforme já visto, o direito à imagem se insere nos direitos da personalidade. Ao violar o direito à imagem da vítima, o agente incorre em dano moral. É importante frisar que a possibilidade de reparação de dano moral não exclui seu caráter absoluto e não patrimonial, uma vez que essa reparação caracteriza uma medida sub-rogatória representando o "*id quod interest*, ou seja, a satisfação de um interesse jurídico de titular de um direito da personalidade violado, que não se confunde com a recomposição do bem jurídico violado, porquanto, em regra, impossível". De acordo com o Prof. Valter Farid[46], a restituição do dano moral não busca uma "amenização de dor ou sofrimento", mas uma compensação financeira a quem teve direitos da personalidade indevidamente violados, conforme disposto no já visto art. 12 do Código Civil e nos incisos V e X do art. 5º da Constituição Federal de 1988:

[44] MENEZES CORDEIRO, Antonio Manuel da Rocha. **A boa-fé no direito civil**. Coimbra: Almedina, 2013, p. 837.

[45] ANTONIO JUNIOR, Valter Farid. Marcas da Administração Pública: exploração econômica, mecanismos de proteção e reparação de danos materiais e morais. Tese (Doutorado em Direito Civil) – Faculdade de Direito, Universidade de São Paulo, 2021, p. 189.

[46] Ibidem, p. 190.

> Art. 5º, V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação [...] [47].

Farid pontua que, em decorrência do fato de o dano moral carecer de parâmetros jurídicos legalmente estabelecidos para sua quantificação, bem como de elementos que definam o que a vítima do dano deixou de auferir com sua ocorrência, cabe ao magistrado a difícil tarefa de arbitramento dessa quantificação, que não pode ser irrisória (incapaz de compensar o prejuízo) nem tampouco excessiva, para não caracterizar o enriquecimento sem causa, vedado pelo Código Civil brasileiro[48].

6. CONSIDERAÇÕES FINAIS

Os estudos até aqui demonstram que os indivíduos lesados pelas *deepfake*s, no que tange a seu direito de personalidade, sobretudo de imagem, podem recorrer ao instituto da responsabilidade civil objetiva para reparar os danos causados pela cruel forma de inteligência artificial generativa que vem causando polêmicas, sobretudo na esfera política da internet e do dia a dia pessoas. A imagem de uma pessoa está inserida entre o que se considera dados pessoais de acordo com o disposto na Lei Geral de Proteção de Dados, além de ser um direito constitucionalmente protegido, sendo esta proteção, inclusive, ulterior ao direito de liberdade de expressão. Esta reparação civil ocorre através da teoria do risco, pois a geração de imagens caracterizadas como *deepfake*s são consideradas risco inerente à máquina. Assim, adotou-se uma equiparação ao direito consumerista para garantir, de forma mais simples, a reparação legal das vítimas de *deepfake*, na qual se responsabiliza o programador de *software* (ora, fornecedor do produto) pelo dano sofrido pela vítima. O provedor de internet, quando não acata a ordem judicial de remover o conteúdo lesivo, também deve, de acordo com o Marco Civil da Internet, ser responsabilizado civilmente.

Quanto a uma eventual titularidade de direito do autor pela inteligência artificial generativa ou de algum de seus componentes, a legislação brasileira não atribui nenhuma personalidade jurídica a ela, sendo esta, portanto, *sui generis*. O fato de esta inteligência artificial não ser uma pessoa jurídica, e tampouco ser titular de direitos, não impede que a doutrina tenha encontrado uma forma de responsabilizá-la civilmente pelos imensos danos causados às pessoas que lhe são vítimas. Essa responsabilização, entretanto, é muito vaga, e possui diversas limitações. Ao caracterizar a relação entre o programador de *software* e a vítima do dano causado pela *deepfake*

[47] BRASIL, Op. cit.

[48] Op. cit.

como relação de consumo, para que se possa atribuir a responsabilidade do dano ao fornecedor (programador), a culpa poderia estar sendo "terceirizada" em prol da reparação da vítima. O fornecedor estaria respondendo por erros e vícios que existem graças à inobservância dos programadores, e pela má-fé de usuários da máquina que viciam o banco de dados. Vários são os agentes que poderiam figurar no polo passivo, a depender do caso concreto, mas dada sua difícil identificação quando se trata da inteligência artificial generativa, que é de funcionamento praticamente autônomo após certo tempo, a figura do programador acaba servindo de "bode expiatório". Além disso, há a questão da boa-fé. Como inferir que um sujeito que está respondendo por erros de terceiros agiu contra este princípio? Dessa forma, cada caso envolvendo *deepfake* e responsabilidade civil mereceria uma análise minuciosa acerca do polo passivo da responsabilização, bem como da incidência da questão da boa-fé objetiva nesses casos, e, para tanto, é imprescindível a existência de uma regulamentação coesa e exemplificativa da inteligência artificial no Brasil, em consonância com o que está sendo feito na Europa, com o advento do *AI Act*.

REFERÊNCIAS BIBLIOGRÁFICAS

AFFONSO, Filipe José Medon. **O direito à imagem na era das deep fakes.** Revista Brasileira de Direito Civil, v. 27, n. 01, p. 251, 2021.

ANTONIO JUNIOR, Valter Farid. **Marcas da Administração Pública**: exploração econômica, mecanismos de proteção e reparação de danos materiais e morais. Tese (Doutorado em Direito Civil) – Faculdade de Direito, Universidade de São Paulo, 2021.

AUGUSTENE, Agne. O que é um *deepfake*? Os perigos de vídeos de IA falsos. **Nordvpn**, fev. 2023. Disponível em: https://nordvpn.com/pt-br/blog/deepfake-o-que-e/. Acesso em: 10 jun. 2024.

BITTAR, Carlos Eduardo Bianca. **Direito de Autor**. 7. ed. Editora Forense, 2019.

BOFF, Salete Oro; ABIDO, Leonardo. O Direito de autor no Brasil de obras produzidas pela Inteligência Artificial. **Revista da Fac. Mineira de Direito (PUC Minas)**, v. 23, n. 45, 2020.

BRASIL. **Constituição Federal de 1988**. Brasília, DF: Congresso Nacional. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 29 mar. 2026.

BRASIL. **Lei nº 9.610, de 19 de fevereiro de 1998**. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Diário Oficial da União. Brasília, fev. 2018.

BRASIL. **Lei nº 9.609, de 19 de fevereiro de 1998**. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências. Diário Oficial da União. Brasília, fev. 1998.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 10 jan. 2002.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informático; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Diário Oficial da União. Brasília, nov. 2012.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial da União. Brasília, abr. 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União. Brasília, ago. 2018.

DE TEFFÉ, Chiara Spadaccini; MEDON, Filipe. Responsabilidade civil e regulação de novas tecnologias: questões acerca da utilização de inteligência artificial na tomada de decisões empresariais. **REI-revista estudos institucionais**, v. 6, n. 1, p. 301-333, 2020.

ESPANHA, Marcelo Bueno et al. A Cambridge Analytica, o marco civil da internet e a lei geral de proteção de dados. **Revista Latino-Americana de Gestão, Tecnologia e Sociedade**, v. 1, n. 1, 2024.

GARCIA, Ana Cristina. Ética e inteligência artificial. **Computação Brasil**, n. 43, p. 14-22, 2020.

GUIMARÃES, Glayder Daywerth Pereira; SILVA, Michael César. Fake news à luz da responsabilidade civil digital: o surgimento de um novo dano social. Revista Jurídica da FA7, v. 16, n. 2, p. 99-114, 2019.

JARDIM, Gustavo Tanger. Fake news, *deepfake* e outras ameaças virtuais: os desafios da responsabilidade civil na rede mundial de computadores. **Revista de Direito da ADVOCEF**, v. 20, n. 36, p. 15-28, 2024.

MENEZES CORDEIRO, Antonio Manuel da Rocha. **A boa-fé no direito civil**. Coimbra: Almedina, 2013.

MOURA, Carlos Manoel Silva; BRAGA, Tiago Emmanuel Nunes. A inteligência artificial e a criação de conteúdo: os vieses que habitam entre nós. **Anais do Workshop de Informação, Dados e Tecnologia-WIDaT**, 2023.

RUSSEL, Stuart; NORVIG, Peter. **Inteligência Artificial**: uma abordagem moderna. Rio de Janeiro: Campus, 2004.

SCHIRRU, Luca. Inteligência artificial e o direito autoral: o domínio público em perspectiva. **Instituto de Tecnologia e Sociedade do Rio (ITSRIO)**, 2019.

SILVA, Gabriela Buarque Pereira **Responsabilidade civil, riscos e inovação tecnológica**: os desafios impostos pela inteligência artificial. Dissertação (Mestrado em Direito) – Universidade Federal de Alagoas, 2020.

SOARES, Mariana Falcão; DE ARAÚJO, Denise Maria Teixeira; SANTOS, Thamilles Sousa. Os impactos dos deepfakes sobre a perspectiva do marco civil da internet. **Caderno de Graduação-Ciências Humanas e Sociais-UNIT-ALAGOAS**, v. 7, n. 1, p. 22-22, 2021.

SOARES, Matheus. IAs generativas são 'fábricas de imagens falsas', aponta estudo. **Desinformante**, mar. 2024. Disponível em: https://desinformante.com.br/ia-generativa-imagens-falsas/. Acesso em: 10 jun. 2024.

SOARES, Matheus. 1 ano da "deepfake do papa": o que mudou? O que virá. **Desinformante**, mar. 2024. Disponível em: https://desinformante.com.br/deepfake-papa/. Acesso em: 10 jun. 2024.

TURING, Alan M. **Computing machinery and intelligence.** Mind, 59, p. 433-460. Disponível em http://phil415.pbworks.com/f/TuringComputing.pdf Acesso em: 10 jun. 2024. ULMER, Eugen. Urheber und Veerlagsrecht. 3.d. Berli: Heidelberg, 1980.

VASCONCELOS, Claudio Lins de. Artigo: A lei europeia sobre IA e os direitos autorais. **UBC**, mar. 2024. Disponível em: https://www.ubc.org.br/publicacoes/noticia/22507/artigo-a-lei-europeia-sobre-ia-e-os-direitos-autorais/ Acesso em: 10 jun. 2024.

Submetido em: 07/01/2025
Aprovado em: 10/09/2025

RESPONSABILIDADE CIVIL POR DANOS CAUSADOS POR SISTEMAS DE INTELIGÊNCIA ARTIFICIAL

Liability for Damages Arising from Artificial Intelligence Systems

Fabio Trabold Gastaldo[1]

SUMÁRIO 1. Introdução; 2. Desenvolvimento; 2.1. Panorama atual do direito brasileiro – vítimas estão protegidas?; 2.2. Responsabilização subjetiva – retrocesso injustificável; 2.3. Desnecessidade de regulação urgente – estado da arte em formação; 3. Conclusão; Referências Bibliográficas.

RESUMO O presente trabalho tem como objetivo principal verificar, por meio de pesquisa em doutrina, se a estruturação normativa da culpa na responsabilidade civil tal como colocada neste momento no direito brasileiro exige atualização e aperfeiçoamento, diante da superveniência fática de sistemas autônomos de inteligência artificial.

Palavras-chave: Responsabilidade Civil. Culpa. Sistemas de Inteligência Artificial.

ABSTRACT This paper aims to analyze, through doctrinal research, whether the normative structure of fault in civil liability, as currently framed in Brazilian law, requires updates and improvements in light of the factual emergence of autonomous artificial intelligence systems.

Keywords: Civil Liability. Fault. Artificial Intelligence Systems.

1. INTRODUÇÃO

No cenário contemporâneo, os avanços tecnológicos no campo da inteligência artificial (IA) têm transformado rápida e radicalmente a forma como as organizações conduzem seus negócios e interagem com os indivíduos. Os sistemas têm evoluído de tal forma a produzir atos e fatos de modo cada vez mais autônomo, com crescente possibilidade de falhas que podem causar danos.

Há muito a doutrina civilista vem se ocupando do tema do desenvolvimento industrial e tecnológico no campo da responsabilidade civil. A teoria do risco (ou responsabilidade civil *objetiva*) tem origem no contexto das primeiras fases históricas da chamada revolução industrial, com o reconhecimento de que a teoria da culpa parecia insuficiente para a reparação das respectivas vítimas.

Numa apertadíssima síntese, pode-se concluir que o direito evoluiu para adotar a responsabilidade objetiva quando a natureza da atividade desenvolvida implicar risco para os direitos de outrem. Em regra, vítimas de eventos causados pela atividade industrial humana, tais como acidentes aéreos, nucleares, de consumo,

[1] Procurador do Estado de São Paulo. Especialista em Direito Administrativo pela Fundação Getúlio Vargas – GVLAW.

DOI: 10.22491/respge.v16i1.1732

entre outros, não necessitam comprovar a culpa do causador do dano para recebimento de indenização.

Todavia, em períodos mais recentes, o crescimento da utilização dos sistemas de inteligência artificial, com máquinas agindo de forma progressivamente autônomas, de acordo com instruções contidas em algoritmos cada vez mais complexos, tem gerado diversos debates na comunidade jurídica mundial a respeito da necessidade de adequação dos diplomas legislativos em vigor à nova realidade tecnológica.

No Brasil, já foram apresentados diversos projetos de lei para regular o tema e, como não poderia deixar de ser, uma das principais discussões travadas nessas proposituras é a da disciplina da responsabilidade civil, mormente no que diz respeito ao seu caráter objetivo ou subjetivo.

Em 27 de outubro de 2021, um grupo de juristas assinou carta aberta ao Senado Federal criticando o texto do artigo 6º, inciso VI, do projeto de lei 21-A/2020, que estabelecia o regime de responsabilidade civil subjetiva como regime padrão aplicável aos danos provocados por sistemas de inteligência artificial, colocando em risco, no entender de seus subscritores, o direito das vítimas de buscar reparação, criando um cenário de irresponsabilização generalizada e tornando praticamente impossível a prova da culpa dos agentes que atuam na cadeia de desenvolvimento e operação de sistemas de inteligência artificial[2].

Posteriormente, em 22 de fevereiro de 2022, outro grupo de juristas, por sua vez, subscreveu um artigo publicado no portal Consultor Jurídico, defendendo um ponto de vista diametralmente oposto, argumentando que a responsabilidade objetiva retira incentivo ao investimento e emprego da tecnologia[3].

Diante da polêmica instaurada, pergunta-se: Especificamente no que diz respeito à responsabilidade civil por danos causados por sistemas de inteligência, as regras constantes do ordenamento jurídico brasileiro são suficientes para tratamento do tema, ou há novos elementos que demandam aprimoramento legislativo?

Considerando o pouco tempo de maturação e convivência com esses sistemas de IA, há necessidade de criar, no presente momento, regras específicas para modificar o regime de responsabilização civil?

Em caso positivo, há justificativa para retorno ao regime da responsabilização subjetiva?

O foco principal do presente estudo não será avaliar os impactos dos riscos da inteligência artificial ou mesmo de possíveis meios de mitigação. Não se cuida,

[2] ESPECIALISTAS criticam responsabilidade subjetiva prevista no PL do marco da IA. **Conjur**, 27 out. 2021. Disponível em: https://www.conjur.com.br/2021-out-27/especialistas-questionam-artigo-pl-marco-legal-ia/. Acesso em: 15 nov. 2023.

[3] MARCO legal da inteligência artificial: ponderações sobre a responsabilidade civil. **Conjur**, 22 fev. 2022. Disponível em: https://www.conjur.com.br/2022-fev-22/opiniao-marco-inteligencia-artificial-responsabilidade-civil/>. Acesso em: 15 nov. 2023.

ademais, de analisar as questões técnicas envolvidas. A prioridade do estudo será analisar o direito material (responsabilidade civil subjetiva ou objetiva) e a sua incidência após o dano sofrido, em tese.

Verificar-se-á, pois, o panorama atual do direito brasileiro em relação à necessidade de a vítima demonstrar a culpa do agente causador do dano. Em seguida, analisar-se-á se a situação fática de momento exige aprimoramento legislativo de modo a salvaguardar as respectivas vítimas e não inibir os avanços tecnológicos.

2. DESENVOLVIMENTO

2.1. *Panorama atual do direito brasileiro – vítimas estão protegidas?*

De início, vale estabelecer a seguinte premissa: historicamente, o problema do desenvolvimento tecnológico e seus reflexos em relação aos danos causados não é novo.

Neste limitado espaço, não cabe esmiuçar a evolução histórica do tratamento jurídico da responsabilidade civil, cujas origens podem ser encontradas no Código de Hamurabi (aproximadamente 1772 a.C.). É necessário estabelecer, todavia, um corte temporal que resgata o século XIX, quando as sociedades do planeta passaram a vivenciar as consequências positivas e negativas do grande – e então inédito – salto tecnológico.

A título de exemplo, as ferrovias de trens de força motriz autônoma (movidos a motor a vapor e, posteriormente, a energia elétrica) começaram a se disseminar pelo mundo em meados do século XIX. No Brasil, sua primeira ferrovia foi inaugurada em 1854, entre o Porto de Mauá e a cidade de Fragoso, no Rio de Janeiro.

Ainda no setor de transportes, o veículo automotor que hoje chamamos de automóvel só começou a ter alcance popular a partir do início do século XX, com o advento da produção em massa por Henry Ford.

O transporte aéreo, por sua vez, passou por expansão comercial após o término da Segunda Guerra Mundial (1945).

Os breves exemplos mencionados, todos do setor de transportes de pessoas, ilustram que, após meados do século XIX, observou-se um aumento exponencial das velocidades nos deslocamentos terrestres da espécie humana, até então dependente de cavalos e respectivas charretes e congêneres. Os tempos de viagem reduziram-se vertiginosamente, permitindo deslocamentos até então inimagináveis.

Em contrapartida – e como seria de se esperar, – observou-se um aumento dos acidentes, tanto no volume de ocorrências quanto na gravidade de suas consequências.

Nesse contexto, resta claro que a responsabilidade civil subjetiva, até então prevalecente nos sistemas civilistas mundo afora, começou a se revelar insuficiente para atendimento das respectivas vítimas dos acidentes que passaram a ocorrer. O progresso técnico veio acompanhado de um crescimento da assimetria de informação entre as vítimas e os demais ocupantes da cadeia produtiva (fabricantes, transportadores, profissionais envolvidos na operação etc.), que acabava por dificultar – senão impedir – a prova da culpa, deixando os lesados indefesos.

Ainda em 1944, essa situação foi notada por José de Aguiar Dias, ao discorrer acerca da responsabilidade objetiva:

> [...] a palavra evolução não condiz com o movimento que vai analisar; a revolução é que deveria, com mais propriedade, aludir, tratando de assunto em que tão vertiginosamente se transformam os dados estabelecidos. Essa mutação acelerada, em face de que "a verdade de hoje, que deve, por sua vez, ceder o passo à verdade de amanhã", se deve ao caráter cada vez mais perigoso da vida contemporânea: o século do automóvel, do avião, da mecanização universal não pode, logicamente, ser uma era de segurança material. A falta desta acarreta uma geral aspiração de segurança jurídica. Se não estamos a coberto dos riscos, tenhamos pelo menos a certeza de que não sofreremos impunemente as consequências da atividade alheia. À fórmula *viver perigosamente*, replicamos com esta outra, que é a sua sanção: *responder pelos nossos atos*[4].

Sobre esses processos técnicos de facilitação da tutela do direito indenizatório da vítima, Carlos Roberto Gonçalves traçou o seguinte quadro cronológico:

> 1 – Primeiramente, procurou-se proporcionar maior facilidade à prova da culpa. Os tribunais, em muitos casos, passaram a examinar com benignidade a prova da culpa produzida pela vítima, extraindo-a de circunstâncias do fato e de outros elementos favoráveis;
>
> 2 – Admissão da teoria do abuso de direito como ato ilícito. A jurisprudência, interpretando a *contrario sensu* o art. 160, inciso I, do CC de 1916, passou a responsabilizar pessoas que abusavam de seu direito, desatendendo à finalidade social para a qual foi criado, lesando terceiros;
>
> 3 – Estabelecimento de casos de presunção de culpa (Súmula 341 do STF; a lei sobre a responsabilidade das estradas de ferro etc.), casos esses em que invertem sempre o ônus da prova, melhorando muito a situação da vítima. Esta não teria de provar a culpa psicológica, subjetiva, do agente, que seria presumida. Bastaria a prova da relação de causalidade entre o ato do agente e o dano experimentado. Para livrar-se da presunção de culpa, o causador da lesão patrimonial ou moral é que teria de produzir prova de inexistência de culpa ou de caso fortuito;
>
> 4 – Admissão de maior número de casos de responsabilidade contratual (táxi, ônibus, trem etc.), que oferecem vantagem para a vítima no tocante à prova, visto que esta precisava provar apenas que não chegou incólume ao seu destino, e que houve, pois, inadimplemento contratual[5].

[4] DIAS, José de Aguiar. **Da Responsabilidade Civil**. Rio de Janeiro: Lumen Juris, p. 64. No mesmo sentido: GONÇALVES, Carlos Roberto. *Responsabilidade Civil*, p. 6.

[5] GONÇALVES, Carlos Roberto. **Comentários ao código civil**. São Paulo: Saraiva, 2003, p. 308-309.

Constatada a dificuldade em provar a culpa do agente causador desses acidentes, o direito evoluiu no sentido reconhecer presunções de culpa, tendendo a converter a responsabilidade subjetiva em objetiva, de modo a posicionar as vítimas dos mencionados acidentes numa situação processual mais favorável.

Com efeito, a principal consequência da responsabilidade civil objetiva é a dispensa da prova de culpa, bastando a demonstração do dano e do nexo causal, simplificando e facilitando o caminho da vítima para obtenção de sua indenização.

Nesse contexto, a responsabilidade civil objetiva vem sendo reconhecida em diversos diplomas no direito brasileiro, valendo destacar o Decreto nº 2.681, de 7 de dezembro de 1912[6], que regula a responsabilidade civil das estradas de ferro e prevê, em seu artigo 17, a responsabilidade objetiva das estradas de ferro pelos desastres que nas suas linhas sucederem aos viajantes e de que resulte a morte, ferimento ou lesão corpórea.

No setor de energia nuclear (artigo 4º da Lei federal nº 6.453, de 17 de outubro de 1977[7]) e aéreo (artigo 256 da Lei federal nº 7.565, de 19 de dezembro de 1986 – Código Brasileiro de Aeronáutica[8]), os respectivos diplomas de regência também preveem a responsabilidade objetiva.

De modo mais abrangente, o § 6º do artigo 37 da Constituição Federal de 1988 prevê a responsabilidade objetiva do Estado por danos causados por seus agentes.

Os artigos 12 e 14 do Código de Defesa do Consumidor (Lei federal nº 8.078, de 11 de setembro de 1990[9]), por sua vez, preveem a responsabilidade objetiva por danos causados por fornecedores de produtos e serviços. Mesmo fora das relações de consumo, o artigo 17 do mesmo diploma equipara a consumidor todas as vítimas do evento danoso.

Posteriormente, o parágrafo único do artigo 927 do Código Civil de 2002 veio a adotar a responsabilidade objetiva quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

Diante do quadro acima, a legislação em vigor no Brasil é suficiente para atendimento de possíveis vítimas em caso de danos sofridos por sistemas de inteligência artificial?

---

[6] BRASIL. **Decreto nº 2.681, de 7 de dezembro de 1912**. Regula a responsabilidade civil das estradas de ferro. Rio de Janeiro, 7 dez. 1912.

[7] BRASIL. **Lei nº 6.453, de 17 de outubro de 1977**. Dispõe sobre a responsabilidade civil por danos nucleares e a responsabilidade criminal por atos relacionados com atividades nucleares e dá outras providências. Diário Oficial da União,18 out.1977.

[8] BRASIL. **Lei nº 7.565, de 19 de dezembro de 1986**. Dispõe sobre o Código Brasileiro de Aeronáutica. Diário Oficial da União, 23 dez. 1986 e retificado 30 dez. 1986.

[9] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, 12 set. 1990.

Para tanto, far-se-á um exercício de subsunção de casos concretos publicados na grande imprensa, em cotejo com o ordenamento jurídico pátrio.

Um primeiro exemplo que vem sendo divulgado rotineiramente na mídia é o dos reconhecimentos faciais equivocados, que têm levado pessoas inocentes à persecução penal injusta, muitas com prisões em flagrante[10]. Invariavelmente, essas vítimas ficam presas por semanas ou meses, até que consigam demonstrar sua real identidade.

Nestes casos, que envolvem prisão por erro na identificação do agente criminoso, há consolidada jurisprudência reconhecendo a responsabilidade objetiva do Estado[11]. Presume-se, pois, que, ao lançar mão de sistemas automatizados de reconhecimento facial, o Estado assume o risco de indenizar por danos causados por eventuais equívocos, não se exigindo da vítima qualquer prova de culpa.

Outro exemplo bastante noticiado é o de acidentes causados por veículos de condução autônoma, já muito comuns em outros países. Segundo matéria publicada em 12 de junho de 2023, acidentes envolvendo carros Tesla em piloto automático já mataram 17 pessoas nos Estados Unidos até aquela data[12].

Uma situação dessas no direito brasileiro, ao que parece, seria facilmente subsumível ao Código de Defesa do Consumidor, seja em relação aos usuários do serviço (responsabilidade pelo fato do produto – artigo 12 da Lei federal nº 8078, de 1990), seja em relação aos pedestres, terceiros na relação jurídica consumerista, mas equiparados a vítimas para fins de responsabilização civil (artigo 17 do mesmo diploma).

Ainda que não houvesse a incidência do Código de Defesa do Consumidor, parece-nos não haver dificuldade, também, em demonstrar a incidência desses fatos ao parágrafo único do artigo 927 do Código Civil, considerada a natureza da atividade que implica, por sua natureza, risco para os direitos de outrem.

A utilização de sistemas de inteligência artificial pode causar danos em inúmeros outros setores da vida humana, como qualquer produto, serviço ou atuação estatal.

---

[10] TAJRA, Alex. Ainda sem regulação, estados prendem centenas de pessoas utilizando reconhecimento facial. **Conjur**, 17 maio 2024. Disponível em: https://www.conjur.com.br/2024-mai-17/sem-regulacao-estados-prendem-centenas-utilizando-reconhecimento-facial/>. Acesso em: 23 maio 2024; "MEDO, frustrado e constrangido", diz homemdetido por engano em estádio após erro do sistema de reconhecimento facial. **Fantástico**, 21 abr. 2024. Disponível em: https://g1.globo.com/fantastico/noticia/2024/04/21/medo-frustrado-e-constrangido-diz-homem-detido-por-engano-em-estadio-apos-erro-do-sistema-de-reconhecimento-facial.ghtml>. Acesso em: 23 maio 2024.

[11] TJSP, Apelação Cível 1066315-62.2022.8.26.0053, j. 08/04/2024; TJSP, Apelação Cível 1072179-81.2022.8.26.0053, j. 11/03/2024; TJSP, Apelação Cível 1001723-97.2023.8.26.0368, j. 29/01/2024; STF, ARE 1011871, Relator Min. RICARDO LEWANDOWSKI, j. 24/11/2016; STF, AI 798396, Relator Min. GILMAR MENDES, j. 25/10/2010.

[12] MOREIRA, Fernando. Acidentes envolvendo carros Tesla em piloto automático já mataram 17 nos EUA. **Extra**, 12 jun. 2023. Disponível em: https://extra.globo.com/blogs/page-not-found/post/2023/06/acidentes-envolvendo-carros-tesla-em-piloto-automatico-ja-mataram-17-nos-eua.ghtml>. Acesso em: 23 maio 2024.

Por mais que esses sistemas ajam com uma autonomia jamais vista, seja por meio de modelos de *machine learning* ou mesmo *deep learning*, a atuação da IA é parte de uma exploração econômica ou prestação de serviço prestado por alguém, pessoa física ou jurídica, e de direito público ou privado.

O que se quer demonstrar é que, *por ora*, o maior ou menor grau de autonomia da máquina não tem o condão de modificar o enquadramento jurídico respectivo, já que ela foi desenvolvida ou explorada *por alguém*, *para alguma finalidade específica*.

A título de exemplo, temos a complexa avaliação da responsabilidade civil do médico, que, com suas inúmeras nuances, exige uma profunda análise de cada caso concreto[13]. O fato de um sistema de inteligência artificial ser utilizado para auxílio no diagnóstico ou no tratamento não altera, por si só, a incidência das normas que regem a responsabilidade civil subjetiva e objetiva. Em muitas situações, inclusive, o próprio médico ou hospital podem se voltar contra as empresas que comercializam essas máquinas, caso elas venham a apontar diagnósticos ou tratamento equivocados.

Vale lembrar que, há muitos anos, cirurgias automatizadas já vêm sendo utilizadas em larga escala, mormente para tratamento de moléstias oculares[14]. Consequentemente, pedidos de indenização vêm sendo ajuizados por eventuais falhas que causam danos aos pacientes[15]. A análise da máquina ou do sistema utilizado certamente será levada em conta pelo julgador na apreciação da natureza subjetiva ou objetiva da responsabilidade civil. O maior ou menor grau de automação da máquina não parece atenuar, todavia, a responsabilidade das respectivas empresas exploradoras.

Outro exemplo de grande impacto ocorrido com empresa a Post Office, que explora os Correios, na Inglaterra, merece uma descrição mais pormenorizada. Em 1999, essa empresa comprou um *software*, de nome Horizon, desenvolvido pela Fujitsu, para fazer a contabilidade unificada de suas treze mil agências, a maioria operada por franqueados. Todavia, o sistema começou a apresentar algumas falhas, tais como o congelamento da tela ao registrar um pagamento. Para tentar equacionar o problema, o usuário acabava por pressionar a tecla *enter*. Todavia, quando isso ocorria, e sem o sistema informar ou alertar de qualquer modo, o *software* contabilizava cada aperto da tecla como um novo pagamento recebido, que não havia ocorrido de fato. A somatória desses erros acabou levando a discrepâncias contábeis entre o caixa dos franqueados e a contabilidade centralizada dos correios. Como resultado, mais de 900 franqueados foram condenados por furto, estelionato e fraude, alguns com pena de prisão. O defeito no sistema como causa de todo o problema só foi

[13] Para aprofundamento: BONNA, Alexandre Pereira; SÁ, Victória Vasconcelos. Responsabilidade civil do médico por erros ocasionados no uso da inteligência artificial. **Revista Brasileira de Direito Civil em Perspectiva**, v. 7, n. 1, jan./jul. 2021.

[14] Disponível em: https://en.wikipedia.org/wiki/LASIK>. Acesso em: 23 maio 2024.

[15] TJMG. Apelação Cível 1.0000.21.053156-2/001, Relator Des. Fernando Caldeira Brant, j. 04/08/2021

descoberto após 16 anos. É intuitivo concluir que diversos danos já haviam sido causados em larga escala[16].

Uma situação dessas no Brasil atrairia a aplicação do artigo 37, § 6º, da Constituição Federal, em relação aos franqueados, sem prejuízo do posterior direito de regresso que a empresa prestadora de serviço público teria contra a empresa que forneceu o *software* defeituoso. Seria caso de responsabilidade nitidamente objetiva em ambos os casos, seja pela atuação estatal, seja pelo cumprimento contratual defeituoso.

Esse exemplo não trata de hipótese absolutamente estranha no direito brasileiro, já que, mais recentemente, a Controladoria Geral da União disponibilizou aos Estados e Municípios o sistema "Alice", que utiliza técnicas de mineração de textos e inteligência artificial para identificação de licitações com suspeitas de irregularidades"[17]. Por mais eficiente que o sistema seja, parece-nos que uma identificação equivocada de "atitude suspeita" poderá gerar danos a possíveis licitantes, com possibilidade de incidência do § 6º do artigo 37 da Constituição Federal. Nada impede que órgãos de controle se valham de sistemas automatizados e IA para cumprimento de suas obrigações institucionais. Mas responderão objetivamente por danos causados pelas respectivas falhas.

No âmbito do transporte aéreo, vale rememorar dois acidentes aéreos ocorridos em 2018 e 2019 com aviões Boeing 737 MAX 8 por falha técnica em sistema automatizado denominado Sistema de Aumento de Características de Manobra (MCAS), que entrou em funcionamento automaticamente por uma falha de sensores da aeronave, levando-a a mergulhar para o chão logo após a decolagem, nos dois casos[18], matando todos os passageiros e tripulantes a bordo, num total de 346 vidas humanas. A propósito, já existem trabalhos acadêmicos avaliando o impacto da crescente automação na operação das aeronaves que, se por um lado trazem, em regra, mais segurança e eficiência nas operações aéreas, acabam, de modo excepcional e isolado, também sendo a causa de acidentes, pelo fato de os pilotos dependerem demasiadamente da automação e tenderem a cometer erros durante situações de emergência que obriguem a assumir os controles de voo manualmente[19].

---

[16] LEMOS, Ronaldo. Fé na tecnologia pode virar prisão. **Folha de S. Paulo**, 31 mar. 2024. Disponível em: https://www1.folha.uol.com.br/colunas/ronaldolemos/2024/03/fe-na-tecnologia-pode-virar-prisao.shtml>. Acesso em: 01 abr. 2024; BRITISH Post Office scandal. Wikipedia. Disponível em: https://en.wikipedia.org/wiki/British_Post_Office_scandal>. Acesso em: 01 abr. 2024.

[17] CGU disponibiliza ferramenta Alice para estados e municípios identificarem licitações com suspeitas de irregularidades. **Controladoria-Geral da União**, 15 maio 2024. Disponível em: https://www.gov.br/cgu/pt-br/assuntos/noticias/2024/05/cgu-disponibiliza-ferramenta-alice-para-estados-e-municipios-identificarem-licitacoes-com-suspeitas-de-irregularidades>. Acesso em: 15 maio 2024.

[18] BOEING 737 MAX 8: o que é o MCAS, o software no centro da tragédia da Ethiopian Airlines. **BBC News**, 14 mar. 2019. Disponível em: https://www.bbc.com/portuguese/internacional-47564737>. Acesso em: 23 maio 2024.

[19] SCUDELER, Yuri Gazzi. **A automação das aeronaves e seu impacto na proficiência técnica dos pilotos**. Monografia (Trabalho de Conclusão de Curso) – Ciências Aeronáuticas da Universidade do Sul de Santa Catarina, 2023.

Trazendo essas questões para a presente análise jurídica, para o passageiro vitimado pouco importa se o acidente foi causado por imprudência do piloto, falha do sistema autônomo ou mesmo imperícia no manuseio dos sistemas da aeronave. Fato é que a empresa aérea deverá ser responsabilizada objetivamente pelos danos causados pelos acidentes, seja pela incidência do Código Brasileiro de Aeronáutica, pelo Código de Defesa do Consumidor ou mesmo pelo Código Civil[20].

Diante dos exemplos acima, verifica-se que, no âmbito específico da responsabilidade civil objetiva, os diplomas vigentes no Brasil asseguram proteção à vítima pelos danos sofridos. Os exemplos de sistemas que tenham causado danos a usuários ou terceiros encontram guarida na atual disciplina da responsabilidade civil objetiva no direito brasileiro.

Diferentemente do que ocorria no século XIX, não se vislumbra, até o presente momento, *discrimen* fático que justifique a modificação da estrutura normativa da responsabilização civil objetiva, valendo relembrar, novamente, que a presente análise não abrange o estudo da necessidade de outros sistemas de proteção jurídica em face do advento das novas tecnologias de inteligência artificial generativa.

Aliás, por essa razão, é o caso de discordar, ao menos por ora, da conclusão contida na Resolução de 16 de fevereiro de 2017 do Parlamento Europeu[21], já que, como visto, a existência de vários intervenientes na cadeia produtiva (o fabricante, o operador, o proprietário, o utilizador) é uma das razões que levou à eliminação do elemento "culpa", de modo a ampliar a proteção jurídica da vítima do evento.

Afinal, como aponta Gustavo Tepedino e Rodrigo da Guia Silva, "em vez de buscar – muitas vezes irrefletida – novas soluções e novos diplomas legais, melhores resultados se haverão de alcançar pelo esforço de releitura dos institutos já conhecidos pela civilística"[22].

[20] BRASIL. Superior Tribunal de Justiça. **REsp n. 1.984.282/SP**, relator Ministro Luis Felipe Salomão. Brasília, DF: STJ, 16 ago. 2022.

[21] "AB. Considerando que, quanto mais autónomos os robôs são, menos podem ser encarados como sendo simples instrumentos nas mãos de outros intervenientes (como o fabricante, o operador, o proprietário, o utilizador etc.); que, por sua vez, tal coloca a questão de saber se as normas ordinárias em matéria de responsabilidade são suficientes ou se apelam a novos princípios e normas para clarificar a responsabilidade jurídica de vários intervenientes no que respeita à responsabilidade por atos e omissões dos robôs, sempre que a causa não possa ser atribuída a um interveniente humano específico e se os atos ou omissões dos robôs que causaram danos pudessem ter sido evitados." Disponível em: https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_PT.html. Acesso em: 29 maio 2024.

[22] TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Desafios da inteligência artificial em matéria de responsabilidade civil. **Revista Brasileira de Direito Civil – RBDCivil**, Belo Horizonte, v. 21, p. 61-86, jul./set. 2019.

2.2. *Responsabilização subjetiva – retrocesso injustificável*

Argumenta-se que a aplicação da responsabilidade objetiva aos danos causados por inteligência artificial pode não ser a abordagem legislativa mais conveniente para o desenvolvimento dos setores envolvidos.

Eduarda Chacon Rosas[23] assinala que a responsabilização objetiva acarreta diversos problemas: obstaculiza a pesquisa e o desenvolvimento em IA; cria empecilhos na implementação de tecnologias que beneficiam significativamente a sociedade, como nas áreas de saúde, educação e segurança pública; gera perda de competividade global em relação a mercados com normas mais flexíveis; cria desigualdades no mercado, já que as maiores empresas terão melhores condições do que as *startups* de se adaptar às exigências regulatórias, levando à concentração de mercado e redução da concorrência; e limita a capacidade de experimentar e testar novas ideias que são essenciais ao avanço tecnológico.

Os argumentos elencados podem ser sintetizados na ideia de que a imputação de responsabilidade objetiva para danos causados por IA poderia desincentivar a inovação e o desenvolvimento tecnológico, com perda de competitividade global. Empresas e desenvolvedores poderiam se ver expostos a riscos legais significativos simplesmente por implementar novas tecnologias, o que poderia levar a um ambiente de aversão ao risco. Isso seria particularmente prejudicial em um campo que depende fortemente de experimentação e evolução contínua.

Antes de analisar esses argumentos, é essencial apontar que o presente trabalho não trata do complexo tema da regulação de IA, mas apenas de um corte, referente ao enquadramento da responsabilidade civil objetiva ou subjetiva por danos causados pelos sistemas de IA. Esse esclarecimento se faz necessário em face da já apontada polêmica existente em face do Projeto de Lei nº 2338[24], de 2023, em curso no Senado Federal, que pretende regular o uso da inteligência artificial no país de modo abrangente, e não apenas sua responsabilidade civil.

---

[23] ROSAS, Eduarda Chacon. A responsabilidade civil e a inteligência artificial. **Jota**, 09 maio 2024. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/elas-no-jota/a-responsabilidade-civil-e-a-inteligencia-artificial>. Acesso em: 24 maio 2024. No mesmo sentido: "[...] a possibilidade de responsabilização, de um lado, poderá incentivar o desenvolvimento de bens e tecnologias mais seguros, claros e eficientes, mas, de outro, poderá acabar impactando negativamente as taxas de desenvolvimento de inovação e a adoção de novos negócios e tecnologias [...], o que seria nocivo para a sociedade de forma geral. Há, portanto, um delicado e importante equilíbrio de interesses a ser atingido". DE TEFFÉ, Chiara Spadaccini; MEDON, Filipe. Responsabilidade Civil e regulação de novas tecnologias: questões acerca da utilização de inteligência artificial na tomada de decisões empresariais. **REI – Revista de Estudos Institucionais**, v. 6, n. 1, 2020, p. 304.

[24] SENADO FEDERAL. **Projeto de Lei nº 2338, de 2023.** Dispõe sobre o uso da Inteligência Artificial. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 30 mar. 2026.

Como afirma Ronaldo Lemos[25] a respeito dessas discussões legislativas, referido projeto de lei carrega uma inspiração no modelo europeu, denominado *AI Act*[26], que prevê diversas obrigações às empresas e estipula uma gradação dos riscos envolvidos. Comentando o estudo publicado pelo Movimento Inovação Digital[27], o autor acrescenta, ainda, que cerca 95% do texto proposto cria obrigações ou estruturas burocráticas para as empresas.

A ponderação é necessária para chamar atenção para uma possível desconexão entre causa e consequência nas críticas à responsabilização objetiva.

Com efeito, os argumentos contrários à responsabilidade civil objetiva parecem mais direcionados ao possível excesso de obrigações constante das propostas legislativas apresentadas do que, propriamente, ao sistema de responsabilização civil hoje vigente no direito brasileiro, que já assegura, em regra, a proteção dos usuários pelo reconhecimento da responsabilidade objetiva, conforme exposto no capítulo anterior.

Como é cediço, o bem jurídico protegido pela responsabilidade civil é a segurança. A obrigação de pagar indenização é a consequência do descumprimento do dever de segurança. Tanto é que o próprio inciso I do artigo 6º do Código de Defesa do Consumidor assegura, como direito básico do consumidor, a proteção da vida, da saúde e da segurança.

Trata-se, pois, de obrigação regulatória imposta aos fornecedores de produtos e serviços que, de fato, acarretam ônus nas respectivas precificações. Todavia, é falacioso o argumento de que referido ônus implicaria num fator impeditivo de investimentos e inovações.

Ora – e já há muitas décadas –, a elaboração do cálculo empresarial deve contabilizar a estimativa do custo da segurança do produto ou serviço[28]:

> Para definir o preço dos produtos e serviços que fornece ao mercado, o empresário realiza um cálculo cada vez mais complexo, que compreende o preço dos seus insumos, a mão de obra, os tributos, a margem de lucro esperada e também as contingências. Parte desses custos pode ser objeto de

[25] LEMOS, Ronaldo. Brasil pode brilhar com inteligência artificial no G20: País precisa ir além de marco regulatório com inspiração clara no modelo europeu. **Folha de S.Paulo**, 12 maio 2024. Disponível em: https://www1.folha.uol.com.br/colunas/ronaldolemos/2024/05/brasil-pode-brilhar-com-inteligencia-artificial-no-g20.shtml>. Acesso em: 10 maio 2024.

[26] LEI da UE sobre IA: primeira regulamentação de inteligência artificial. **Parlamento Europeu**, 12 jun. 2023. Disponível em: https://www.europarl.europa.eu/topics/pt/article/20230601STO93804/lei-da-ue-sobre-ia-primeira-regulamentacao-de-inteligencia-artificial. Acesso em: 27 maio 2024.

[27] MID divulga Raio-X do substituto de regulação de IA (perfil dos artigos do PL 2.338/2023). **Movimento Inovação Digital** [*s. d.*]. Disponível em: https://movimentoinova.org.br/2024/05/08/mid-divulga-raio-x-do-do-substituto-de-regulacao-de-ia-perfil-dos-artigos-do-pl-2-338-2023/>. Acesso em: 27 maio 2024.

[28] COELHO, Fábio Ulhoa, **Curso de direito comercial, volume 1**: Direito Empresa. 22. ed. rev. e atual. São Paulo: Thomson Reuters Brasil, 2018.

> um cálculo matemático, sujeito a variáveis controladas quantitativamente. Outra parte, contudo, exige um cálculo menos preciso, mas ainda assim indispensável à preservação da margem de lucros. Nessa última categoria encontram-se as contingências, como greves prolongadas, quebra de safra, instabilizações políticas, acidentes etc. Estes fatos podem interferir de forma acentuada nas contas do empresário, reduzindo ou comprometendo sua lucratividade ou até mesmo levando-o à falência. Proponho chamar-se essa segunda modalidade de cálculo pelo nome "qualitativo", em referência às inúmeras variáveis não inteiramente controladas por quantificações.
>
> Nesse sentido, nota-se que algumas normas jurídicas representam, para o empresário, um importante elemento de custo. São desta natureza, por exemplo, grande parte das normas de direito do trabalho (excetuam-se as disciplinadoras de regimes especiais, como a do empregado doméstico), de direito tributário (quando relacionadas a tributos do interesse da empresa), de direito previdenciário (as referentes às contribuições do empregador e, também, às do empregado), ambiental, urbanístico e outros. Por evidente, também o direito comercial integra esse grupo de ramos jurídicos, cujas normas podem influir nos custos da empresa. Para facilitar o desenvolvimento da matéria, vou me referir a tais normas pela expressão "direito-custo". Qualquer alteração no direito-custo interfere, em diferentes medidas, com as contas dos empresários e, em decorrência, com o preço dos produtos e serviços oferecidos no mercado. Isto é, cada nova obrigação que se impõe ao empresário, de cunho fiscal, trabalhista, previdenciário, ambiental, urbanístico, contratual etc., representa aumento de custos para a atividade empresarial e aumento do preço dos produtos e serviços para os seus adquirentes e consumidores.

E prossegue, assinalando que o "cálculo empresarial é condição de preservação do lucro e este, por sua vez, é a alavanca das atividades econômicas no capitalismo."[29]

Sobre o tema específico da responsabilidade civil objetiva, calha transcrever integralmente o trecho abaixo:

> Direito-custo -
>
> a) Responsabilidade civil - *este é o tema que melhor exemplifica a aplicação das categorias aqui propostas de cálculo empresarial e direito-custo, notadamente quanto à discussão da natureza subjetiva ou objetiva de cada hipótese de responsabilização*. De tato, muitos acidentes podem ocorrer no ambiente empresarial (acidente de trânsito), ou mesmo em razão do consumo de bens industrializados ou de serviços (fornecimento perigoso ou defeituoso), e a imputação ao empresário da responsabilidade objetiva pela indenização dos prejuízos decorrentes importa a criação de um claro elemento de custo.

[29] Ibidem, p. 55.

> Assim, o empresário responde subjetivamente pelos acidentes de trânsito, quando o condutor do veículo da empresa é o responsável pelos danos. Isto é, a demonstração da culpa ou dolo do empresário como causa, mesmo remota, do acidente é condição para a sua responsabilização. Se o evento danoso decorre de culpa exclusiva do outro motorista envolvido no evento, caso fortuito ou força maior, o empresário não será responsável por indenizar os danos. A responsabilidade do empresário, no caso de acidente de trânsito, portanto, é subjetiva. *No entanto, ele responde independentemente de culpa pelos danos derivados de acidente de consumo provocados por defeitos em produto ou serviço (CDC, arts. 12 e 14).*
>
> *Nessa hipótese, a sua responsabilidade é objetiva, quer dizer, existe mesmo que ele tenha dotado sua empresa da mais avançada tecnologia de produção e observe os mais rigorosos padrões de controle de qualidade*[30].

E, assim, arremata com precisão:

> Ao editar regra de responsabilidade objetiva, *o direito está criando um novo elemento de custo para o empresário. Para cumprir a lei sem sacrifício da lucratividade de seu empreendimento, ele deve procurar definir, por cálculos apropriados, a probabilidade da ocorrência de acidentes de consumo, bem como a provável dimensão de suas consequências econômicas*. Esses dados o empresário considera no cômputo dos preços de seus produtos ou serviços, repassando a cada consumidor uma quota-parte, por assim dizer, das repercussões previsíveis do fornecimento defeituoso. Em outros termos, *o empresário dilui, socializa entre os consumidores, realoca as perdas estimadas por acidente de consumo, reunindo recursos para atender à regra da responsabilidade civil independente de culpa (para uma discussão sobre os limites do* spreading of losses*, ver Calabresi, 1961). A operação prévia ao repasse das perdas por acidente de consumo para os próprios consumidores, mediante a fixação do preço dos produtos ou serviços vendidos, é viabilizada pelo cálculo empresarial*[31].

Em suma, e de acordo com o ordenamento jurídico vigente há décadas, o cálculo empresarial envolve a avaliação dos custos e benefícios associados a cada decisão que uma empresa pode tomar, identificando os riscos envolvidos em cada decisão, *incluindo riscos legais de responsabilização objetiva por qualquer produto ou serviço colocado no mercado*.

Não se pode descurar do que é mais relevante: o investimento em segurança de produtos e serviços no mercado não se trata de uma mera opção, ao contrário. Eliminar o fator segurança no cálculo empresarial implica em verdadeira fraude contábil, como assinala José de Aguiar Dias:

[30] Ibidem, p. 57, grifos nossos.

[31] Ibidem, p. 58, grifos nossos.

> *[...] as perdas e danos provenientes dos acidentes inevitáveis na exploração de uma empresa devem ser incluídos nas despesas do negócio. Imputar as perdas às vítimas dos acidentes é, sem nenhuma dúvida, falsear o balanço da empresa*. É a ideia de ADOLFO MERKEL, UNGER e RODOLFO MERKEL, que a reduziu a esta proposição: *quem desenvolve em seu próprio interesse uma atividade qualquer, deve sofrer as consequências dela provenientes*[32].

Ou seja, a responsabilidade civil objetiva exige que as empresas incorporem a segurança e a prevenção em seus cálculos empresariais. Isso resulta em uma maior atenção aos riscos associados aos produtos e serviços, promovendo investimentos que buscam minimizar esses riscos. A lógica desse fator econômico é de que o investimento em segurança deve ser menor que o custo do pagamento da indenização.

No que diz respeito à responsabilidade civil objetiva, o direito posto já estabelece um ambiente de previsibilidade e segurança jurídica, pois há décadas o mercado já conhece as consequências jurídicas de suas atividades, facilitando a precificação do risco no cálculo empresarial.

Nesse aspecto, partindo dessa premissa, qual seja, de que o simples apontamento da responsabilidade objetiva inibiria investimentos e inovação, cabe outra indagação, numa inversão de raciocínio: o direito vigente permite investimentos em inovação e tecnologia sem que o custo da segurança do produto ou serviço também seja contemplado nesse cálculo?

A resposta está com Rafael de Freitas Valle Dresch:

> a responsabilidade civil baseada na culpa dos agentes, na prática, significa inviabilizar – ou ao menos dificultar de maneira significativa – o ressarcimento dos danos causados às pessoas em virtude da dificuldade de prova de culpa num contexto marcado por tecnologia que avança exponencialmente[33].

A responsabilidade civil subjetiva aplicada apenas para o setor de tecnologia que aplique a inteligência artificial significa, na prática, trazer uma exceção à regra empresarial da responsabilização objetiva, que só terá um efeito: a desproteção das vítimas e a criação de um cenário de desconfiança.

---

[32] Ibidem, p. 53-54, grifos nossos.

[33] DRESCH, Rafael De Freitas Valle. A responsabilidade civil e os produtos com inteligência artificial. **Migalhas**, 23 dez. 2021. Disponível em: https://www.migalhas.com.br/coluna/licoes-filosoficas-do-direito-privado/357083/a-responsabilidade-civil-e-os-produtos-com-inteligencia-artificial>. Acesso em: 23 maio 2024.

2.3. Desnecessidade de regulação urgente – estado da arte em formação

De acordo com o direito posto, no que diz respeito ao aspecto específico da responsabilidade civil, parece-nos induvidoso que as vítimas de eventuais danos causados por IA se encontram protegidas pelo ordenamento em vigor, já que dispensadas da prova da culpa.

Ademais, de acordo com a evolução do instituto da responsabilidade civil objetiva e os fatos históricos relacionados, não há nenhuma lógica no afrouxamento do rigor das regras hoje vigentes em favor de um suposto fomento aos investimentos.

Estabelecidas tais premissas, cabe avaliar se a estruturação normativa da responsabilidade civil, tal como disciplinada no direito brasileiro, demanda atualização e aperfeiçoamento, diante do advento dessa nova realidade tecnológica. Em outras palavras, há necessidade de estabelecer um maior detalhamento casuístico legislativo na proteção das vítimas que sofrem danos causados por sistemas de IA no presente momento?

A discussão se aproxima do complexo tema da **análise de impacto legislativo** (AIL), que muito embora venha sendo objeto de acalorada discussão no âmbito acadêmico, está longe de ser uma realidade na rotina da produção legislativa brasileira. Segundo Victor Marcel Pinheiro, um dos fatores que dificultam a implementação da AIL no Brasil é termos "uma cultura de elaboração legislativa ainda fundada em uma visão voluntarista do exercício do poder político." [34]

Inexistindo AIL sistematizada na produção legislativa nacional, resta, pois, tentar avaliar esses impactos examinando as discussões legislativas mais relevantes sobre o tema no Congresso Nacional.

Com efeito, o PL 21/20, que cuida de estabelecer princípios, direitos e deveres para o uso de inteligência artificial no Brasil, foi aprovado na Câmara dos Deputados em regime de urgência em 2021, após cerca de apenas três meses de tramitação, o que acabou gerando muitas críticas devido à ausência de tempo hábil para discussão com a sociedade[35], além das polêmicas já descritas no Capítulo I acerca da responsabilidade civil ser objetiva ou subjetiva.

Ao receber o PL da Câmara, em 30 de março de 2022, o Senado Federal instituiu uma Comissão de Juristas (CJSUBIA) para elaboração de um projeto substitutivo

[34] "[...] no âmbito dos países membros da OCDE (Organização para a Cooperação e Desenvolvimento Econômico) a realização de AIR sobre projetos de lei (aqui denominada de AIL) já é realidade há muitos anos. Atualmente, todos os países que pertencem a essa organização e a União Europeia exigem a AIL para os projetos de lei mais relevantes apresentados perante os parlamentos nacionais". PINHEIRO, Victor Marcel. Por que a análise de impacto legislativo ainda não é realidade no Brasil? **Conjur**, 18 out. 2022. Disponível em: https://www.conjur.com.br/2022-out-18/fabrica-leis-analise-impacto-legislativo-nao-realidade-pais/>. Acesso em: 29 maio 2024.

[35] MARCO Legal da Inteligência Artificial no Brasil (PL 2338/2023). **Opice Blum**, 5 maio 2023. Disponível em: https://opiceblum.com.br/marco-legal-da-inteligencia-artificial-no-brasil-pl-2338-2023/>. Acesso em: 15 nov. 2023.

para regulamentação da IA[36]. Após diversas audiências públicas e consulta a mais de cinquenta especialistas de diversos setores, a CJSUBIA elaborou, em maio de 2023, extenso relatório final de conclusão dos trabalhos da comissão, acompanhado do texto de anteprojeto de lei que foi convertido no PL nº 2338/2023, apresentado pelo Senador Rodrigo Pacheco, Presidente do Senado Federal, com previsão de responsabilidade objetiva para os sistemas de alto risco ou risco excessivo e de culpa presumida para os demais modelos de IA[37]. Na prática, nada muito diferente do que estabelecem as leis em vigor.

Em seguida, o senador Marcos Pontes apresentou emenda substitutiva ao PL 2338/2023, modificando substancialmente o texto anterior, propondo que o enquadramento da hipótese de responsabilidade civil dependeria do respectivo nível de risco e seria distribuída de acordo com o tipo de agente envolvido, exigindo a demonstração de uma complexa cadeia de partícipes[38].

Finalmente, em 24 de abril de 2024 foi divulgado relatório preliminar substitutivo ao PL nº 2338/2023, de relatoria do senador Eduardo Gomes, elaborado pela Comissão Temporária Interna Sobre Inteligência Artificial no Brasil (CTIA)[39], presidida pelo senador Carlos Viana, que propôs o retorno ao regime da responsabilidade civil objetiva para os sistemas de risco alto ou excessivo, e da culpa presumida, para os demais[40].

Vale acrescentar que, durante o curso das discussões legislativas, o ChatGPT foi lançado mundialmente em novembro de 2022 pela empresa norte-americana OpenAI, que, aplicando o conceito de IA generativa, anunciou ser capaz de gerar respostas conversacionais coerentes e relevantes associadas a uma ampla variedade de assuntos, além da possibilidade de gerar textos, imagens e músicas inéditos.

O impacto midiático decorrente do anúncio do ChatGPT e a mera expectativa de transformação profunda na sociedade potencializou ainda mais o já existente

[36] SENADO FEDERAL. **Ato do Presidente do Senado Federal n° 4, de 2022**. Institui Comissão de Juristas responsável por subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei nº 5.051, de 2019, 21, de 2020, e 872, de 2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil. Brasília, DF: Senado Federal, 2022. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/152136>. Acesso em: 31 mar. 2026.

[37] Op. cit.

[38] SENADO FEDERAL. **Substitutivo ao projeto de Lei 2.338/2023**. Gabinete do Senador Astronauta Marcos Pontes. Brasília, DF: Senado Federal, 2023 Disponível em: https://legis.senado.leg.br/sdleggetter/documento?dm=9514745&ts=1702407086758&disposition=inline>. Acesso em: 29 maio 2024.

[39] SENADO FEDERAL. **Comissão Temporária Interna sobre Inteligência Artificial no Brasil**. Disponível em: https://legis.senado.leg.br/comissoes/comissao?codcol=2629>. Acesso em: 31 mar. 2026.

[40] SENADO FEDERAL. Comissão Temporária Interna sobre Inteligência Artificial no Brasil. **Texto Preliminar – Senador Eduardo Gomes.** Disponível em: https://legis.senado.leg.br/comissoes/arquivos?ap=8139&codcol=2629>. Acesso em: 29 maio 2024.

debate global em torno dos projetos de regulação da tecnologia e dos impactos das novas tecnologias[41].

No momento de conclusão deste trabalho (junho de 2024), a única certeza que se tem é que o estado da arte da tecnologia de inteligência artificial generativa está longe de se consolidar, estando em pleno processo de transformação no campo da ciência.

Por essa razão, a velocidade das transformações tem sido de tal ordem que eventuais leis criadas nesse contexto podem se tornar rapidamente obsoletas e inadequadas para tratamento do problema, gerando ainda mais insegurança jurídica.

Ademais, a eficácia jurídica na regulação de qualquer tema exige um profundo conhecimento do problema que se está a regular. No caso da IA generativa, ocorre exatamente o contrário, ou seja, o cenário é de instabilidade e total assimetria de informação, tanto no aspecto técnico quanto no direcionamento da aplicação e utilização das novas tecnologias.

Cristina Godoy Bernardo de Oliveira critica a generalidade e a falta de ações estratégicas concretas nas atuais propostas, que muitas vezes apenas reiteram princípios já estabelecidos em leis existentes, e destaca a ausência de uma estrutura de governança robusta e multissetorial que poderia fornecer a base para uma regulamentação mais detalhada e adaptada aos desafios que a IA pode apresentar[42].

Conforme alerta Gustavo Tepedino:

> [...] não seria possível lidar com tantas e tão velozes inovações com base exclusivamente em regras codificadas ou estabelecidas em leis especiais. Isto porque a técnica regulamentar, por mais detalhada que seja, mostra-se insuficiente para solucionar problemas que, a cada dia, desafiam a imaginação do legislador e do magistrado[43].

Dessa forma, contrariamente ao que se espera de inovações legislativas – segurança jurídica e pacificação social – legislar em meio a um contexto de transformação tecnológica rápida e contínua pode gerar um quadro de maior imprevisibilidade e caos.

Assim, revela-se recomendável que o legislador adote uma abordagem cautelosa, acompanhando de perto os futuros desdobramentos, com a maior profundidade técnica possível.

---

[41] RÊGO, Vital do. **Aviso nº 251– GP/TCU**, de 12 de abril de 2024. Brasília, DF: TCU, 12 abr. 2024. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2989443&filename=Tramitacao-REQ%20251/2025%20CFFC>. Acesso em: 07 jun. 2024.

[42] DE OLIVEIRA, Cristina Godoy Bernardo. Desafios da regulação do digital e da inteligência artificial no Brasil. **Revista USP**, n. 135. out. 2022. Disponível em: https://www.revistas.usp.br/revusp/article/view/206257/189893>. Acesso em: 5 abr. 2024.

[43] TEPEDINO, Gustavo. As tecnologias e a renovação do Direito Civil. **OABRJ**, 12 jun. 2019. Disponível em: https://www.oabrj.org.br/colunistas/gustavo-tepedino/as-tecnologias-renovacao-direito-civil>. Acesso em: 29 maio 2024.

Por essa razão, revelou-se oportuna a fala do Senador Eduardo Gomes, atual relator do nº PL 2338/2023:

> A CTIA apresentou seu relatório preliminar sobre diversos Projetos de Lei relacionados ao uso da Inteligência Artificial no Brasil. Com a presença de importantes figuras políticas e especialistas, destacaram-se pontos como a importância de uma regulação dinâmica e aberta ao diálogo, a necessidade de mitigar riscos sem inibir a inovação e a perspectiva de um campo fértil para o desenvolvimento da IA no país.
>
> O relatório preliminar propõe uma abordagem que mescla práticas de diferentes países e enfatiza *a proteção dos direitos dos cidadãos, sem urgência na regulamentação, mas sim na proteção desses direitos*.
>
> Agora, é momento de estudar e colaborar na construção da melhor regulação para o Brasil, visando governar a IA ao invés de sermos governados por ela. A expectativa é que a legislação seja sancionada durante a reunião de cúpula do G20, em novembro deste ano"[44].

Chiara Spadaccini de Teffé e Filipe Medon concordam, acrescentando que não existem dados, experiência e imaginação suficientes para prever quais os impactos associados a um determinado robô ou IA, o que prejudica, em parte, eventuais intervenções em termos normativos e regulatórios[45].

Devido à tecnologia ainda estar amadurecendo, não há a compreensão completa do objeto a ser regulado, sendo prematura a regulação no presente momento.

Todavia, se por um lado o cenário é de insegurança factual, de outro há razoável segurança jurídica no enfrentamento dos problemas apresentados até o presente momento. Sob a ótica da responsabilidade civil objetiva, possíveis vítimas de eventos causados por esses sistemas estão protegidas, como visto.

Assim, a prudência nas intervenções legislativas é a medida que melhor se impõe no presente momento, sem prejuízo do Estado buscar reduzir a assimetria de informação existente, estruturando-se tecnicamente para melhor acompanhar os desdobramentos das inovações tecnológicas, de modo a verificar, com consistência, os fatos que exigem aprimoramento legislativo.

3. CONCLUSÃO

Diante de todo o exposto, uma conclusão se chega: do ponto de vista da produção legislativa, o momento é de cautela.

[44] ARAÚJO, Janaína. Eduardo Gomes apresenta relatório preliminar sobre regulação da IA. **Senado Notícias**, 24 abr. 2024. Disponível em: https://www12.senado.leg.br/noticias/audios/2024/04/eduardo-gomes-apresenta-relatorio-preliminar-sobre-regulacao-da-ia>. Acesso em: 29 maio 2024.

[45] DE TEFFÉ, op. cit.

Muito embora seja legítima a preocupação com as consequências decorrentes dos avanços da IA, do ponto de vista da proteção das vítimas, a responsabilidade civil objetiva já é garantida pelos diplomas legais em vigor. O direito posto oferece um nível substancial de proteção e segurança aos cidadãos.

De outro lado, o ordenamento jurídico vigente já prevê a necessidade de integração dos custos de segurança no cálculo empresarial, inclusive na precificação dos produtos e serviços respectivos, obrigando as empresas a incorporar medidas de prevenção e segurança em seus processos de desenvolvimento e de produção. Longe de inibir investimentos, a manutenção deste *status* normativo promove um ambiente de previsibilidade, segurança jurídica e confiança. Pela lógica econômica, incentiva-se a segurança sem que isso implique em sacrificar investimentos e inovações tecnológicas.

Um bom exemplo histórico dessa realidade é facilmente verificável no setor aéreo, cuja Convenção para a Unificação de Certas Regras Relativas ao Transporte Aéreo Internacional, celebrada em Montreal, em 28 de maio de 1999[46], prevê a responsabilidade civil objetiva em caso de morte ou de lesão corporal de passageiro. Longe de "inibir investimentos", é fato que a cada ano que passa, as viagens aéreas tornam-se mais seguras[47,48], muito embora seja um dos setores de maior expansão no planeta.

Desse modo, do ponto de vista da segurança das possíveis vítimas e pelo que se conhece da IA até o presente momento, o arcabouço legal atual já oferece mecanismos eficazes para lidar com os potenciais riscos associados ao uso da IA.

Isso não significa que o aperfeiçoamento regulatório não seja necessário. Contudo, é essencial que essa regulação seja feita de maneira ponderada e informada, evitando-se uma rápida obsolescência das futuras normas, além dos transtornos decorrentes da respectiva aplicação dessas normas. Em outras palavras, sequer se sabe em que patamar está a IA nos dias atuais. O que se dirá do impacto da aplicação de regras jurídicas editadas especificamente para tratar dessa realidade ainda desconhecida?

---

[46] Ratificada no Brasil pelo Decreto Federal nº 5.910, de 27 de setembro de 2006: Artigo 17, item 1: "*O transportador é responsável pelo dano causado em caso de morte ou de lesão corporal de um passageiro, desde que o acidente que causou a morte ou a lesão haja ocorrido a bordo da aeronave ou durante quaisquer operações de embarque ou desembarque*." Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/decreto/d5910.htm>. Acesso em: 31 mar. 2026.

[47] "A taxa de acidentes fatais para grandes acidentes aéreos no transporte aéreo comercial [em 2023] é de 0,09 acidentes fatais por milhão de voos, em comparação com 0,10 por milhão em 2022. Esta é uma taxa de menos de um acidente fatal a cada quinze milhões de voos e é significativamente inferior à média de dez anos de 0,20 acidentes fatais por milhão de voos que observamos nos dados..."Disponível em: https://www.airway.com.br/seguranca-no-ar-2023-teve-apenas-dois-acidentes-fatais-com-aeronaves-comerciais/>. Acesso em: 6 jun. 2024.

[48] 2023 Safest Year for Flying By Several Parameters. **IATA**, 28 feb. 2024. Disponível em: https://www.iata.org/en/pressroom/2024-releases/2024-02-28-01/>. Acesso em: 6 jun. 2024.

Basta observar quão díspares têm sido o comportamento de diversos países como Estados Unidos, Reino Unido e União Europeia, entre outros, no que diz respeito à regulação da IA[49].

Segundo artigo publicado no *The New York Times*, reproduzido no jornal *Folha de S.Paulo*:

> Legisladores e reguladores em Bruxelas, Washington e em outros lugares estão perdendo a batalha para regular a IA e estão correndo para acompanhar, à medida que crescem as preocupações de que a poderosa tecnologia automatize empregos, acelere a disseminação de desinformação e eventualmente desenvolva seu próprio tipo de inteligência.
>
> As nações têm se movido rapidamente para lidar com os perigos potenciais da IA, mas os funcionários europeus foram pegos de surpresa pela evolução da tecnologia, enquanto os legisladores dos EUA admitem abertamente que mal entendem como ela funciona.
>
> [...]
>
> Na raiz das ações fragmentadas está uma incompatibilidade fundamental. *Os sistemas de IA estão avançando tão rapidamente e de forma imprevisível que legisladores e reguladores não conseguem acompanhar*.
>
> Essa lacuna tem sido agravada por um déficit de conhecimento em IA nos governos, burocracias labirínticas e medos de que muitas regras possam limitar, mesmo que sem querer, os benefícios da tecnologia.
>
> Mesmo na Europa, talvez o regulador de tecnologia mais agressivo do mundo, a IA tem confundido os formuladores de políticas[50].

André Zanatta Fernandes de Castro, Fernanda Mascarenhas Marques e Bernardo Fernandes Kauffman compartilham dessa preocupação, assinalando que a abordagem mais adequada é a que vem sendo adotada pelo Reino Unido, no sentido de aproveitar a estrutura jurídica vigente e capacitar reguladores para lidar com as dificuldades e oportunidades que surgem do desenvolvimento e da implementação da IA em seus respectivos setores. Dessa forma, permite-se a instituição mais segura

[49] DE CASTRO, André Zanatta Fernandes; MARQUES, Fernanda Mascarenhas; KAUFFMAN, Bernardo Fernandes. A regulamentação da IA nos EUA e no Reino Unido. **Jota**, 2 jun. 2024. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-regulamentacao-da-ia-nos-eua-e-no-reino-unido>. Acesso em: 31 mar. 2026.

[50] SATARIANO, Adam; KANG, Cecilia. Como os países estão perdendo a corrida para regulamentar a IA - Europa e EUA, alarmados com o poder da tecnologia, tentam encontrar uma resposta enquanto seu desenvolvimento acelera. **Folha de S. Paulo**, 6 dez. 2023. Disponível em: https://www1.folha.uol.com.br/tec/2023/12/como-os-paises-estao-perdendo-a-corrida-para-regulamentar-a-ia.shtml>. Acesso em: 4 jun. 2024.

de futuras regras que surjam de evidências e riscos especificamente identificados, não sanados pelo ordenamento jurídico vigente[51].

Diferentemente do que vem ocorrendo no Reino Unido, parte dos projetos apresentados no Congresso Nacional se inspiraram diretamente no modelo regulatório criado pela União Europeia (*EU Artificial Intelligence Act - AIA*[52]), que regulou minuciosamente o tema, fazendo uma meticulosa estruturação que prioriza a análise de riscos e obrigações de compliance. No entanto, a abrangência e o potencial de restrição colocam sérias e preocupantes dúvidas a respeito da capacidade de adaptação às rápidas evoluções tecnológicas e inovações futuras.

As diferentes vertentes desse debate já estão sendo colocadas à prova por diversos países. Uma boa lição de humildade é ter um pouco de paciência e aguardar como a situação se desenvolverá mundo afora. Enquanto isso, os entes estatais devem se instrumentalizar para reduzir ao máximo a assimetria de informação hoje existente, de modo a permitir um monitoramento do estado da arte, até para identificações de riscos reais que exijam uma regulação mais detida e específica em matéria de inteligência artificial.

REFERÊNCIAS BIBLIOGRÁFICAS

BOEING 737 MAX 8: o que é o MCAS, o software no centro da tragédia da Ethiopian Airlines. **BBC News**, 14 mar. 2019. Disponível em: https://www.bbc.com/portuguese/internacional-47564737. Acesso em: 23 maio 2024.

BONNA, Alexandre Pereira; SÁ, Victória Vasconcelos. Responsabilidade civil do médico por erros ocasionados no uso da inteligência artificial. **Revista Brasileira de Direito Civil em Perspectiva**, v. 7, p. 45-66, jan./jul. 2021. Disponível em: https://www.indexlaw.org/index.php/direitocivil/article/view/7754/pdf. Acesso em: 7 jun. 2024.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. Diário Oficial da União, 5 out. 1988.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União, 11 jan. 2002.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, 12 set. 1990.

BRASIL. **Lei nº 7.565, de 19 de dezembro de 1986**. Dispõe sobre o Código Brasileiro de Aeronáutica. Diário Oficial da União, 23 dez. 1986 e retificado 30 dez. 1986.

[51] DE CASTRO, op. cit.

[52] PARLAMENTO EUROPEU. **Relatório que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica**. 27 jan. 2017. Disponível em: https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_PT.html>. Acesso em: 29 maio 2024.

BRASIL. **Lei nº 6.453, de 17 de outubro de 1977**. Dispõe sobre a responsabilidade civil por danos nucleares e a responsabilidade criminal por atos relacionados com atividades nucleares e dá outras providências. Diário Oficial da União,18 out.1977.

BRASIL. **Lei nº 3.071, de 1º de janeiro de 1916**. Código Civil dos Estados Unidos do Brasil. Diário Oficial da União, 5 jan. 1916.

BRASIL. **Decreto nº 2.681, de 7 de dezembro de 1912**. Regula a responsabilidade civil das estradas de ferro. CLBR, 1912.

BRASIL. Superior Tribunal de Justiça. **REsp n. 1.984.282/SP**, relator Ministro Luis Felipe Salomão. Brasília, DF: STJ, 16 ago. 2022.

BRITISH Post Office scandal. **Wikipedia**. Disponível em: https://en.wikipedia.org/wiki/British_Post_Office_scandal. Acesso em: 01 abr. 2024.

CGU disponibiliza ferramenta Alice para estados e municípios identificarem licitações com suspeitas de irregularidades. **Controladoria-Geral da União**, 15 maio 2024. Disponível em: https://www.gov.br/cgu/pt-br/assuntos/noticias/2024/05/cgu-disponibiliza-ferramenta-alice-para-estados-e-municipios-identificarem-licitacoes-com-suspeitas-de-irregularidades. Acesso em: 15 maio 2024.

COELHO, Fábio Ulhoa, **Curso de direito comercial, volume 1**: Direito Empresa. 22. ed. rev. e atual. São Paulo: Thomson Reuters Brasil, 2018.

DE CASTRO, André Zanatta Fernandes; MARQUES, Fernanda Mascarenhas; KAUFFMAN, Bernardo Fernandes. A regulamentação da IA nos EUA e no Reino Unido. **Jota**, 2 jun. 2024. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-regulamentacao-da-ia-nos-eua-e-no-reino-unido. Acesso em: 31 mar. 2026.

DE OLIVEIRA, Cristina Godoy Bernardo. Desafios da regulação do digital e da inteligência artificial no Brasil. **Revista USP**, n. 135. out. 2022. Disponível em: https://www.revistas.usp.br/revusp/article/view/206257/189893. Acesso em: 5 abr. 2024.

DE TEFFÉ, Chiara Spadaccini; MEDON, Filipe. Responsabilidade Civil e regulação de novas tecnologias: questões acerca da utilização de inteligência artificial na tomada de decisões empresariais. **Revista Estudos Institucionais**, v. 6, n. 1, p. 301-333, jan./abr. 2020.

DIAS, José de Aguiar. **Da Responsabilidade Civil**. Rio de Janeiro: Forense, 1944.

DRESCH, Rafael De Freitas Valle. A responsabilidade civil e os produtos com inteligência artificial. **Migalhas**, 23 dez. 2021. Disponível em: https://www.migalhas.com.br/coluna/licoes-filosoficas-do-direito-privado/357083/a-responsabilidade-civil-e-os-produtos-com-inteligencia-artificial. Acesso em: 23 maio 2024.

GONÇALVES, Carlos Roberto. **Responsabilidade Civil**. 5. ed. São Paulo: Saraiva, 1994.

GONÇALVES, Carlos Roberto. **Comentários ao código civil**. São Paulo: Saraiva, 2003.

IRRESPONSABILIZAÇÃO generalizada. Especialistas criticam responsabilidade subjetiva prevista no PL do marco da IA. **Conjur**, 27 out. 2021. Disponível em: https://www.conjur.com.br/2021-out-27/especialistas-questionam-artigo-pl-marco-legal-ia/. Acesso em: 15 nov. 2023.

LEMOS, Ronaldo. Brasil pode brilhar com inteligência artificial no G20: País precisa ir além de marco regulatório com inspiração clara no modelo europeu. **Folha de S.Paulo**, 12 maio 2024. Disponível em: https://www1.folha.uol.com.br/colunas/ronaldolemos/2024/05/brasil-pode-brilhar-com-inteligencia-artificial-no-g20.shtml. Acesso em: 10 maio 2024.

LEMOS, Ronaldo. Fé na tecnologia pode virar prisão: Inteligência artificial é software como qualquer outro; não se pode confiar nela sem questionamentos. **Folha de S. Paulo**.

31 mar. 2024. Disponível em: https://www1.folha.uol.com.br/colunas/ronaldolemos/2024/03/fe-na-tecnologia-pode-virar-prisao.shtml. Acesso em: 1 abr. 2024.

MARCO Legal da Inteligência Artificial: ponderações sobre a responsabilidade civil. **Conjur,** 22 fev. 2022. Disponível em: https://www.conjur.com.br/2022-fev-22/opiniao-marco-inteligencia-artificial-responsabilidade-civil/. Acesso em: 15 nov. 2023.

MARCO Legal da Inteligência Artificial no Brasil (PL 2338/2023). **Opice Blum**, 5 maio 2023. Disponível em: https://opiceblum.com.br/marco-legal-da-inteligencia-artificial-no-brasil-pl-2338-2023/. Acesso em: 15 nov. 2023.

"MEDO, frustrado e constrangido", diz homemdetido por engano em estádio após erro do sistema de reconhecimento facial. **Fantástico**, 21 abr. 2024. Disponível em: https://g1.globo.com/fantastico/noticia/2024/04/21/medo-frustrado-e-constrangido-diz-homem-detido-por-engano-em-estadio-apos-erro-do-sistema-de-reconhecimento-facial.ghtml. Acesso em: 23 maio 2024.

MID divulga Raio-X do substituto de regulação de IA (perfil dos artigos do PL 2.338/2023). **Movimento Inovação Digital** [s. d.]. Disponível em: https://movimentoinova.org.br/2024/05/08/mid-divulga-raio-x-do-do-substituto-de-regulacao-de-ia-perfil-dos-artigos-do-pl-2-338-2023/. Acesso em: 27 maio 2024.

MOREIRA, Fernando. Acidentes envolvendo carros Tesla em piloto automático já mataram 17 nos EUA. **Extra**, 12 jun. 2023. Disponível em: https://extra.globo.com/blogs/page-not-found/post/2023/06/acidentes-envolvendo-carros-tesla-em-piloto-automatico-ja-mataram-17-nos-eua.ghtml. Acesso em: 23 maio 2024.

PARLAMENTO EUROPEU. **Lei da UE sobre IA: primeira regulamentação de inteligência artificial**. 12 jun. 2023. Disponível em: https://www.europarl.europa.eu/topics/pt/article/20230601STO93804/lei-da-ue-sobre-ia-primeira-regulamentacao-de-inteligencia-artificial. Acesso em: 27 maio 2024.

PARLAMENTO EUROPEU. **Relatório que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica**. 27 jan. 2017. Disponível em: https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_PT.html. Acesso em: 29 maio 2024.

PARLAMENTO EUROPEU. **Regulamento (UE) 2024 que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828** (Regulamento da Inteligência Artificial). Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_PT.pdf. Acesso em: 6 jun. 2024.

PINHEIRO, Victor Marcel. Fábrica de leis. Por que a análise de impacto legislativo ainda não é realidade no Brasil? **Conjur**, 18 out. 2022. Disponível em: https://www.conjur.com.br/2022-out-18/fabrica-leis-analise-impacto-legislativo-nao-realidade-pais/. Acesso em: 29 maio 2024.

ROSAS, Eduarda Chacon. A responsabilidade civil e a inteligência artificial. **Jota**, 9 maio 2024. Disponível em: https://beta.jota.info/noticia/a-responsabilidade-civil-e-a-inteligencia-artificial. Acesso em: 7 jun. 2024.

SATARIANO, Adam; KANG, Cecilia. Como os países estão perdendo a corrida para regulamentar a IA - Europa e EUA, alarmados com o poder da tecnologia, tentam encontrar uma resposta enquanto seu desenvolvimento acelera. **Folha de S. Paulo**, 6 dez. 2023. Disponível em: https://www1.folha.uol.com.br/tec/2023/12/como-os-paises-estao-perdendo-a-corrida-para-regulamentar-a-ia.shtml. Acesso em: 4 jun. 2024.

SCUDELER, Yuri Gazzi. **A automação das aeronaves e seu impacto na proficiência técnica dos pilotos**. Monografia (Trabalho de Conclusão de Curso) – Ciências Aeronáuticas da Universidade do Sul de Santa Catarina, 2023.

SENADO FEDERAL. **Ato do Presidente do Senado Federal n° 4, de 2022**. Institui Comissão de Juristas responsável por subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei nº 5.051, de 2019, 21, de 2020, e 872, de 2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/152136. Acesso em: 7 jun. 2024.

SENADO FEDERAL. **Comissão Temporária Interna sobre Inteligência Artificial no Brasil**. Disponível em: https://legis.senado.leg.br/comissoes/comissao?codcol=2629. Acesso em: 31 mar. 2026.

SENADO FEDERAL. CTIA. **Texto Preliminar – Senador Eduardo Gomes**. Disponível em: https://legis.senado.leg.br/comissoes/arquivos?ap=8139&codcol=2629. Acesso em: 29 maio 2024.

SENADO FEDERAL. **Projeto de Lei nº 2338, de 2023**. Dispõe sobre o uso da Inteligência Artificial. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 30 mar. 2026.

SENADO FEDERAL. **Substitutivo ao projeto de Lei 2.338/2023**. Gabinete do Senador Astronauta Marcos Pontes. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9514745&ts=1702407086758&disposition=inline. Acesso em: 29 maio 2024.

TAJRA, Alex. Vigiar e punir: Ainda sem regulação, estados prendem centenas de pessoas utilizando reconhecimento facial. **Conjur**, 17 maio 2024. Disponível em https://www.conjur.com.br/2024-mai-17/sem-regulacao-estados-prendem-centenas-utilizando-reconhecimento-facial/. Acesso em: 23 maio 2024.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Desafios da inteligência artificial em matéria de responsabilidade civil. **Revista Brasileira de Direito Civil – RBDCivil**, Belo Horizonte, v. 21, p. 61-86, jul./set. 2019.

TEPEDINO, Gustavo. As tecnologias e a renovação do Direito Civil. **OABRJ**, 12 jun. 20219. Disponível em: https://www.oabrj.org.br/colunistas/gustavo-tepedino/as-tecnologias-renovacao-direito-civil. Acesso em: 29 maio 2024.

TRIBUNAL DE CONTAS DA UNIÃO. **Riscos da Regulação da Inteligência Artificial no Brasil**. Possíveis Impactos na Estratégia Brasileira de Inteligência Artificial (Ebia). Aviso nº 251 – GP/TCU, de 12 de abril de 2024. Disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=9596181&ts=1715114416263&disposition=inline. Acesso em: 7 jun. 2024.

Submetido em: 07/01/2025
*Aprovado em:*18/07/2025

O PENSAMENTO HUMANO NO CONTEXTO DA INFÂNCIA E ADOLESCÊNCIA: REFLEXÕES JURÍDICAS E TECNOLÓGICAS

Human Thought in the Context of Childhood and Adolescence: Legal and Technological Reflections

Fernanda Papassoni dos Santos[1]

SUMÁRIO 1. Introdução; 2. Criação de mecanismos jurídicos para proteção mental da criança e do adolescente; 2.1 Iniciativa brasileira à luz da Declaração da Organização dos Estados Americanos (2023); Princípios 4 e 9 da Declaração da Organização dos Estados Americanos; 3. Conclusão; Referências Bibliográficas.

RESUMO O escopo do presente artigo é demonstrar a necessidade de criação de mecanismos legais para proteção jurídica da mente ante o potencial impacto dos avanços em tecnologia e inteligência artificial nas funções mental e cognitiva de crianças e adolescentes. A análise dos neurodireitos no contexto da infância e juventude terá como base a Declaração de Princípios Interamericanos sobre Neurociências, Neurotecnologias e Direitos humanos da Organização dos Estados Americanos (OEA). Os princípios ali elencados visam proteger os direitos fundamentais já consagrados de todo cidadão, que poderiam ser afetados pela aplicação indiscriminada de inovações científico-tecnológicas, recomendando esforços na proteção de parcelas da sociedade com maior vulnerabilidade. Utilizaremos metodologia expositiva, de modo a comparar a situação jurídica brasileira com o paradigma da Declaração da OEA. Como resultado, opinaremos pela inclusão de proteção jurídica específica à mente humana como forma de cumprimento do dever do Estado e da Sociedade de proporcionar proteção prioritária e integral à criança e ao adolescente.

Palavras-chave: Neurodireitos. Neurotecnologia. Direitos humanos. Infância. Juventude.

ABSTRACT The scope of this article is to demonstrate the need to create legal mechanisms for the legal protection of the mind in the face of the potential impact of advances in technology and artificial intelligence on the mental and cognitive functions of children and adolescents. The analysis of neurorights in the context of children and youth will be based on the Declaration of Inter-American Principles on Neurosciences, Neurotechnologies, and Human Rights of the Organization of American States (OAS). The principles listed there aim to protect the already established fundamental rights of every citizen, which could be affected by the indiscriminate application of scientific-technological innovations, concentrating efforts on protecting the most vulnerable parts of society. As a result, we will opine for the inclusion of specific legal protection to the human mind as a way of fulfilling the duty of the State and Society to provide priority and comprehensive protection to children and adolescents.

Keywords: Neurorights. Neurotechnology. Human Rights. Childhood. Youth.

[1] Graduada em Direito pela Faculdade de Direito de Bauru – Instituição Toledo de Ensino (2010), com extensão em Gestão de Pessoas e Compliance Trabalhista pela Fundação Getulio Vargas – FGV (2019). Pós-graduada em Tecnologias Ferroviárias (MBI/SENAI, 2022) e em Direito Digital e Inovações Tecnológicas pela Escola Superior da PGE-SP (2024). Atua na Companhia Paulista de Trens Metropolitanos (CPTM), com experiência em contencioso cível e trabalhista.

DOI: 10.22491/respge.v16i1.1733

1. INTRODUÇÃO

O comportamento social e as relações homem-máquina mudaram significativamente ao longo dos anos e, em especial, nas últimas décadas, com advento e avanço das tecnologias aliadas à inteligência artificial. A capacidade de evolução destes mecanismos é imensurável, e empresas e pesquisadores trabalham de forma desenfreada para buscar soluções inovadoras que possam desvendar o mecanismo da mente humana.

É fato que as neurotecnologias possuem enorme potencial para promover bem-estar social melhorando significativamente a saúde e a qualidade de vida da população, uma vez que os estudos se dedicam, majoritariamente, a entender os processos para prevenção, cura ou tratamento de doenças mentais e neurológicas. Todavia, incluem dispositivos capazes de ler e modificar a atividade dos neurônios, levantando preocupações sobre os efeitos não regulamentados e os riscos para os direitos humanos, como a liberdade de pensamento e a integridade mental. Nesse sentido, tais inovações trazem consigo dilemas éticos, morais e sociais que precisarão ser plenamente abarcados pelo ordenamento jurídico, transcendendo a proteção já existente para dados pessoais.

Rafael Yuste, neurobiólogo e professor da Universidade de Columbia, afirma que "A privacidade máxima de uma pessoa é o que ela pensa, mas agora já começa a ser possível decifrar isso"[2]. Juntamente à sua equipe de pesquisa, divulgou estudos nos quais foi possível manipular o comportamento de roedores, intervindo diretamente no cérebro destes animais. "Pela primeira vez na história, estamos diante da possibilidade real de os pensamentos humanos serem decodificados ou manipulados por meio da tecnologia"[3].

Yuste sugere cinco aspectos para preservação e proteção mental, definindo como "Novos Direitos Humanos para a Era da Neurotecnologia". São eles: a privacidade mental, a identidade pessoal, o livre-arbítrio, a proteção contra vieses algorítmicos e o acesso igualitário à tecnologia.

Outro estudo que se aprofunda no desenvolvimento de soluções e equipamentos voltados ao monitoramento da atividade cerebral é o da Neuralink, empresa norte-americana. Nela, busca-se o desenvolvimento de um implante neural que tem como objetivo de monitorar e captar os sinais cerebrais da área implantada. As informações e os dados obtidos serão transmitidos para um computador, para que sejam processados e interpretados, desvendando a intenção de movimento da

[2] YUSTE, Rafael et al. Four ethical priorities for neurotechnologies and AI. **Nature**, n. 551, p. 159-163, 2017. Disponível em: https://www.nature.com/articles/551159a. Acesso em: 30 jan. 2024.

[3] YUSTE, Rafael. "La privacidad máxima de una persona es lo que piensa": el neurocientífico que impulsa los 'neuroderechos'. **El País**, 2019. Disponível em: https://elpais.com/ciencia/2019/11/05/actualidad/1572948777_301315.html. Acesso em: 22 abr. 2026.

pessoa. A empresa afirma que o intuito é fazer com que pessoas com lesões neurológicas, medular ou que sofram de esclerose lateral amiotrófica (ELA), por exemplo, possam voltar a ter movimentos nos membros afetados. Em 30 de janeiro de 2024, a empresa divulgou a realização do primeiro implante do *chip* sem fio, Telepathy, em um cérebro humano[4].

Como podemos observar, estamos diante de uma realidade presente, não futura. Assim, não se olvida a necessidade de prevenção e antecipação dos órgãos legislativos para enfrentar os desafios éticos, legais e sociais fomentados com as inovações em neurotecnologia.

> From an international governance approach, UNESCO has proved that intergovernmental organizations are already playing a valuable role in addressing this need for clarification and in urging their Member States to grant protection in their legislations to emerging new forms of violations of fundamental rights. This can be inferred from the International Bioethics Committee (IBC) recommendations to States included in the Report of the International Bioethics Committee of UNESCO (IBC) on the ethical issues of neurotechnology, 15 December 2021[5].

Um marco importante e que direciona este movimento foi a aprovação em 2023, no âmbito do Comitê Jurídico interamericano da Organização dos Estados Americanos (OEA), da Declaração Interamericana de Princípios sobre Neurociências, Neurotecnologias e Direitos Humanos, demonstrando o compromisso com a proteção dos direitos individuais face aos avanços tecnológicos[6].

Na América do Sul, o Chile foi pioneiro na inclusão da proteção à integridade mental em sua Constituição. Na regulamentação, o artigo 19 da Constituição Política da República, foi alterado para constar que:

> El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización

[4] JACKSON, Patrick. Como funciona o Telepathy, chip cerebral que Elon Musk diz ter sido implantado em uma pessoa. **BBC News**, 30 jan. 2024. Disponível em: https://www.bbc.com/portuguese/articles/cd182g1gp27o. Acesso em: 31 mar. 2026.

[5] "A partir de uma abordagem de governança internacional, a UNESCO provou que as organizações intergovernamentais já estão desempenhando um papel valioso ao abordar essa necessidade de esclarecimento e ao instar seus Estados-Membros a conceder proteção em suas legislações a novas formas emergentes de violações de direitos fundamentais. Isso pode ser inferido das recomendações do Comitê Internacional de Bioética (IBC) aos Estados incluídos no Relatório do Comitê Internacional de Bioética da UNESCO (IBC) sobre as questões éticas da neurotecnologia, 15 de dezembro de 2021." (GULLOTA, p. 27., tradução nossa)

[6] OECD. **Recommendation on Responsible Innovation in Neurotechnology**. Disponível em: https://www.oecd.org/science/recommendation-on-responsible-innovation-in-neurotechnology.htm. Acesso em: 31 mar. 2026.

> en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella. (LEY CHILE - LEY 21383)[7]

Recentemente, com fundamento na alteração legislativa, a Suprema Corte do país proferiu decisão histórica contra a empresa de neurotecnologia Emotiv por violação da privacidade mental, processo sob o nº 105.065-2023. Guido Girardi, ex-senador, processou a empresa Emotiv alegando o não consentimento com a captura de dados pelo dispositivo "Insigth", além do desconhecimento sobre o armazenamento e utilização desses dados cerebrais. Em julgamento, o tribunal determinou a remoção dos neurodados de Guido Girardi tanto de seus portais quanto do armazenamento em nuvem[8].

O Brasil segue o caminho chileno. Em 13 de junho de 2023, foi apresentada a Proposta de Emenda Complementar nº 29, que propõe a preservação da integridade mental e a transparência algorítmica dentre os direitos e garantias fundamentais previstos no Artigo 5º da Constituição Federal. No momento, aguarda a designação de relator na Comissão de Constituição, Justiça e Cidadania[9].

Em âmbito estadual, destaca-se a Proposta de Emenda Complementar 298, de 2023, aprovada e promulgada em 20 de dezembro de 2023, que alterou o parágrafo único do artigo 235 da Constituição do Estado do Rio Grande do Sul. A emenda instituiu a proteção da identidade mental contra qualquer pesquisa que afete o cérebro e sua atividade, sem o consentimento do indivíduo[10].

Nota-se, portanto, um forte movimento de protagonismo da América do Sul ao fomento dos neurodireitos, demonstrando um notável comprometimento com a coesão entre o estímulo à inovação e a proteção aos direitos dos indivíduos.

> This tremendous scientific progress must be fostered and supported and cannot be stopped. This is true even if the thought-provoking speakers who participated in the more ethical and legal panel from day two described the "dark side" of these technologies when applied to the human brain. Some of the reported risks, which are all the more serious when affecting children and adolescent brains still under development, are more conceptual and philosophical and relate to the capacity of neurotechnology to interfere with our humanness. The scientific community is called upon to make

[7] "O desenvolvimento científico e tecnológico estará a serviço das pessoas e se levará a cabo com respeito à vida e à integridade física e psíquica. A lei regulará os requisitos, condições e restrições para sua utilização nas pessoas, devendo resguardar especialmente a atividade cerebral, assim como as informações provenientes dela." (LEI CHILE – 21383, tradução nossa).

[8] CHILE. Corte Constitucional. Processo nº 105.065-2023, relatora Ministra Ángela.

[9] BRASIL. **Proposta de Emenda complementar nº 29, de 2023**. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/158095. Acesso em: 28 jan. 2024.

[10] BRASIL. **Constituição do Estado do Rio Grande do Sul**. Disponível em: https://www2.al.rs.gov.br/dal/LinkClick.aspx?fileticket=WQdIfqNoXO4%3d&tabid=3683&mid=5359. Acesso em: 28 jan. 2024.

> a continued effort to monitor and assess new advancements to prevent dehumanization from taking place in the name of efficiency/productivity[11].

A importância de uma governança eficaz é garantir que o avanço dessas tecnologias beneficie a sociedade, protegendo os indivíduos contra possíveis abusos.

E dentro deste universo, uma atenção especial deve ser voltada ao público infantojuvenil na condição de grupo vulnerável. Vulnerabilidade significa a capacidade do indivíduo ou do grupo social de decidir sobre sua situação de risco, estando diretamente associada a fatores individuais, familiares, culturais, sociais, políticos, econômicos e biológicos[12].

O sistema jurídico brasileiro possui importantes instrumentos garantidores de proteção à infância e à juventude como a Constituição Federal, o Estatuto da Criança e do Adolescente (ECA) e a Convenção sobre os Direitos da Criança. O princípio do melhor interesse norteia tais regramentos visando assegurar a fruição plena e efetiva de todos os direitos ali reconhecidos, bem como o desenvolvimento global da criança, de modo a garantir sua integridade física, moral e psicológica e a promover sua dignidade.

Esse conjunto normativo permeia a base para a recomendação de inclusão de proteção específica para os neurodireitos como um direito fundamental face à potencial utilização abusiva da tecnologia.

2. CRIAÇÃO DE MECANISMOS JURÍDICOS PARA PROTEÇÃO MENTAL DA CRIANÇA E DO ADOLESCENTE

De acordo com a Organização Mundial da Saúde (OMS), a fase de adolescência se encerra aos 20 anos incompletos. No Brasil, o ECA, em consonância com o Código Civil, dispõe como marco os 18 anos incompletos[13].

Do ponto de vista objetivo, para efeito de legislação e doutrina, é preciso definir uma data exata; no entanto, no seguimento deste artigo, não adentraremos neste mérito, até mesmo por não haver um consenso quanto à faixa etária em que esse desenvolvimento se dá por completo. Busca-se, neste capítulo, demonstrar a vulnerabilidade na exposição ao risco durante a fase infantojuvenil, que, independentemente

[11] "Este tremendo progresso científico deve ser fomentado e apoiado e não pode ser travado. Isso é verdade mesmo que os palestrantes instigantes que participaram do painel mais ético e legal do segundo dia tenham descrito o 'lado sombrio' dessas tecnologias quando aplicadas ao cérebro humano. Alguns dos riscos relatados, que são ainda mais graves quando afetam crianças e adolescentes cérebros ainda em desenvolvimento, são mais conceituais e filosóficos e se relacionam com a capacidade da neurotecnologia". GULLOTA, p. 27, tradução nossa.

[12] BRASIL. Ministério da Saúde. Secretaria de Atenção à Saúde. Área de Saúde do Adolescente e do Jovem. **Marco legal**: saúde, um direito de adolescentes. Brasília: Ministério da Saúde, 2007, p. 60. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/07_0400_M.pdf>. Acesso em: 30 maio 2024.

[13] Ibidem.

da idade final, é uma fase de crescimento, evolução, descobertas de formação biológica, psíquica e social e o potencial resultado que o uso de tecnologia tem no desenvolvimento cerebral deste público, sugere a necessidade e, principalmente, o dever de proteção por parte do Estado e da sociedade.

Eduardo Jorge da Silva, neuropediatra e coordenador da rede Ética, Saúde, Segurança e Educação Mundo Digital (ESSE), explica o efeito da tecnologia no neurodesenvolvimento de crianças e adolescentes. Segundo ele, a exposição deste grupo se dá em razão do desenvolvimento natural do cérebro humano. Nascemos com uma grande quantidade de neurônios que, com o passar do tempo, desaparecem. Esses neurônios se comunicam através de sinapses com um pico de produção entre oito e dez anos e na fase da adolescência são estas ligações que vão formar o indivíduo como cidadão. Além da questão genética, é preciso que o ambiente seja favorável a um desenvolvimento saudável. A criança e o adolescente precisam, dentre tantas coisas, ter experiências e estímulos sociais, pois são estes que farão a associação ao mundo real. Como exemplo, Eduardo menciona crianças que, durante a pandemia do coronavírus, não foram expostas ao meio social e desenvolveram comportamentos semelhantes aos do Transtorno do Espectro Autista (TEA), porém, quando inseridas no ambiente escolar, não mais apresentaram esses comportamentos[14].

Eduardo cita também que há evidências de que um fluxo constante de informações para as crianças e os adolescentes altera sua dinâmica cerebral. Fatores como o estresse, a necessidade e a exposição a conteúdos aumentam a produção dos hormônios cortisol e dopamina. O estímulo repetitivo induz o aumento da produção de dopamina no organismo, conhecido como hormônio da recompensa, necessitando cada vez mais de novos estímulos para produção. A mesma dinâmica funciona para a produção de cortisol. Isto significa que existem agentes químicos envolvidos neste processo de desenvolvimento.

Afirma, ainda, que há estudos comprovando que o uso excessivo de mídias provoca alterações nas ligações entre a substância branca e a substância cinza do cérebro, influenciando a dinâmica de sua formação, especialmente o lobo frontal, que é o responsável pela função comportamental e cognitiva. A empatia, a flexibilidade de entendimento, a regulação corporal, entre outros, está relacionada ao lobo frontal. No entanto, Eduardo ressalta que a tecnologia pode e deve ser uma aliada no processo de formação, entretanto o uso deve ser supervisionado.

A medicina indica, portanto, que o desenvolvimento completo do cérebro humano se dá apenas no início da fase adulta. Até este momento, o cérebro de crianças e adolescentes possui grande neuroplasticidade, ou seja, uma maior capacidade de reestruturação do sistema nervoso em resposta às mudanças externas. E é

[14] JUSTIÇA. Conselho Nacional. Webinário Saúde Mental e Demandas Judiciais: Ações necessárias (manhã). **YouTube**, 6 out. 2023. Disponível em: https://www.youtube.com/live/hKRt5tDPzXE?si=RmrZsprgmh0Zj8k4. Acesso em: 4 fev. 2024.

justamente este aspecto normal de desenvolvimento que o coloca o público infantil e de adolescentes em uma situação de vulnerabilidade.

Esta vulnerabilidade, além das questões físicas e naturais, está interrelacionada ainda à fragilidade e a dependência dos responsáveis legais, colocando-os em situações de submissão ao ambiente em que se encontram, expondo-os a uma variedade de riscos, desafios e refletindo a necessidade de uma abordagem múltipla para o amparo desta população.

Para a proteção e diminuição dessas vulnerabilidades, é essencial a implementação de políticas públicas eficazes, o que inclui uma legislação protetora dos direitos das crianças e adolescentes em sua integralidade e requer um esforço conjunto de governos, comunidades e famílias, sustentando um ambiente seguro, com suporte adequado para o desenvolvimento íntegro e saudável.

2.1 *Iniciativa brasileira à luz da Declaração da Organização dos Estados Americanos (2023)*

Através da Organização das Nações Unidas, a comunidade internacional, a partir de 1948, com a Declaração Universal dos Direitos Humanos, se uniu para firmar um compromisso: garantir a todos os indivíduos, sem distinção de qualquer natureza, direitos básicos para uma vida digna. Esse marco inicial deu origem a uma série de convenções internacionais, tecendo uma rede de cooperação e mecanismos de controle para assegurar o cumprimento desses direitos fundamentais.

Ao longo do tempo, o conteúdo inicial dos direitos humanos e seus instrumentos de proteção não ficaram estagnados. Em resposta às novas realidades sociais, a comunidade internacional caminhou para um processo contínuo de aprimoramento e expansão desses direitos. Diversos pactos, tanto genéricos quanto específicos, foram elaborados, sedimentando o reconhecimento de direitos universais nos planos individual, coletivo e social.

Um dos exemplos dessa evolução é a consagração do direito à saúde e da proteção especial da criança em 1966 com a consolidação dos direitos humanos ao aprovar dois instrumentos jurídicos fundamentais: o Pacto Internacional dos Direitos Civis e Políticos (PIDCP) e o Pacto Internacional dos Direitos Econômicos, Sociais e Culturais (PIDESC), conhecidos como Pactos de Nova York. Através desses pactos, as nações signatárias assumiram o compromisso de garantir e implementar esses direitos fundamentais, reconhecendo a importância da saúde e do bem-estar das crianças para o desenvolvimento pleno das sociedades, o que podemos depreender do artigo 24[15]:

[15] BRASIL, Ministério da Saúde, op. cit., p. 21-22.

> Art. 24 - 1. Toda criança terá direito, sem discriminação alguma por motivo de cor, sexo, língua, religião, origem nacional ou social, situação econômica ou nascimento, às medidas de proteção que a sua condição de menor requer por parte de sua família, da sociedade e do Estado.
>
> 2. Toda criança deverá ser registrada imediatamente após seu nascimento e deverá receber um nome.
>
> 3. Toda criança terá o direito de adquirir uma nacionalidade[16].

Ao contrário da Declaração Universal, os pactos são instrumentos juridicamente vinculativos para os Estados signatários, o que significa que eles são obrigados a implementar e respeitar os direitos neles previstos. O Brasil ratificou os Pactos de Nova York apenas em 1992 e 1994, respectivamente, reforçando a gama de instrumentos fundamentais para a defesa dos direitos humanos no país.

Antes disso, porém, a Constituição Federal do Brasil, em 1988, já instituía nos artigos 227 e 228 proteções específicas para crianças e adolescentes. Ali firmou-se a responsabilidade da família, da sociedade e do Estado em assegurar à criança e ao adolescente, 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 do dever de protegê-los de toda forma de negligência e violência.

Isso significa que todos os seus direitos devem ser garantidos com precedência e por cada indivíduo. Além disso, estabelece-se que são pessoas em desenvolvimento, o que nos leva a reconhecer sua vulnerabilidade.

Outrossim, o Brasil é signatário da Convenção sobre os Direitos da Criança, adotada pela Assembleia Geral das Nações Unidas em 1989. Ainda, no Estatuto da Criança e do Adolescente, instituído pela Lei nº 8.069 de 13 de julho de 1990, as proteções a este público são mais abrangentes e detalhadas, englobando os diversos aspectos de direitos e bem-estar previstos na Constituição Federal.

A proteção integral é, portanto, não apenas uma diretriz legal, mas também um compromisso internacional assumido pelo país para sustentar que os direitos de crianças e adolescentes sejam plenamente respeitados e promovidos. Todos estes normativos asseguraram o que, até então, tinha-se como a base para a construção digna de um indivíduo. Porém, frente ao avanço das neurotecnologias capazes de ler, gravar, monitorar e eventualmente modificar atividades mentais, sobrevém nova preocupação, essencial para a fruição plena da dignidade, liberdade e valor do ser humano. E proporcionar o direito à integridade e privacidade mental ou reinterpretar

[16] BRASIL. **Decreto nº 592, de 6 de julho de 1992**. Pacto Internacional sobre Direitos Civis e Políticos. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Acesso em: 31 mar. 2026.

os direitos já existentes, englobando os neurodireitos, é garantir a possibilidade de construção da identidade pessoal em sua integridade.

Neste contexto, a Declaração de Princípios Interamericanos sobre Neurociências, Neurotecnologias e Direitos Humanos, publicada em 2023, surge trazendo novas diretrizes e princípios para orientar a aplicação e o desenvolvimento das neurociências e neurotecnologias dentro de um cenário de respeito e promoção aos direitos humanos, refletindo uma preocupação crescente com as implicações éticas, sociais e legais das avançadas tecnologias e pesquisas no campo da neurociência.

Dentre estas diretrizes está a proteção do uso ou divulgação de informações neurais não autorizadas e a garantia de que os indivíduos estejam plenamente informados sobre os riscos e benefícios antes de participar de pesquisas ou utilizar equipamentos de neurotecnologia, além de assegurar o respeito à capacidade dos indivíduos de tomar suas próprias decisões.

Como já afirmado, a elaboração desta declaração é um passo fundamental para o desenvolvimento responsável e ético envolvendo neurociências e neurotecnologias, promovendo um equilíbrio entre inovação e proteção dos direitos humanos.

É importante destacar que o campo dos neurodireitos é relativamente recente e está evoluindo tanto no cenário internacional quanto no Brasil com a participação ativa de especialistas em neurociências, juristas, filósofos e a sociedade civil. Iniciativas regulatórias começam a existir e precisam continuar a se desenvolver à medida que emergem as questões éticas, legais e sociais, como foi o caso dos dados pessoais, incluída no ordenamento jurídico brasileiro por meio da Emenda Constitucional nº 115/21, que elenca a proteção aos dados pessoais dentre os direitos e garantias fundamentais, inclusive resguardando crianças e adolescentes[17].

Ocorre que as questões trazidas pelo uso de inteligência artificial e algoritmos no campo da Neurotecnologia por vezes extrapolam as questões postas para dados pessoais, necessitando não apenas da proteção à privacidade como também da preservação da integridade física e mental.

Destarte, a discussão sobre neurodireitos hoje se desenvolve principalmente em meio acadêmico não obstante contar com importantes iniciativas legislativas que abarcam essas questões. Dentre elas, destaca-se a Proposta de Emenda Complementar nº 29, apresentada em 13 de junho de 2023, a qual propõe a preservação da integridade mental e a transparência algorítmica dentre os direitos e garantias fundamentais previstos no Artigo 5º da Constituição Federal. Após a promulgação, o mencionado artigo passará a vigorar com a inclusão do inciso LXXX:

[17] 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 fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 31 mar. 2026.

> Art.5º LXXX – o desenvolvimento científico e tecnológico assegurará a integridade mental e a transparência algorítmica, nos termos da lei.

No momento, a Proposta de Emenda Complementar aguarda a designação de relator na Comissão de Constituição, Justiça e Cidadania. Em sua justificativa, é possível notar que o legislador brasileiro, ciente do entusiasmo e da esperança que a neurociência traz para o tratamento de enfermidades, preocupa-se com os limites éticos e normativos que estes mecanismos atingirão e já sinaliza um dever de proteção a crianças e adolescentes.

> Novos espaços axiológicos, éticos e de ação humana estão sendo criados a partir do intenso desenvolvimento da neurotecnologia – com a evolução das técnicas de interface conectiva entre o cérebro e a máquina – e da consolidação do uso de algoritmos de inteligência artificial nas relações cotidianas entre o ser humano e os sistemas computacionais, especialmente em situações que envolvem processos decisórios.
>
> Os exemplos práticos trazidos pela literatura e por estudos acadêmicos a respeito dessas situações geram, sem sombra de dúvidas, esperança e grande expectativa sobre o futuro promissor que a tecnologia pode proporcionar à economia e, na área da saúde, ao tratamento e até mesmo à cura de doenças. [...]
>
> Ainda, é consenso que mecanismos de inteligência artificial estão promovendo grandes mudanças propositivas no cotidiano social, acelerando procedimentos, unindo vontades e auxiliando na busca por soluções, sobretudo em plataformas de pesquisa virtual.
>
> Contudo, os citados avanços ascendem fundada e real preocupação a respeito dos limites éticos e normativos a serem observados pela neurotecnologia, trazendo à tona, também, discussões e estudos cada vez mais frequentes sobre a dependência digital, em especial nas crianças e nos adolescentes[18].

Alinhado a este pensamento e assumindo a vanguarda de proteção aos neurodireitos, o Estado do Rio Grande do Sul promoveu a alteração de sua Constituição através da Emenda Constitucional nº 85/2023, tornando-se o primeiro no Brasil e inserindo-se como um dos pioneiros no mundo a regular o tema.

O dispositivo foi aprovado e promulgado em 20/12/2023, através da Proposta de Emenda Complementar nº 298, de 2023 e modificou o parágrafo único do artigo 235 da Constituição Estadual, estabelecendo a proteção da integridade

[18] BRASIL. **Proposta de Emenda complementar nº 29, de 2023**. Altera a Constituição Federal para incluir, entre os direitos e garantias fundamentais, a proteção à integridade mental e à transparência algorítmica. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/158095. Acesso em: 31 mar. 2026.

mental contra qualquer pesquisa que afete o cérebro e sua atividade sem o consentimento do indivíduo.

> Art. 1.º O parágrafo único do artigo 235 da Constituição do Estado do Rio Grande do Sul passa a ter a seguinte redação:
>
> "Art. 235. ..... Parágrafo único. A política e a pesquisa científica e tecnológica basear-se-ão no respeito à vida, à saúde, à dignidade humana, à integridade mental do ser humano e aos valores culturais do povo, na proteção, controle e recuperação do meio ambiente, e no aproveitamento dos recursos naturais."
>
> Art. 2.º Esta Emenda à Constituição entra em vigor na data de sua publicação.

A medida reconhece a importância da integridade mental e reforça a ideia da jornada dos direitos humanos como um processo contínuo de construção e aprimoramento.

Roberto Andorno, Professor Associado de Bioética e Direito Biomédico da Faculdade de Direito e Pesquisador Sênior e Coordenador do Programa de Doutorado em Ética e Direito Biomédico da Faculdade de Medicina da Universidade de Zurique, Suíça, ressalva, contudo, que, ao avaliarmos se é necessário criar direitos ou expandir os já existentes para enfrentar novos desafios, é crucial ter cautela para determinar se essas medidas são realmente necessárias. Sem uma análise minuciosa, é possível contribuir para o problema da proliferação excessiva de direitos, prejudicando o conceito fundamental dos direitos humanos. Sustenta, por fim, que as ameaças potenciais à humanidade trazidas pelo progresso das neurotecnologias são tão grandes que justificam a proteção oferecida pelo arcabouço dos direitos humanos. O cérebro, que está intrinsecamente ligado aos nossos pensamentos, às memórias e à essência de quem somos, produz dados extremamente complexos e relevantes, mais do que qualquer outro tipo de informação pessoal. Adicionalmente, a possibilidade de as neurotecnologias modificarem essas informações cerebrais, afetando a identidade e o comportamento, indica uma variedade de perigos inéditos para a integridade pessoal que requerem uma resposta firme e bem fundamentada da lei, especialmente no que diz respeito aos direitos humanos[19].

Nesse sentido, observa-se que o nosso país está efetivamente se posicionando para enfrentar os desafios e oportunidades trazidos por tecnologias emergentes que podem influenciar diretamente o cérebro e a mente humana, pendendo para a inclusão de novos dispositivos legais.

[19] ANDORNO, Roberto. The Risks and Challenges of Neurotechnologies for Human Rights. **Why human rights are crucial inresponding to the challenges posedby neurotechnologies**, 2023, p. 29. Disponível em: https://www.academia.edu/95093078/Why_human_rights_are_crucial_in_responding_to_the_challenges_posed_by_neurotechnologies>. Acesso em: 31 mar. 2026.

Apesar dos avanços significativos, ainda há muitos desafios para a plena implementação, dentre eles a desigualdade social, a violência, a falta de acesso a serviços básicos e a discriminação. No entanto, as importantes iniciativas são ferramentas essenciais para a construção de uma sociedade mais justa e equitativa no Brasil.

2.2 *Princípios 4 e 9 da Declaração da Organização dos Estados Americanos*

Conforme já mencionado anteriormente, a Declaração de Princípios Interamericanos sobre Neurociências, Neurotecnologias e Direitos Humanos busca estabelecer diretrizes para a aplicação e o desenvolvimento das neurociências e neurotecnologias. Abordaremos neste artigo os princípios 4 e 9, que, embora compartilhem o objetivo de promover o uso ético e responsável das neurotecnologias, se concentram em diferentes aspectos.

O Princípio 4 reconhece a autonomia cerebral como um direito fundamental, garantindo o direito de cada indivíduo de tomar decisões livres e informadas sobre suas próprias funções cerebrais. Esse princípio reconhece a importância da autodeterminação pessoal e da liberdade individual no contexto das neurotecnologias.

Neste princípio, a necessidade de consentimento expresso e informado é um requisito indispensável para o acesso à coleta de informações cerebrais. Todo indivíduo tem o direito de controlar o que acontece com seu próprio cérebro, incluindo a coleta, o uso e o compartilhamento de dados neurais. Ressalva, ainda, a possibilidade de revogação, assegurando que cada pessoa mantenha o controle sobre suas próprias capacidades cognitivas e emocionais, e recomenda atenção especial a crianças e adolescentes considerando as vulnerabilidades que podem afetar a capacidade destas de consentir, como deficiências cognitivas e situações de dependência.

> Princípio 4: Consentimiento expreso e informado de los datos neuronales. El consentimiento de la persona titular de los datos neuronales es un requisito imprescindible para el acceso a la recopilación de la información cerebral. Es fundamental garantizar el consentimiento libre, informado, expreso, específico, inequívoco, libre de vicios, respecto al acceso o tratamiento de la actividad neuronal. El consentimiento otorgado puede ser revocable en todo momento. Se requiere especial protección para el caso de niñas, niños y adolescentes, así como de personas con discapacidad, personas mayores y personas privadas de la libertad [20].

[20] Princípio 4: Consentimento expresso e informado dos dados neurais. O consentimento do titular dos dados neurais é um requisito indispensável para o acesso à coleta de informações cerebrais. É essencial garantir o consentimento livre, informado, expresso, específico, inequívoco e livre de vícios, em relação ao acesso ou ao tratamento da atividade neuronal. O consentimento concedido pode ser revogado a qualquer momento. Proteção especial é necessária para crianças e adolescentes, bem como para pessoas com deficiência, idosos e pessoas privadas de liberdade (OECD. Recommendation on Responsible Innovation in Neurotechnology, tradução nossa).

O consentimento é uma forma de consenso voluntário e informado, expresso por uma pessoa, permitindo algo. Portanto, é fundamental que esta pessoa tenha plena compreensão daquilo que está consentindo, incluindo quaisquer riscos ou implicações associadas e como garantia de que as decisões sejam tomadas com base em informações completas e inteligíveis.

Porém, na fase infantojuvenil, a expressão do consentimento é uma questão complexa, uma vez que envolve o reconhecimento progressivo da autonomia de crianças e adolescentes, considerando sua capacidade de entendimento e decisão.

No Brasil, o consentimento nesta fase, especialmente em contextos que envolvem tratamentos médicos, participação em pesquisas ou outras situações que requeiram autorização, ciência, concordância, deve ser dado pelos pais ou responsáveis legais.

Deve-se considerar que as decisões dos responsáveis repercutem diretamente no desenvolvimento e no futuro das crianças e dos adolescentes. Escolhas relacionadas à educação, ao estilo de vida, aos valores transmitidos e ao ambiente emocional em casa podem influenciar significativamente o bem-estar psicológico, as oportunidades acadêmicas e profissionais, assim como a saúde física e mental dos filhos. Da mesma forma, as decisões sobre alimentação, atividade física e uso de tecnologia afetam diretamente a saúde física das crianças e seu desenvolvimento cognitivo[21].

No caso de adolescentes, o Estatuto da Criança e do Adolescente enfatiza o direito à opinião em decisões que os afetam, respeitando sua capacidade de entendimento e maturidade. Tal abordagem se dá de maneira implícita, uma vez que não há um artigo específico dispondo expressamente sobre o consentimento informado de crianças e adolescentes de forma geral.

Temos ainda as Resoluções CNS 196/1996 e CNS 466/2012, do Conselho Nacional de Saúde, que são relevantes neste contexto e estabelecem diretrizes éticas para a participação de crianças e adolescentes em pesquisas, destacando a importância do consentimento informado dos pais ou responsáveis legais e, quando possível, o consentimento da própria criança ou adolescente, considerando sua capacidade de compreensão. O processo de consentimento livre e esclarecido para a participação voluntária em pesquisas enfatiza a importância de respeitar a vontade da criança e do adolescente, além do consentimento dos responsáveis legais. É importante envolver a criança no processo de decisão, respeitando sua capacidade de entendimento e dando-lhe a oportunidade de expressar sua opinião sobre a intervenção. Este assentimento garante que a criança tenha um papel ativo e que suas percepções e sentimentos sejam considerados.

Todavia, já mencionamos que a infância e a adolescência são períodos críticos para o desenvolvimento cognitivo e emocional. Durante essas fases, o cérebro

[21] JUSTIÇA, op. cit.

passa por mudanças significativas que influenciam a capacidade de pensar, aprender e processar informações, ou seja, dentre os diversos grupos, podemos infirmar o quão sensível é a questão quando considerado o fator idade.

Ao correlacionarmos com a proteção de dados pessoais, destacamos a dimensão do consentimento livre e informado. Isto porque a permissão para o armazenamento de dados pressupõe a possibilidade de criação de *big datas*, com informações desde a mais tenra idade, tomando proporções inimagináveis.

> No que diz respeito aos dados coletados de crianças e adolescentes, pode-se dizer que a situação se agrava ainda mais, visto que o acesso às tecnologias pela população infantojuvenil tem começado cada vez mais cedo. A consequência disso é que, caso não haja uma proteção devida de seus dados pessoais, o mapeamento acima referido ocorrerá desde a tenra idade da pessoa, ou seja, as crianças e adolescentes de hoje terão uma vida, na prática, quase que completamente armazenada por Big Data e se submeterão a processos profiling, em outros termos, a criação de perfis que predizem determinados comportamentos[22].

Nota-se, portanto, que o consentimento funciona como uma ferramenta essencial para garantir a autonomia dos indivíduos sobre suas informações. Na era digital, em que a coleta e o processamento de dados se tornaram práticas comuns, o consentir adquire uma relevância ainda maior, atuando como um mecanismo de empoderamento do usuário, permitindo-lhe decidir conscientemente sobre a utilização de seus dados. Assim, o consentimento não apenas protege o indivíduo contra o uso indevido de suas informações, mas também promove uma cultura de transparência e responsabilidade entre aqueles que manipulam dados pessoais. E, nessa condição, o consentimento impacta o direito à privacidade.

O direito à privacidade é um direito fundamental que protege a liberdade individual e a dignidade da pessoa humana. O desafio de manter a privacidade se intensifica à medida que o avanço tecnológico acontece, exigindo reinterpretações ou criações legislativas, além de boas práticas no campo da ética. Um equilíbrio entre segurança, inovação tecnológica e o respeito à privacidade é crucial para a proteção dos direitos fundamentais na sociedade.

Portanto, é primordial que os pais estejam cientes do impacto de suas decisões e busquem um equilíbrio que promova o desenvolvimento saudável de seus filhos. Crianças e adolescentes têm sim o direito à informação sobre suas próprias funções cerebrais, seus pensamentos, sentimentos e memórias e de serem protegidos contra qualquer forma de manipulação ou controle mental.

[22] LOPES, Ferla Paula. Tratamento de dados pessoais de crianças e adolescentes na lgpd: primeiras impressões. Instituto Brasileiro de Direito de Família, 3 ago. 2020. Disponível em: fam.org.br/artigos/1518/Tratamento+de+dados+pessoais+de+crian%C3%A7as+e+adolescentes+na+lgpd:+primeiras+impress%C3%B5es>. Acesso em: 31 mar. 2026.

Roberto Andorno afirma que as novas tecnologias trazem consigo riscos inéditos para os direitos humanos e a dignidade, especialmente no que diz respeito à privacidade mental. Dispositivos neurotecnológicos têm a capacidade de captar e guardar uma vasta quantidade e diversidade de informação mental, que pode ser acessada por outros sem a permissão do indivíduo, ou mediante um consentimento obtido de maneira fraudulenta ou forçada. Diversos agentes podem estar interessados nesses dados, desde empresas buscando vantagens de marketing, empregadores desejando monitorar a atenção de seus funcionários, escolas avaliando o foco de estudantes em sala de aula, até governos autoritários em busca de dissidentes[23].

Neste aspecto, os princípios 4 e 9 se correlacionam. Ao reconhecer a vulnerabilidade de crianças e adolescentes a manipulações, pressões e influências externas, surge o dever do Estado de promover o bem-estar desta população.

E a Declaração Interamericana de Princípios sobre Neurociências, Neurotecnologias e Direitos Humanos estabelece claramente a responsabilidade dos Estados em garantir o uso ético e responsável das neurotecnologias, protegendo a privacidade dos pensamentos, sentimentos e memórias das pessoas, limitando o acesso e o uso de dados neurobiológicos e neuropsicológicos.

O Princípio 9 traduz a necessidade de criar mecanismos eficazes de supervisão e fiscalização que promovam a conformidade com os padrões internacionais de direitos humanos, previnam e mitiguem riscos e protejam grupos vulneráveis.

> Princípio 9: Supervisión y fiscalización de las neurotecnologías. Los Estados están llamados a ejercer una función contralora de supervisión y fiscalización, estableciendo una autoridad nacional competente, técnicamente especializada, funcionalmente autónoma e independiente, para garantizar que el uso y la aplicación de las neurotecnologías se desarrolle conforme a los estándares internacionales en materia de derechos humanos a efectos de evitar y prevenir los riesgos e impactos negativos en los derechos de las personas, teniendo especial cuidado en la protección de derechos en niñas, niños y adolescentes y personas con discapacidad y personas privadas de libertad[24].

[23] ANDORNO, Roberto; LAVAZZA, Andrea. How to deal with mind-reading technologies. **Frontiers in Psychology**, 14 nov. 2023. Disponível em: https://pmc.ncbi.nlm.nih.gov/articles/PMC10682168/>. Acesso em: 31 mar. 2026.

[24] Princípio 9: Supervisão e fiscalização das neurotecnologias. Os Estados são chamados a exercer uma função de controle de supervisão e fiscalização, estabelecendo uma autoridade nacional competente, tecnicamente especializada, funcionalmente autônoma e independente, para garantir que o uso e a aplicação das neurotecnologias se desenvolvam conforme os padrões internacionais em matéria de direitos humanos, a fim de evitar e prevenir os riscos e impactos negativos nos direitos das pessoas, tendo especial cuidado na proteção dos direitos de crianças e adolescentes, pessoas com deficiência e pessoas privadas de liberdade (OECD. Recommendation on Responsible Innovation in Neurotechnology, tradução nossa).

Já mencionamos que a proteção integral de crianças e adolescentes é um princípio sacramentado pela Constituição Federal e pelo Estatuto da Criança e do Adolescente. Este princípio assegura que crianças e adolescentes são sujeitos de direitos, devendo ter todas as suas necessidades básicas atendidas – incluindo saúde, alimentação, educação, lazer, profissionalização, cultura, dignidade, respeito, liberdade e convivência familiar e comunitária – e ser protegidos de qualquer forma de negligência, discriminação, exploração, violência, crueldade e opressão. Esta proteção implica no reconhecimento de crianças e adolescentes como prioridade absoluta por parte da família, da sociedade e do Estado e visa garantir o desenvolvimento físico, mental, moral, espiritual e social deste público.

Dessa forma, o que se nota é que as crianças e adolescentes, além de serem pessoas como todas as outras – e, portanto, titulares de direitos – possuem uma característica exclusiva e fundamental: são seres em desenvolvimento. Tanto o é que ainda não possuem capacidade absoluta (artigos 3º e 4º do Código Civil), fato que corrobora a necessidade de uma proteção ainda maior, a fim de que o desenvolvimento completo das suas personalidades seja não apenas protegido, mas também promovido[25].

E para proteger as particularidades desse desenvolvimento, o direito precisa se adaptar, reinterpretando normas e princípios para abarcar a proteção integral da criança e do adolescente, assegurando seus direitos fundamentais e protegendo contra novas situações que são postas, especialmente, com o avanço tecnológico.

A tecnologia desempenha um papel dúbio: é tanto uma ferramenta para o desenvolvimento cognitivo quanto uma fonte de riscos potenciais. Plataformas educacionais e recursos digitais expandem os horizontes de aprendizado, oferecendo oportunidades inovadoras para o desenvolvimento do pensamento crítico e criativo. No entanto, a exposição desregulada a dispositivos eletrônicos e a conteúdo *online* pode ter efeitos adversos, incluindo a redução da atenção, o vício em tela e a interferência no desenvolvimento social e emocional, como afirmado pelo Dr. Eduardo Jorge, ou seja, o avanço tecnológico apresenta ao mesmo tempo desafios e oportunidades significativas.

A educação para a cidadania digital torna-se, portanto, um pilar fundamental para equipar as novas gerações com as ferramentas necessárias para navegar com segurança e eficácia no cenário tecnológico em constante mudança.

Neste cenário, o Estado e as famílias, através da educação, desempenham um papel fundamental para garantir o uso seguro e responsável da tecnologia. A educação é um pilar fundamental para que novas gerações possam conviver num ambiente tecnológico em constante mudança.

Mas não é só. Tratando-se de neurotecnologia e dos potenciais impactos sobre os direitos fundamentais de uma população vulnerável, a Organização para a

[25] TEIXEIRA, op. cit.

Cooperação e Desenvolvimento Econômico (OCDE) recomenda que o Estado deve assumir um papel regulamentador com a supervisão e fiscalização das neurotecnologias. Isso envolve não apenas a garantia de que essas tecnologias sejam seguras e eficazes, mas também que seu uso esteja alinhado com os princípios éticos e de direitos humanos, além de estarem em conformidade com os padrões internacionais, o que culmina com a necessidade de proteção contra o uso não consentido de tecnologias capazes de realizar um mapeamento mental, trazendo consigo o risco de atravessar a privacidade mental de um indivíduo.

A criação de uma autoridade nacional competente, tecnicamente especializada e funcionalmente autônoma é fundamental para o estabelecimento de um sistema de governança eficaz para as neurotecnologias. A autoridade deve contar com especialistas em neurociência, neurotecnologia, ética, direito e outras áreas relevantes para garantir a compreensão profunda das implicações das neurotecnologias, além de ter autonomia para tomar decisões e agir de forma independente, sem interferência indevida de interesses políticos ou econômicos, garantindo imparcialidade e objetividade em suas ações.

Essa autoridade teria como responsabilidade não apenas a regulamentação e fiscalização do setor, mas também a promoção de pesquisa e desenvolvimento responsáveis, garantindo que os avanços tecnológicos beneficiem a sociedade como um todo.

A supervisão e fiscalização das neurotecnologias se põe de forma complexa, exigindo colaboração entre governos, indústria, comunidade científica e sociedade civil. Ao equilibrar os benefícios potenciais dessas tecnologias com a necessidade de proteger os direitos humanos, podemos navegar neste novo território de maneira responsável e ética, garantindo que as neurotecnologias sirvam ao bem comum.

Roberto Andorno afirma que, além dos regulamentos que podem ser adotados a nível nacional, também são necessários alguns padrões internacionais mínimos relativos à neurotecnologia. Ele entende que, à medida que a ciência se torna cada vez mais globalizada, uma resposta coerente e eficaz aos novos desafios colocados pela ciência deverá também ser global[26].

Recorda que, por volta do final da década de 1990, a comunidade internacional fez esforços significativos, especialmente no âmbito da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), para enfrentar os então novos desafios colocados pela tecnologia genética e para adotar declarações internacionais específicas. Além disso, recomenda que à semelhança do que aconteceu com a "revolução genética", sejam desenvolvidas normas internacionais específicas de direitos humanos para lidar com a neurorevolução em curso.

[26] ANDORNO; LAVAZZA, op. cit.

Ressalta que o relatório sobre as questões éticas da neurotecnologia adotado pelo Comitê Internacional de Bioética da UNESCO (IBC) em dezembro de 2021 é um bom norte (UNESCO, IBC 2021). Este relatório refere-se explicitamente à possibilidade de desenvolver uma Declaração Internacional sobre Direitos Humanos e Neurotecnologia com o objetivo de proteger valores como, entre outros, a dignidade humana, a integridade mental, a privacidade mental, a identidade pessoal e a liberdade de pensamento. Ao mesmo tempo, incentiva os Estados-Membros a garantirem que as leis nacionais sejam adaptadas para proteger estes valores. O caminho a seguir rumo a este objetivo ambicioso exigirá esforços significativos e uma cooperação estreita entre os Estados e outras partes interessadas relevantes.

As crianças e adolescentes são particularmente suscetíveis aos riscos potenciais das neurotecnologias. Portanto, medidas de proteção especiais devem ser implementadas para esse grupo, garantindo que seus direitos sejam resguardados. Isso pode incluir restrições ao uso de neurotecnologias em escolas, a exigência de consentimento informado robusto e a proteção contra a exploração comercial. Campanhas de conscientização e educação sobre neurociências e neurotecnologias também são bons parâmetros para disseminar informação aos pais ou responsáveis legais os riscos e benefícios dessas tecnologias, permitindo debates públicos e decisões mais conscientes.

> O Brasil, ao buscar integrar em sua Constituição norma de proteção específica à proteção jurídica da mente, se juntaria a outros atores globais e se colocaria em posição de protagonismo global no assunto ao demonstrar a exata compreensão do momento tecnológico vivenciado no mundo, mostrando responsabilidade com a pessoa humana ao mesmo tempo em que reafirmaria o compromisso com o desenvolvimento científico e tecnológico, em clara aderência a recomendações já emanadas de órgãos como a Organização para a Cooperação e Desenvolvimento Econômico – OCDE[27].

É fundamental, portanto, que os países, inclusive o Brasil, elaborem leis e regulamentações específicas sobre o uso de neurotecnologias em crianças e adolescentes, definindo critérios éticos e científicos para sua aplicação.

3. CONCLUSÃO

A necessidade de inserção de uma proteção legal específica em neurodireitos se põe como uma forma de assegurar o progresso científico e tecnológico com respeito à dignidade da pessoa humana e sua autonomia de vontade.

[27] PINTARELLI, Camila. A proteção jurídica da mente. **Revista de Direito**, p. 14. Disponível em: https://periodicos.unisa.br/index.php/direitosaude/article/view/396/458. Acesso em: 2 jun. 2024.

A discussão sobre neurodireitos insere-se com relevante importância em um cenário mundial, sendo imprescindível que este debate transcenda o nível acadêmico e a construção de um futuro que respeite os limites éticos e os direitos humanos em um ambiente tecnológico em evolução exige um movimento político e jurídico engajado e comprometido com direitos individuais e coletivos.

Os avanços em neurociências e neurotecnologias têm o potencial de afetar profundamente a mente e o comportamento humano. Isso inclui intervenções que podem alterar pensamentos, emoções e memórias. Nesse contexto, os direitos humanos são fundamentais para proteger a dignidade e a integridade dos indivíduos, assegurando que essas tecnologias não sejam usadas de forma a desrespeitar ou explorar as pessoas.

Um dos pilares dos direitos humanos é justamente a autonomia individual. No campo dos neurodireitos, isso se traduz na necessidade de obter consentimento informado para qualquer intervenção neurotecnológica. As pessoas devem ter o direito de tomar decisões livres e informadas sobre o uso de tecnologias que possam afetar suas capacidades cognitivas e emocionais.

Ademais, os dados neurais são extremamente sensíveis e podem revelar aspectos profundos e íntimos da mente humana. A proteção da privacidade é um direito humano essencial, garantindo que informações pessoais e neurais sejam protegidas contra uso indevido e acesso não autorizado.

São os direitos humanos que também asseguram que todos os indivíduos, independentemente de suas circunstâncias, tenham acesso igual aos benefícios dessas tecnologias e não sejam alvo de discriminação ou injustiças e fornecem um quadro ético para orientar o desenvolvimento e a aplicação de neurotecnologias. Eles estabelecem padrões e princípios que ajudam a garantir que o progresso científico e tecnológico seja conduzido de maneira ética e responsável, respeitando os direitos e a dignidade de todos os seres humanos.

No universo de crianças e adolescentes, a inclusão de proteção específica dos neurodireitos, reconhecendo a vulnerabilidade e a importância do desenvolvimento saudável nesta faixa etária, é fundamental para resguardar a integridade mental, a privacidade cognitiva e a autonomia desses jovens.

O respeito aos neurodireitos de crianças e adolescentes não apenas os protege em seu desenvolvimento individual, mas também serve como base para o exercício pleno de seus direitos e liberdades no futuro, formando verdadeiros cidadãos. Neste contexto, a educação e a conscientização sobre os neurodireitos desde a infância tornam-se peças-chave para promover uma cultura de respeito e proteção no ambiente digital e tecnológico, devendo ser encarado como um investimento presente e futuro da sociedade.

Ao garantir que os neurodireitos sejam respeitados e promovidos, estaremos, não só protegendo este público contra potenciais abusos e violações, mas também fomentando o desenvolvimento de uma geração mais consciente, ética e preparada.

Inúmeros são os desafios. A maioria dos países ainda não possui leis ou regulamentações específicas sobre o uso de neurotecnologias em crianças e adolescentes, criando um vazio legal que pode facilitar o uso indevido dessas tecnologias. Pais, profissionais e a própria sociedade em geral ainda não possuem conhecimento suficiente sobre as neurotecnologias e seus impactos potenciais em crianças e adolescentes, dificultando a tomada de decisões informadas e éticas.

Assim, mostra-se fundamental a elaboração de leis ou regulamentações específicas sobre o uso de neurotecnologias em crianças e adolescentes, definindo critérios éticos e científicos para sua aplicação, com rigorosos protocolos de segurança.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDORNO, Roberto. The Risks and Challenges of Neurotechnologies for Human Rights. **Why human rights are crucial inresponding to the challenges posedby neurotechnologies**, 2023, p. 29. Disponível em: https://www.academia.edu/95093078/Why_human_rights_are_crucial_in_responding_to_the_challenges_posed_by_neurotechnologies. Acesso em: 31 mar. 2026.

ANDORNO, Roberto; LAVAZZA, Andrea. How to deal with mind-reading technologies. **Frontiers in Psychology**, 14 nov. 2023. Disponível em: https://pmc.ncbi.nlm.nih.gov/articles/PMC10682168/. Acesso em: 31 mar. 2026.

BRASIL. **Constituição do Estado do Rio Grande do Sul**. Disponível em: https://www2.al.rs.gov.br/dal/LinkClick.aspx?fileticket=WQdIfqNoXO4%3d&tabid=3683&mid=5359. Acesso em: 28 jan. 2024.

BRASIL. **Decreto nº 99.710, de 21 de novembro de 1990**. Promulga a Convenção sobre os Direitos da Criança. Brasília, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D99710.htm. Acesso em: 28 jan. 2024.

BRASIL. **Decreto nº 592, de 6 de julho de 1992**. Atos Internacionais. Pacto Internacional sobre Direitos Civis e Políticos. Promulgação. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Acesso em: 25 abr. 2024.

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 fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em 31 mar. 2026.

BRASIL. Ministério da Saúde. Secretaria de Atenção à Saúde. Área de Saúde do Adolescente e do Jovem. **Marco legal: saúde, um direito de adolescentes**. Brasília: Ministério da Saúde, 2007. p. 60. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/07_0400_M.pdf. Acesso em: 30 maio 2024.

BRASIL. **Proposta de Emenda complementar nº 29, de 2023**. Altera a Constituição Federal para incluir, entre os direitos e garantias fundamentais, a proteção à integridade mental e à transparência algorítmica. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/158095. Acesso em: 31 mar. 2026.

CHILE, Corte Constitucional, **processo nº 105.065-2023**, relatora Ministra Ángela Vivanco, j. em 09/08/2023. Disponível em: https://www.doe.cl/alerta/11082023/2023081100. Acesso em: 16 fev. 2024.

CONSELHO NACIONAL DE SAÚDE. **Resolução nº 196 de 10 de outubro de 1996**. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/cns/1996/res0196_10_10_1996.html. Acesso em: 5 mar. 2024.

CONSELHO NACIONAL DE SAÚDE. **Resolução nº 466 de 12 de dezembro de 2012**. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/cns/2013/res0466_12_12_2012.html. Acesso em: 5 mar. 2024.

CONVENTION ON THE RIGHTS OF THE CHILD. **General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1). UN Doc CRC/C/GC/14.** [s.l.], 2013. Disponível em: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2fC%2fGC%2f14&Lang=en. Acesso em: 24 jan. 2024.

EL MOSTRADOR CULTURA. **Chile en la historia mundial: primer país que tendrá ley de neuroderechos.** Disponível em: https://www.elmostrador.cl/cultura/2021/09/23/chile-en-la-historia-mundial-primer-pais-que-tendra-ley-de-neuroderechos/. Acesso em: 31 mar. 2026.

FERNANDES, Elora; MEDON, Filipe. Proteção de crianças e adolescentes na LGPD: desafios interpretativos. **Revista Eletrônica da PGE-RJ**, [S. l.], v. 4, n. 2, 2021. DOI: 10.46818/pge.v4i2.232

FERREIRA, Rafaela. A América Latina na frente pelo reconhecimento dos neurodireitos. **Iris**, 20 set. 2023. Disponível em: https://irisbh.com.br/a-america-latina-na-frente-pelo-reconhecimento-dos-neurodireitos/. Acesso em: 30 jan. 2024.

JACKSON, Patrick. Como funciona o Telepathy, chip cerebral que Elon Musk diz ter sido implantado em uma pessoa. **BBC News**, 30 jan. 2024. Disponível em: https://www.bbc.com/portuguese/articles/cd182g1gp27o. Acesso em: 31 mar. 2026.

JUSTIÇA. Conselho Nacional**. Webnário Saúde Mental e Demandas Judiciais: Ações necessárias (manhã)**. YouTube, 6 de outubro de 2023. Disponível em: https://www.youtube.com/live/hKRt5tDPzXE?si=RmrZsprgmh0Zj8k4. Acesso em: 4 fev. 2024.

LEY CHILE. Ley 21383. **Biblioteca del Congreso Nacional (bcn.cl).** Disponível em: https://www.bcn.cl/leychile/navegar?idNorma=1166983. Acesso em: 31 mar. 2026.

LOPES, Ferla Paula. Tratamento de dados pessoais de crianças e adolescentes na lgpd: primeiras impressões. **Instituto Brasileiro de Direito de Família**, 3 ago. 2020. Disponível em: https://ibdfam.org.br/artigos/1518/Tratamento+de+dados+pessoais+de+crian%C3%A7as+e+adolescentes+na+lgpd:+primeiras+impress%C3%B5es. Acesso em: 7 mar. 2024.

OECD. **Recommendation on Responsible Innovation in Neurotechnology**. Disponível em: https://www.oecd.org/science/recommendation-on-responsible-innovation-in-neurotechnology.htm. Acesso em: 30 jan. 2024

PINTARELLI, Camila. **A proteção jurídica da mente. Revista de Direito**. Disponível em: https://periodicos.unisa.br/index.php/direitosaude/article/view/396/458. Acesso em: 2 jun. 2024.

UNESCO. Risks and challenges of neurotechnologis for human rights. **University of Milan and State University of New York,** 2023. Disponível em: https://unesdoc.unesco.org/in/documentViewer.xhtml?v=2.1.196&id=p::usmarcdef_0000384185&file=/in/rest/annotationSVC/DownloadWatermarkedAttachment/attach_import_ac1c0bf2-cca6-4244-adce-fba123807ace%3F_%3D384185eng.pdf&locale=en&multi=true&ark=/ark:/48223/pf0000384185/PDF/384185eng.pdf#%5B%7B%22num%22%3A106%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C0%2C871%2C0%5D. Acesso em: 7 mar. 2024.

YUSTE, Rafael. "La privacidad máxima de una persona es lo que piensa": el neurocientífico que impulsa los 'neuroderechos'. **El País**, 2019. Disponível em: https://elpais.com/ciencia/2019/11/05/actualidad/1572948777_301315.html. Acesso em: 22 abr. 2026.

YUSTE, Rafael *et al*. Four ethical priorities for neurotechnologies and AI. **Nature**, n. 551, p. 159-163, 2017. Disponível em: https://www.nature.com/articles/551159a. Acesso em: 30 jan. 2024.

Submetido em: 07/01/2025
Aprovado em: 13/06/2025

A "RESSURREIÇÃO DIGITAL" E O PROJETO DE LEI Nº 3.592/2023, DO SENADO FEDERAL: A AUTORIZAÇÃO FAMILIAR E A MANIFESTAÇÃO DE VONTADE DO ARTISTA QUANDO VIVO

"Digital Resurrection" and Bill No. 3.592/2023 of the Brazilian Federal Senate: Family Authorization and the Artist's Expression of Will While Alive

Henrique José de Agostinho Cintra[1]

SUMÁRIO 1. Introdução: "A ressurreição digital" e o Projeto de Lei nº 3592/2023, do Senado Federal; 2. Dos direitos da personalidade; 2.1. Direito de imagem; 2.2. Direito à voz; 3. Dos direitos autorais; 4. Conclusão; Referências Bibliográficas.

RESUMO O presente trabalho tem por objetivo averiguar, com amparo na literatura que trata dos Direitos da Personalidade e dos Direitos Autorais, quais são os requisitos legais para que a imagem e a voz de artistas falecidos sejam utilizadas para a ressurreição digital por meio de ferramentas de inteligência artificial. Assim, o foco do presente trabalho será esclarecer a seguinte questão de pesquisa: "É suficiente a autorização dada pelo artista em vida ou por seus herdeiros, prevista no artigo 2º do Projeto de Lei nº 3592/2023, do Senado Federal, para que a imagem e a voz do artista falecido sejam utilizadas para criação de novas obras artísticas com a ajuda de inteligência artificial?". Para tanto, o autor desse trabalho se valeu de pesquisa que levou em consideração a revisão da literatura sobre o tema, inclusive a legislação correlata.

Palavras-chave: Direitos da Personalidade. Direito Autoral. Inteligência Artificial. Ressurreição Digital. Autorização.

ABSTRACT The purpose of this study is to investigate, based on literature addressing Personality Rights and Copyright, what the legal requirements are for the image and voice of deceased artists to be used for digital resurrection through artificial intelligence tools. Therefore, the focus of this study will be to clarify the following research question: "Is the authorization given by the artist during his life or by their heirs, as provided in Article 2 of Bill No. 3592/2023 of the Federal Senate, sufficient for the image and voice of the deceased artist to be used for the creation of new artistic works with the help of artificial intelligence?" To this end, the author of this study used research that considered a review of the literature on the subject, including related legislation.

Keywords: Personality Rights. Copyright Law. Artificial Intelligence. Digital Resurrection. Authorization.

1. INTRODUÇÃO: "A RESSURREIÇÃO DIGITAL" E O PROJETO DE LEI Nº 3592/2023, DO SENADO FEDERAL

O advento da internet e a difusão dos computadores pelo mundo (antes limitados a países desenvolvidos), com início em meados da década de 1990, deram

[1] Procurador do Estado de São Paulo. Especialista em Direito Tributário pela Universidade de São Paulo. Graduado em Direito pela Universidade Presbiteriana Mackenzie e em Ciências Contábeis pela Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo (USP).

DOI: 10.22491/*respge*.v16i1.1734

início ao que hoje se convenciona chamar de "Quarta Revolução Industrial", ou ainda, Indústria 4.0. No entanto, os avanços promovidos por esses dois elementos não se limitaram ao âmbito industrial (ou empresarial), ampliando-se para outros campos, inclusive o cultural, um aspecto da vida humana que sempre esteve atrelado aos avanços tecnológicos, como na primeira utilização registrada de tinta a óleo no ano de 650 a.C.

Mais recentemente, a década de 2020 tem sido marcada por avanços expressivos no campo da ciência da computação, como os novos desenvolvimentos no campo da internet das coisas (*internet of things* – IoT) (eletrodomésticos, automóveis e aeronaves que se beneficiam da conexão com a internet), o aprendizado de máquina e a inteligência artificial (IA). No que tange à IA, sua associação a sistemas avançados de computação gráfica e à emulação de aspectos humanos têm feito com que sejam utilizadas a imagem e a voz de artistas mortos para fins comerciais e artísticos. Essa realidade tem gerado diversos questionamentos na imprensa e nas redes sociais acerca dos aspectos éticos desse procedimento.

Principalmente em relação à utilização da inteligência artificial, em associação a sistemas avançados de computação gráfica e à recriação de voz humana, tem se tornado cada vez mais frequente essa dúvida. O exemplo recente mais conhecido no âmbito brasileiro foi a utilização da imagem e da voz, recriadas artificialmente, de Elis Regina, cantora falecida em 1982, para uma peça publicitária da montadora de automóveis Volkswagen[2].

Nesta peça, a atriz Ana Rios, que tem certa semelhança física com Elis Regina, foi filmada e, sobre seu rosto, foi inserido digitalmente o rosto reconstruído da cantora falecida, que então apareceu ao lado de sua filha, Maria Rita, cantando "Como nossos pais", canção de autoria de Belchior, veiculada em julho de 2023 e que ainda se encontra disponível no canal oficial da empresa no YouTube[3].

O uso dessa tecnologia também foi o mote das greves do sindicato dos roteiristas dos Estados Unidos (Writer's Guild of America), bem como do sindicato de atrizes e atores de Hollywood (Screen Actors Guild-American Federation of Television and Radio Artists – SAG-AFTRA), este último liderado pela atriz Fran Drescher, famosa pelo seriado *The Nanny*. Enquanto os roteiristas se preocupavam com as habilidades criativas dos Large Language Models (LLMs), que se tornaram conhecidos no ano de 2023 com a fama do ChatGPT, criado pela empresa OpenAI, as atrizes e os atores, em especial os figurantes, se preocupam com a utilização massificada da inteligência artificial para a criação de personagens e, também, com a recriação

[2] VIEIRA, Luíza. Comercial da Volkswagen com Elis Regina levanta debate sobre ditadura e nazismo; entenda, **O Povo**, 5 jul. 2023. Disponível em: https://www.opovo.com.br/noticias/politica/2023/07/05/comercial-da-volkswagen-com-elis-regina-levanta-debate-sobre-ditadura-e-nazismo-entenda.html. Acesso em: 3 mar. 2026.

[3] Disponível em: https://youtu.be/aMl54-kqphE?si=nvBq0ohG42Ezi7rF. Acesso em: 3 mar. 2026.

tecnológica de profissionais já falecidos, como no já antecipado filme com James Dean, ator falecido em 1955.

Um último exemplo, mais recente, diz respeito à canção "Now and then", dos Beatles, banda cuja atividade se encerrou ainda na década de 1970, mas que, com o uso de trechos de gravações antigas e o auxílio de ferramentas de inteligência artificial, pôde lançar uma música nova que conta com a voz de John Lennon, falecido em 1980.

Em vista desse cenário e motivado pela polêmica criada nas redes sociais e na imprensa envolvendo a já mencionada publicidade, foi apresentado o Projeto de Lei nº 3.592/2023, de autoria do Senador Rodrigo Cunha, cuja justificativa cita a referida peça publicitária, com vistas a regular a utilização da inteligência artificial para "ressuscitar digitalmente" artistas mortos.

Em seu artigo 2º, o referido projeto de lei estabelece que "o uso da imagem de uma pessoa falecida por meio de IA requer o consentimento prévio e expresso da pessoa em vida ou, na ausência deste, dos familiares mais próximos", enquanto seu parágrafo único dispõe que o "consentimento deve ser obtido de forma clara, inequívoca e documentada, e deve especificar os fins para os quais a imagem ou áudio serão utilizados"[4].

Como pode-se observar, a legislação busca solucionar o uso da inteligência artificial de maneira limitada ao uso da imagem de pessoa falecida (não tratando de outros aspectos personalíssimos da expressão artística, como a voz, apesar de mencionar "áudio"), além de trazer um instituto *sui generis* e, até então, inexistente no Direito brasileiro, que é a autorização dada por "familiares próximos" para o uso da imagem e do áudio da pessoa falecida.

No entanto, da disposição do artigo 2º acima mencionado surgem alguns questionamentos, a começar pela prevalência da opinião do artista em relação àquela exarada por seus "parentes próximos" ou, mais tecnicamente, seus herdeiros na forma da lei[5]. Poderiam os herdeiros dispor de maneira diversa daquela que o artista falecido dispôs?

Quanto aos artistas que faleceram antes mesmo da invenção de ferramentas de inteligência artificial capazes de reproduzir a imagem e a voz humana, poderiam os herdeiros, na forma da lei, autorizar tal uso? Este trabalho tem o propósito de contribuir com esse debate.

[4] BRASIL. Senado Federal. **Projeto de Lei nº 3.592/2023**. Brasília, DF: Senado Federal, 2023. Art. 2º.

[5] BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Código Civil. Brasília, DF: Senado Federal, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 3 abr. 2026. Art. 1.829.

2. DOS DIREITOS DA PERSONALIDADE

Com o advento da Constituição Federal de 1988 (CF/88)[6], os direitos da personalidade ganharam um destaque especial no ordenamento brasileiro, sendo a dignidade da pessoa humana alçada à qualidade de fundamento da República (art. 1º, III).

No âmbito infraconstitucional, os direitos da personalidade são tratados a partir do artigo 11 do Código Civil e gozam de especial proteção pelo direito pátrio, sendo assegurados desde o nascimento com vida da pessoa natural, ficando a salvo os direitos do nascituro desde a concepção (artigo 2º), e perpetuando-se mesmo após a morte.

Esses direitos decorrem, remotamente, dos direitos naturais segundo Caio Mário da Silva Pereira, para quem "encontra, pois, boa sustentação, proclamar que a origem remota dos direitos da personalidade assenta no direito natural" e que "os direitos da personalidade, como categoria, são considerados como inerentes à pessoa humana, independentemente de seu reconhecimento pela ordem positiva"[7].

Considerando não haver um conceito legal, coube à doutrina tal função. Carlos Alberto Bittar assim os define:

> São direitos ínsitos na pessoa, em função de sua própria estruturação física, mental e moral. Daí, são dotados de certas particularidades, que lhes conferem posição singular no cenário dos direitos privados, de que avultam, desde logo, as seguintes: a intransmissibilidade e a irrenunciabilidade, que se antepõem, inclusive como limites à própria ação do titular (que não pode eliminá-los por ato de vontade, mas, de outro lado, deles, sob certos aspectos, pode dispor, como, por exemplo, a licença para uso de imagem, dentre outras hipóteses). Contudo, esse consentimento não desnatura o direito, representando, ao revés, exercício de faculdade inerente ao titular (e que lhe é privativa) e à de terceiro (não comportando, de uma parte, uso por terceiro sem expressa autorização do titular e, quando juridicamente possível, e, de outra, execução forçada, em qualquer situação, eis que incompatível com a sua essencialidade)[8].

Ainda, os direitos da personalidade não possuem apreciação econômica, não podem ser cedidos, são imprescritíveis e podem ser opostos a terceiros, isto é, pode-se impor o respeito a tais direitos frente a eventuais violações.

---

[6] BRASIL. **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: 3 abr. 2026.

[7] PEREIRA, Caio Mário da Silva. **Direito Civil: alguns aspectos de sua evolução**. Rio de Janeiro: Forense, 2001, p. 23-25.

[8] BITTAR, Carlos Alberto. **Os direitos da personalidade**. Rio de Janeiro: Forense Universitária, 1989, p. 15.

Sendo o artista a expressão máxima da exteriorização de elementos personalíssimos, que incluem não apenas uma aparência singular, mas também trejeitos, timbre de voz e, até mesmo, expressões vocais únicas, mostra-se necessária a análise destes elementos frente ao avanço das ferramentas de inteligência artificial.

Assim, entre os direitos da personalidade relevantes para o objeto deste trabalho, destacam-se os direitos à imagem e à voz.

2.1. *Direito de imagem*

Quanto ao direito de imagem, a Constituição Federal assegura "o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem"[9] e, em reforço, a inviolabilidade da "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"[10].

No mesmo sentido do art. 5º, X, da Constituição, o artigo 20 do Código Civil dispõe que:

> Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais[11].

No âmbito da doutrina, Carlos Alberto Bittar assim o conceitua:

> Consiste no direito que a pessoa tem sobre a sua forma plástica e respectivos componentes distintos (rosto, olhos, perfil, busto etc.) que a individualizam no seio da coletividade. Incide, pois, sobre a conformação física da pessoa, compreendendo esse direito um conjunto de caracteres que a identifica no meio social. Por outras palavras, é o vínculo que une a pessoa à sua expressão externa, tomada no conjunto, ou em partes significativas (como a boca, os olhos, as pernas, enquanto individualizadoras da pessoa)[12].

O doutrinador Adriano de Cupis afirma que o direito à imagem decorre do direito ao resguardo e que sua tutela é propriamente um direito de oposição, isto é, o titular tem o direito de impedir que terceiros se valham de maneira desautorizada

[9] BRASIL, **Constituição da República Federativa do Brasil de 1988**, *op. cit.*, art. 5º, V.

[10] *Ibid*., art. 5º, X.

[11] BRASIL, **Lei nº 10.406, de 10 de janeiro de 2002**, *op. cit.*, art. 20.

[12] BITTAR, *op. cit.*, p. 40, grifo nosso.

de sua imagem, seja no campo fotográfico, na pintura, na escultura, no teatro ou no cinema, e traz um exemplo do passado que se aplica à presente discussão:

> […] já se sustentou que esta tutela pode aplicar-se mesmo à reprodução teatral ou cinematográfica da pessoa, isto é, às hipóteses em que um artista, através da figura, do gesto, da atitude, reproduz na cena ou na película a pessoa. É o caso da chamada máscara cênica, isto é, a representação da pessoa em um espetáculo público. Quer esta representação esteja diretamente prevista nas normas referidas, quer deva recorrer-se à analogia, certo é que o direito à imagem assegura ao indivíduo a defesa contra este, como contra os outros modos de difusão da sua imagem. Deve notar-se que a representação teatral ou cinematográfica pode resultar particularmente expressiva, podendo fixar-se na memória do espectador, bem mais do que, por exemplo, o retrato reproduzido em um jornal ilustrado, o qual é geralmente olhado mais ou menos de forma rápida, por alto. Além do mais, a voz do artista reforça o efeito da reprodução, completando o retrato e tornando-o mais eficaz - o que avoluma, de fato, a ilusão de ter diante de si a pessoa representada[13].

Fala-se, ainda, em uma evolução desse direito, indo além da identificação com a forma plástica ou a aparência da pessoa, de modo que ele abarca a imagem-retrato e a imagem-atributo. Segundo Zanini:

> imagem-retrato está baseada no aspecto visual, caracterizando-se pela representação total ou parcial do corpo capaz de identificar a pessoa, seja de forma gráfica, plástica, fotográfica e até mesmo dinâmica no cinema ou na televisão[14].

Ou seja, a imagem-retrato consiste na concepção tradicional de imagem, aquela apreciada pelos olhos humanos e na interpretação que o cérebro humano dá àquela imagem.

Quanto à imagem-atributo, D'Amico, dessa vez mencionando Denis Borges Barbosa, ressalta ser esta "de grande valia para obras publicitárias, que visam persuadir o consumidor a adquirir determinado bem por meio da identificação das qualidades deste com os atributos da pessoa utilizada em na [sic] obra publicitária"[15].

Associado à imagem-atributo está todo o conjunto de ideias e posicionamentos manifestados pela pessoa – seja de forma pública ou privada –, que conformam seu caráter e indicam sua visão de mundo. Essas posições são relevantes

[13] CUPIS, Adriano de. **Os direitos da personalidade**. Tradução de Afonso Celso Furtado Rezende. São Paulo: Quorum, 2008, p. 90.

[14] *Apud* D'AMICO, Gustavo Fortunato. **Ressurreição Digital**: aspectos jurídicos e repercussões. Curitiba: IODA, 2021, p. 79.

[15] *Ibid.*, p. 60 et seq.

para qualquer ser humano, mas, ainda mais para um artista, já que a confusão entre criador e criatura, no âmbito artístico, tanto pode servir para a atração quanto para a rejeição do público consumidor.

Exemplos disso são as situações ocorridas durante a recente pandemia de covid-19, em que artistas consagrados que se manifestaram contra as vacinas acabaram por receber notícias negativas na imprensa e foram até mesmo ignorados por grandes veículos de mídia que anteriormente os tinham em contrato.

Assim, eventual reprodução da imagem-retrato que esteja em descompasso com a imagem-atributo poderia, ao menos em tese, importar em violação desse direito da personalidade, passível de intervenção judicial.

2.2. Direito à voz

Em relação ao direito à voz, este tem assento constitucional no art. 5º, XXVIII, "a", que garante a "proteção às participações individuais em obras coletivas e à reprodução da imagem e voz humanas, inclusive nas atividades desportivas"[16].

De maneira sucinta, Bittar assim o descreve:

> Trata-se de direito que incide sobre a emanação sonora natural da pessoa, proveniente do aparelho fonador e exercitada em toda a sua evolução para adquirir, na fase adulta, a sua conformação definitiva. Envolvendo o som, por via de tonalidades diferentes, - que, por técnicas adequadas de treinamento, podem ser aprimoradas, ou direcionadas – acaba por adquirir contornos próprios, suscetíveis de individualizar a pessoa no meio social […]. Embora componente físico – e, como tal, integrante do conjunto da imagem da pessoa – destacou-se para ganhar individualidade, frente ao uso isolado, principalmente em rádio e em gravações, identificando pessoas e estilos vários. Possibilita seja a pessoa mentalmente visualizada por associação, perenizando-se pela fixação [17].

Conquanto, à época em que promulgada a Constituição e em que escrito o trecho acima pelo eminente doutrinador, a realidade indicasse que a voz de determinada pessoa somente poderia ser perpetuada por meio de gravações (em LPs, fitas cassete e outros meios físicos) – possível origem do termo "áudio" utilizado no Projeto de Lei nº 3.592/2023[18] – a realidade é que as possibilidades de uso da voz de artistas vão muito além de simples gravações. Tanto que os meios artísticos trazem a possibilidade de reprodução de artistas, e suas vozes, ao menos desde 2013.

[16] BRASIL, **Constituição da República Federativa do Brasil de 1988**, *op. cit.*, art. 5º, XXVIII, "a".

[17] BITTAR, *op. cit.*, p. 60 et seq.

[18] BRASIL. **Projeto de Lei nº 3.592/2023**, *op. cit*.

No filme de animação *The Congress* (sem título em português), do diretor Ari Folman, uma personagem (cuja voz é da atriz Robin Wright) concorda em vender os direitos de sua imagem e voz para uma empresa de entretenimento. A empresa cria uma versão digital dela, que é usada para produzir filmes e programas de TV. A ideia de recriar a voz e a imagem de uma pessoa é central na trama.

Já no episódio "Rachel, Jack and Ashley Too", de 2019, da série *Black Mirror*, uma estrela da música pop chamada Ashley O (interpretada pela atriz Miley Cyrus) tem sua personalidade digitalizada e transformada em uma boneca robótica chamada Ashley Too. A boneca replica a voz e o comportamento da cantora, criando uma experiência perturbadora para os fãs. Nessa perspectiva, esse tema se tornou realidade com o lançamento de várias obras com a recriação da voz de artistas famosos já falecidos.

O álbum *Lost Tapes of the 27 Club* contém quatro músicas que se valem da inteligência artificial para recriação de letras, música e da voz de quatro artistas falecidos aos 27 anos de idade: Jimi Hendrix, Jim Morrison, Kurt Cobain e Amy Winehouse. O resultado é impressionante, com a voz gerada pelos processos computacionais sendo indistinguível, ao menos para o ouvinte leigo, da voz do artista falecido.

E, assim como ocorre com o direito de imagem, é certo que a voz notável de um artista falecido deve ser protegida da recriação irrestrita por ferramentas de inteligência artificial.

Isso porque, conquanto o timbre da voz seja único para cada um dos bilhões de seres humanos, em virtude não apenas da forma e tamanho das cordas vocais de um indivíduo, mas também do tamanho e forma do resto do corpo humano, especialmente o trato vocal, e da maneira pela qual os sons da fala são habitualmente formados e articulados, é certo que a precisão com que a recriação das características personalíssimas da voz é realizada pelos programas de inteligência artificial pode levar à apropriação indevida da fama de um determinado artista para a promoção de uma obra de arte de cuja criação não participou.

Assim é que a proteção desse direito da personalidade é muito relevante para artistas que atuam nas áreas musical e audiovisual, sendo certo que também essa característica humana – como ocorre com a imagem – pode ser objeto de disposições especiais do artista enquanto ainda vivo, e qualquer utilização *post mortem* está sujeita a tais disposições, bem como às opiniões que o artista tenha publicizado em vida.

É possível, aqui, traçar um contraponto entre a regulação que se propõe para o uso da voz (e também da imagem) do artista falecido e a doação de órgãos. No caso desse ato de extremo altruísmo, a lei e a praxe determinam que a vontade do cônjuge ou dos parentes de primeiro e segundo graus prevalece sobre a vontade do próprio indivíduo doador manifestada em vida.

Porém, quanto à ressurreição digital, entende-se descabido que a oposição de herdeiros possa ir de encontro à autorização anterior concedida pelo artista falecido, a exemplo do que ocorre na doação de órgãos. Isso porque não se está aqui diante de uma questão ética ou de uma disposição do próprio corpo, mas sim de uma

obra artística, em que a individualidade e a liberdade artística devem ser privilegiadas, ainda que a contragosto de parentes.

Herdeiros estes que devem obedecer à vocação hereditária prevista no art. 1.829 do Código Civil; isto é, em primeiro lugar, aos descendentes em concorrência com o cônjuge supérstite, observadas as exceções quanto ao regime de casamento; em sequência, aos ascendentes, também em concorrência com o cônjuge sobrevivente; em terceiro lugar, ao próprio cônjuge sobrevivente; e, em quarto e último lugar, aos colaterais.

3. DOS DIREITOS AUTORAIS

Dos direitos da personalidade surgem os direitos autorais, tanto que, na produção doutrinária anterior à Lei nº 9.610/1998[19], o "direito às criações intelectuais" era tratado como parte dos direitos da personalidade.

Ao regular os direitos autorais, o Brasil adotou a corrente dualista. D'Amico, citando Bittar, ensina que:

> os direitos autorais não pertencem nem aos direitos reais – direitos patrimoniais – e nem aos direitos pessoais, ligados aos direitos morais, justamente porque os direitos autorais possuem ligação direta com ambas as categorias. Dessa forma, é necessário o reconhecimento de que eles constituem, em verdade, uma nova modalidade de direitos privados, ou *sui generis*. São, portanto, direitos de cunho intelectual que resguardam tanto a exploração dos direitos patrimoniais, quanto os vínculos que existem entre o autor e sua obra[20].

Nesse sentido, os direitos autorais são conceituados como o "ramo do Direito Privado que regula as relações jurídicas, advindas da criação e da utilização econômica de obras intelectuais estéticas e compreendidas na literatura, nas artes e nas ciências"[21].

Assim, diferentemente do que ocorre com os direitos da personalidade, os direitos autorais possuem não apenas um caráter moral, inerente à pessoa e, em alguns casos intransmissível por morte[22], mas também um aspecto patrimonial, que pode ser objeto de negócios jurídicos onerosos, como define a legislação[23].

[19] BRASIL. **Lei nº 9.610, de 19 de fevereiro de 1998**. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Brasília, DF: Presidência da República, 1998.

[20] D'AMICO, *op. cit.*, p. 30 et seq.

[21] *Ibid.*, p. 28 et seq.

[22] BRASIL. **Lei nº 9.610, de 19 de fevereiro de 1998**, *op. cit.*, art. 24, § 1º.

[23] *Ibid.*, arts. 28 e seguintes.

Dúvidas não há de que os autores, compositores de músicas e diretores de obras audiovisuais possuem segurança especial atribuída pela lei à utilização de suas obras com fins patrimoniais por terceiros, eis que lhes é assegurado o gozo exclusivo por 70 anos, a contar do primeiro dia do ano subsequente à morte[24].

Especificamente no caso de profissionais cuja expressão artística se revela em performances nas quais a exibição de elementos corporais é indissociável da própria arte, como as artes cênicas e musicais – neste ponto em especial o canto –, a utilização de elementos personalíssimos, como a imagem e a voz, para a recriação de obras com o auxílio de inteligência artificial, no momento posterior à morte do artista, apresenta-se como possível violação aos direitos autorais.

Isso porque o artista intérprete ou executante tem, por força do disposto no art. 90, da Lei nº 9.610/1998, "o direito exclusivo de, a título oneroso ou gratuito, autorizar ou proibir"[25], a "fixação de suas interpretações ou execuções"[26], bem como "a reprodução, a execução pública e a locação das suas interpretações ou execuções fixadas"[27].

Por execução fixada entende-se a gravação ou reprodução de uma interpretação musical ou fonograma em um meio tangível, como um CD, DVD, fita cassete ou arquivo digital. Isso inclui a captura de performances musicais, como shows ao vivo, concertos em estúdio, recitais, peças teatrais e a preservação dessas interpretações em mídias físicas ou digitais.

Assim, as disposições legais mencionadas acima resguardam, de maneira induvidosa, a utilização não autorizada das imagens e vozes de artistas para o fim de promover sua ressurreição digital, nos termos do art. 90, § 2º, da mesma lei.

E, muito embora o art. 90, § 1º faça a ressalva de que em obras coletivas os direitos do art. 90, *caput*, devam ser exercidos pelo diretor do conjunto, entende-se mais correta, ante a novidade trazida pela inteligência artificial, a interpretação de que também o artista, individualmente considerado, possa impedir a utilização das imagens ou gravações da sua voz para nova produção audiovisual ou musical, seja por ato próprio em vida ou por manifestação de seus herdeiros.

Entendimento idêntico deve ser garantido aos herdeiros no caso de o artista já falecido não ter feito qualquer manifestação quanto à autorização ou à vedação da utilização de sua imagem ou voz.

E, à semelhança do que ocorre com a discussão relativa aos direitos da personalidade, eventual ato de vontade do artista manifestado em vida, como em um contrato firmado com o estúdio de gravação, que tenha vedado a utilização de gravações

[24] *Ibid.*, arts. 41, 43-44.

[25] *Ibid.*, art. 90.

[26] Ibid., art 90, inciso I.

[27] *Ibid.*, art. 90, inciso II.

que envolvam a sua pessoa em obras posteriores criadas por inteligência artificial, não pode ser suprido ou reformado por manifestação de seus herdeiros – ou "parentes próximos", como quer o Projeto de Lei nº 3.592/2023 – em sentido oposto, sob pena de se privilegiar interesses econômicos em detrimento dos direitos morais do autor ou dos direitos conexos do intérprete.

4. CONCLUSÃO

A possibilidade de utilização da imagem e da voz de artistas mortos para a ressurreição digital deve estar limitada, em primeiro lugar, pela opinião do artista, tanto a manifestada expressamente, em escritos ou gravações (audiovisuais ou de captação de áudio), quanto a demonstrada pela imagem-atributo do artista quando vivo, por meio de seus posicionamentos públicos e que possam ser comprováveis por quaisquer meios de prova em direito admitidos.

Especialmente relevante é a ofensa à opinião do artista morto, já que, uma vez encerrada sua vida, aquelas opiniões que tenham sido registradas, por quaisquer meios idôneos (imprensa, livros, escritos ou gravações particulares) devem ser consideradas em eventual recriação de sua obra por ferramentas de inteligência artificial. Isso se deve não somente pelo respeito ao morto, mas também pelo caráter indissociável existente entre a imagem de uma pessoa notória, sua obra artística e suas opiniões publicizadas.

Entende-se, assim, que, havendo uma manifestação do artista em vida no sentido de que determinada posição política, manifestação cultural, empreendimento econômico ou qualquer outro engenho humano estava em descompasso com sua visão de mundo, a utilização de ferramentas de inteligência artificial para a recriação da imagem do artista, com a geração de uma obra artística ou mesmo uma peça publicitária que sugira seu endosso àquela determinada manifestação da criatividade humana, deve ser vedada.

No entanto, caso não seja obedecida a intenção manifestada pelo artista, cabe aos herdeiros, na forma da lei (art. 1.829, Código Civil) – mas não aos "parentes próximos", figura inexistente na ordenação civil brasileira e que é mencionada de maneira atécnica no Projeto de Lei nº 3.592/2023 – postular judicialmente a proibição da utilização da imagem do artista falecido, bem como o recebimento de indenização, conforme a Súmula 642 do Superior Tribunal de Justiça, segundo a qual "o direito à indenização por danos morais transmite-se com o falecimento do titular, possuindo os herdeiros da vítima legitimidade ativa para ajuizar ou prosseguir a ação indenizatória"[28]. No limite, pode-se buscar a vedação de sua reprodução ou mesmo a retirada de circulação dos meios de divulgação.

[28] BRASIL. Superior Tribunal de Justiça. **Súmulas do Superior Tribunal de Justiça**. Brasília: STJ, 2015. v. 1.

E, em havendo conflito entre a manifestação expressa pelo artista falecido e seus herdeiros – e não "parentes próximos", frise-se –, em que alguns destes últimos autorizem a utilização da imagem e da voz do morto para a ressurreição digital, há evidente interesse de outro(s) em fazer prevalecer a opinião e a figura pública do artista falecido. Nesse caso, a intervenção judicial é perfeitamente justificável, cabendo ao magistrado, assim como em outras hipóteses de interesses conflitantes, dirimir a lide.

É possível, aqui, traçar um contraponto entre a regulação que se propõe para o uso da imagem do artista falecido e a doação de órgãos. No caso deste ato de extremo altruísmo, a praxe é de que a vontade dos parentes de primeiro e segundo graus prevalece sobre a vontade do próprio indivíduo doador.

Não se entende possível, no entanto, que a oposição de herdeiros possa ir de encontro à autorização anterior concedida pelo artista falecido, a exemplo do que ocorre na doação de órgãos, em que é praxe dos médicos, calcada em orientação do Conselho Regional de Medicina[29], que a opinião dos parentes prevaleça em relação à manifestação do falecido, dada, por exemplo, em sua carteira de identidade, com a expressão "doador de órgãos e tecidos".

Assim o é porque, diferentemente da disposição do próprio corpo – em que aspectos éticos e religiosos prevalecem –, na (re)utilização da imagem e da voz, os elementos estéticos e mesmo patrimoniais, que são exclusivos do autor (art. 28, Lei nº 9.610/1998), devem ter prioridade, resguardando-se a livre manifestação de vontade do artista.

REFERÊNCIAS BIBLIOGRÁFICAS

BITTAR, Carlos Alberto. **Os direitos da personalidade**. Rio de Janeiro: Forense Universitária, 1989.

BRASIL. **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: 3 abr. 2026.

BRASIL. **Lei nº 9.610, de 19 de fevereiro de 1998**. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Brasília, DF: Presidência da República, 1998.

BRASIL. **Lei nº10.406, de 10 de janeiro de 2002**. Código Civil. Brasília, DF: Senado Federal, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 3 abr. 2026.

[29] BRASIL. Conselho Federal de Medicina. Resolução CFM nº 2.173, de 23 de novembro de 2017. Define os critérios do diagnóstico de morte encefálica. **Diário Oficial**, Brasília, 15 dez. 2017, Seção I, p. 274-276.

BRASIL. Senado Federal. **Projeto de Lei nº 3.592/2023**. Brasília, DF: Senado Federal, 2023.

BRASIL. Superior Tribunal de Justiça. **Súmulas do Superior Tribunal de Justiça**. Brasília: STJ, 2015. v. 1.

BRASIL. Conselho Federal de Medicina. Resolução CFM nº 2.173, de 23 de novembro de 2017. Define os critérios do diagnóstico de morte encefálica. **Diário Oficial**, Brasília, 15 dez. 2017, Seção I, p. 274-276.

CUPIS, Adriano de. **Os direitos da personalidade**. Tradução de Afonso Celso Furtado Rezende. São Paulo: Quorum, 2008.

D'AMICO, Gustavo Fortunato. **Ressurreição Digital**: aspectos jurídicos e repercussões. Curitiba: IODA, 2021.

FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência Artificial e Direito**. 2. ed. revista, atualizada e ampliada. São Paulo: Revista dos Tribunais, 2020.GILCHRIST, Alasdair. **Industry 4.0**: The Industrial Internet of Things. New York: Apress, 2016.

MONTEIRO FILHO, Raphael de Barros. **Comentários ao novo Código Civil**: das pessoas (Arts. 1 a 78). Rio de Janeiro: Forense, 2010. v. 1.

OLIVEIRA, Fábia. Regina Duarte se revolta contra obrigatoriedade de vacina em crianças. **Metrópoles**, 4 jan. 2024. Disponível em https://www.metropoles.com/colunas/fabia-oliveira/regina-duarte-se-revolta-contra-obrigatoriedade-de-vacina-em-criancas. Acesso em: 3 mar. 2026.

PARODI. Alessandro. The Beatles to releases AI-powered new song with Lennon's voice. **Reuters**, 2 nov. 2023. Disponível em: https://www.msn.com/en-ca/entertainment/other/the-beatles-to-release-ai-powered-new-song-with-lennons-voice/ar-AA1jhGUC. Acesso em: 14 abr. 2026.

PEREIRA, Caio Mário da Silva. **Direito Civil: alguns aspectos de sua evolução**. Rio de Janeiro: Forense, 2001.

PULVER, Andrew; SHOARD, Catherine. The Hollywood actors' strike: everything you need to know. **The Guardian**, 14 jul. 2023. Disponível em: https://www.theguardian.com/culture/2023/jul/14/the-hollywood-actors-strike-everything-you-need-to-know. Acesso em: 3 mar. 2026.

REGINA Duarte publica fake news sobre vacina contra a Covid-19 para crianças. **Folha de S.Paulo**, 4 jan. 2024. Disponível em https://www1.folha.uol.com.br/ilustrada/2024/01/regina-duarte-publica-fake-news-sobre-vacina-contra-a-covid-19-para-criancas.shtml. Acesso em: 15 maio 2024.

REUTERS. **World's oldest oil paintings in Afghanistan**. Disponível em: https://www.reuters.com/article/idUSISL260424/. Acesso em: 3 mar. 2026.

ROCHA, Katiane Rosa da, *et. al.*. Entrevista Familiar. In: GARCIA, Clotilde Druck; GARCIA, Valter Duro; PEREIRA, Japão Dröse (org.). **Manual de doação e transplantes**: informações práticas sobre todas as etapas do processo de doação de órgãos e transplante. Porto Alegre: Libretos, 2017. p. 104-105.

SHAH, Simone. The Writers Strike Is Taking a Stand on AI. **Time**, 11 dez. 2023. Disponível em: https://time.com/6277158/writers-strike-ai-wga-screenwriting/. Acesso em: 3 mar. 2026.

TOMAZETTE, Marlon. **Direito digital e inteligência artificial**: diálogos entre Brasil e Europa. Indaiatuba: Editora Foco, 2021. Edição Kindle.

VIEIRA, Luíza. Comercial da Volkswagen com Elis Regina levanta debate sobre ditadura e nazismo; entenda. **O Povo**, 5 jul. 2023. Disponível em: https://www.opovo.com.br/noticias/politica/2023/07/05/comercial-da-volkswagen-com-elis-regina-levanta-debate-sobre-ditadura-e-nazismo-entenda.html. Acesso em: 3 mar. 2026.

ZANETTI, Laysa. Apelativo, comercial com Elis e Maria Rita não entendeu "Como Nossos Pais". **Splah Uol**, 4 jul. 2023. Disponível em: https://www.uol.com.br/splash/noticias/2023/07/04/apelativo-comercial-com-elis-e-maria-rita-nao-entendeu-como-nossos-pais.htm. Acesso em: 3 mar. 2026.

Submetido em: 07/01/2025
Aprovado em: 10/06/2025

TECNOLOGIA E SAÚDE: A PROTEÇÃO DE DADOS NO SISTEMA ÚNICO DE SAÚDE E A TELEMEDICINA

Technology and Health: Data Protection in the Unified Health System and Telemedicine

Izadora Rodrigues Normando Simões[1]

SUMÁRIO 1. Introdução; 2. A LGPD e a Proteção dos Dados; 3. Dados de Saúde: Estrutura Legal; 3.1 Os dados na Constituição Federal de 1988; 3.2. Direito à saúde; 4. A LGPD: A Proteção de Dados de Saúde; 5. Dados Pessoais da Saúde: Dados Sensíveis; 6. Construção de Políticas Públicas – Controle e Avaliação; 6. 1. Tecnologia e Saúde: a Telemedicina e a Proteção de Dados; 7. Conclusão; Referências Bibliográficas.

RESUMO O presente artigo discorre sobre a Lei Geral de Proteção de Dados (LGPD), instituída pela Lei Federal nº 13.709, de 14 de agosto de 2018, regulamentada no âmbito do Estado de São Paulo pelo Decreto nº 65.347, de 9 de dezembro de 2020, explorando a perspectiva dos dados pessoais relativos à saúde, os quais requerem melhor estudo, diante do ambiente desafiador proporcionado pelas novas tecnologias, o armazenamento em grande escala de bancos de dados e pela telemedicina. O propósito é despertar a atenção ao fato de que, sem a devida regulamentação e conformidade com a LGPD, dados sensíveis de saúde podem ser utilizados para diversos fins éticos duvidosos, por vezes de forma irregular ou ilícita. No intuito de melhor desenvolver o tema, após breve desenvolvimento sobre questões conceituais atinentes ao assunto em testilha, propõe-se uma análise legislativa, com pesquisa bibliográfica e leitura crítica de doutrinas, dissertações, artigos acadêmicos e científicos. Pretende-se concluir com a investigação dos principais desafios a serem trabalhados pelos operadores imersos no fluxo da telemedicina.

Palavras-chave: LGPD. Dados Sensíveis. SUS. Telemedicina.

ABSTRACT This article examines the General Data Protection Law (LGPD), enacted by Federal Law No. 13,709 of August 14, 2018, and regulated within the State of São Paulo by Decree No. 65,347 of December 9, 2020. It explores the perspective of personal health data, which requires further study in light of the challenging environment created by new technologies, large-scale data storage, and telemedicine. The purpose is to draw attention to the fact that, without proper regulation and compliance with the LGPD, sensitive health data may be used for various ethically questionable purposes, sometimes in an irregular or unlawful manner. In order to further develop the topic, after a brief discussion of conceptual issues related to the subject at hand, a legislative analysis is proposed, based on bibliographic research and critical reading of legal doctrines, dissertations, and academic and scientific articles. The study aims to conclude by investigating the main challenges to be addressed by professionals operating within the telemedicine framework.

Keywords: General Data Protection Law (LGPD). Sensitive Data. Unified Health System (SUS). Telemedicine.

[1] Graduação em Direito pela Universidade Paulista. Pós-graduação em Direito Administrativo, Processo Civil e Direito Digital e Inovação pela Escola Superior da Procuradoria-Geral do Estado de São Paulo.

DOI: 10.22491/*respge*.v16i1.1735

1. INTRODUÇÃO

A crise sanitária global causada pela emergência em saúde pública da covid-19[2] conduziu a um significativo avanço na transformação digital da área da saúde, havendo, em curto espaço de tempo, um uso exponencial de tecnologias digitais de informação e comunicação (TICs), entre elas a telemedicina e a telessaúde, na relação entre os profissionais de saúde e os pacientes, trazendo novos contornos para fins de assistência, educação, pesquisa, prevenção de doenças e lesões, gestão e promoção da saúde.

A tecnologia vem permitindo, ainda, entre outros pontos: o armazenamento em grande escala e o volume de dados estruturados e não estruturados, provenientes de várias fontes e bases de dados, cujo contexto ultrapassa o conceito de telemedicina; aplicativos que tratam em massa dados de saúde; prontuário eletrônico do paciente[3], ou seja, há todo um cenário tecnológico hoje que envolve a área da saúde.

A Lei Federal nº 14.510[4], de 27 de dezembro de 2022, consagrou a telessaúde no Brasil, alterando a Lei Orgânica da Saúde (Lei nº 8.080, de 19.09.90), que estrutura o Sistema Único de Saúde (SUS), para autorizar e disciplinar a prática em todo o território nacional. Sendo assim, reconhecida a modalidade de Teleatendimento dentro da cadeia de serviços do SUS.

A telessaúde é um conceito amplo, que envolve diferentes serviços remotos de assistência, diagnóstico, educação e pesquisa em saúde, além de ser um método

---

[2] A Emergência em Saúde Pública de Âmbito Nacional em decorrência da Infecção Humana pelo novo coronavírus (2019-nCoV), denominado oficialmente de vírus SARS-CoV-2, foi decretada pela Portaria GM-MS nº 188, de 3 de fevereiro de 2020, e encerrada pela Portaria GM/MS nº 913, de 22 de abril de 2022. Destacam-se algumas medidas no âmbito do Estado de São Paulo, após a imposição da quarentena no contexto da pandemia da COVID-19, pelo Decreto nº 64.881, de 22/03/2020, podem ser verificadas nas seguintes normas: Decreto nº 64.994, de 28/05/2020; Decreto nº 65.044, de 03/07/2020; Decreto nº 65.100, de 29/07/2020; Decreto nº 65.110, de 05/08/2020; Decreto nº 65.141 de 19/08/2020; Decreto nº 65.163, de 02/09/2020; Resolução SS-127, de 11/09/2020; Decreto nº 65.319, de 30/11/2020; Decreto nº 65.460, de 08/01/2021; Decreto nº 65.487 de 22/01/2021; Decreto nº 65.529 de 19/02/2021; Decreto nº 65.545 de 03/03/2021; Decreto nº 65.563 de 11/03/2021; Decreto nº 65.596 de 26/03/2021; Decreto nº 65.613 de 09/04/2021; Decreto nº 65.635 de 16/04/2021; Decreto nº. 65.663 de 30/04/2021; Decreto nº 65.680 de 07/05/2021; Decreto nº 65.716 de 21/05/2021; Decreto nº 65.731 de 28/05/2021; Decreto 65.792, de 11/06/2021; Decreto nº 65.839, de 30/06/2021; Decreto nº 65.856, de 07/07/2021; Decreto nº 65.897, de 30/07/2021 e, por fim, o Decreto nº 67.529, de 03/03/2023, que retirou a obrigatoriedade do uso de máscara.

[3] Para fins de exemplificação, sugere-se consulta ao: (I) Seade Coronavírus. Disponível em: https://coronavirus.seade.gov.br/?utm_source=portal&utm_medium=banner&utm__campaign=bo%20letim-completo.%20%C3%9Altimo%20acesso%20em%2010%2F06%2F2021. Acesso em 30 mar. 2026; (II) Painel de Monitoramento (Divisão de Dengue, Chikungunya e Zica). Disponível em https://dengue.saude.sp.gov.br/dengue/. Último acesso em: 25 maio 2024.

[4] BRASIL. Lei nº 14.510, de 27 de dezembro de 2022. Altera a Lei nº 8.080, de 19 de setembro de 1990, para autorizar e disciplinar a prática da telessaúde em todo o território nacional, e a Lei nº 13.146, de 6 de julho de 2015; e revoga a Lei nº 13.989, de 15 de abril de 2020. **Diário Oficial**, Brasília, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14510.htm. Acesso em: 30 mar. 2026.

que abrange outros profissionais da saúde. Enquanto a telemedicina, regulamentada pela Resolução do Conselho Federal de Medicina nº 2.314, de 20.04.22[5], é um "braço" da telessaúde e se dedica ao suporte diagnóstico remoto, por meio de soluções como laudos médicos à distância e uma segunda opinião qualificada, por exemplo. Utilizada especificamente para serviços médicos, refere-se a atos e procedimentos realizados por ou sob responsabilidade de um médico; assim, a assistência (remota) à saúde se realiza pelas ações de diferentes profissionais. O médico não é o mais importante e nem o único agente no processo.

A tecnologia em saúde permite o tratamento massivo e síncrono de dados de saúde por diversos meios digitais, por vezes, sem interação com o paciente. Seu avanço permite o aumento do tráfego síncrono de dados pessoais sensíveis, como os de saúde, em diferentes meios digitais, integrados por meio de *Application Programming Interfaces* (APIs), tornando a saúde digital vulnerável a ataques cibernéticos e outros tipos de incidentes.

A tecnologia na área da saúde é uma importante aliada e um caminho sem volta, e vai impactar, cada vez mais rapidamente, as formas de pesquisar, prevenir, diagnosticar e tratar doenças[6].

Ainda, o tratamento irregular, ilícito ou inseguro, sem a devida regulamentação e fiscalização, dos dados sensíveis corpóreos que trafegam hoje no complexo ecossistema da saúde digital pode resultar na utilização desses dados com objeto de análise e na aplicação de técnicas avançadas para criar classificações, perfilizações e, inclusive, previsões e padrões comportamentais que permitem a oferta de serviços adicionais e de produtos a partir do tratamento secundário (e terciário) de dados pessoais sensíveis de saúde. Trata-se de atividade de "alto risco", com potencial discriminatório e lesivo para o sujeito mais vulnerável, o paciente digital, resumido a informações contidas em vastos bancos de dados.

A legislação brasileira, ao contrário do Regulamento da União Europeia 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, General Data Protection Regulation (GDPR)[7], não definiu diretamente o conceito de "dados pessoais relativos à saúde". Cabe ao intérprete buscar essa definição no quadro legislativo atual e acompanhar o desdobramento do tema por meio das orientações da Agência Nacional de Proteção De Dados (ANPD), pela própria compreensão do

[5] CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 2.314/2022. Define e regulamenta a telemedicina, como forma de serviços médicos mediados por tecnologias de comunicação. **Diário oficial**, Brasília, 5 maio 2022, Seção I, p. 227.

[6] Sugere-se consulta ao sítio eletrônico "#Vacinajá", no qual é possível verificar as doses de vacinas aplicadas por município do estado de São Paulo, segundo diversos indicadores. Disponível em: https://vacinaja.sp.gov.br/vacinometro/. Acesso em: 30 maio 2024.

[7] UNIÃO EUROPEIA. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – GDPR)**. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679. Acesso em: 30 mar. 2026.

problema pelos gestores do SUS e pelo aprimoramento dos instrumentos jurídicos, com foco na relação titular–controlador–operador–encarregado–agentes de tratamento, em especial, nos convênios e contratos de gestão de saúde e, eventualmente, em decisões judiciais.

A definição deve coincidir com o conceito amplo de saúde, adotado pelo artigo 3º da Lei Federal nº 8.080, de 19 de setembro de 1990[8], com determinantes e condicionantes que contemplem, inclusive, o bem-estar físico, mental e social. Nesse sentido, perfazendo este "conceito ampliado de saúde", conforme o § 1º do artigo 11 da LGPD: dados pessoais, em princípio "comuns", como a geolocalização, a depender dos cruzamentos e inferências, podem revelar dados pessoais sensíveis de saúde, mitigando a tese da taxatividade estática do artigo 5º, II, da LGPD.

O tema ainda carece da devida regulamentação e há muito o que evoluir; como mencionado, dados sensíveis de saúde podem ser utilizados para diversos fins eticamente delicados e duvidosos, e com vantagem econômica, caso tratados de maneira irregular ou ilícita. A título de exemplo, podem: determinar quem vai ter um emprego ou não, com base nas condições de saúde; induzir demissões, com base em decisões automatizadas com o uso de algoritmos; definir qual o preço que uma pessoa pagará em seu plano de saúde; definir o valor do financiamento imobiliário, com base em potencial diagnóstico, como diabetes tipo II, conforme perfil de consumo na farmácia (ao informar o Cadastro de Pessoa Física - CPF); definir que tipo de condições de saúde serão admitidas nas políticas de imigração entre países; e induzir uma pessoa a determinados comportamentos, como os relacionados à vacinação.

Desse modo, o presente trabalho pretende apresentar essas questões e fazer uma breve análise da necessidade de aprimoramento de processos e protocolos para a proteção de dados pessoais relativos à área da saúde, em especial, na telemedicina.

2. A LGPD E A PROTEÇÃO DOS DADOS

Nas últimas décadas, vivemos um intenso processo de transformação digital, e a presença da tecnologia da informação se apresenta como mediadora nas mais diversas relações humanas com as máquinas, que estão cada vez mais autônomas. Em um mundo digital em constante evolução, a quantidade de informações e dados gerados na interação entre dispositivos tecnológicos e pessoas é incalculável.

Ainda que muitas vezes não se deem conta, as pessoas passaram a ser geradoras de dados. Isso ocorre porque, nas mais diversas relações – seja em compras em farmácias, em simples pesquisas em sites de busca de informações, na manutenção

[8] BRASIL. Lei nº 8.080, de 15 de dezembro de 1990. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências. **Diário Oficial**, Brasília, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8080.htm. Acesso em: 30 mar. 2026.

de perfil em redes sociais, na abertura de contas em banco, na utilização de ferramentas de vigilância, por meio de reconhecimento facial ou biométrico, em serviços de saúde etc. – dados pessoais são extraídos, transferidos e armazenados em inúmeros bancos de dados, nos quais nossa identidade é permanentemente analisada e utilizadas para os mais diferentes fins, tanto por instituições privadas quanto por instituições públicas.

No entender de Chiara Teffé[9]:

> Os dados contam histórias sobre nós: indivíduos, grupos e sociedade. Quanto mais dados pessoais tratados e tecnologias sofisticadas empregadas, mais perfis serão criados e análises e predições realizadas. A partir de informações pessoais, é possível conhecer hábitos, comportamentos, gostos preferências, descendências, estado de saúde e crenças de uma pessoa. Ao longo do tempo, a qualidade e a precisão das análises vêm sendo aperfeiçoadas, havendo inclusive a utilização de complexas estruturas de inteligência artificial nos processos, e seus resultados utilizados para os mais variados fins, por instituições públicas e privadas.

No que tange ao setor público, observa Lucas Borges[10] que:

> […] entre outras inovações, o processo de digitalização permite que informações que, há algumas décadas, estavam registradas apenas de forma analógica, muitas vezes impressas em documentos arquivados em armários nas diversas repartições públicas, possam ser armazenadas em formato digital, em computadores com alta capacidade de processamento. Com isso, é possível não somente ampliar e acelerar a coleta de informações pessoais, como também inferir novas informações ou realizar o cruzamento entre as diversas bases de dados, destinando-as para múltiplas finalidades, em particular mediante o seu uso compartilhado com outros órgãos públicos e entidades privadas.

Nessa crescente transformação digital e produção de informações, os dados pessoais tornaram-se ativos valiosos para governos e empresas, sendo certo que a falta de proteção adequada desses dados pode levar a abusos, violações de privacidade, roubo de identidade e outros crimes cibernéticos.

Não há dúvidas de que a transformação digital vem resultando em inúmeros benefícios para a sociedade, e apresenta-se como um processo fundamental para ampliar a eficiência, não apenas no setor privado, mas também na atuação do Estado (como prestador de serviços, na sua função de formular políticas públicas e

[9] TEFFÉ, Chiara Spadaccini de. **Problemas de direito civil**: homenagem aos 30 anos de cátedra do professor Gustavo Tepedino por seus orientandos e ex-orientandos. Rio de Janeiro: Forense, 2021, p. 97.

[10] CARVALHO, Lucas Borges de. O Poder Público e a proteção de dados pessoais no Brasil: novos desafios, velhas práticas administrativas. **Revista de Direito Administrativo**, Rio de Janeiro, v. 282, n. 2, p. 133-162, 2023, p. 16-17.

na garantia de direitos sociais, como os relacionados à educação, à saúde e ao trabalho). Entretanto, como mencionado, isso trouxe desafios importantes ao Direito, especialmente no que tange à proteção da privacidade dos indivíduos, uma vez que se ampliam os riscos de abusos e de violação aos direitos dos titulares, que podem ocorrer pelo mau uso de seus dados.

A Constituição Federal de 1988 estabelece em seu artigo 5º, inciso X, a garantia de proteção dos direitos fundamentais da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação, sendo este princípio constitucional a base para a proteção da privacidade no contexto digital.

Nessa perspectiva fática (constante evolução digital em que dados são gerados indiscriminadamente) e constitucional (proteção aos direitos fundamentais da privacidade, intimidade e liberdade), a LGPD[11] tem como disciplina o respeito à privacidade, à autodeterminação informativa, à liberdade de expressão, de informação, de comunicação e de opinião, à inviolabilidade da intimidade, da honra e da imagem, ao desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor, aos direitos humanos, ao livre desenvolvimento da personalidade, à dignidade e ao exercício da cidadania pelas pessoas naturais (art. 2°, LGPD), nas mais diversas relações estabelecidas entre pessoas naturais e/ou pessoas jurídicas, e às tecnologias.

Aplicada tanto no setor público quanto no privado, assim como nos ambientes físico e virtual, estabelecendo regras para a coleta, armazenamento, tratamento e compartilhamento de dados, a LGPD impõe a completa releitura de todas as formas de tratamento de dados pessoais, nas mais diversas áreas. Nessa linha, defende Beatriz Freitas Santos que, ao estabelecer regras claras para a coleta, o armazenamento, o tratamento e o compartilhamento de dados, "a LGPD busca proteger os direitos fundamentais de liberdade e privacidade, promovendo também a segurança jurídica e o desenvolvimento econômico e tecnológico do Brasil"[12].

Pode-se dizer que a LGPD, ao proteger os dados pessoais, desempenha um papel crucial no cenário da transformação digital, pois fornece as bases para a confiança dos cidadãos e consumidores, sendo essencial para fortalecer a proteção efetiva dos direitos individuais, promovendo a confiança de investidores, empresas e cidadãos no ambiente digital.

[11] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispões sobre a Lei Geral de Proteção de Dados. **Diário Oficial**, Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 mar. 2026.

[12] SANTOS, Beatriz Freitas. Lei Geral de Proteção de Dados (LGPD) e a garantia de proteção dos direitos fundamentais de liberdade e de privacidade dos cidadãos à luz do Direito Constitucional. **Aporia Jurídica**, Ponta Grossa v. 1, n. 19, 2023.

Além disso, a LGPD contribui para melhorar a governança de dados e fomentar a justiça e a igualdade no acesso e na utilização de informações pessoais. A legislação também tem impacto na forma como as organizações gerenciam os dados, incentivando a adoção de práticas responsáveis e transparentes, evitando o mau uso das informações e promovendo a conscientização sobre a importância da proteção de dados. Em resumo, a LGPD é fundamental para garantir a segurança, a privacidade e a confiabilidade nos ambientes físico e digital, além de fortalecer a proteção dos direitos individuais e promover o desenvolvimento sustentável da inovação no Brasil.

Vale destacar que a LGPD contém expressa previsão de aplicação de suas normas às pessoas jurídicas de direito público (art. 1°):

> […] as quais devem observar princípios gerais como os da necessidade, finalidade e adequação (art. 6º), além de obrigações específicas de transparência (art. 23). Da mesma forma, aos usuários de serviços públicos foram assegurados importantes direitos, tais como os de acesso aos dados e correção de dados incompletos, inexatos ou desatualizados (art. 18, II e III), de oposição a tratamento efetuado sem consentimento (art. 18, § 2º) e de revisão de decisões automatizadas (art. 20). Por fim, em caso de irregularidades, a Autoridade Nacional de Proteção de Dados (ANPD) pode aplicar sanções administrativas a entidades e órgãos públicos (art. 52, § 3º)[13].

Nas relações com as instituições públicas, deve-se considerar que o cidadão é o elo mais frágil e vulnerável, uma vez que suas informações pessoais são coletadas de forma compulsória e, se não adotadas as devidas salvaguardas, podem ser utilizadas para fins abusivos, associados às práticas de discriminação ou de vigilância.

A coleta de informações dos cidadãos pelo Estado está muito bem estabelecida e estruturada, envolvendo quantidades massivas de dados pessoais, muitas vezes, armazenadas em formato digital e tratadas de forma automatizada. Nesse sentido, os dados pessoais constituem um insumo relevante para ampliar a eficiência da ação estatal, por exemplo, por meio do compartilhamento de informações entre entidades e órgãos públicos ou, ainda, mediante à produção de evidências que embasam a formulação de políticas públicas.

Como ressalta Miriam Wimmer[14]:

> A questão sobre o quão bem o Estado deve conhecer seus cidadãos já foi enfrentada em variados contextos e em diferentes momentos históricos, tendo por pano de fundo o reconhecimento de que, ao mesmo tempo que o tratamento de dados pessoais pelo Estado é pré-requisito para o exercício

[13] CARVALHO, *op. cit.*, p. 2.

[14] WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo poder público. *In*: MENDES, Laura, *et al*. (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021, p. 273.

> da cidadania, a expansão da quantidade e da variedade de dados pessoais custodiados pelo Estado suscita riscos de violações de direitos. Dito de outro modo, a visibilidade do Estado sobre seus cidadãos permite ampliar a sua capacidade de intervenção, tenha ela por objetivo atingir finalidades sociais justas (e.g., viabilizar a distribuição de benefícios sociais) ou nefastas.

Quanto ao processo de coleta massiva de dados pessoais, alerta Lucas Borges[15] que este gera um "excedente comportamental", ou seja:

> […] uma espécie de sobrevalor, que transcende os propósitos originais da operação de coleta. Como consequência, mesmo após exauridos os seus objetivos iniciais, o uso de um conjunto de dados pessoais tende a permanecer atrativo e valioso para outras finalidades. Esse uso subsequente e contínuo dos dados pessoais permite gerar um valor adicional significativo – seja ele de ordem pública, política ou econômica – a um custo marginal reduzido, em particular diante da possibilidade de realização de novas inferências a partir de técnicas de análise de dados ou de simples agregação de novas informações, entre outras possibilidades, sempre visando ao controle, à previsão e ao direcionamento de comportamentos.

É importante salientar que, conforme a legislação, no setor público, o tratamento de dados pessoais para propósitos distintos daqueles que justificaram a coleta inicial deve, entre outras condições, sempre atender a uma finalidade pública. Conforme disposto de forma expressa no seu art. 26, a LGPD estabelece que "o uso compartilhado de dados pessoais pelo Poder Público deve atender à finalidade específica de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas".

É fundamental que a LGPD e sua aplicação continuem a ser aprimoradas e aperfeiçoadas, a fim de se manterem atualizadas e relevantes em um ambiente digital em constante evolução. Investir em educação e conscientização sobre a importância da privacidade e da proteção de dados é uma ferramenta eficaz para promover uma cultura de respeito à privacidade e à segurança digital.

3. DADOS DE SAÚDE: ESTRUTURA LEGAL

3.1 Os *dados na Constituição Federal de 1988*

A Constituição Federal de 1988 originalmente previu a proteção do acesso a dados e informações pela criação de instrumento processual denominado *Habeas Datas* (art. 5°, inciso LXXII), nos seguintes termos:

[15] CARVALHO, *op. cit.*, p. 10.

> LXXII - conceder-se-á *"habeas-data"*:
>
> a) para assegurar o **conhecimento de informações** relativas à pessoa do impetrante, constantes de registros ou **bancos de dados de entidades governamentais ou de caráter público;**
>
> **b) para a retificação** de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; […][16]

No ano de 2022, foi incluída, pela Emenda Constitucional nº 115/2022[17], a proteção de dados pessoais entre os direitos e garantias fundamentais, inclusive digitais, dando competência privativa a União para legislar sobre a proteção e o tratamento de dados pessoais: "XXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais (Incluído pela Emenda Constitucional nº 115, de 2022)".

Classificou-se a emenda constitucional como uma "medida meritória" que reforça a segurança jurídica e favorece os investimentos em tecnologia no Brasil, a qual complementa, lastreia e reforça dispositivos inseridos recentemente na legislação ordinária, como o Marco Civil da Internet, de 2014, e a Lei Geral de Proteção de Dados, de 2018[18].

Assim, como dito, a emenda constitucional incorporou a proteção dos dados pessoais ao catálogo de direitos e garantias fundamentais, alçando, a despeito das intersecções e articulações com outros direitos, esse direito à categoria de direito fundamental autônomo, com esfera de proteção própria, acabando por atribuir, de modo inquestionável, o pleno regime jurídico constitucional de direito fundamental, material e formal.

Conforme bem elucida Ingo Sarlet[19]:

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

---

[16] BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial**, Brasília, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 8 abr. 2026. Grifo nosso.

[17] 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 fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial**, Brasília, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 8 abr. 2026.

[18] PROMULGADA emenda constitucional de proteção de dados. **Agência Senado**, 10 fev. 2022. Disponível em: https://www12.senado.leg.br/noticias/materias/2022/02/10/promulgada-emenda-constitucional-de-protecao-de-dados. Acesso em: 8 abr. 2026.

[19] SARLET, Ingo. A EC 115/22 e a proteção de dados pessoais como Direito Fundamental I. **Consultor Jurídico**, 2022. Disponível em: https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental/. Acesso em: 30 mar. 2026.

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

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

4) Mediante a redação dada pela EC 115/22, o direito fundamental à proteção de dados pessoais passa a estar submetido a uma expressa reserva legal simples, que empodera o legislador infraconstitucional para efeito de estabelecer intervenções restritivas no âmbito de proteção do direito, implicando, por outro lado, a observância das exigências da reserva de lei, pela de inconstitucionalidade da restrição.

5) O direito fundamental à proteção de dados assume particular relevância, pelo fato da existência de uma série de lacunas regulatórias, porto que a LGPD não contempla os setores da segurança nacional, segurança pública, investigação criminal, execução penal, apenas para citar os mais relevantes. Por tal razão, como o reconhecimento do referido direito fundamentas, para a inexistir uma "zona livre" de proteção dos dados pessoais na ordem jurídica brasileira.

Por fim, importa destacar que nos termos do artigo 5°, §§ 2° e 3°, da CF/88, o marco normativo que concretiza e formata o âmbito de proteção do direito fundamental à proteção de dados pessoais é, também, integrado pelos tratados internacionais de direitos humanos ratificados pelo Brasil, destacando-se a Convenção Americana de São José da Costa Rica e o Pacto Internacional de Direitos Civis e Políticos.

3.2. *Direito à Saúde*

A Constituição Federal de 1988 criou a Seguridade Social como um conjunto integrado de ações de iniciativa do poder público e da sociedade, destinada a assegurar os direitos relativos à saúde, à previdência e à assistência social, nos termos do artigo 194, *caput*, da Constituição Federal.

Inovou ao criar três estruturas distintas dentro da seguridade social: saúde, previdência e assistência social, financiadas por toda a sociedade, de forma direta e indireta, nos termos da lei, mediante recursos provenientes dos orçamentos da União, dos Estados, do Distrito Federal e dos Municípios, além da previsão de contribuições sociais.

Na nossa Carta Constitucional de 1988, a saúde passou a ser definida como um direito fundamental de todos (artigo 6º) e um dever a ser garantido pelo Estado, "garantido mediante políticas sociais e econômicas que visem à redução do risco de

doença e de outros agravos e ao acesso universal e igualitário às ações e serviços para sua promoção, proteção e recuperação"[20], instituindo, assim, o princípio da universalidade no atendimento à saúde.

Contemplando este entendimento, o SUS é o conjunto de ações e serviços de saúde, prestados por órgãos e instituições públicas dos três âmbitos da federação, da administração direta e indireta e das fundações mantidas pelo poder público, com validade em todo o território nacional, regulamentados estruturalmente pela Lei nº 8.080, de 19 de dezembro de 1990, conhecida como a Lei Orgânica da Saúde (LOS), complementada pela Lei nº 8.142, de 28 de dezembro de 1990, matrizes do sistema no âmbito infraconstitucional.

Importante destacar, ainda, que, para cumprir esse princípio constitucional, foi facultado aos gestores do SUS complementar a oferta dos serviços de assistência à saúde em cooperação com entidades privadas de assistência à saúde (artigos 197 e 199, § 1°, da CF/88). Dito isto, participam do SUS não somente as entidades públicas, mas também a iniciativa privada[21].

A concretização do direito à saúde pressupõe respeito aos princípios da igualdade, do acesso universal e da integralidade. A sua estrutura pressupõe a participação consciente da comunidade e o fortalecimento do sistema federativo, por ter sido desenhado com base em uma rede hierarquizada e regionalizada, com ênfase na atuação dos Municípios e nas medidas de prevenção.

Além dos princípios constitucionais aplicáveis aos direitos fundamentais e à seguridade social (art. 194, parágrafo único, CF), há os princípios específicos, previstos na Constituição Federal e no art. 7º da LOS, que deverão ser aplicados a todas as ações e serviços públicos que integram o SUS, incluindo a rede pública e os serviços privados contratados ou conveniados.

Entre eles, cabe destacar o princípio da informação, o qual compreende duas vertentes: i) aspecto individual, em que as pessoas assistidas têm o direito de saber os dados sobre sua saúde; ii) aspecto coletivo, que compreende o direito à divulgação de informações quanto ao potencial dos serviços de saúde e a sua utilização pelo usuário[22]. Dessa forma, é importante entender que o trâmite de dados na área da

---

[20] BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial**, Brasília, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 8 abr. 2026. Art. 6º.

[21] No mesmo sentido, a Lei Federal n° 8.080/1990, prevê nos artigos 4°, § 2°, e 24, que "A iniciativa privada poderá participar do Sistema Único de Saúde (SUS), em caráter complementar. Art. 24: Quando as suas disponibilidades forem insuficientes para garantir a cobertura assistencial à população de uma determinada área, o Sistema Único de Saúde (SUS) poderá recorrer aos serviços ofertados pela iniciativa privada. BRASIL. **Lei nº 8.080, de 15 de dezembro de 1990**, *op. cit*.

[22] WERNER, Patricia Ulson Pizarro. Direito à saúde. *In*: CAMPILONGO, Celso Fernandes; GONZAGA, Alvaro de Azevedo; FREIRE, André Luiz (coord.). **Enciclopédia jurídica da PUC-SP**. 2. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2021. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/170/edicao-2/direito-a-saude. Acesso em: 30 mar. 2026.

saúde deve respeitar harmoniosamente a proteção dos dados e o acesso, conforme a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI) (Lei Federal nº 12.527/11).

Nesse cenário, diante da quantidade de órgãos e entidades envolvidos, é possível visualizar a grande complexidade da questão do fluxo de dados em um sistema inserido em uma rede regionalizada e hierarquizada, que abrange: (i) os vários níveis da federação, com fluxo entre União, Estados e Municípios; e (ii) a relação entre as diversas categorias, como saúde pública propriamente dita, saúde complementar (§ 1º, art. 199, CF/88) e saúde suplementar.

A integração dos serviços de saúde no formato de rede no contexto federativo, incluindo, segundo Werner, Municípios, "Consórcios Municipais, Estados, Distrito Federal e União"[23], cada qual exercendo suas atribuições fixadas em lei, de modo articulado com a programação da rede regionalizada e hierarquizada[24], para que não haja sobreposição de serviços, mas, ao mesmo tempo, se garanta o amplo acesso a todos, é um desafio.

Na saúde, há uma série de sistemas informatizados por meio dos quais dados pessoais de saúde são inseridos e tratados, tais como: o Sistema Nacional de Informação em Saúde (DATASUS)[25], o Sistema de Informação sobre Mortalidade (SIM), o Sistema de Informações sobre Nascidos Vivos (SINASC), o Sistema de Informações de Internações Hospitalares (SIH), os prontuários eletrônicos, os aplicativos que tratam em massa de dados de saúde, entre outros. Dito isto, existe uma enorme quantidade de dados a serem controlados, sendo imperiosa a necessidade de se enfrentar a complexidade semântica para categorizá-los; afinal, o próprio conceito de saúde traz uma amplitude intrínseca que requer atenta análise.

O Brasil adere, em sua legislação, ao conceito fixado pela Organização Mundial da Saúde (OMS) como um "estado de completo bem-estar físico, mental e social e consiste somente na ausência de uma doença ou enfermidade"[26].

Na sequência, estabelecem-se os princípios que devem guiar a compreensão da saúde, que podem ser sintetizados nos seguintes pontos:

---

[23] WERNER, *op. cit*, item 3.5.

[24] Rede hierarquizada compreende o desenho da complexidade dos fluxos e das conexões dos serviços e ações de saúde nos planos micro, meso e macroinstitucionais.

[25] Gerenciado pela União, pelo Departamento de Informática do SUS (DATASUS), que contém sistemas integrados de: (i) informatização de ambiente hospitalar; (ii) informações sobre orçamentos públicos em saúde, (iii) descentralização do Sistema de Informações Hospitalares do SUS (SIH/SUS); (iv) cadastro nacional de estabelecimentos do SUS; e) cadastro nacional e sistema de informações do programa nacional de imunizações Sistemas de Informação em Saúde – Ministério da Saúde.

[26] ORGANIZAÇÃO MUNDIAL DA SAÚDE (OMS). **Constituição da Organização Mundial da Saúde**. Genebra: OMS, 1946.

> Igualdade: é um direito fundamental garantido a todo ser humano, sem distinção de raça, religião, ideologia política e condição econômica social; (ii) Paz e segurança: a saúde de todos os povos é uma condição fundamental para atingir a paz e a segurança, por depender de uma ampla cooperação das pessoas e do Estado; (iii) Fomento e proteção evita o perigo comum: os resultados alcançados por cada Estado no fomento e desenvolvimento da proteção à saúde são valiosos para todos; principalmente, em relação às doenças transmissíveis que constituem um período comum; (iv) Desenvolvimento da criança: a criança tem uma importância fundamental, sendo indispensável o estimulo à capacidade de viver em harmonia com o mundo que muda constantemente; (v) Conhecimento: estender para todos os povos os benefícios dos conhecimentos médicos, psicológicos e afins são essenciais para alcançar o mais alto grau de saúde; (vi) Informação: a opinião pública bem informada e a cooperação ativa por parte do público são de importância capital para a melhoria da saúde de um povo; (vii) Responsabilidade do Estado: o governo tem responsabilidade pela saúde de seu povo, principalmente, deve adotar medidas sanitárias e sociais adequadas[27].

Destaca-se a realização da I Conferência Internacional sobre Cuidados Primários de Saúde em Alma-Ata, no Cazaquistão, quando se fixou a política de "Saúde para Todos no Ano 2000", pacto assinado por 134 países, com grande influência nas diretrizes adotadas pelo Brasil, por ressaltar a importância dos cuidados primários de saúde[28].

A partir desse breve contexto, fica evidente a alta complexidade do tema que envolve dados de saúde e a sua proteção, uma vez que é inerente a dificuldade de se estabelecer o controle rigoroso de cada parte do processo de trâmite dos dados, sendo complexo controlar a aplicação das regras de resguardo, capacitar e conscientizar todos os atores e partes envolvidos.

4. A LGPD: A PROTEÇÃO DE DADOS DE SAÚDE

A LGPD prevê que a proteção dos dados deve ser guiada pelos princípios da boa-fé e do interesse público envolvido, fixando os seguintes preceitos hermenêuticos em seu artigo 6º[29]:

> 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;

[27] *Ibid.*

[28] WERNER, *op. cit.*

[29] BRASIL. Lei nº 13.709, de 14 de agosto de 2018, *op. cit.*, art. 6º.

> 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.

É uma Lei que traz uma série de instrumentos e garantias para aumentar o poder e o controle do titular sobre seus dados, priorizando a autodeterminação informativa, uma vez que, no entender de Chiara Teffé[30]:

> Vivemos em um ambiente marcado por elevada assimetria informacional: uma parte, geralmente grandes empresas e Estados, detém mais poder, recursos e melhores informações do que a outra, o cidadão comum, por vezes, consumidor nas relações desenvolvidas. […] Tal assimetria informacional não se revela apenas no poder que os agentes dispõem sobre os dados pessoais de terceiros, mas, também nas novas modalidades de negócios, em que informações pessoais de seus usuários representam uma das bases centrais do sistema desenvolvido.

Dentro dessa dinâmica, a LGPD se apresenta com um caráter preventivo, com o objetivo de evitar danos e vazamento de dados. Essa lógica preventiva é muito

[30] TEFFÉ, Chiara Spadaccini de, *op. cit.*, p. 15.

clara quando pensamos no cuidado que a referida norma impõe no tratamento de dados e nos direitos dos titulares que ali são inseridos, bem como, pelo próprio relatório de impacto à proteção de dados que é mencionado no inciso XVII do artigo 5°.

Conforme bem elucida Chiara Teffé:

> A norma traz a lógica de *privacy by design* (art. 46, § 6°, da LGPD)[31], ao preconizar que a privacidade e a proteção de dados devem ser consideradas desde sua concepção e durante todo o ciclo de vida de projetos, sistemas, serviços, produtos e processos que envolvam o tratamento de dados, especialmente se eles foram sensíveis, devendo, por consequência, ser incluídas avaliações prévias de impacto, medidas técnicas e organizacionais adequadas e instrumentos de prestação de contas (*accountability*)[32].

A área da saúde entra na LGPD em pesquisa e saúde pública (art. 13), bem como na qualificação da coleta e do tratamento de dados pessoais sensíveis (art. 11). Especialmente os §§ 3º e 4º do art. 11 abordam a questão da vedação do uso econômico dos dados pessoais sensíveis. O § 4º do art. 11 trouxe importante flexibilização do conceito de que todo compartilhamento de dados sobre paciente é permitido, desde que em benefício dos titulares. Isso ocorre porque, na medicina, os dados não são utilizados somente para tratar de um indivíduo, mas, também, para criar protocolos para o próximo paciente, sendo certo que sempre haverá o compartilhamento de dados na saúde, tendo em vista que todo protocolo médico foi criado com base em evidências, e estas nada mais são do que dados.

Para o tratamento de dados pessoais se estabelece, como regra geral, o consentimento pelo titular do dado, abrindo espaço para o tratamento dos dados nas hipóteses do artigo 7° da LGPD. Assim, cabe destacar no âmbito da saúde, os seguintes pontos: fornecimento de consentimento pelo titular; cumprimento de obrigação legal ou regulatória pelo controlador; ou pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres; realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais e, conforme acréscimo realizado em 2019, tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária[33].

---

[31] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**, *op. cit*.

[32] TEFFÉ, Chiara Spadaccini de, *op. cit*., p. 209-210.

[33] Redação dada pela Lei nº 13.853, de 2019. BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. **Diário Oficial**, Brasília, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 8 abr. 2026.

O consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular, referindo-se às finalidades determinadas, sendo certo que as autorizações genéricas para o tratamento de dados pessoais serão nulas, cabendo ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto na Lei, sendo vedado o tratamento de dados pessoais mediante vício de consentimento (art. 8º, LGPD).

Ademais, é necessário criar a possibilidade de o sistema permitir a revogação, a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificando-se os tratamentos realizados sob amparo do consentimento anteriormente manifestado, enquanto não houver requerimento de eliminação, nos termos do art. 8º, § 5º, c/c o inciso VI do caput do art. 18 da LGPD.

Hoje, cada unidade da rede do SUS possui um sistema próprio de controle, o que é ampliado pelos serviços contratados via saúde complementar, razão, pela qual, estabelecer regras de unificação e controle trariam segurança e maior eficiência no SUS.

5. DADOS PESSOAIS DA SAÚDE: DADOS SENSÍVEIS

Os dados pessoais de saúde são uma categoria especial de informações que requerem proteção adicional, devido à sua natureza íntima e pessoal, sendo considerados sensíveis por expressa disposição legal (art. 5º, II, LGPD).

A lei define o que é dado pessoal e o que é dado pessoal sensível. Dado pessoal é a informação relacionada à pessoa natural identificada ou identificável (art. 5º, I, LGPD), enquanto os dados pessoais sensíveis (art. 5°, II, LGPD) são definidos como aqueles que compreendem:

> […] 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[34].

É de extrema relevância a classificação trazida pela lei, conceituando dados pessoais e dados sensíveis, uma vez que os dados sensíveis apresentam um maior risco quando do seu mau uso, podendo ensejar discriminações ilícitas ou abusivas ao seu titular, devendo, portanto, ser protegidos de forma ampliada.

Assim, entende-se que, ao categorizar os dados pessoais sensíveis, a LGPD visa tutelar de forma ampliada as informações que comumente são utilizadas em processos discriminatórios ilícitos ou abusivos.

Esse é um tema de extrema importância, pois, atualmente, percebe-se, também, a possibilidade de inferências sensíveis a partir do tratamento de dados que

[34] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**, *op. cit*.

não são, na origem, sensíveis. Por exemplo: com a geolocalização de uma pessoa, pode-se chegar a dados relativos à saúde, a questões políticas e a questões religiosas; dados financeiros de uma pessoa, em determinados casos, direcionam a informações de saúde, tais como, despesas e reembolso médico. Nesse sentido, é importante a atenção para as possibilidades de inferência sensíveis com o cruzamento de dados, a atuação de inteligência artificial e o *Big Data,* que atuam diretamente nessas relações. Como se denota, atualmente, vive-se em um cenário em que é relativamente simples inferir ou mesmo extrair dados sensíveis nas mais diversas relações.

Proteger dados sensíveis é essencial para evitar cenários discriminatórios, de preconceito, ilícitos, abusivos e estigmatizantes. Proteger dados sensíveis, também, é fundamental para que se garanta a liberdade das pessoas naturais e para facilitar o acesso a bens e serviços. É nesse cenário que a aplicação da LGPD se mostra importante, especialmente no cuidado relativo aos dados pessoais sensíveis e o próprio direito antidiscriminação.

A regra é que o dado pessoal de saúde é sensível e seu tratamento deve ocorrer: (i) quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; (ii) sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (art. 11, LGPD).

A lei prevê hipóteses de exceção, as quais devem ser interpretadas de maneira restritiva, das quais se destacam: quando houver o consentimento para finalidades específicas; quando não houver o fornecimento de consentimento do titular, poderá haver exceção por força do cumprimento de obrigação legal ou regulatória pelo controlador (art. 11, LGPD).

A Administração poderá tratar dados compartilhados necessários à execução de políticas públicas previstas em leis ou regulamentos e autorizar a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis.

Outra possibilidade ocorre no caso de proteção da vida ou da incolumidade física do titular ou de terceiro e na tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária[35].

Atenção especial deve ser concedida aos dados pessoais de saúde de pacientes, pois é vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde, com o objetivo de obter vantagem econômica, exceto nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º do art. 11 da LGPD, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados (art. 11, § 4º, LGPD), e para permitir: i) a portabilidade de dados quando solicitada pelo titular; ou ii) as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de saúde.

Da mesma forma, é importante destacar que, até no âmbito da saúde suplementar, 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 (art. 11, § 5º, LGPD).

O Poder Público deve dar especial atenção à área de Ciência, Tecnologia e Informação (CT&I), na qual o controle dos dados dos pacientes deve ser muito rigoroso, inclusive no controle da denominada pseudonimização, ou seja, 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, LGPD).

Destacam-se os critérios a serem utilizados nos estudos em saúde pública:

> Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.
>
> § 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.
>
> § 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.

[35] Redação dada pela Lei nº 13.853, de 2019. BRASIL. **Lei nº 13.853, de 8 de julho de 2019**, *op. cit*.

> § 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências[36].

Na área da saúde, sabemos que são possíveis as mais diversas discriminações, por esse motivo é necessário um cuidado adicional com os titulares de dados. Acrescente-se que, especialmente na área da saúde, é possível considerar como titular de dados, não só a criança, o adolescente e o adulto, mas até mesmo o nascituro, que já tem dados de saúde sendo tratados em exames pré-natais, exames laboratoriais de gravidez, entre outros.

Destaca-se que o nascituro nem tem personalidade jurídica, conforme o art. 2º do Código Civil, mas já tem informações sobre ele sendo tratadas.

Há aplicativos de controle da gestação, assim, essa preocupação com os dados de saúde é algo que preocupa desde o momento da concepção até o final da vida.

Nesse contexto, os dados falam sobre o nosso passado, presente e futuro. Dados pessoais falam sobre a nossa ascendência, nossa descendência, a nossa propensão a doenças e a nossa resposta a medicamentos; assim, é importante o estabelecimento de *compliance* voltado para a área específica da saúde, com normas e boas práticas direcionadas a esse setor.

No rol de dados sensíveis, temos várias categorias: questões raciais, questões étnicas, questões biométricas, questões genéticas e religiosas. São temas extremamente relevantes que exigem, por si só, um cuidado apurado, especialmente na área da saúde. O consentimento, sendo livre e informado, é de extrema relevância, bem como a existência de normas técnicas e jurídicas voltadas à proteção desses direitos.

Hoje, há uma preocupação com o tratamento de dados que não envolva um dado sensível, mas que tenham um viés discriminatório. É importe compreender com cuidado a dinamicidade das categorias e os diversos processos discriminatórios existentes em nossa sociedade.

Nesse sentido, o enunciado 690 da IX Jornada do Conselho da Justiça Federal (CJF) (que teve uma comissão específica para o Direito Digital) dispõe que: "A proteção ampliada conferida a LGPD aos dados sensíveis deverá ser também aplicada aos casos em que houver tratamento sensível de dados pessoais, tal como observado no § 1º do art. 11 da LGPD"[37].

Houve, nesse enunciado, uma atenção às inferências sensíveis e aos tratamentos que revelam informações sensíveis. É necessário, então, que prestemos atenção tanto à proteção ampliada, que sempre deve ser conferida, mas, também às

[36] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**, *op. cit*.

[37] CONSELHO DA JUSTIÇA FEDERAL (CJF). **IX Jornada Direito Civil**: comemoração dos 20 anos da Lei nº 10.406/2022 e da instituição da Jornada de Direito Civil: enunciados aprovados. Brasília: Conselho da Justiça Federal, Centro de Estudos Judiciários, 2022, p. 49.

possibilidades de inferências sensíveis e à obtenção de resultados sensíveis a partir de tratamento de dados. Isso é fundamental para o cenário democrático no Brasil e com os próprios direitos fundamentais.

Nesse aspecto, é importante tratar com muito cuidado a gestão de riscos nos processos que envolvem dados sensíveis, bem como assegurar que haja uma aplicação concreta do *data protection by design and default*, observando-se com muito cuidado as bases legais do art. 11 da LGPD. Assim, se houver uma relação que revele dados sensíveis, isso, desde já, atrai um rol de dados mais restrito. Da mesma forma, é importante a elaboração de relatório de impacto à proteção de dados pessoais, quando houver um tratamento de dado sensível, especialmente de alto risco. O risco é um elemento que atrai, como regra, o relatório de impacto, e geralmente ao tratar dado sensível, haverá um elemento de risco, no mínimo, em âmbito médio. O relatório de risco se mostra como uma boa prática e extremamente importante para a proteção de dados.

O fluxo de dados que merece atenção, especialmente na área da saúde, é o fluxo de dados sensíveis que envolve hipervulneráveis: crianças, adolescentes, idosos, pessoas com deficiência ou pessoas que tenham uma vulnerabilidade agravada por condições particulares. Neste ínterim, deve-se manter o olhar atento ao fluxo de dados e aos sujeitos, quando pensarmos na gestão de risco e no desenvolvimento de boas práticas.

Cabe destacar que a Autoridade Nacional de Proteção de Dados (ANPD) não fixou orientações específicas para os dados sensíveis de saúde, mas disciplinou parâmetros para o Tratamento de Dados Pessoais pelo Poder Público (Versão 2.0, jun./23), com foco no critério da avaliação da compatibilidade entre a finalidade original e o uso secundário de determinado caso, por exemplo, quando se utiliza um dado de saúde para monitorar uma política pública de vacinação ou para o compartilhamento de dados de pesquisa. Assim, conclui-se que há conformidade com o princípio da finalidade, desde que se garanta a pseudonimização ou a anonimização dos dados, nos termos do art. 13 e do Capítulo IV da LGPD[38].

Destacou-se também a hipótese, muito comum na área da saúde, da ocorrência de um novo compartilhamento ou transferência posterior dos dados, entre o recebedor dos dados no âmbito do próprio setor público ou para entes do setor privado. A orientação fixada é no sentido de que, "entre outras possibilidades, o instrumento que rege o uso compartilhado dos dados pode vedar a realização de novo compartilhamento ou, ainda, autorizá-lo sob determinadas condições, observadas as normas

[38] AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo. Tratamento de Dados Pessoais pelo Poder Público**. Versão 2.0, jun. 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 30 mar. 2026.

aplicáveis"[39], como exemplo citou o caso de dados pessoais disponibilizados para a realização de estudos em saúde pública, no qual se deve aplicar o critério estabelecido no artigo 13,§ 2.º, da LGPD, que impõe ao órgão de pesquisa a responsabilidade pela segurança da informação e expressamente não permite, "em circunstância alguma, a transferência dos dados a terceiro".

Na mesma seara da pesquisa na área da saúde, a ANPD reforçou a ideia da proteção jurídica especial dos dados sensíveis de saúde ao mencionar "a vedação de serem revelados dados pessoais sensíveis por ocasião da divulgação de resultados de estudos em saúde pública (art. 13, § 1º,LGPD"[40], e fixou a orientação de que, nos casos de estudos em saúde pública, deve-se adotar medidas adicionais de prevenção e segurança para o tratamento de dados sensíveis, tais como o seu armazenamento em ambiente controlado e seguro, bem como, sempre que possível, a sua anonimização ou pseudonimização[41].

O Ministério da Saúde publicou a Portaria GM/MS nº 3.232, de 1º de março de 2024, que instituiu o Programa SUS Digital, que, entre outros pontos, versou sobre os objetivos gerais e específicos, a abrangência, as diretrizes, a operacionalização, a coordenação e a governança, bem como as competências de cada esfera de governo do programa. Nesse contexto, o artigo 4º, II, da Portaria estabeleceu o conceito de "dado pessoal sensível de saúde" como sendo "dado relativo à saúde de um titular de dados ou à atenção à saúde a ele prestada que revele informações sobre sua saúde física ou mental no presente, passado ou futuro".

Segundo Analluza Bolivas Dallari[42],

> […] a definição de "dado pessoal sensível de saúde" é um importante passo para ampliar a proteção de direitos fundamentais do titular-paciente, uma vez que "a Lei 13.709 de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais, LGPD) não conceitua dados pessoais sensíveis (artigo 5º, II da LGPD)". O conceito traçado pela Portaria GM/MS 3.232/2024 "condiz com a perspectiva ampliada de saúde, segundo o artigo 3º da Lei 8.080 de 19 de setembro de 1990, que versa sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes (Lei Orgânica da Saúde), estando alinhado, ainda, com o considerando 35 do Regulamento da União Europeia 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016".

[39] *Ibid*., p. 34.

[40] *Ibid*., p. 38.

[41] *Ibid*., p. 40-41.

[42] DALLARI, Analluza Bolivar. SUS Digital e o conceito de dado pessoal sensível de saúde. **JOTA**, 26 mar. 2024. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/sus-digital-e-o-conceito-de--dado-pessoal-sensivel-de-saude-26032024. Acesso em: 30 mar. 2026.

O conceito de "dado pessoal sensível de saúde", adotado pelo Ministério da Saúde, dialoga com o § 1º, do artigo 11, da LGPD, uma vez que este atrai para as hipóteses do artigo 11 da LGPD o tratamento de dados pessoais, cuja finalidade revele, a depender das técnicas aplicadas de tratamento e de inferências cada vez mais sofisticadas, dados pessoais sensíveis e que, assim, possam causar dano ao titular.

Enfim, observa-se que a adoção do conceito de "dado pessoal sensível de saúde", na Portaria do Ministério da Saúde, que alcança passado, presente e futuro, marca um avanço importante na proteção de direitos fundamentais de liberdade, de privacidade e do livre desenvolvimento da personalidade da pessoa natural titular de dados, no contexto da transformação digital da saúde.

6. CONSTRUÇÃO DE POLÍTICAS PÚBLICAS – CONTROLE E AVALIAÇÃO

A avaliação das políticas públicas foi um tema introduzido recentemente na Constituição Federal, pela Emenda Constitucional nº 109/2021, nos seguintes termos:

> Art 37 - § 16. Os órgãos e entidades da administração pública, individual ou conjuntamente, devem realizar avaliação das políticas públicas, inclusive com divulgação do objeto a ser avaliado e dos resultados alcançados, na forma da lei.

Dessa forma, resta evidente que há necessidade de se criar uma política pública específica para a concretização da preservação dos dados de saúde na categoria de "dados sensíveis", em especial para preservar os usuários do SUS, incluindo as ações no campo da saúde complementar. Como controladores, cabem aos gestores do SUS adotar as medidas harmônicas válidas para todos os níveis federais, com o fim de garantir a devida proteção em face de terceiros, e o acesso seguro ao titular do dado.

6.1. *Tecnologia e Saúde: a Telemedicina e a Proteção de Dados*

As experiências efetivas de telemedicina e telessaúde no Brasil tiveram início na década de 1990. Essas iniciativas aconteceram tanto na área pública quanto na área privada, além do âmbito de algumas universidades[43]. Com a pandemia da covid-19, ocorreu uma grande oportunidade para a o crescimento da utilização da telemedicina, pois ela (a pandemia) forçou o isolamento social e, portanto, a necessidade, tanto do trabalho remoto como também do acesso de forma remota a uma série de serviços, incluindo a saúde.

[43] KHOURI, Sumaia Georges El. **Telemedicina**: análise da sua evolução no Brasil. 2003. Dissertação (Mestrado em Ciências) – Universidade de São Paulo, São Paulo, 2003. Disponível em: https://teses.usp.br/teses/disponiveis/5/5160/tde-24102007-143128/publico/sumaiagekhouri.pdf. Acesso em: 30 mar. 2026.

A telemedicina é regulamentada pela Resolução CFM nº 2.314, de 20 de abril de 2022, considerando que cabe ao CFM disciplinar o exercício profissional médico e zelar pela boa prática médica no país, a qual segue como parâmetro a Declaração da Word Medical Association (WMA) sobre os princípios éticos da telemedicina[44].

O artigo 1º da referida Resolução define a Telemedicina como o "exercício da medicina mediado por Tecnologias Digitais, de Informação e de Comunicação (TDICs), para fins de assistência, educação, pesquisa, prevenção de doenças e lesões, gestão e promoção de saúde"[45], sendo permitida, conforme o seu artigo 2º, em tempo real *on-line* (síncrona) ou *off-line* (assíncrona), dentro do território nacional.

Pode ser exercida nas seguintes modalidades de teleatendimentos médicos: i) Teleconsulta; ii) Teleinterconsulta; iii) Telediagnóstico; iv) Telecirurgia; v) Telemonitoramento ou televigilância; vi) Teletriagem; vii) Teleconsultoria (art. 5º).

Importante destacar que, conforme estabelece o parágrafo único do artigo 15 da citada Resolução, em todo atendimento por telemedicina deve ser assegurado o consentimento explícito, no qual o paciente ou seu representante legal deve estar consciente de que as suas informações pessoais podem ser compartilhadas e sobre o seu direito de negar permissão para isso, salvo em situação de emergência médica.

Deve ser assegurado que as pessoas jurídicas que prestarem serviços de telemedicina, plataformas de comunicação e arquivamento de dados, deverão ter sede estabelecida em território brasileiro e estar inscritas no Conselho Regional de Medicina do Estado, onde estão sediadas, com a respectiva responsabilidade técnica de médico, regularmente inscrito no mesmo Conselho (artigo 17). No caso de o prestador ser pessoa física, deverá ser médico devidamente inscrito no Conselho Regional de Medicina de sua jurisdição e informar a entidade a sua opção de uso de telemedicina.

Nesse contexto, é necessário zelar pelo respeito ao Código de Ética Médica, considerando o grande fluxo de dados e informações que se estabelece entre médicos e entre médicos e pacientes.

O CFM fixa diretrizes a serem seguidas, partindo do pressuposto de que a consulta médica presencial é o padrão a ser seguido. A relação cada vez mais tecnológica entre médicos e pacientes, deve visar ao benefício e aos melhores resultados ao paciente. Assim, o médico deve avaliar se a telemedicina é o método mais adequado às necessidades do paciente, naquela situação determinada.

Os dados e imagens dos pacientes constantes nos registros do prontuário devem ser preservados nos termos da lei e das orientações do CFM, pertinentes à guarda, ao manuseio, à integridade, à veracidade, à confidencialidade, à privacidade, à irrefutabilidade e à garantia do sigilo profissional das informações, por meio do

[44] WORLD MEDICAL ASSOCIATION (WMA). **Declaración de la AMM sobre la ética de la telemedicina**. 2018. Disponível em: https://www.wma.net/es/policies-post/declaracion-de-la-amm-sobre-la-etica-de-la-telemedicina/. Acesso em: 30 mar. 2026.

[45] CFM. **Resolução CFM nº 2.314/2022**, *op. cit.*, art. 1º.

prontuário médico físico ou no uso de sistemas informacionais, em Sistema de Registro Eletrônico de Saúde (SRES) do paciente, atendendo aos padrões de representação, terminologia e interoperabilidade.

Cabe destacar o art. 3º § 2º da Resolução CFM nº 2.314:

> Art 3. § 2º O SRES utilizado deve possibilitar a captura, o armazenamento, a apresentação, a transmissão e a impressão da informação digital e identificada em saúde e atender integralmente aos requisitos do Nível de Garantia de Segurança 2 (NGS2), no padrão da infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) ou outro padrão legalmente aceito[46].

Os dados relacionados ao atendimento realizado via telemedicina, como os de anamnese e dados propedêuticos, resultados de exames complementares e a conduta médica adotada, devem ser preservados, conforme a legislação vigente, sob guarda do médico responsável pelo atendimento em consultório próprio ou do diretor/responsável técnico, no caso de interveniência de empresa e/ou instituição (art. 3º, § 3º, Resolução CFM nº 2.314).

É importante destacar, na área da saúde complementar, que, em caso de contratação de serviços terceirizados de arquivamento, a responsabilidade pela guarda de dados de pacientes e do atendimento deve ser contratualmente compartilhada entre o médico e a contratada, de modo que o SRES deve propiciar interoperabilidade/intercambialidade, com utilização de protocolos flexíveis, pelos quais dois ou mais sistemas possam se comunicar de forma eficaz e com garantia de confidencialidade, privacidade e integridade dos dados (art. 3º, §§ 4º e 5º, Resolução CFM nº 2.314).

Importante ressaltar que, a telemedicina não se resume ao atendimento paciente-médico por meio de uma ferramenta tecnológica. Ela envolve vários instrumentos: o estabelecimento de saúde, uma plataforma de emissão de documentos médicos eletrônicos, a farmácia etc., ou seja, os instrumentos que envolvem a telemedicina são interconectados com diversos operadores de dados da saúde e outros que não são da área da saúde, que não têm licença sanitária, como as plataformas de emissão de documentos médicos eletrônicos.

Ademais, a videoconferência é apenas uma pequena parcela da telemedicina, como explica o Professor Chao Lung Wen[47]:

> A telemedicina, mais do que um recurso tecnológico para proporcionar atividades a distância, a telemedicina adquire efetividade quando ela está associada a um plano estratégico de saúde e vinculado a um processo de logística de distribuição de serviços de saúde.

---

[46] *Ibid.*, art. 3º, § 2º.

[47] WEN, Chao Lung. Telemedicina e a telessaúde: uma abordagem sob a visão de estratégia de saúde apoiada por tecnologia. **Chao Lung Wen**, 30 jan. 2002. Disponível em: https://chaowen.med.br/artigos/telemedicina-e-a-telessaude-uma-abordagem-sob-a-visao-de-estrategia-de-saude-apoiada-por-tecnologia/. Acesso em: 30 mar. 2026.

Melhor dizendo, a telemedicina não é uma ferramenta, mas um método que vai desde o paciente adentrar a plataforma, ter sua identidade verificada, ocorrer a elegibilidade do serviço, até a adequação da tecnologia, ou seja, a verificação de se o paciente está em condições de conectividade, a realização da consulta, a emissão de documentos e a obtenção do consentimento informado.

A telemedicina é um método de se praticar a medicina, sem grandes diferenças no raciocínio clínico médico ou nas condutas adotadas, estando o paciente a distância ou presencial. No entanto, o intuito principal é a transparência das informações, o paciente precisa saber quais são as limitações do método, e o termo de consentimento ajudará a cientificá-lo.

Hoje a telemedicina não é limitada por questões tecnológicas. No entanto, o que há são barreiras de processo, ou seja, de como você implementa um processo de atendimento que seja seguro, que garanta a privacidade dos dados e que garanta a boa prática da medicina.

Nesse aspecto, é importante tratar com muito cuidado a gestão de riscos nos processos que envolvem dados sensíveis, bem como assegurar que haja uma aplicação concreta do *data protection by design and default*, observando-se com muito cuidado as bases legais do art. 11 da LGPD. Havendo uma relação que revele dados sensíveis, isso, desde já, atrai um rol de dados mais restrito. Nesta esteira, faz-se muito importante a elaboração de relatório de impacto à proteção de dados pessoais, quando houver um tratamento de dado sensível, especialmente de alto risco.

7. CONCLUSÃO

A proteção de dados pessoais sensíveis de saúde ganha relevância e novos desafios de forma diretamente proporcional ao desenvolvimento de novas tecnologias e inovações na área da saúde. Se, por um lado, a evolução da medicina proporciona a produção de ferramentas que garantem melhor qualidade e mais precisão na prevenção e no tratamento de doenças, bem como, o aprimoramento da modelagem das políticas públicas, com a otimização da coleta de dados mais precisos e da identificação das necessidades de cada região de saúde, por outro, há patente risco na manipulação e no aumento do tráfego de dados, considerando que os dados pessoais dos pacientes tornam-se ativos valiosos para os governos e empresas, sujeitos a abusos, violações de privacidade, roubo de identidade e outros tantos crimes cibernéticos.

O desafio é compor, de forma harmônica e segura, várias realidades interligadas, as quais devem evoluir de forma conjunta na proteção dos dados, em suas várias dimensões: inovação em saúde, proteção dos direitos fundamentais do indivíduo e transparência.

A questão perpassa pelos desafios impostos pela enorme rede hierarquizada e regionalizada que delineiam o projeto constitucional do SUS, um dos maiores do mundo, o que demonstra a necessidade de se harmonizar o tema em todos os níveis

da federação, por meio de políticas públicas específicas, visando à devida regulamentação e à oferta da infraestrutura necessária para lidar com os dados gerados, bem como educar os usuários do SUS, médicos e todos que compõem a área de saúde e burocrática a adotarem boas práticas, controlarem e avaliarem as políticas públicas com a eficiência e rapidez que a área da evolução tecnológica requer.

A definição de "dados pessoais sensíveis de saúde" deve coincidir com a extensa concepção da própria noção de saúde, a qual considera como determinantes e condicionantes que contemplem, inclusive, o bem-estar físico, mental e social, segundo o artigo 3º da LOS. Pois bem, perfazendo este "conceito ampliado de saúde" conforme o § 1º do artigo 11 da LGPD, dados pessoais em princípio "comuns", como a geolocalização, a depender dos cruzamentos e inferências, podem revelar dados pessoais sensíveis de saúde, mitigando a tese da taxatividade estática do artigo 5º, II, da LGPD.

A telessaúde é uma realidade prevista na Lei Federal n.º 14.510/2022 que alterou a LOS, sendo reconhecida a modalidade de teleatendimento dentro da cadeia de serviços do SUS. Toda a construção de sua implementação pressupõe respeito aos termos da LGPD, considerando que a proteção dos dados pessoais vai fornecer as bases para a confiança dos cidadãos nas instituições públicas e privadas no ambiente digital, sendo essencial para fortalecer a proteção efetiva dos direitos fundamentais individuais.

A legislação brasileira, ao contrário do Regulamento UE 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, GDPR[48], não definiu diretamente o conceito de "dados pessoais relativos à saúde". Cabe ao intérprete buscar essa definição no quadro legislativo atual e acompanhar o desdobramento do tema por meio das orientações da ANPD, pela própria compreensão do problema pelos gestores do SUS e pelo aprimoramento dos instrumentos jurídicos, com foco na relação titular–controlador–operador–encarregado–agentes de tratamento, em especial, nos convênios e contratos de gestão de saúde e, eventualmente, em decisões judiciais.

Faz-se, então, necessário construir, a partir da ideia de dados pessoais sensíveis, balizas para garantir o trâmite dos dados na área da saúde, incluindo a criação de mecanismos claros e a compreensão de como será realizado o tratamento dos dados, com o fim de garantir os princípios gerais de proteção e os direitos do titular, como o direito de acesso, bloqueio, eliminação e transferência.

A ANPD não fixou orientação específica para os dados sensíveis de saúde, mas disciplinou parâmetros para o "Tratamento de Dados Pessoais pelo Poder Público" (Versão 2.0, jun./23), com foco no critério da avaliação da compatibilidade entre a finalidade original e o uso secundário de determinado caso, com foco nos dados na área das pesquisas em saúde, como o compartilhamento, a transferência, a anonimização ou a pseudonimização dos dados.

[48] UNIÃO EUROPEIA. **Regulation (EU) 2016/679… (GDPR)**. *op. cit*.

O Ministério da Saúde traçou paradigmas na Portaria GM/MS nº 3.232/2024, em consenso com a perspectiva ampliada de saúde, segundo o artigo 3º da LOS e com o Regulamento da União Europeia 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, no sentido de que dado pessoal sensível de saúde é aquele "dado relativo à saúde de um titular de dados ou à atenção à saúde a ele prestada que revele informações sobre sua saúde física ou mental no presente, passado ou futuro" (artigo 4º, inciso II).

O conceito de "dado pessoal sensível de saúde" vem sendo construído no âmbito nacional, com a importante introdução da dimensão de tempo e espaço – no passado, presente e futuro –, representando um avanço importante na proteção de direitos fundamentais de liberdade, de privacidade e do livre desenvolvimento da personalidade da pessoa natural titular de dados, no contexto da transformação digital da saúde.

REFERÊNCIAS BIBLIOGRÁFICAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo. Tratamento de Dados Pessoais pelo Poder Público**. Versão 2.0, jun. 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 30 mar. 2026.

AMARAL, Igor Silva, *et al*. Segurança cibernética para dispositivos móveis. **Revista Multidisciplinar do Nordeste Mineiro**, Teófilo Otoni, v. 1, n. 1, 2024. Disponível em: https://pdfs.semanticscholar.org/a614/b93eed8282012a0c503d1c771a123b5c99d8.pdf. Acesso em: 30 mar. 2026.

ARAUJO, Alex Rodrigues. **Métodos e técnicas de segurança para dispositivos IOT**: uma revisão sistemática da literatura. 2023. Monografia (Superior em Telemática) – Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, Campina Grande, 2023, Disponível em: https://repositorio.ifpb.edu.br/bitstream/177683/3547/1/Araujo%2C%20Alex%20Rodrigues%20-%20TCC.pdf. Acesso em: 30 mar. 2026.

BAHIA, Claudio José Amaral, *et al*. Direito à proteção de dados: trajetória e delineações do reconhecimento como um direito fundamental autônomo no Brasil. **Revista da Faculdade de Direito da UERJ**, Rio de Janeiro, n. 43, 2024. Disponível em: https://www.e-publicacoes.uerj.br/index.php/rfduerj/article/view/67486?utm_source=chatgpt.com. Acesso em: 30 mar. 2026.

BARBOSA, Wuerles Bessa, *et al*. Impacto da telemedicina na prestação de cuidados de saúde em áreas rurais e remotas. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 9, n. 8, p. 191-201, 2023. Disponível em: https://periodicorease.pro.br/rease/article/view/10855?utm_source=chatgpt.com. Acesso em: 30 mar. 2026.

BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial**, Brasília, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 8 abr. 2026.

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 fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial**, Brasília, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 8 abr. 2026.

BRASIL. Lei nº 8.080, de 15 de dezembro de 1990. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências. **Diário Oficial**, Brasília, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8080.htm. Acesso em: 30 mar. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispões sobre a Lei Geral de Proteção de Dados. **Diário Oficial**, Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 mar. 2026.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. **Diário Oficial**, Brasília, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 8 abr. 2026.

BRASIL. Lei nº 14.510, de 27 de dezembro de 2022. Altera a Lei nº 8.080, de 19 de setembro de 1990, para autorizar e disciplinar a prática da telessaúde em todo o território nacional, e a Lei nº 13.146, de 6 de julho de 2015; e revoga a Lei nº 13.989, de 15 de abril de 2020. **Diário Oficial**, Brasília, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14510.htm. Acesso em: 30 mar. 2026.

BRASIL. **Guia de boas práticas para implementação na Administração Pública Federal**. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 30 mar. 2026.

CARVALHO, Lucas Borges de. O Poder Público e a proteção de dados pessoais no Brasil: novos desafios, velhas práticas administrativas. **Revista de Direito Administrativo**, Rio de Janeiro, v. 282, n. 2, p. 133-162, 2023.

CONFEDERAÇÃO NACIONAL DE SAÚDE. **Código de boas Práticas:** Proteção de dados para Prestadores Privados de Serviços em Saúde. Brasília: CNSaúde, 2021. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em: 30 mar. 2026.

CONSELHO DA JUSTIÇA FEDERAL (CJF). **IX Jornada Direito Civil**: comemoração dos 20 anos da Lei nº 10.406/2022 e da instituição da Jornada de Direito Civil: enunciados aprovados. Brasília: Conselho da Justiça Federal, Centro de Estudos Judiciários, 2022.

CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 2.314/2022. Define e regulamenta a telemedicina, como forma de serviços médicos mediados por tecnologias de comunicação. **Diário oficial**, Brasília, 5 maio 2022, Seção I, p. 227.

COSTA, Gustavo Amancio da; LIMA, Miqueias Sales de. **Exploração de vulnerabilidades em sistemas operacionais Linux**. 2023. Monografia (Bacharel em Tecnologia em Segurança da Informação) – Faculdade de Tecnologia de Americana "Ministro Ralph Biasi", Americana, 2023. Disponível em: https://ric.cps.sp.gov.br/handle/123456789/15462. Acesso em: 30 mar. 2026.

COSTA JUNIOR, Jose Cassio**. Os desafios da Lei Geral de Proteção de Dados para pequenas empresas**: um estudo de caso em uma distribuidora em Natal/RN. 2023. Monografia (Bacharel em Administração) – Universidade Federal do Rio Grande do Norte, Natal, 2023. Disponível em: https://repositorio.ufrn.br/server/api/core/bitstreams/da63035a-ad57-4151-810e-57614745c088/content. Acesso em: 30 mar. 2026.

DALLARI, Analluza Bolivar. SUS Digital e o conceito de dado pessoal sensível de saúde. **JOTA**, 26 mar. 2024. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/sus-digital-e-o-conceito-de-dado-pessoal-sensivel-de-saude-26032024. Acesso em: 30 mar. 2026.

GRANEMANN, Gabriel Maddalozzo. **Fatores que influenciam a intenção de uso da telemedicina no Brasil pelos pacientes**: um estudo exploratório via modelagem estrutural. 2021. Monografia (Bacharel em Engenharia de Produção) – Universidade de Brasília, Brasília, 2021. Disponível em: https://bdm.unb.br/bitstream/10483/34143/1/2021_GabrielMaddalozzoGranemann_tcc.pdf. Acesso em: 30 mar. 2026.

KHOURI, Sumaia Georges El. **Telemedicina**: análise da sua evolução no Brasil. 2003. Dissertação (Mestrado em Ciências) – Universidade de São Paulo, São Paulo, 2003. Disponível em: https://teses.usp.br/teses/disponiveis/5/5160/tde-24102007-143128/publico/sumaiagekhouri.pdf. Acesso em: 30 mar. 2026.

NIUKA, Josias Kuvingua Bernardo. **A Proteção de Dados Pessoais de Saúde à luz do RGPD**. 2023. Dissertação (Mestrado) – Universidade de Coimbra, Faculdade de Direito, Coimbra, 2023. Disponível em: https://estudogeral.uc.pt/retrieve/265833/Dissertac%CC%A7a%CC%83o%20juri%CC%81dico-forense%20Mestrado_Josias%20Niuka_12jun23.pdf. Acesso em: 30 mar. 2026.

OLIVEIRA, Larissa de Jesus; NOVAIS, Thyara Gonçalves. Lei geral de proteção de dados pessoais: responsabilidade civil no vazamento de informações. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 10, n. 5, p. 1614-1631, 2024. Disponível em: https://periodicorease.pro.br/rease/article/view/13668. Acesso em: 30 mar. 2026.

ORGANIZAÇÃO MUNDIAL DA SAÚDE (OMS). **Constituição da Organização Mundial da Saúde**. Genebra: OMS, 1946.

PROMULGADA emenda constitucional de proteção de dados. **Agência Senado**, 10 fev. 2022. Disponível em: https://www12.senado.leg.br/noticias/materias/2022/02/10/promulgada-emenda-constitucional-de-protecao-de-dados. Acesso em: 8 abr. 2026.

SANTOS, Beatriz Freitas. Lei Geral de Proteção de Dados (LGPD) e a garantia de proteção dos direitos fundamentais de liberdade e de privacidade dos cidadãos a luz do Direito Constitucional. **Aporia Jurídica**, Ponta Grossa v. 1, n. 19, 2023.

SARLET, Ingo. A EC 115/22 e a proteção de dados pessoais como Direito Fundamental I. **Consultor Jurídico**, 2022. Disponível em: https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental/. Acesso em: 30 mar. 2026.

SILVA, Angélica Baptista. **Telessaúde no Brasil**: conceitos e aplicações. Rio de Janeiro: Editora DOC, 2014.

SILVA, Kaian Notier Gomes da; OLIVEIRA, Rômulo de Morais. Conflito entre o princípio da publicidade tratado na lei 6.015/73 e os dados sensíveis tratados pela Lei Geral de Proteção de Dados-LGPD nas serventias extrajudiciais. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 10, n. 5, p. 2091-2107, 2024. Disponível em: https://periodicorease.pro.br/rease/article/view/13986. Acesso em: 30 mar. 2026.

SOBROZA, Bianca Amaral; ARRUDA, Juliana Gonçalves de; MARINI, Bruno. Vazamento de dados pessoais sensíveis de pacientes atendidos por instituições de saúde como forma de violência hospitalar: uma análise global sob o viés da bioética e do biodireito. **Revista de Direito Magis**, Betim, v. 2, n. 1, 2023. Disponível em: https://periodico.agej.com.br/index.php/revistamagis/article/view/44. Acesso em: 30 mar. 2026.

SOUZA, Julio César de. **Um estudo de caso sobre medidas de segurança para preservar a confidencialidade e integridade das informações**. 2024. Monografia (Bacharel em Engenharia da Computação) – Universidade Federal de Mato Grosso, Várzea Grande, 2024. https://bdm.ufmt.br/bitstream/1/3954/1/TCC_2024_Julio%20C%C3%A9sar%20de%20Souza.pdf. Acesso em: 30 mar. 2026.

TEFFÉ, Chiara Spadaccini de. **Problemas de direito civil**: homenagem aos 30 anos de cátedra do professor Gustavo Tepedino por seus orientandos e ex-orientandos. Rio de Janeiro: Forense, 2021.

UNIÃO EUROPEIA. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – GDPR)**. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679. Acesso em: 30 mar. 2026

WEN, Chao Lung. Telemedicina e a telessaúde: uma abordagem sob a visão de estratégia de saúde apoiada por tecnologia. **Chao Lung Wen**, 30 jan. 2002. Disponível em: https://chaowen.med.br/artigos/telemedicina-e-a-telessaude-uma-abordagem-sob-a-visao-de-estrategia-de-saude-apoiada-por-tecnologia/. Acesso em: 30 mar. 2026.

WERNER, Patricia Ulson Pizarro. Direito à saúde. *In*: CAMPILONGO, Celso Fernandes; GONZAGA, Alvaro de Azevedo; FREIRE, André Luiz (coord.). **Enciclopédia jurídica da PUC-SP**. 2. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2021. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/170/edicao-2/direito-a-saude. Acesso em: 30 mar. 2026.

WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo poder público. *In*: MENDES, Laura, *et al*. (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

WORLD MEDICAL ASSOCIATION (WMA). **Declaración de la AMM sobre la ética de la telemedicina**. 2018. Disponível em: https://www.wma.net/es/policies-post/declaracion-de-la-amm-sobre-la-etica-de-la-telemedicina/. Acesso em: 30 mar. 2026.

Submetido em: 02/12/2024
Aprovado em: 16/09/2025

USO DE BASES DE DADOS EM SAÚDE E A PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Use of health databases and privacy and personal data protection

Néa Miwa Kashiwagi[1]
Zillá Oliva Roma[2]

SUMÁRIO 1. Introdução; 2. A proteção de dados no Brasil; 3. Os dados de saúde; 4. A proteção de dados em pesquisas de saúde; 5. Anonimização e pseudoanonimização de base de dados; 6. Conclusões; Referências Bibliográficas.

RESUMO Bases de dados secundárias têm sido fontes de informação importantes para o desenvolvimento de pesquisas em saúde, cujos resultados irão contribuir para o aprimoramento de protocolos assistenciais e políticas públicas. A Lei Geral de Proteção de Dados (LGPD), além de consolidar conceitos já presentes em normas técnicas e códigos de ética existentes no campo da pesquisa, tais como o sigilo de dados e a autodeterminação informativa, trouxe um novo olhar sobre as novas demandas tecnológicas relacionadas ao uso massivo de informações. Sendo assim, a utilização de técnicas de anonimização e pseudoanonimização para o tratamento de dados pessoais deve ser aplicada de forma que busque o equilíbrio entre garantir o sigilo dos dados e não comprometer a qualidade da informação. Para isso, é necessário o desenvolvimento de algoritmos e metodologias de controle de dados científicos. Algumas iniciativas têm sido desenvolvidas, como os Centros de Dados orientados para pesquisa, que fornecem infraestrutura e profissionais especializados em gerenciar diferentes bases de dados, e os movimentos de compartilhamento de dados abertos que, em consonância com as medidas de proteção de dados pessoais, disponibilizam dados para incentivar o desenvolvimento de pesquisas em saúde.

Palavras-chave: Proteção de Dados. LGPD. Pesquisa em Saúde. Base de Dados. Saúde Pública.

ABSTRACT Secondary databases are important sources of information for the development of health research, whose results will contribute to the improvement of care protocols and public policies. The Brazilian General Data Protection Law (LGPD), in addition to consolidating concepts already present in existing technical standards and ethical codes in the field of research, such as data confidentiality and informational self-determination, has brought a new perspective on the technological demands of massive information use. Therefore, the use of anonymization and pseudo-anonymization techniques for processing personal data must aim to strike a balance between ensuring data confidentiality without compromising information quality. This requires the development of algorithms and methodologies for managing

[1] Enfermeira do Centro de Vigilância Sanitária da Secretaria de Estado da Saúde de São Paulo e Analista em Epidemiologia do Hospital Israelita Albert Einstein. Mestre em Medicina Preventiva pela Universidade de São Paulo. Especialista em Administração Hospitalar pela Universidade de São Paulo.

[2] Procuradora do Estado de São Paulo. Doutora e Mestra em Direito Processual Civil pela Universidade de São Paulo (USP). Autora do livro "Tutela jurisdicional e direito à saúde: análise crítica da farmacialização do Judiciário" e de artigos jurídicos. Membra da Comissão Especial de Direito Constitucional da OAB/SP. Professora em cursos diversos. Palestrante.

DOI: 10.22491/respge.v16i1.1736

scientific data. Some initiatives have been developed, such as Research-Oriented Data Centers, which provide infrastructure and specialized professionals to manage different databases, and Open Data Sharing movements, which make data available in compliance with personal data protection measures to support the development of health research.

Keywords: Data Protection. General Data Protection Regulation. Health Services Research. Database. Public Health.

1. INTRODUÇÃO

O artigo de Warren e Brandeis intitulado "The right to privacy"[3] foi o marco inicial do conceito de privacidade, cuja expressão se pautou no individualismo e no direito de ser deixado só. Por ter características patrimonialistas, restringia-se às classes tipicamente burguesas. No entanto, essa visão, corroborada pelo crescimento do fluxo de informações digitais, constituiu-se como pré-condição fundamental para o exercício de diversas outras liberdades fundamentais[4].

A partir do conceito inicial de privacidade associado ao isolamento, refúgio ou segredo, a noção de privacidade recebe influências sociais, como a relação do indivíduo com o Estado, as reivindicações de classes trabalhadoras por direitos e, juntamente com o aumento da capacidade técnica de processamento de informações, que moldaram e ampliaram o uso de informações pessoais, amparadas pela necessidade de eficiência e controle[5].

O Estado foi o primeiro a coletar, tratar e utilizar dados pessoais sob a justificativa de uma Administração Pública mais eficiente. No entanto, quanto mais se conhece os cidadãos, maior o poder estatal sobre eles, sendo esse forte controle social característico de regimes totalitários[6].

A tecnologia trouxe, ao longo dos anos, maior rapidez na coleta e no tratamento das informações. Seu avanço permitiu que qualquer instrumento, desde um celular até uma simples torradeira, seja capaz de captar, coletar, armazenar, processar e analisar informações dos indivíduos, empresas e governos durante as atividades corriqueiras. Além disso, esse progresso contribui para a formatação de produtos personalizados, os quais vêm sendo gradativamente substituídos por mercados ricos em dados.

---

[3] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, Cambridge, v. IV, n. 15, dez. 1890. Disponível em: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acesso em: 3 abr. 2026.

[4] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 30-47.

[5] Ibid.

[6] Ibid.

Consequentemente, muitas informações não são coletadas por necessidade, mas pela facilidade em sua obtenção e "[…] independentemente do paradigma tecnológico, o controle da informação foi sempre um elemento essencial na definição de poderes dentro de uma sociedade […]"[7] [8].

O campo da saúde vem acompanhando essa transformação com dados que passam a ser digitais de forma crescente e com o desenvolvimento de tecnologias, como o *Big Data* (grandes dados ou megadados), incorporando técnicas de análise sofisticadas que possibilitam o desenvolvimento de novas formas de produção de conhecimento em escala.

Contudo, ao mesmo tempo em que grandes bancos de dados podem fornecer insumos para o desenvolvimento de conhecimentos científicos que beneficiam a sociedade e o desenvolvimento de políticas públicas, emergem riscos de reidentificação[9] e possíveis ataques cibernéticos que podem comprometer tanto a proteção dos participantes da pesquisa, quanto a autonomia, a privacidade e a confidencialidade de suas informações.

O presente estudo tem como objetivo compreender a relação entre dados utilizados em pesquisas de saúde e a privacidade e proteção de dados pessoais, buscando-se explorar os possíveis caminhos de convergência para garantir tanto o direito à saúde, quanto o direito à privacidade da população na utilização de novas tecnologias de uso massivo da informação.

2. A PROTEÇÃO DE DADOS NO BRASIL

As primeiras discussões sobre a necessidade de regulamentos sobre privacidade e proteção de dados no mundo remontam a meados da década de 1960,

---

[7] Ibid.

[8] ABRAMOVAY, Ricardo; ZANATTA, Rafael Augusto Ferreira. Dados Pessoais Abertos: Pilares dos Novos Mercados Digitais? **RDU**, Porto Alegre, v. 16, n. 90, p. 155-178, 2019.

[9] A reidentificação consiste no processo de reassociar dados anonimizados ou pseudoanonimizados a um indivíduo específico, representando um sério risco à privacidade e à conformidade com a LGPD. O uso de inteligência artificial (IA) e o cruzamento de bases de dados (quase identificadores) tornam a reidentificação possível, exigindo técnicas robustas de proteção, como a anonimização eficaz e a privacidade diferencial. "A proliferação de informações publicamente disponíveis online, combinada com hardware de computador cada vez mais poderoso, tornou possível a reidentificação de dados 'anonimizados'. Isso significa que dados apagados agora podem ser rastreados até o usuário individual a quem se referem. A reidentificação de dados apagados é comumente realizada combinando dois ou mais conjuntos de dados para encontrar o mesmo usuário em ambos. Essa informação combinada frequentemente revela informações de identificação direta sobre um indivíduo. A reidentificação de dados anonimizados tem sérias implicações para a privacidade e para as políticas públicas, à medida que reguladores, empresas e consumidores lutam para definir privacidade na era moderna do registro permanente". LUBARSKY, Boris. Reidentificação de dados "anonimizados". **Georgetown Law Technology Review**, 2017. Disponível em: https://georgetownlawtechreview-org.translate.goog/re-identification-of-anonymized-data/GLTR-04-2017/?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt&_x_tr_pto=tc. Acesso em: 3 abr. 2026.

tendo sido a Alemanha o primeiro país a elaborar um marco regulatório sobre o tema, em 1970[10].

Nos últimos 20 anos, vários países produziram normas, totalizando 142 países com legislação específica sobre privacidade e proteção de dados [11]. No Brasil, a privacidade e a proteção de dados pessoais estão contempladas na Constituição Federal sob as garantias de: liberdade de expressão (art. 5º, inc. IX; art. 220), direito à informação (art. 5º, inc. XIV; art. 220), salvaguarda da vida privada e da intimidade (art. 5º, inc. X) e do domicílio (art. 5º, inc. XI), bem como o sigilo de sua correspondência, das comunicação telegráficas e telefônicas e de seus dados (art. 5º, inc. XII), e a concessão de *habeas-data* (art. 5º, inc. LXII).

Outras legislações, como o Código Civil (art. 23)[12] e o Código de Defesa do Consumidor (CDC)[13], trazem algumas garantias de proteção à vida privada e às informações cadastrais. No entanto, mostravam-se insuficientes, principalmente diante das novas circunstâncias decorrentes da evolução tecnológica, tais como o uso abusivo de informações pessoais armazenadas em bancos de dados, que poderiam ser utilizados para fins diversos daqueles que motivaram sua coleta[14].

A Emenda Constitucional nº 115, de 10 de fevereiro de 2022, a fim de assegurar "a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais […]"[15], incluiu dois incisos no art. 5º da Constituição: o LXXIX, que garante o direito à proteção de dados pessoais, inclusive em meios digitais; e o XXVI que determina a criação de ações de fiscalização dos tratamentos de dados pessoais; ao art. 22, acresceu a responsabilidade da União diante da proteção e do tratamento de dados pessoais, conforme o inciso XXX.

Em 14 de agosto, de 2018, com a promulgação da Lei Geral de Proteção de Dados (LGPD)[16], estruturou-se a base normativa dedicada à disciplina da proteção

[10] DONEDA, Danilo. A LGPD como elemento estruturante do modelo brasileiro de proteção de dados. In: **Lei geral de proteção de dados (Lei nº 13.709/2018)**: a caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters; Revista dos Tribunais, 2020, p. 243-255.

[11] Ibid.

[12] BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**, Brasília, DF, 10 jan. 2002.

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

[14] DONEDA, 2021, *op. cit.*, p. 267-368.

[15] 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 fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial da União**, Brasília, 2022.

[16] 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 jun. 2024.

de dados, na qual se estabeleceram os princípios de proteção aplicáveis a diferentes situações de tratamento de dados pessoais, garantindo-se a proteção dos direitos fundamentais de liberdade e personalidade[17].

A LGPD, além de consolidar elementos já presentes na ordem jurídica, incluiu conceitos novos e próprios de proteção de dados, seus princípios, os direitos do titular e as regras de tratamento que consideram o risco dessa atividade. A lei traz um instrumental jurídico próprio, sendo aplicável em diferentes atividades econômicas e instituições, sejam elas públicas ou privadas, em diferentes cenários e situações, incorporando-se à sociedade os parâmetros utilizados globalmente sobre regulação e proteção de dados[18].

3. OS DADOS DE SAÚDE

A utilização de bases de dados de saúde como instrumento de apoio na identificação de epidemias que assolam a sociedade não é recente. Estudos clássicos, como o surto de cólera em Londres, em 1854, em que o médico John Snow estudou sua transmissão a partir do mapeamento das casas com enfermos e da identificação de determinado poço de água como fonte de contaminação; bem como Florence Nightingale, que demonstrou em gráficos que a principal causa de morte entre os soldados da Guerra da Criméia foi infecção por feridas de guerra não tratadas, são exemplos de que a aplicação de dados por métodos estatísticos e epidemiológicos pode ser essencial para se compreender e definir estratégias de combate às doenças[19] [20].

A Epidemiologia, enquanto campo científico que estuda a dinâmica da saúde e do adoecimento das populações, a partir dos anos 1960, passou por uma transformação histórica de suas práticas com o desenvolvimento de modelos matemáticos e técnicas analíticas complexas, graças à introdução da computação eletrônica, que permitiu a análise de grandes bases de dados e a sistematização do conhecimento epidemiológico[21].

No Brasil, os primeiros passos para a construção de bases de dados de saúde começaram em 1977, com a padronização dos registros de óbito e a criação de um sistema informatizado para a coleta de dados dos atestados de óbito e a formatação dos dados de produção hospitalar pelo extinto Instituto Nacional de Assistência Médica da Previdência Social (Inamps). Ao longo do tempo, essas iniciativas foram

---

[17] DONEDA, 2020, *op. cit.*

[18] Ibid.

[19] SALSBURG, David. **Uma senhora toma chá…**: Como a estatística revolucionou a ciência no século XX. São Paulo: Zahar, 2009.

[20] SNOW, John. **Sobre a maneira de transmissão do cólera**. São Paulo: Hucitec, 1999.

[21] ALMEIDA FILHO, Naomar de. Bases históricas da Epidemiologia. **Cadernos de Saúde Pública**, Rio de Janeiro, v. 2, n. 3, p. 304-311, set. 1986.

aprimoradas e se tornaram o Sistema de Informações de Mortalidade (SIM) e o Sistema de Internações Hospitalares (SIH-SUS)[22].

Em 1988, a criação do Sistema Único de Saúde (SUS) trouxe a garantia constitucional do direito à saúde que se materializa em forma de políticas públicas voltadas para a redução de riscos e agravos à saúde, bem como para o acesso às ações e serviços públicos de saúde, prioritariamente preventivos, mas sem prejuízo das atividades assistenciais. Logo, o Sistema Nacional de Vigilância em Saúde (SNVS) tem um papel importante no desenvolvimento da coleta de dados, na consolidação e na análise de informações que identifiquem riscos e agravos à saúde e que sirvam como subsídios para o planejamento de medidas de promoção da saúde e redução de morbidades[23].

A Política Nacional em Vigilância em Saúde (PNVS), como política pública de Estado e função essencial do SUS, orienta o modelo de atenção, no qual as ações de vigilância em saúde são definidas em todos os níveis de atenção do SUS e a Vigilância em Saúde é descrita como "o processo contínuo e sistemático de coleta, consolidação, análise de dados e disseminação de informações sobre eventos relacionados à saúde", que visam ao "planejamento e à implementação de medidas de saúde pública, incluindo a regulação, intervenção e atuação em condicionantes e determinantes da saúde, para a proteção e promoção da saúde da população, prevenção e controle de riscos, agravos e doenças", conforme § 1º do art. 2º da Resolução n. 588/2018[24].

Além do SIM e do SIH, podemos citar o Sistema Nacional de Notificação Compulsória (SINAN), que consiste na comunicação obrigatória das doenças de notificação compulsória à autoridade de saúde, realizada por profissionais da área (médicos, enfermeiros, fisioterapeutas, entre outros) ou pelo responsável pelo estabelecimento de saúde, seja público ou privado, sobre a ocorrência de suspeita ou confirmação de doença, agravo ou evento de saúde pública.

Esse sistema de alerta é primordial para a identificação de emergências de saúde pública que representam risco imediato à saúde e que demandam a implantação de estratégias oportunas para a contenção da doença. Um exemplo de monitorização de doenças de grande impacto na saúde pública foi a identificação dos primeiros casos de covid-19 no Brasil, que motivaram as primeiras medidas de isolamento social como forma de contenção da doença[25].

---

[22] LIMA, Claudia Risso de Araujo *et al*. Departamento de Informática do SUS – DATASUS: a experiência de disseminação de informações em saúde. In: BRASIL (org.). **A experiência brasileira em sistemas de informação em saúde**. Brasília: Editora do Ministério da Saúde, 2009. v. 1, p. 109-128.

[23] *Ibid*.

[24] BRASIL. Conselho Nacional de Saúde. **Resolução nº 588, de 12 de julho de 2018.** Institui a Política Nacional de Vigilância em Saúde (PNVS). Brasília, DF: Conselho Nacional de Saúde, 2018. Disponível em: https://conselho.saude.gov.br/resolucoes/2018/Reso588.pdf . Acesso em 3 abr. 2026.

[25] BRASIL. Ministério da Saúde. **Portaria nº 188, de 3 de fevereiro de 2020**. Declara Emergência em Saúde Pública de importância Nacional (ESPIN) em decorrência da Infecção Humana pelo novo Coronavírus (2019-nCoV). Brasília, DF: Ministério da Saúde, 2020.

O Sistema de Informações de Nascidos Vivos (SINASC), implantado pelo Ministério da Saúde, em 1990, tem como objetivo garantir o registro sistemático de informações de nascidos vivos no país. A Declaração de Nascido Vivo (DN) é o documento padrão de preenchimento obrigatório em todo o território nacional, cuja emissão e distribuição são de responsabilidade do Ministério da Saúde, enquanto as Secretarias Estaduais e Municipais de Saúde realizam a distribuição das DN nas maternidades e controlam o fluxo de informação das DN entre os estabelecimentos de saúde, cartórios de registro civil e profissionais de saúde autônomos que realizam partos domiciliares[26].

Em três vias pré-numeradas sequencialmente, os estabelecimentos de saúde realizam o preenchimento da via impressa com dados da mãe (idade, raça e atividade econômica), pré-natal (número de consultas de pré-natal), parto (tipo de parto, idade gestacional) e recém-nascido (peso, altura, Apgar ao nascimento), e inserem as informações em uma base de dados digital. Tais informações são utilizadas pelos gestores municipais e estaduais como subsídios para o planejamento de políticas públicas, além de construírem uma base de dados amplamente utilizada em pesquisas científicas[27].

Em um estudo de revisão sobre o SINASC[28], o acesso amplo de suas bases de dados possibilitou o desenvolvimento de diferentes publicações científicas por instituições renomadas de pesquisa e por serviços de saúde assistenciais, que desenvolvem análises temporais, estudos de prevalência, diagnósticos de saúde e desenvolvimento de indicadores de qualidade. Como exemplo, podemos citar o acompanhamento da taxa de mortalidade neonatal, que, do total de nascimentos no período, apresenta a proporção de crianças que morrem na primeira semana de vida, sendo que altas taxas podem sinalizar falhas na assistência pré-natal, parto e risco à saúde do nascituro.

Além das bases de dados voltadas à vigilância em saúde, o prontuário médico é uma importante fonte de informação da saúde dos indivíduos. Trata-se de um documento utilizado por estabelecimentos assistenciais de saúde, no qual são registrados dados do paciente: demográficos, queixas de saúde, história familiar e pessoal, estilo de vida, procedimentos de saúde, pregressos, histórico de doenças, uso de medicamentos, resultados de exames e procedimentos, entre outros. Essas informações possibilitam que a equipe assistencial registre, monitore e avalie a evolução do paciente frente a uma doença ou risco de saúde, e defina condutas assistenciais que levem à recuperação da saúde do paciente.

---

[26] BRASIL. Ministério da Saúde. **Sistemas de informação em saúde**. 2024. Disponível em: https://www.gov.br/aids/pt-br/svsa-na-gestao-municipal/agravos-e-doencas-cronicas-nao-transmissiveis/links-de-interesse-sobre-agravos-e-doencas-cronicas-nao-transmissiveis/sistemas-de-informacao-em-saude. Acesso em: 17 jun. 2024.

[27] *Ibid*.

[28] PAIVA, Natália Santana, *et al*. Sistema de informações sobre nascidos vivos: um estudo de revisão. **Ciência & Saúde Coletiva**, Rio de Janeiro, v. 16, supl. 1, p. 1211-1220, 2011.

Para garantir a qualidade do registro dos dados, o Conselho Federal de Medicina (CFM) definiu os itens obrigatórios na composição de um prontuário[29]. No entanto, cada serviço de saúde tem autonomia para elaborar seus próprios formulários, a forma de registro dos dados e o sistema de informação que irá adotar quando o prontuário é digital. Ainda que haja uma heterogeneidade de sistemas no mercado e que, em geral, não se comunicam, os sistemas de inteligência artificial possibilitarão, em breve, a associação de dados hospitalares de diferentes serviços ou bases de dados diversas de forma precisa e rápida.

Na área de saúde, as pesquisas científicas possuem diferentes metodologias. Em relação ao tipo de coleta de dados, duas formas são apresentadas: pesquisas com base de dados primários, quando estes são coletados com a finalidade específica da pesquisa, isto é, a metodologia de coleta, tendo os formulários elaborados somente para a pesquisa em desenvolvimento; já a pesquisa com base de dados secundárias utiliza fontes já existentes, construídas para outra finalidade (dados demográficos, epidemiológicos, clínicos, diagnósticos e terapêuticos), e que podem vir a ser utilizadas para o desenvolvimento de uma pesquisa científica.

Pela própria construção do raciocínio clínico que provém da associação de diversos fatores de risco, que podem provocar e definir a evolução de uma doença ou situação de saúde, a coleta de dados na área da saúde dispõe, além do cotidiano da assistência à saúde, de dados que podem consolidar indicadores e fornecer informações de apoio à gestão de saúde e elaboração de fontes de dados para o desenvolvimento de pesquisas científicas. A utilização de bases de dados secundárias, como fonte de informação para o desenvolvimento de pesquisas científicas, tem sido uma opção mais acessível e ágil em relação às pesquisas com base de dados primários, que, pela própria configuração, demandam maior volume de recursos financeiros e recursos humanos treinados e específicos.

Logo, verifica-se que há a necessidade de se criar uma agenda de tratamento de dados sem violar a privacidade e a proteção de dados. Da mesma forma que a circulação da informação pode ser benéfica por possibilitar o desenvolvimento de pesquisas e políticas públicas que contribuirão com a saúde, podendo oferecer mais oportunidades aos cidadãos; por outro lado, ela pode trazer aspectos negativos, como

[29] A Resolução CFM 1.638/2002 do Conselho Federal de Medicina, no art. 5º, define os itens obrigatórios no prontuário médico, seja eletrônico ou de papel: "[…] a. Identificação do paciente – nome completo, data de nascimento (dia, mês e ano com quatro dígitos), sexo, nome da mãe, naturalidade (indicando o município e o estado de nascimento), endereço completo (nome da via pública, número, complemento, bairro/distrito, município, estado e CEP); b. Anamnese, exame físico, exames complementares solicitados e seus respectivos resultados, hipóteses diagnósticas, diagnóstico definitivo e tratamento efetuado; c. Evolução diária do paciente, com data e hora, discriminação de todos os procedimentos aos quais o mesmo foi submetido e identificação dos profissionais que os realizaram, assinados eletronicamente quando elaborados e/ou armazenados em meio eletrônico […]". CONSELHO FEDERAL DE MEDICINA. Resolução nº 1.638/2002. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. **Diário Oficial da União**, Brasília, 2002.

incidentes de segurança e a consequente exposição de dados pessoais. Na saúde, em especial, a divulgação de dados sensíveis pode causar constrangimentos, discriminações e outras consequências danosas aos seus titulares.

Algumas frentes de promoção ao compartilhamento de dados em prol da ciência têm se empenhado em estabelecer diretrizes que busquem o equilíbrio entre o uso de bases de dados secundárias e a proteção dos dados.

O Movimento da Ciência Aberta, por exemplo, é uma iniciativa de financiadores de pesquisas científicas, governamentais e não-governamentais de vários países, que buscam promover o acesso aberto a publicações e dados científicos gerados em pesquisas, em especial as que são geradas com recursos públicos, com o intuito de disseminar conhecimentos que beneficiem a sociedade como parte integrante de políticas públicas. Para isso, essas frentes elaboram princípios e recomendações para garantir a convergência e a padronização do tratamento e do compartilhamento dos dados, de acordo com princípios éticos e regulatórios aceitos globalmente[30].

4. A PROTEÇÃO DOS DADOS EM PESQUISAS DE SAÚDE

A privacidade, o uso e o tratamento de dados pessoais sempre foram motivo de preocupação no campo da pesquisa em saúde. O Código de Nuremberg (1947), como resposta aos cruéis experimentos com seres humanos ocorridos durante o Holocausto, trouxe os princípios éticos que permeiam a pesquisa envolvendo seres humanos, dentre eles, o consentimento voluntário. Logo, ao participante deve ser assegurado o direito ao conhecimento e à compreensão da pesquisa e o direito à livre escolha, pelo qual se garante autonomia em suas decisões. Em 1975, a privacidade foi inserida na Declaração de Helsinque, na qual se determinou a responsabilidade dos pesquisadores de adotarem medidas para garantir a privacidade, a integridade física e mental, e a personalidade do indivíduo. O conceito de confidencialidade das informações foi incorporado a essa declaração em 2000[31].

No Brasil, a privacidade dos sujeitos da pesquisa e o sigilo das informações foram definidos na Resolução CNS nº 466/2012[32] do Conselho Nacional de Saúde. Entre os fundamentos éticos, a confidencialidade, a privacidade e a proteção da imagem e da pessoa são citados no item III.2.i, o qual prevê que o pesquisador

[30] ALMEIDA, Betânia de Araújo; PIMENTA, Denise Moraes; BARRETO, Mauricio Lima. Compartilhamento e abertura de dados na Ciência Aberta e a pesquisa em saúde pública na Lei Geral de Proteção de Dados. **Bahia Análise & Dados**, Salvador, v. 31, n. 2, p. 78-92, 2021.

[31] DALLARI, Analluza Bolivar. Enquadramento do contrato de pesquisa clínica à luz das normas de aplicação imediata brasileiras. In: DALLARI, Analluza Bolivar (org.). **Contrato de Pesquisa Clínica**: aspectos práticos e jurídicos. São Paulo: Revista dos Tribunais, 2019, p. 163-2010.

[32] BRASIL. Ministério da Saúde. Conselho Nacional de Saúde. **Resolução nº 466, de 12 de dezembro de 2012.** Aprova as diretrizes e normas regulamentadoras de pesquisas envolvendo seres humanos. Brasília, DF: Ministério da Saúde, 2012.

é responsável por "[…] manter os dados da pesquisa em arquivo, físico ou digital, sob sua guarda e responsabilidade, por um período de cinco anos após o término da pesquisa", conforme o item XI.2.f.

O Código de Ética Médica[33] traz definições importantes sobre o prontuário médico, não podendo o profissional negar ao paciente e seus familiares o acesso aos prontuários, ou deixar de informá-los sobre seu estado de saúde e riscos envolvidos. O médico deve manter sigilo das informações resultantes do desempenho de suas funções e as informações do prontuário devem ser guardadas de forma sigilosa. No âmbito da pesquisa, o mesmo Código cita a responsabilidade desse profissional ao participar de pesquisas que envolvem seres humanos ou qualquer outro animal, devendo seguir as normas éticas brasileiras e proteger a vulnerabilidade dos sujeitos da pesquisa.

Muitos aspectos contidos na LGPD, como o respeito à privacidade, o sigilo dos dados e a autodeterminação informativa, já faziam parte da rotina das pesquisas científicas. O Termo de Consentimento Livre e Esclarecido, por exemplo, sempre foi instrumento obrigatório aplicado em pesquisas com dados primários, garantindo autonomia, acesso às informações e proteção da privacidade dos participantes da pesquisa. Sendo assim, observa-se uma convergência entre as normativas do CEP/CONEP com a LGPD. No entanto, são necessários esforços institucionais para a adequação de situações novas como o *Big Data*[34].

A pesquisa com bases de dados secundárias, dada a categorização de suas variáveis e a apresentação dos resultados de forma agregada, não faria referência a dados individuais de seus participantes. No entanto, tais pesquisas podem trazer um risco de discriminação não direcionado a uma pessoa em particular, mas a um grupo de pessoas com características em comum (status social, econômico, etnia, gênero) e, também, em algumas situações em que a identificação pessoal se faz necessária para agregar dados de diferentes fontes de informação, sob risco de exposição de dados sensíveis. Esses riscos podem ser catalisados, ainda, por algoritmos de reidentificação e tais situações devem ser avaliadas com critério, tendo seus riscos mitigados[35].

A LGPD prevê o tratamento de dados pessoais (art. 7º) e de dados sensíveis (art. 11) em estudos feitos por órgãos de pesquisa, desde que seja garantida a

[33] O Código de Ética Médica define em: Princípios Fundamentais, inciso XI – "O médico guardará sigilo a respeito das informações de que detenha conhecimento no desempenho de suas funções, com exceção dos casos previstos em lei e X – Documentos Médicos; Art. 88. Negar, ao paciente, acesso a seu prontuário, deixar de lhe fornecer cópia quando solicitada, bem como deixar de lhe dar explicações necessárias à sua compreensão, salvo quando ocasionarem riscos ao próprio paciente ou a terceiros".

[34] ALMEIDA, Betânia de Araújo. Ética em pesquisa e dados sensíveis: o que muda? In: SILVA, Angélica Baptista; CUNHA, Francisco José Aragão Pedrosa (orgs.). **Lei geral de proteção de dados e o controle social da saúde.** Porto Alegre: Rede Unida, 2023, p. 280-291.

[35] BARRETO, Maurício Lima; ALMEIDA, Bethânia de Araújo; DONEDA, Danilo. Uso e Proteção de Dados Pessoais na Pesquisa Científica. **RDU**, Porto Alegre, v. 16, n. 90, p. 179-194, 2019.

anonimização dos dados pelos agentes de tratamento. Prevê-se, também, o desenvolvimento de estudos em saúde pública (art. 13) que devem seguir alguns cuidados específicos: os dados pessoais devem ser tratados exclusivamente no órgão de pesquisa, restritos à finalidade da pesquisa; além disso, devem ser mantidos em ambiente controlado e seguro, sendo aplicada a anonimização ou pseudoanonimização sempre que possível, de acordo com as normas éticas em pesquisa.

A pesquisa, por realizar o tratamento de dados pessoais, deve buscar o equilíbrio entre proteger o direito dos titulares de dados e garantir o interesse público a partir de métodos que protejam esses dados com o mínimo de processamento para alcançar os objetivos da pesquisa, reduzindo o risco de sua inutilização. Uma vez que a ética em pesquisa faz parte da legalidade do tratamento de dados, o Sistema CEP/CONEP e a Autoridade Nacional de Proteção de Dados (ANPD) devem estabelecer, em conjunto com a comunidade científica, as normas necessárias para a salvaguarda da dignidade, os direitos e a segurança dos participantes em pesquisas cuja fonte de informação são bancos de dados administrativos[36].

Em junho de 2023, a ANPD publicou o guia orientativo intitulado "Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas", como resultado de um estudo técnico que apresenta boas práticas no tratamento de dados pessoais em pesquisa como orientação aos agentes de tratamento[37].

Conforme o guia, o regime jurídico do tratamento de dados pessoais para fins acadêmicos e de pesquisas tem maior flexibilidade, sem prejuízo à liberdade de expressão, à liberdade acadêmica e à promoção da inovação científica e tecnológica, desde que sejam tomadas medidas adequadas de proteção de dados dos titulares e seja seguido o princípio da boa-fé[38], conforme previsto no art. 6º da LGPD[39].

5. ANONIMIZAÇÃO E PSEUDOANONIMIZAÇÃO DE BASES DE DADOS

Dado pessoal e dado anônimo são opostos na medida em que o primeiro permite a identificação de um indivíduo e o segundo busca ocultar suas características, impedindo sua identificação. A partir de técnicas de anonimização (supressão, generalização, randomização e pseudoanonimização), um dado pessoal pode

[36] BARRETO; ALMEIDA; DONEDA, 2019, *op. cit*.

[37] VARGAS, Andressa Girotto, *et al*. **Guia Orientativo**: tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas. Brasília, DF: Autoridade Nacional de Proteção de Dados, 2023.

[38] I. finalidade, II. adequação, III. necessidade, IV. livre acesso, V. qualidade dos dados, VI. transparência, VII. segurança, VIII. prevenção, IX. não discriminação e X. responsabilização e prestação de contas.

[39] VARGAS *et al.*, *op. cit*.

tornar-se um dado anônimo, sendo essa uma das formas de assegurar a confidencialidade desse dado[40].

O desenvolvimento de técnicas e algoritmos de anonimização em bases secundárias pode reduzir o risco de reidentificação e consequentes ataques cibernéticos. Em tese, um dado anonimizado seria suficiente para garantir a confidencialidade e a proteção dos dados, dispensando o consentimento do usuário e mitigando-se o viés de seleção. Porém, quanto maior o grau de anonimização, mais as informações deixam de fornecer conteúdos relevantes, tornando-se inúteis. Por outro lado, se forem mantidos os dados em sua integridade, o risco de reidentificação cresce substancialmente[41].

Em uma revisão sistemática que avaliou a capacidade de anonimização de 75 (setenta e cinco) algoritmos demográficos, 18 (dezoito) algoritmos de diagnóstico médico e 3 (três) sobre dados genéticos, os autores concluíram que combinação de diferentes técnicas e a aplicação adequada dos algoritmos podem reduzir o risco de reidentificação. No entanto, algoritmos mais eficientes para diagnóstico médico e dados genéticos precisam ser desenvolvidos[42].

O processo de anonimização envolve uma série de riscos que o agente de tratamento deve considerar[43]:

a) grandes volumes de dados têm maiores chances de estabelecerem o processo reverso da identificação, dado o aumento das chances de acerto das associações. Por isso, devem ser aplicadas técnicas mais robustas;

b) a natureza dos dados define o quanto um dado pode proporcionar informações valiosas, como, por exemplo, informações financeiras e de consumo podem ser mais atrativas por identificarem possíveis vítimas de extorsão;

c) a cadeia da atividade de tratamento de dados, na qual quanto maior o número de sujeitos que compartilham ou geram a base de dados, maior o risco de reidentificação;

d) o gerenciamento de identidades e a segmentação referem-se ao controle do acesso dos atores aos dados, reduzindo-se as chances de que pessoas capazes unam as informações, reconheçam um indivíduo e monitorem as atividades dos agentes de tratamento;

---

[40] BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. In: DONEDA, Danilo.; MENDES, Laura Schertel Mendes; CUEVA, Ricardo Villas Bôas, (orgs.). **Lei geral de proteção de dados (Lei nº 13.709/2018)**: a caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Revista dos Tribunais, 2020, p. 39-54.

[41] SEPAS, Ali, *et al*. Algorithms to anonymize structured medical and healthcare data: A systematic review. ***Frontiers in Bioinformatics***, v. 2, 2022, p. 1-11.

[42] *Ibid*.

[43] BIONI, *op. cit.*, p. 39-54.

e) a inclusão de cláusulas contratuais que delimitem as atividades dos agentes de tratamento ou proíbam o processo de anonimização; e

f) as técnicas de anonimização devem ser atualizadas continuamente para que não se tornem defasadas e para que as bases não fiquem vulneráveis a técnicas novas de reidentificação.

No §4º do art. 13 da LGPD, a pseudoanonimização é definida como um tratamento do dado pessoal de tal forma que não há possibilidade de associação, direta ou indiretamente, a um indivíduo, mas que o agente de tratamento pode, por meio de informação adicional e em ambiente seguro e controlado, reverter suas características originais que caracterizam determinado indivíduo. O uso da pseudoanonimização está restrito a estudos de saúde pública.

A aplicação de técnicas de anonimização requer conhecimento técnico sofisticado, especializado e, a depender do grau de complexidade da base de dados, implica custos mais elevados. Em alguns países foram criados centros de dados orientados para pesquisa que desenvolvem espaços com infraestrutura adequada e profissionais especializados, além de elaborarem políticas de governança de dados com objetivo de prover acesso a dados de qualidade, de forma segura e controlada para pesquisas, avaliações e informações que subsidiem políticas públicas.

Geralmente, são organizações em parceria com o governo, universidades e instituições de pesquisa que agregam grandes de bases de dados de registros administrativos que, apesar de não terem sido coletadas para fins de pesquisa, podem ser utilizadas em projetos de pesquisa. Tais centros, após o tratamento de dados e a desidentificação dos indivíduos, viabilizam o acesso integrado de bases de dados às pesquisas científicas, buscando um equilíbrio entre o desenvolvimento da ciência para o benefício coletivo e a garantia da proteção dos dados pessoais.

Cite-se, ainda, a iniciativa brasileira promovida pela Fiocruz, que é o Centro de Integração de Dados e Conhecimentos para a Saúde (CIDACS)[44].

6. CONCLUSÕES

Na área da pesquisa em saúde, a LGPD instigou os atores envolvidos no tratamento de dados a revisitarem os fluxos de informações e, a partir daí, identificarem os pontos de vulnerabilidade e possíveis falhas na garantia da privacidade dos indivíduos e na proteção dos dados pessoais.

Em um primeiro momento, sua aplicação trouxe dúvidas que levaram muitos órgãos de pesquisa e comitês de ética em pesquisa a recusarem a utilização de bases de dados secundárias em razão da impossibilidade de consentimento dos titulares.

[44] BARRETO; ALMEIDA; DONEDA, 2019, *op. cit.*

No entanto, com o passar do tempo e uma melhor compreensão da LGPD, os órgãos de pesquisa buscaram se adequar e atingir o equilíbrio entre a proteção dos dados pessoais e o desenvolvimento de pesquisas científicas, sem prejuízo do potencial que as bases de dados em saúde podem fornecer para o desenvolvimento científico, tecnológico e de inovação, além das garantias de liberdade de expressão e pluralismo de ideias, bem como da liberdade acadêmica.

A aplicação de técnicas de anonimização por meio do desenvolvimento de algoritmos é uma possibilidade para a garantia da proteção dos dados. Porém, deve-se considerar os custos de desenvolvimento dessas ferramentas e a necessidade de profissionais especializados e em constante atualização, uma vez que, a cada dia, os dados se tornam ativos valiosos, aumentando as chances de reidentificação e, consequentemente, de ataques cibernéticos que podem levar a constrangimentos, à exposição de dados pessoais ou a situações mais graves como extorsões e roubos.

A criação de centros de dados orientados para pesquisa pode ser uma opção, cenário no qual se concentrariam as condições necessárias para o desenvolvimento de mecanismos de anonimização, com o controle dos dados pessoais de forma a garantir sua proteção.

Atualmente, muitos dados estão restritos às mãos de um número limitado de empresas e instituições (públicas e privadas) que podem direcionar o uso de dados para seu próprio interesse, o qual nem sempre estará em consonância com as necessidades da sociedade. O compartilhamento de dados abertos, desde que garanta a privacidade dos sujeitos e proteção dos dados pessoais, deve ser incentivado para que possam ser disponibilizados para o maior número de pesquisadores e órgãos de pesquisa, buscando-se ampliar o conhecimento, reduzir a concentração de poder e beneficiar a sociedade com ética e responsabilidade.

REFERÊNCIAS BILIOGRÁFICAS

ABRAMOVAY, Ricardo; ZANATTA, Rafael Augusto Ferreira. Dados Pessoais Abertos: Pilares dos Novos Mercados Digitais? **RDU**, Porto Alegre, v. 16, n. 90, p. 155-178, 2019.

ALMEIDA, Betânia de Araújo. Ética em pesquisa e dados sensíveis: o que muda? In: SILVA, Angélica Baptista; CUNHA, Francisco José Aragão Pedrosa (orgs.). **Lei geral de proteção de dados e o controle social da saúde.** Porto Alegre: Rede Unida, 2023, p. 280-291.

ALMEIDA, Betânia de Araújo.; PIMENTA, Denise Moraes; BARRETO, Mauricio Lima. Compartilhamento e abertura de dados na Ciência Aberta e a pesquisa em saúde pública na Lei Geral de Proteção de Dados. **Bahia Análise & Dados**, Salvador, v. 31, n. 2, p. 78-92, 2021. ALMEIDA FILHO, Naomar de. Bases históricas da Epidemiologia. **Cadernos de Saúde Pública**, Rio de Janeiro, v. 2, n. 3, p. 304-311, set. 1986.

BARRETO, Maurício Lima; ALMEIDA, Bethânia de Araújo; DONEDA, Danilo. Uso e Proteção de Dados Pessoais na Pesquisa Científica. **RDU**, Porto Alegre, v. 16, n. 90, p. 179-194, 2019.

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. In: DONEDA, Danilo.; MENDES, Laura Schertel Mendes; CUEVA, Ricardo Villas Bôas, (orgs.). **Lei geral de proteção de dados (Lei nº 13.709/2018**): a caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Revista dos Tribunais, 2020, p. 39-54.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 3 mar. 2024.

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 fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial da União**, Brasília, 2022.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União**, Brasília, DF, 1990.BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**, Brasília, DF, 10 jan. 2002.

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 jun. 2024.

BRASIL. Ministério da Saúde. Conselho Nacional de Saúde. **Resolução nº 466, de 12 de dezembro de 2012**. Aprova as diretrizes e normas regulamentadoras de pesquisas envolvendo seres humanos. Brasília, DF: Ministério da Saúde, 2012.

BRASIL. Conselho Nacional de Saúde. **Resolução nº 588, de 12 de julho de 2018.** Institui a Política Nacional de Vigilância em Saúde (PNVS). Brasília, DF: Conselho Nacional de Saúde, 2018. Disponível em: https://conselho.saude.gov.br/resolucoes/2018/Reso588.pdf. Acesso em 3 abr. 2026.

BRASIL. Ministério da Saúde. **Sistemas de informação em saúde**. 2024. Disponível em: https://www.gov.br/aids/pt-br/svsa-na-gestao-municipal/agravos-e-doencas-cronicas-nao-transmissiveis/links-de-interesse-sobre-agravos-e-doencas-cronicas-nao-transmissiveis/sistemas-de-informacao-em-saude. Acesso em: 3 mar. 2026.

BRASIL. Ministério da Saúde. **Portaria nº 188, de 3 de fevereiro de 2020**. Declara Emergência em Saúde Pública de importância Nacional (ESPIN) em decorrência da Infecção Humana pelo novo Coronavírus (2019-nCoV). Brasília, DF: Ministério da Saúde, 2020.

CONSELHO FEDERAL DE MEDICINA. Resolução nº 1.638/2002. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. **Diário Oficial da União**, Brasília, 2002.

DALLARI, Analluza Bolivar. Enquadramento do contrato de pesquisa clínica à luz das normas de aplicação imediata brasileiras. In: DALLARI, Analluza Bolivar (org.). **Contrato de Pesquisa Clínica**: aspectos práticos e jurídicos. São Paulo: Revista dos Tribunais, 2019, p. 163-2010.

DONEDA, Danilo. A LGPD como elemento estruturante do modelo brasileiro de proteção de dados. In: **Lei geral de proteção de dados (Lei nº 13.709/2018)**: a caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters; Revista dos Tribunais, 2020, p. 243-255.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo: Thomson Reuters Brasil, 2021, p. 30-47.

LIMA, Claudia Risso de Araujo *et al*. Departamento de Informática do SUS – DATASUS: a experiência de disseminação de informações em saúde. In: BRASIL (org.). **A experiência brasileira em sistemas de informação em saúde**. Brasília: Editora do Ministério da Saúde, 2009. v. 1. p. 109-128.

LUBARSKY, Boris. Reidentificação de dados "anonimizados". **Georgetown Law Technology Review**, 2017. Disponível em: https://georgetownlawtechreview-org.translate.goog/re-identification-of-anonymized-data/GLTR-04-2017/?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt&_x_tr_pto=tc. Acesso em: 3 abr. 2026.

PAIVA, Natália Santana, *et al*. Sistema de informações sobre nascidos vivos: um estudo de revisão. **Ciência & Saúde Coletiva**, Rio de Janeiro, v. 16, supl. 1, p. 1211-1220, 2011.

SALSBURG, David. **Uma senhora toma chá…**: Como a estatística revolucionou a ciência no século XX. São Paulo: Zahar, 2009.

SEPAS, Ali, *et al*. Algorithms to anonymize structured medical and healthcare data: A systematic review. **Frontiers in Bioinformatics**, Lausanne, v. 2, 2022, p. 1-11.

SNOW, John. **Sobre a maneira de transmissão do cólera**. São Paulo: Hucitec, 1999.

VARGAS, Andressa Girotto, *et al*. **Guia Orientativo**: tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas. Brasília, DF: Autoridade Nacional de Proteção de Dados, 2023.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, Cambridge, v. IV, n. 15, dez. 1890. Disponível em: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acesso em: 3 abr. 2026.

Submetido em: 23/01/2025
Aprovado em: 22/01/2026

ANÁLISE FACIAL E PROTEÇÃO DE DADOS PESSOAIS

Facial analysis and personal data protection

Murilo Arakaki[1]

SUMÁRIO 1. Introdução; 2. Direito de Imagem; 3. Biometria Facial; 4. Análise Facial; 5. Identificação Facial; 6. Discriminação Algorítmica; 7. Neurodireitos; 8. Conclusão; Referências Bibliográficas.

RESUMO O presente artigo tem como objetivo explorar a atuação dos sistemas de análise facial para classificar indivíduos em categorias de gênero, faixa etária e humor, bem como sua implicação no campo de incidência da norma de proteção de dados pessoais. Ademais, apresenta-se a distinção em relação aos sistemas de reconhecimento facial, cujo propósito principal é a identificação ou a autenticação do indivíduo, e discute-se em que medida essa diferença pode ser relevante para a aplicação da norma jurídica. Por fim, abordam-se outras possíveis implicações acerca da utilização daqueles sistemas: a discriminação algorítmica e os neurodireitos.

Palavras-chave: Dados Pessoais. Dados Pessoais Sensíveis. Análise Facial. Categorização. Reconhecimento Facial. Identificação.

ABSTRACT This article aims to verify the proceeding of facial analysis systems to classify individuals into categories such as gender, age group and mood, and its implication in the incidence of the personal data protection regulation. Furthermore, it presentes the distinction with facial recognition systems, whose main purpose is the identification or authentication of the individual, and discusses the extent to which this difference may be relevant for the application of the legal norm. Finally, it adresses other possible implications of those systems: algorithmic discrimination and neurorights.

Keywords: Personal Data. Sensitive Personal Data. Facial Anaysis. Categorization. Facial Recognition. Identification.

1. INTRODUÇÃO

O desenvolvimento e a difusão de tecnologias digitais, como a inteligência artificial (IA), o *Big Data*, a internet das coisas (IoT), a computação em nuvem (*cloud computing*), a realidade aumentada (RA) e outras, têm transformado a vida das pessoas. Se por um lado, isso ocorre de forma veloz e impactante, sem paralelo comparável na história, por outro, dá-se de modo imperceptível ou naturalizado, no qual dados pessoais são fornecidos, coletados, observados, inferidos e tratados sem que os titulares se sintam necessariamente expostos, manipulados, prejudicados ou

[1] Assessor no Gabinete da Presidência da ARTESP. Advogado, Especialista em Direito Público Municipal pela ESGCP do TCMSP, Especialista em Direito Digital e Inovação Tecnológica pela ESPGE/SP. Engenheiro Eletrônico pela Unicamp. MBA em Tecnologia da Informação pela FIPECAFI.

DOI: 10.22491/*respge*.v16i1.1737

abusados. Desse modo, as pessoas passam a existir no mundo real e no mundo digital, por vezes mais neste do que naquele, em termos de implicações e consequências.

A esse respeito, Teffé[2] explica que o ser humano tende a ter um prolongamento e uma projeção de si no ambiente digital em razão do fenômeno da datificação:

> Vive-se intensamente, nos últimos tempos, o fenômeno da *datificação*: ato de datificar (pôr em dados) a vida e as relações de uma pessoa. As informações são formatadas de maneira que possam ser registradas, monitoradas e analisadas, permitindo a extração de mais informações e a análise preditiva dos sujeitos, o que facilita, sobremaneira, inferências de caráter sensível sobre eles.

Também externando preocupação similar, Rodotà[3], em defesa da dignidade humana e redimensionamento de princípios fundamentais consolidados, criou a teoria do corpo eletrônico para proteger o ser humano da exploração abusiva de seus dados pessoais:

> A dignidade é explicitamente referida no início do Código de proteção de dados pessoais (Decreto Legislativo 196/2003, art. 2º)[4]. O "corpo eletrônico", o conjunto de informações que constroem a nossa identidade, é assim remetido ao corpo físico: a dignidade torna-se o liame forte para reconstruir a integridade da pessoa (Carta dos Direitos Fundamentais da União Europeia, art. 3º), para evitar que a pessoa seja considerada uma espécie de "mina a céu aberto" onde qualquer pessoa possa alcançar qualquer informação e, assim, criar perfis individuais, familiares e grupais, tornando a pessoa objeto de poderes externos, que podem falsificá-la, construí-la em formas consistentes com as necessidades de uma sociedade de vigilância, de seleção social, de cálculo econômico. A Carta dos Direitos Fundamentais da União Europeia reafirmou a proibição de fazer do corpo um objeto lucrativo. Previsto para o corpo físico, esse princípio pode ser estendido ao corpo eletrônico, como já fazem algumas normas, como as que preveem a autorização pública para tratar os chamados dados sensíveis, que dizem respeito aos aspectos mais íntimos da vida ou à posição social da pessoa. Aqui, o princípio da dignidade é combinado com o da igualdade, para evitar discriminações ou estigmatizações sociais.

---

[2] TEFFÉ, Chiara Spadaccini de. **Dados pessoais sensíveis**: qualificação, tratamento e boas práticas. Indaiatuba: Editora Foco, 2022, p. 68.

[3] RODOTÀ, Stefano. A antropologia do homo dignus. Tradução de Maria Celina Bodin de Moraes. **Civilistica.com**, Rio de Janeiro, v. 6, n. 2, 2017. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/08/STEFANO-RODOTA-A-antropologia-do-homo-dignus.pdf. Acesso em: 27 mar. 2026. p. 15.

[4] BRASIL. Decreto Legislativo nº 196, de 2003. Aprova o texto da Convenção sobre o Cibercrime, celebrada em Budapeste, em 23 de novembro de 2001. **Diário Oficial da União**, Brasília, DF, 2003.

Nesse sentido, o aprimoramento das tecnologias de processamento digital de imagens faciais e a sua proliferação, viabilizada pelo crescente aumento da capacidade computacional e de armazenamento de dados, aliados ao barateamento e à disponibilidade, em escala global, de dispositivos de captura cada vez mais precisos e sensíveis, têm despertado grandes interesses, não apenas comerciais, mas também no campo do direito. Assim, discute-se a distinção entre sistemas de reconhecimento facial e de análise facial, bem como a eventual relevância jurídica dessa diferença.

Posto desse modo, o objetivo deste trabalho é avaliar em que medida essa distinção é relevante para o direito e em que extensão eventualmente afeta a aplicação da norma protetiva de dados pessoais. Ainda que se possa admitir que os sistemas de análise facial e de reconhecimento de emoções faciais não operam no campo da identificação ou da autenticação de indivíduos, pois tratam com dados impessoais ou anônimos, também se tem como objetivo explorar outras implicações jurídicas decorrentes desse tratamento, como eventuais condutas discriminatórias advindas de decisões automatizadas produzidas por esses sistemas, bem como o eventual alcance a outros campos do direito, como os neurodireitos.

2. DIREITO DE IMAGEM

A imagem facial humana é o principal objeto de tratamento dos sistemas de reconhecimento facial e de análise facial. Como será visto mais adiante, a distinção mais relevante entre esses sistemas consiste mais no propósito do tratamento ou no resultado do processamento dos dados faciais do que nas técnicas computacionais empregadas: ambos os sistemas partem da captura e da detecção da imagem facial para fins de identificação, autenticação ou avaliação do indivíduo. Assim sendo, importa inicialmente contextualizar a relevância jurídica da imagem facial humana, uma vez que se pretende confrontar a análise facial com a proteção de dados pessoais.

Basicamente, há dois aspectos aos quais a imagem humana pode ser associada: (i) à imagem como fotografia, ou ao registro das características físicas do indivíduo que o distinguem das demais pessoas; e (ii) à imagem como projeção social do indivíduo que o representa na sociedade. Assim, Diniz[5] diferencia imagem-retrato e imagem-atributo da seguinte forma:

> A imagem-retrato é a representação física da pessoa, como um todo ou em partes separadas do corpo (nariz, olhos, sorriso etc.) desde que identificáveis, implicando o reconhecimento de seu titular, por meio de fotografia, escultura, desenho, pintura, interpretação dramática, cinematografia, televisão, sites etc., que requer autorização do retratado (CF, art. 5º, X).

[5] DINIZ, Maria H. **Curso de Direito Civil Brasileiro**: teoria geral do direito civil. São Paulo, SP: Saraiva, 2023, p. 53.

> A imagem-atributo é o conjunto de caracteres ou qualidades cultivados pela pessoa, reconhecidos socialmente (CF, art. 5º, V), como habilidade, competência, lealdade, pontualidade etc. A imagem abrange também a reprodução, romanceada em livro, filme, ou novela, da vida de pessoa de notoriedade.

Assim sendo, o direito de imagem, insculpido no artigo 20 do Código Civil Brasileiro (CC)[6], abarca adequadamente esses dois aspectos, impedindo a exposição ou a utilização comercial indevida da imagem-retrato do indivíduo, bem como a alteração não autorizada de sua imagem-atributo, que atinja sua reputação perante a sociedade:

> Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.

Vale observar que, apesar de os direitos à intimidade, à vida privada e à honra estarem usualmente relacionados ao direito à imagem, tratam-se de direitos autônomos, em que um não depende necessariamente do outro para o seu exercício e tutela. Assim, por exemplo, ainda que a divulgação indevida da imagem de alguém não viole sua intimidade, vida privada ou honra, subsiste o dever de reparação pela ausência de autorização, conforme entendimento sumulado do Superior Tribunal de Justiça (STJ): "Independe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais"[7].

Embora a autonomia desses institutos pareça inquestionável, até mesmo pelo texto constitucional do artigo 5º, X, colacionado a seguir, que os trata de modo destacado e independente, indaga-se acerca do objeto da autorização: a exposição ou a utilização da imagem, ou a mera captação desta.

> Art. 5º [...]
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;[8]

---

[6] BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 27 mar. 2026.

[7] BRASIL. Superior Tribunal de Justiça. **Súmula nº 403**. DJe 24 nov. 2009. Disponível em: https://www.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2014_38_capSumula403.pdf. Acesso em: 27 mar. 2026.

[8] BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 27 mar. 2026.

Nesse sentido, a inteligência do artigo 20, do CC, parece fundar-se na percepção utilitarista da imagem pessoal: a mera captação, sem o efetivo emprego ou a divulgação da imagem, não teria utilidade prática e, portanto, não haveria ofensa ao direito de imagem, uma vez que não há exposição da imagem-retrato e, tampouco, alteração da imagem-atributo, dispensando, assim, a autorização do indivíduo. Por outro lado, justamente por conta dessa aparente indissociabilidade de captação e de divulgação, Affonso[9] entende que:

> A ratio da codificação vigente é de que a mera captação já dependeria do consentimento do seu titular, porque haveria "uma *presumptio hominis* de que a fixação fotográfica da imagem destina-se à posterior reprodução. Por isso, deve ser deferido ao titular o direito de autorizar, e negar, a captação de sua imagem. A divulgação ou reprodução constitui extensão de uma lesão já ocorrida". Assim, no atual estado da arte da doutrina, entende-se que o direito à imagem precede à sua divulgação, sendo protegida já a mera captação da imagem.

Entretanto, sistemas de análise facial ou de reconhecimento de emoções faciais procuram associar atributos faciais mensuráveis de imagens humanas capturadas a categorias como gênero, faixa etária e humor, em tese, sem qualquer propósito de divulgação ou exposição das imagens, até porque somente os dados dos atributos faciais são armazenados e processados. Dessa forma, parece que a lógica do artigo 20, c.c, poderia ser rompida nesse caso, tornando facultativo o prévio consentimento para a captura da imagem facial, desde que não ocorra a exposição ou a difusão desta. Esse aspecto utilitarista, que consistente na divulgação da imagem capturada, parece ser relevante para o exercício do direito de imagem, ainda que essa exposição se concretize por qualquer meio, seria imprescindível a sua ocorrência para caracterização de violação:

> O direito à imagem consiste na prerrogativa que o sujeito tem de autorizar ou não a exposição, reprodução ou divulgação de sua imagem, que não se limita aos aspectos físicos, mas abrange a concretização da representação física, moral e psíquica do titular, a exteriorização da personalidade. Além de não se restringir à representação fotográfica, o direito à imagem engloba toda e qualquer representação plástica, gráfica ou fotográfica de uma pessoa ou de um objeto, ou, ainda, por qualquer outro meio de caracterização de seus atributos. Explica Adriano de Cupis que a imagem dos indivíduos é resguardada independente da forma ou meio como é representada, sendo indiferente a forma como é representada, sendo "certo é que o direito à

[9] AFFONSO, Filipe José Medon. O direito à imagem na era das deep fakes. **Revista Brasileira de Direito Civil**, Rio de Janeiro, v. 27, n. 1, p. 251-277, 2021. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/438. Acesso em: 27 mar. 2026.

> imagem assegura ao indivíduo a defesa contra este, como contra os outros modos de difusão de sua imagem"[10].

Nessa ordem de pensamento, outra indagação aparentemente relevante se refere à necessidade de determinação do titular da imagem facial para que o direito de imagem possa ser exercido. Se o indivíduo for indeterminado, assim considerado uma pessoa desconhecida, e, simultaneamente, indeterminável, assim considerado aquela cujos dados disponíveis a seu respeito sejam insuficientes para reconhecê-la, parece não fazer sentido falar em direito de imagem, uma vez que não se identifica o seu titular e, portanto, torna-se impraticável a tutela de seus direitos.

Novamente, os sistemas de análise facial ou de reconhecimento de emoções faciais atuam no processamento de dados representativos de atributos faciais, como a forma e o posicionamento de sobrancelhas, olhos, narinas, lábios, formato do rosto e orelhas para estimar gênero, faixa etária e humor da imagem facial. Assim, além de a identificação do indivíduo não ser o propósito desses sistemas, os atributos faciais coletados, em regra, não são suficientes para identificá-lo. Conforme ressalva Loureiro[11], a relevância jurídica da imagem humana passa pela possibilidade de identificação do indivíduo:

> Mas foi Walter Moraes quem nos apresentou uma definição verdadeiramente ampla de imagem, que vai além do caráter visual: "Toda expressão formal e sensível da personalidade de um homem é imagem para o Direito". A imagem constitui um sinal sensível da personalidade: revela para o mundo exterior o ser imaterial da personalidade interior, delineia-a, dá-lhe forma. A ideia de imagem, para o direito, pressupõe figura humana. Não se refere somente à sua reprodução visual, mas também à imagem sonora da fonografia e da radiodifusão, às partes de corpo (boca, nariz, olhos etc., **desde que suficientes à identificação do indivíduo**), aos gestos e expressões dinâmicas da personalidade.

Por fim, ainda se indaga a respeito da autorização implícita do indivíduo que frequenta determinados ambientes para a captura de sua imagem e o consequente processamento de atributos faciais com a finalidade de classificação de gênero, faixa etária e humor, de forma a melhorar a assertividade no provimento de serviços individuais e coletivos. Se o indivíduo for adequadamente informado sobre as circunstâncias e as condições de captura e processamento de dados faciais, e

[10] SIQUEIRA, Dirceu Pereira; VIEIRA, Ana Elisa Silva Fernandes. Os limites à reconstrução digital da imagem na sociedade tecnológica. **Revista Eletrônica do Curso de Direito da UFSM**, Santa Maria, v. 17, n. 3, e67299, 2022, p. 4. Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/67299. Acesso em: 27 mar. 2026.

[11] LOUREIRO, Henrique Vergueiro. **Direito à imagem**. 2005. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2005, p. 58. Disponível em: https://repositorio.pucsp.br/jspui/handle/handle/5983. Acesso em: 27 mar. 2026. grifo nosso.

demonstrar aceitá-las por permanecer e frequentar o ambiente monitorado, poderia se concluir pela autorização tácita, uma vez que o indivíduo não evidenciaria expectativa diversa. Nesse ponto, Affonso observa que, em determinadas situações, não se trata de consentimento tácito, mas de limitação ao direito de imagem em benefício do interesse público:

> Fala-se, ainda, numa noção de consentimento tácito, que, no caso das fotografias, pode ser "tão usual quanto a celebração de termos por escrito, uma vez que a simples pose para foto já pode consistir em concordância para a sua captura". Antonio Chaves, por exemplo, apontava como hipótese de consentimento presumido o caso de uma pessoa que comparece em público em companhia de uma pessoa famosa, passando, então, a sofrer uma limitação do seu direito à imagem decorrente de sua notoriedade. No mesmo sentido, Adriano de Cupis, para quem, àquele que "participa em um acontecimento ou em uma cerimónia de interesse público ou ocorrida em público, pode mesmo atribuir-se o consentimento tácito da reprodução da sua imagem, em várias cópias enquadradas nos ditos acontecimentos ou cerimónias. Objeta-se, contudo, que nessas situações não haveria consentimento tácito propriamente dito, mas, sim, uma série de limites impostos ao direito à imagem da pessoa pelo interesse público, o que tornaria desnecessária a autorização do titular. Tais limites se diferenciariam da autorização tácita, pois se se estivesse "tratando de autorização, ainda que implícita, haveria o poder de oposição do titular à publicação"[12].

Assim, de forma similar, se a análise facial ou o reconhecimento de emoções faciais, cujo propósito não é a identificação de indivíduos, mas a sua classificação em gênero, faixa etária e humor, for benéfica à coletividade, por exemplo mediante melhorias no provimento de serviços, parece razoável que o direito individualizado de imagem possa ser proporcionalmente atenuado ou limitado, de forma que o direito de um não prejudique em demasia o direito de muitos.

3. BIOMETRIA FACIAL

A imagem facial humana dispõe de inúmeros atributos biométricos que podem ser capturados e processados para diversas finalidades, como a identificação ou a autenticação do indivíduo por meio de sistemas de reconhecimento facial, bem como a avaliação ou a categorização do indivíduo utilizando-se sistemas de análise facial ou de reconhecimento de emoções faciais. No primeiro exemplo, dados biométricos do indivíduo são coletados e tratados com o objetivo de confirmar a sua identidade; portanto, trata-se de um conjunto de dados biométricos personalizados, individualizados e únicos, capaz de distinguir inequivocamente um indivíduo de

[12] AFFONSO, *op. cit.*, p. 255-256.

outro. Por outro lado, no segundo, o tratamento de dados biométricos do indivíduo se presta para classificá-lo em categorias como gênero, faixa etária e humor, mas não para identificá-lo.

Em que pese a diferenciação de propósitos, os sistemas de identificação ou autenticação facial e de análise ou reconhecimento de emoções faciais utilizam dados biométricos de indivíduos para atingir seus objetivos. Assim sendo, importa compreender a relevância jurídica dessa distinção, especialmente porque a Lei Geral de Proteção de Dados (LGPD) considera os dados biométricos como dados pessoais sensíveis, cujos requisitos ou bases legais autorizativas de tratamento são mais rígidos em relação àqueles dispensados para o tratamento de dados pessoais comuns ou não sensíveis:

> Art. 5º Para os fins desta Lei, considera-se:
>
> […]
>
> II - dado pessoal **sensível**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou **biométrico**, quando vinculado a uma pessoa natural[13];

Contudo, embora a LGPD aponte o dado biométrico como exemplo de dado pessoal sensível, a Lei não o define ou conceitua, deixando, aparentemente como técnica legislativa, a cargo da legislação, da doutrina e da jurisprudência essa tarefa, amoldando-se à casuística das demandas sociais. Nesse contexto, a Autoridade Nacional de Proteção de Dados (ANPD) tem canalizado esforços para debater, fiscalizar e regulamentar o tratamento de dados biométricos, como o estudo "Biometria de reconhecimento facial", no Radar Tecnológico de 2024[14]; a inclusão do tratamento de dados biométricos na Agenda Regulatória da autarquia para o biênio 2025-2026[15]; a fiscalização do uso de sistemas de reconhecimento facial na venda

[13] 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/L13709compilado.htm. Acesso em: 27 mar. 2026. Grifo nosso.

[14] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Radar Tecnológico nº 2 – Biometria e Reconhecimento Facial**. Brasília, DF: ANPD, 2024b. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/. Acesso em: 27 mar. 2026.

[15] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Agenda Regulatória para o Biênio 2025-2026**. Brasília, DF: ANPD, 2024a. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/processo_regulatorio/agenda-regulatoria-1. Acesso em: 27 mar. 2026.

de ingressos e na entrada de estádios de futebol[16]; e a tomada de subsídios sobre tratamento de dados biométricos[17].

Tratam-se de iniciativas recentes nessa seara, em que a produção legislativa e jurisprudencial parece ainda incipiente. Entretanto, o conceito de dado biométrico deve considerar aspectos humanos para além da fisiologia. Nesse sentido, embora menos recente, o Decreto Federal nº 10.046/2019[18], que dispõe sobre a governança no compartilhamento de dados, assim regulamenta:

> Art. 2º Para fins deste Decreto, considera-se:
>
> […]
>
> II - atributos biométricos - características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar.

A partir dessa definição, percebe-se que os atributos ou dados biométricos não se restringem a características biológicas, mas abrangem também características comportamentais do indivíduo, desde que passíveis de mensuração. Dessa forma, no caso de dados faciais, o posicionamento e o formato dos olhos, do nariz, da boca, das orelhas e do rosto, bem como a forma de expressar emoções por meio da movimentação ou da articulação daqueles elementos faciais, são considerados dados biométricos por se tratarem de características mensuráveis da face de uma pessoa natural. Apesar desse esclarecimento, a norma não especifica o propósito da coleta de atributos biométricos, referindo-se apenas ao reconhecimento automatizado, o qual parece condizente com o objetivo primordial de identificação do indivíduo. Com efeito, segundo entendimento de Teffé[19], tanto os atributos fisiológicos quanto os comportamentais mensurados teriam como objetivo o estabelecimento da identidade de alguém:

> A biometria é a ciência de se estabelecer a identidade de alguém, a partir da medição e análise de seus atributos fisiológicos ou comportamentais

[16] AUTORIDADE 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, DF: ANPD, 2025b. 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: 27 mar 2026.

[17] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **ANPD abre Tomada de Subsídios sobre Tratamento de Dados Biométricos**. Brasília, DF: ANPD, 2025a. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-tomada-de-subsidios-sobre-tratamento-de-dados-biometricos. Acesso em: 27 mar. 2026.

[18] BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 27 mar. 2026.

[19] TEFFÉ, *op. cit.*, p. 149.

> mensuráveis. No primeiro caso, são exemplos a impressão digital, o reconhecimento da íris, a identificação por retina, a definição dos traços do rosto, a arcada dentária, a geometria da mão e a altura da pessoa. As medidas fisiológicas geralmente oferecem o benefício de permanecer mais estáveis ao longo da vida de um indivíduo. No segundo caso, é possível mencionar: a forma como a pessoa digita, como anda, gestos característicos, dinâmica da assinatura (velocidade do movimento da caneta, acelerações, pressão exercida e inclinação), a altura que o indivíduo costuma segurar o celular, a forma com que ele movimenta o mouse do computador, a pressão que ele exerce no teclado ou na tela e, até mesmo, como corrige as palavras. Com o aprendizado de máquina e a inteligência artificial, é possível entender e analisar como uma pessoa se comporta no computador ou no celular, por exemplo.

Nessa linha de raciocínio, considerando que o propósito dos sistemas de análise facial ou de reconhecimento de emoções faciais é a classificação de indivíduos em categorias como gênero, faixa etária e humor, mas não a sua identificação, as informações coletadas das faces não seriam consideradas dados biométricos, pelo menos na acepção empregada no âmbito da legislação de proteção de dados pessoais. Esse entendimento reforça a ideia de que o significado do termo "biometria" ou "dado biométrico", a partir apenas de sua etimologia, não seria um caminho seguro e suficiente para compreender o sentido e o alcance da norma jurídica.

Nesse contexto, poderia se dividir ou classificar os dados biométricos de acordo com uma escala de força ou capacidade de identificar o indivíduo, na qual identificadores fortes possibilitariam a identificação unívoca de uma pessoa natural. Por outro lado, indicadores mais fracos não teriam essa habilidade, por não tratar pessoas de forma individualizada ou única, mas sim agrupadas em categorias que apresentam características biométricas comuns como gênero, faixa etária e humor, conforme apontam Wendehorst e Duller[20] em um estudo realizado acerca do reconhecimento biométrico e da detecção comportamental:

> Biometrics may be divided in various ways, one of them being 'strong', 'weak', and 'soft' identifiers. Strong identifiers allow or confirm the unique identification of a natural person, e.g. fingerprints, iris, and retina. Weak biometrics are features that are 'less unique' or 'less stable', e.g. body shape, behavioural patterns, voice, and body sounds. Soft biometrics comprise features that are generic in nature and not uniquely associated with a person, e.g. gender or age.

[20] WENDEHORST, Christiane; DULLER, Yannic. **Biometric Recognition and behavioural detection**. Policy Department for Citizens' Rights and Constitutional Affairs, PE 696.968 , Aug. 2021, p. 13. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf. Acesso em: 27 mar. 2026.

Considerando essa classificação de dados biométricos, os sistemas de análise facial ou de reconhecimento de emoções faciais podem ser entendidos como técnicas de categorização, uma vez que os identificadores biométricos empregados por eles são adequados apenas para designar pessoas em categorias específicas, e não para identificá-las individualmente. Entretanto, vale ressaltar que, se uma pessoa for designada em diferentes categorias de forma cumulativa e, dependendo das circunstâncias, como o número e a granularidade de categorias, a identidade do indivíduo poderá ser obtida ou confirmada:

> Biometric techniques can, in the light of their primary function, be divided into techniques of biometric authentication or identification, categorisation, and detection. […] Biometric categorisation is a term that is less common than biometric identification, also because the rise of biometric categorisation techniques has only come with the increasing use of 'soft' or 'weak' biometrics. Data that are as such not (or not necessarily) suited for the unique identification of a natural person may nevertheless be suited for assigning natural persons to specific categories, such as sex, age, ethnic origin or health. Needless to say, where a particular natural person is assigned to several different categories, the cumulative assignment may, depending on circumstances such as number and granularity of categories, allow or confirm the identification of that natural person[21].

Ainda que pareça inicialmente contraintuitivo, o processamento de dados biométricos faciais e a sua finalidade, seja a identificação ou a categorização, são aspectos relevantes ao enquadramento desses dados como pessoais ou sensíveis, ao menos para fins de aplicação da norma jurídica. Ao observar a imagem facial de um indivíduo, qualquer pessoa de juízo mediano seria capaz de identificá-lo, se for conhecido, e de determinar, com razoável acurácia, seu gênero, faixa etária e humor: a imagem facial carrega todas essas informações biométricas e, portanto, a sua simples captura já parece constituí-la em dado pessoal comum e sensível. Contudo, deve-se considerar que o cérebro humano, instantaneamente, observa, captura, processa e reage diante da imagem facial de forma indissociável, o que se mostra inviável para sistemas computacionais. Nesse sentido, ensina Teffé[22] que:

> De acordo com o Information Commissioner's Office (ICO), se você processar fotografias digitais de pessoas, esses dados não serão automaticamente biométricos, mesmo que sejam usados para fins de identificação. Embora uma imagem digital possa permitir a identificação por meio de características físicas, ela só se tornará um dado biométrico se você realizar um "processamento técnico específico". Normalmente, isso envolve

[21] *Ibid*., p. 20-21.

[22] TEFFÉ, *op. cit.*, p. 150.

> o uso dos dados da imagem para criar um modelo digital individual ou perfil, que, por sua vez, você usará para correspondência automática de imagens e identificação.

Na mesma direção, o Considerando 51 do Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation – GDPR) também observa que o processamento, por meios técnicos específicos que permitam a identificação ou autenticação do indivíduo, é requisito para o enquadramento do tratamento de categorias especiais de dados pessoais[23]:

> Considerando 51 do GDPR. […] O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular.

A propósito, se os dados faciais capturados para fins de análise facial ou de reconhecimento de emoções faciais forem ineficazes para a identificação do indivíduo, sequer seriam considerados dados pessoais, na medida em que, embora se refiram à pessoa natural, não se trata de um indivíduo determinado ou determinável. Assim, a possibilidade de identificação pessoal é o requisito essencial e, em regra, imprescindível, não somente para a determinação de dados biométricos, mas também para a assunção do dado como pessoal.

Com efeito, o Article 29 Data Protection Working Party da Comissão Europeia[24] emitiu o Opinativo nº 02/2012 a respeito do reconhecimento facial e do dado pessoal, para esclarecer que um conjunto de atributos distintivos usado somente em um sistema de categorização não conteria, em regra, informação suficiente para identificar um indivíduo, mas apenas para realizar a categorização, por exemplo, masculino ou feminino, e, nesse caso, não seria considerado dado pessoal:

> 4.1. Digital images as personal data. When a digital image contains an individual's face which is clearly visible and allows for that individual to be identified it would be considered personal data. A template or set of distinctive features used only in a categorisation system would not, in general, contain sufficient information to identify an individual. It should only

[23] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679. Acesso em: 27 mar. 2026.

[24] EUROPEAN COMMISSION. ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 2/2012 on the concept of personal data**. Bruxelas, 2012. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm. Acesso em: 27 mar. 2026.

> contain sufficient information to perform the categorisation (e.g. male or female). In this case it would not be personal data provided the template (or the result) is not associated with an individual's record, profile or the original image (which will still be considered personal data).

Apesar disso, assim como o propósito da aplicação distingue os sistemas de identificação ou autenticação facial dos sistemas de análise ou reconhecimento de emoções faciais, a repercussão pessoal do tratamento de dados relativos à pessoa natural, ainda que indeterminada ou indeterminável, pode ser um critério distintivo entre dado pessoal e dado não pessoal ou anônimo. Em outros termos, o dado poderá ser considerado pessoal, mesmo que não se relacione com uma pessoa natural identificada ou identificável, desde que o seu tratamento possa interferir no âmbito pessoal de alguém, embora desconhecido, como se verá mais adiante.

Por fim, no âmbito do enquadramento dos dados faciais biométricos, vale indagar acerca da relação entre o dado pessoal e o dado pessoal sensível. A partir da primeira interpretação dos incisos I e II do artigo 5º da LGPD, parece tratar-se de relação de qualificação, em que o dado pessoal sensível é espécie do gênero dado pessoal[25]:

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - **dado pessoal**: informação relacionada a pessoa natural identificada ou identificável;
>
> II - **dado pessoal sensível: dado pessoal** sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Em defesa por uma tutela ampliada das informações pessoais, Teffé[26] também parece entender que os dados pessoais sensíveis são espécies de dados pessoais:

> A LGPD em seu Art. 5º, inciso II, trouxe **espécies** de dados pessoais considerados sensíveis: "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". Todavia, não esclareceu o que seriam dados sensíveis em termos conceituais, não definiu suas **espécies** nem se posicionou quanto à qualidade de seu rol: se taxativo ou exemplificativo.

[25] BRASIL, **Lei nº 13.709, de 14 de agosto de 2018**, *op. cit.*, grifo nosso.

[26] TEFFÉ, *op. cit.*, p. 22, grifo nosso.

Inicialmente, essa colocação parece fazer sentido, porque há de se reconhecer a existência de uma classe especial de dados pessoais, cujo tratamento potencializa condutas ilícitas ou discriminatórias. Entretanto, Teffé[27] observa que a distinção entre dado pessoal geral e dado sensível "torna-se cada vez mais fluída, pois aparentemente qualquer dado pode se tornar sensível, se for encontrada uma maneira de, a partir dele, serem inferidas informações sobre atributos assim protegidos". Dessa forma, pode-se concluir que não é necessariamente a natureza do dado pessoal, comum ou sensível, que conduz ao comportamento ou à decisão automatizada ilícita ou discriminatória, mas o tratamento desse dado pessoal. A esse respeito, Teffé[28] alerta sobre o tratamento sensível de dados pessoais comuns:

> Entende-se que, além de se realizar uma proteção mais ampla dos dados sensíveis, tal proteção também deverá ser observada nos casos em que houver tratamento sensível de dados pessoais. Isso porque, com base estritamente em considerações a respeito da natureza dos dados tratados, nem sempre será possível predizer os efeitos que o tratamento poderá causar em seu titular ou em interesses coletivos lato sensu. Inferências e conclusões geradoras de informações sensíveis bem como tratamentos sensíveis de informações que apresentem claro viés discriminatório ilícito ou abusivo deverão, por consequência, receber proteções ampliadas. Recomenda-se, então, que sejam verificadas, entre outras questões apontadas neste livro, as intenções do controlador e se, a partir do tratamento realizado, era previsível que os dados poderiam revelar informações sensíveis.

Essa lógica também poderia ser aplicada ao tratamento de dados não pessoais ou anônimos. Considerando que os dados biométricos faciais capturados por sistemas de análise facial ou de reconhecimento de emoções faciais são insuficientes para a identificação dos titulares, tratam-se, então, de dados não pessoais ou anônimos. Contudo, ainda assim, o tratamento pode ser potencialmente sensível, na medida em que decisões automatizadas decorrentes desse tratamento podem se revelar ilícitas por viés ou discriminação algorítmica.

4. ANÁLISE FACIAL

A análise facial, no contexto do processamento automatizado de características da face humana, pode ser conceituada como a categorização de atributos faciais mensuráveis em classes previamente determinadas, as quais expressam condições ou circunstâncias humanas, como faixa etária, gênero e humor. Embora o fluxo de

[27] *Ibid.*, p. 67.

[28] I*bid.*, p. 62-63.

processamento de dados da análise facial seja razoavelmente similar ao do reconhecimento facial, as duas tecnologias não devem ser consideradas idênticas ou intercambiáveis, seja porque têm propósitos distintos, seja porque têm repercussões jurídicas próprias, a depender das aplicações em casos concretos.

De acordo com estudos de Li e Jain[29], geralmente, "um sistema de reconhecimento facial consiste em quatro módulos: detecção, alinhamento, extração de atributos e comparação"[30]. A detecção facial segmenta áreas da face, distinguindo-as da imagem de fundo. O alinhamento facial tem como objetivo a localização mais precisa e a estimativa da escala da face detectada. Os componentes faciais, como olhos, nariz, boca e contorno facial, são localizados com base nesses pontos de localização; em seguida, a imagem da face é então normalizada em relação às propriedades geométricas, como tamanho e posição, e às propriedades fotométricas, como iluminação e escala de cinza. Depois que a face é normalizada, a extração de atributos é executada para se obter informações efetivamente úteis, a fim de distinguir faces de diferentes pessoas. No módulo de comparação, o conjunto de atributos extraídos da face é comparado com os registrados no banco de dados, assim, a identidade da face é indicada pelo sistema quando a comparação atinge um nível razoável de confiança, ou, caso contrário, indica uma face desconhecida.

Usualmente, as aplicações mais difundidas e conhecidas dos sistemas de reconhecimento facial são a verificação ou autenticação facial e a identificação facial. Segundo Zuk[31], a verificação facial é o processo de determinação de que alguém é quem declara ser. Tal processo é chamado de comparação um-para-um (1:1). Por exemplo, quando um usuário tenta desbloquear seu telefone celular com o seu rosto, o algoritmo compara a face do usuário com a imagem armazenada do proprietário; se a pontuação de similaridade for elevada o suficiente, a identidade do usuário é confirmada e o é celular desbloqueado. Outras aplicações incluem o embarque em voos e a autorização de pagamentos. De fato, não são as imagens das faces efetivamente comparadas, mas os seus atributos.

Por outro lado, a identificação facial compara uma face desconhecida com um banco de dados de imagens. Esse tipo de comparação é chamado de um-para-muitos (1:N). Por exemplo, algoritmos de identificação facial podem checar a face capturada por uma câmera de vigilância com uma base de dados contendo faces de criminosos procurados. Assim, a identificação facial compreende um desafio computacional mais elaborado, pois o algoritmo deve "vasculhar" toda a base de dados em busca da identidade da face a ser reconhecida, com grau de confiança

[29] LI, Sant Z.; JAIN, Anil K. **Handbook of face recognition**. New York: Springer, 2005. p. 2-3.

[30] Tradução livre do original: "A face recognition system generally consists of four modules […]: detection, alignment, feature extraction, and matching […]".

[31] ZUK, Ofir. The State of Facial Recognition Today. **Datagen.tech**, 2024. Disponível em: https://datagen.tech/blog/the-state-of-facial-recognition-today/. Acesso em: 12 fev. 2024.

aceitável. Mesmo admitindo essa diferença computacional, a verificação ou autenticação facial e a identificação facial atuam com um propósito comum: identificar o titular dos atributos faciais capturados.

Nesse sentido, a análise facial se diferencia do reconhecimento facial de modo estrito, uma vez que não há interesse na identificação do titular dos atributos faciais, mas no significado de suas expressões faciais, conforme explica Bastos e Esteves[32]:

> Em sentido estrito, as tecnologias de reconhecimento facial tratam o rosto apenas como um index de identidade, desconsiderando sua expressiva capacidade de comunicação e interação social. Estabelecem seu marco de identidade para então ligar o rosto coletado (input) com a sua identidade no mundo real (output). Procuram responder a seguinte problemática: "A qual pessoa pertence esse rosto coletado"? É o que se denomina de reconhecimento facial em sentido estrito, ou seja, o reconhecimento apenas da identidade. Por outro lado, a análise automatizada de expressão facial tenta controlar os diversos significados que uma face individual pode transmitir para identificar sinais afetivos, expressões, emoções, humor, etc. Mesmo com objetivos finais diferentes, os primeiros passos da análise automatizada de expressão facial são os mesmos do reconhecimento facial em sentido estrito: detectar uma face e a extração de características.

Enquanto o reconhecimento facial utiliza dados únicos e específicos de uma pessoa para responder a questões como "quem é você?", no caso de identificação facial, ou "você realmente é quem diz ser?", no caso de verificação ou autenticação facial, a análise facial ou o reconhecimento de emoção facial (*facial emotion recognition* – FER) é o processo de mapeamento de expressões faciais com o objetivo de identificar emoções, como aversão, alegria, raiva, surpresa, medo e tristeza, em uma face humana, por meio de *software* de processamento de imagem. Assim, a interpretação das emoções humanas se diferencia do reconhecimento facial, o qual visa identificar uma pessoa, e não uma emoção[33].

Apesar da incapacidade de identificar pessoas, os sistemas de análise facial visam agrupar indivíduos em classes previamente determinadas, de acordo com atributos faciais mensuráveis que expressam condições ou circunstâncias humanas, como faixa etária, gênero e humor. Esse agrupamento de indivíduos, segundo critérios que os unem, como mesma faixa etária, mesmo gênero ou mesmo humor, pode ser considerado a formação de perfil comportamental a que se refere o art. 12, § 2º,

[32] BASTOS, Elísio Augusto Velloso; ESTEVES, Vitória Barros. Tecnologias de reconhecimento facial: um estudo a partir do contexto de vigilância digital e sutil. **Revista Direitos Democráticos & Estado Moderno**, São Paulo, n. 3, p. 216-240, jul./dez. 2021. Disponível em: https://revistas.pucsp.br/index.php/DDEM/article/view/53875/38321. Acesso em: 27 mar. 2026.

[33] THALES. **Facial recognition**: top 7 trends (tech, vendors, use cases). 2021. Disponível em: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition. Acesso em: 27 mar. 2026.

da LGPD. Assim sendo, se o perfil de determinada classe for a base para a tomada de alguma decisão que possa interferir no âmbito pessoal de alguém, então os atributos faciais coletados serão considerados dados pessoais, mesmo sem necessariamente identificar o titular desses dados.

Trata-se da análise consequencialista trazida por Bioni[34], segundo a qual, o conceito de dado pessoal deve ser compreendido não apenas a partir do atributo da identificabilidade, mas também do seu desdobramento na esfera pessoal:

> Muitas vezes, processos de decisões automatizados valem-se desses perfis que não necessariamente identificam uma pessoa em específico, mas um grupo – grouping. É pelo fato de ela estar catalogada, inserida, referenciada ou estratificada nesse grupo que uma série de decisões serão tomadas a seu respeito, ainda que sem individualizá-la diretamente a priori. Como já apontado no início deste subcapítulo, essa é uma metodologia bastante comum em muitos modelos de negócios que se valem de dados estatísticos de grupos para o direcionamento de conteúdo e publicidade, ainda que não seja possível identificar as pessoas que compõem aquela massa.

Desse modo, sempre que a análise facial implicar repercussão no âmbito pessoal de alguém, haverá a incidência protetiva da LGPD e, portanto, os atributos faciais assim tratados serão considerados dados pessoais, ainda que não se possa identificar o seu titular individualmente. Por outro lado, em sentido oposto, se nenhum interesse pessoal for afetado com as decisões tomadas a partir da análise facial, então os atributos faciais processados não serão dados pessoais e, consequentemente, estarão fora do alcance da LGPD.

5. IDENTIFICAÇÃO FACIAL

A identificação a partir da imagem facial do titular é um elemento relevante e indispensável no contexto do direito à proteção de dados pessoais. Segundo a LGPD[35], dado pessoal é "informação relacionada a pessoa natural identificada ou identificável"; assim, percebe-se que o ordenamento pátrio adota o conceito amplo de identificação do titular do dado pessoal, não se restringindo à pessoa natural identificada, mas alcançando também a pessoa natural passível de identificação por qualquer meio, bastando ser identificável. Nesse sentido, a imagem facial que se relaciona à pessoa natural identificada ou identificável é um dado pessoal, caso contrário, em tese, não.

[34] BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. São Paulo: Grupo GEN, 2021, p. 77.

[35] BRASIL, **Lei nº 13.709, de 14 de agosto de 2018**, *op. cit*.

Pelo menos para fins de incidência da LGPD, um dado não poderá ser considerado pessoal se não puder ser relacionado à pessoa natural ou, mesmo relacionado, se essa pessoa não for identificada nem puder ser identificada por qualquer meio. Assim sendo, um dado não pessoal ou um dado impessoal é a informação que não se refere a uma pessoa natural em particular ou se refere a uma pessoa natural anônima (não identificada nem identificável).

Parece fazer sentido que informações dessa natureza sejam expurgadas do campo de incidência da LGPD, na medida em que o objeto da proteção imposta pela norma jurídica não é o dado em si, mas os direitos de liberdade do seu titular. Afinal, segundo Teffé[36]:

> O oferecimento aos cidadãos de instrumentos que lhes garantam assumir efetivamente controle acerca do uso e da integridade de suas informações representa garantia de tutela da própria dignidade da pessoa humana, tendo em vista o papel predominante da informação para as escolhas do indivíduo.

Assim, se não há um titular específico ou se o titular é anônimo, em tese, não haveria de se falar em ameaça ou lesão aos direitos ou liberdades fundamentais. Por exemplo, o número de inscrição no Cadastro de Pessoas Físicas (CPF) do Ministério da Fazenda pode ser considerado um dado pessoal, uma vez que o seu titular pode ter interesse em que o tratamento dessa informação esteja sob o seu controle e seja realizado de acordo com sua disposição ou autorização, em conformidade com as disposições legais, de forma a proteger seus direitos e liberdades. Por outro lado, se determinado número de CPF for inválido[37], ou mesmo válido e ainda não tiver sido atribuído a alguém[38], ou ainda se estiver associado a uma pessoa desconhecida, o tratamento isolado desse dado poderá não representar ameaça ou lesão a direitos, seja porque não há um titular (número inválido ou não atribuído) ou o titular é anônimo (pessoa desconhecida).

Pensamento similar pode ser aplicado à imagem facial humana. Se uma imagem facial não estiver relacionada a uma pessoa natural ou estiver relacionada a pessoa natural indeterminada e indeterminável, a princípio, essa imagem não deve ser

[36] TEFFÉ, *op. cit.*, p. 40.

[37] Para fins deste exemplo, considera-se válido o número de CPF que atenda aos critérios da fórmula em Javascript disponibilizados pela Secretaria da Receita Federal do Brasil (SRFB). Isso não significa que a situação cadastral de inscrição esteja regular junto à SRFB.

[38] O número de CPF é único para cada pessoa natural: não é possível que a mesma pessoa tenha mais de um número de CPF, assim como não é possível que o mesmo número de CPF esteja associado a mais de uma pessoa natural. Em razão dessa natureza unívoca, o número de CPF é amplamente utilizado como atributo-chave em banco de dados para distinguir registros de pessoas naturais distintas. Na fase de teste de desenvolvimento de softwares, é comum a utilização de geradores randômicos de números válidos de CPF pelos programadores, assim, é possível que números válidos, ainda não atribuídos a qualquer pessoa natural pela SRFB, estejam sendo gerados e processados.

considerada dado pessoal, em termos de aplicação da LGPD. Uma imagem facial surpreendentemente realista de uma pessoa que não existe pode ser criada por algoritmo de inteligência artificial: segundo o *website*, o "Unreal Person" é um gerador de imagem treinado por bilhões de faces humanas com o objetivo de produzir uma face completamente nova de alguém que não existe[39]; portanto, não se trata de dado pessoal, pois o titular não existe no mundo real. Pela outra via, se a imagem facial se relacionar a uma pessoa natural anônima, igualmente não se trata de dado pessoal, pois o titular é desconhecido.

Em contrapartida, considerando o raciocínio protetivo disciplinado pela LGPD, em que a tutela é direcionada aos direitos e liberdades da pessoa natural, e não aos seus dados em si, se excepcionalmente o tratamento da imagem facial anônima repercutir em sua esfera pessoal, haverá incidência da LGPD por via reflexa. Nesse caso, restará prejudicada ou esvaziada a discussão sobre se, nesse caso, a imagem facial anônima é um dado pessoal ou não, para fins de aplicação da LGPD, pois a afetação do interesse pessoal já é causa bastante para invocar a proteção normativa. Contudo, apesar desse esvaziamento, para se manter a coerência com o objeto de manejo da norma, nessa situação, ainda que anônima, a imagem facial será considerada um dado pessoal.

A esse respeito, um caso emblemático ocorreu em São Paulo (SP), envolvendo a então loja conceito chamada "Hering Experience", em que o Departamento de Proteção e Defesa do Consumidor (DPDC) instaurou um processo administrativo[40] em face da Cia Hering (representada), em razão de coleta e do processamento indevido de dados pessoais de clientes por meio de recursos tecnológicos de reconhecimento facial. Sustentava a representada que a tecnologia de detecção facial (*video analytics*) empregada não poderia ser confundida com reconhecimento facial e, portanto, não haveria possibilidade de identificação do consumidor, mas somente o diagnóstico estimado de gênero, faixa etária e humor, para gestão de mídia direcionada no interior do ambiente da loja, afastando, assim, qualquer violação legal, por não se tratar de dados pessoais.

Nesse caso, além das infrações consumeristas, o IDEC também apontou violações a preceitos da LGPD, sustentando que a diferenciação entre detecção e reconhecimento facial seria mera distinção de nomenclatura, havendo efetivamente tratamento não autorizado de dados pessoais. Apesar disso, a Secretaria Nacional do Consumidor (Senacon) considerou prejudicada essa questão, uma vez que, embora publicada, à época dos fatos, a LGPD ainda não estava em vigor, e concluiu pela violação aos preceitos do Código de Defesa do Consumidor (CDC) e aos

[39] UNREAL PERSON. **This person does not exist**. [*S. l.*]: Unreal Person, 2023. Disponível em: https://www.unrealperson.com/. Acesso em: 27 mar. 2026.

[40] SEI nº 08012.001387/2019-11 do Ministério da Justiça e Segurança Pública.

direitos de personalidade e imagem dos consumidores, aplicando uma multa de R$ 58.767,00 à representada.

Apesar de a controvérsia acerca da caracterização de dado pessoal ter sido relativizada para fins de decisão da Senacon nessa situação, à luz do presente estudo, talvez a argumentação da representada pudesse se enquadrar no âmbito da análise facial, e a captação e o processamento de dados faciais tratados como dados genuinamente anônimos desde a origem, e não anonimizados posteriormente. Contudo, como visto anteriormente, mesmo o anonimato não seria argumento suficiente para afastar a incidência da LGPD e, portanto, por outras vias, a violação aos direitos restaria comprovada, se a esfera pessoal dos consumidores fosse atingida.

Questão relevante que se coloca é a que trata do anonimato absoluto ou relativo do titular da informação. Se a imagem facial estiver associada a pessoa natural inicialmente indeterminada, mas determinável, ou seja, passível de identificação do titular por qualquer meio, então estar-se-á diante de um autêntico dado pessoal, o qual reclamaria a incidência da LGPD. Assim sendo, o anonimato relativo não seria suficiente para afastar a proteção disciplinada pela LGPD, mas somente o anonimato absoluto seria capaz de descaracterizar a imagem facial como dado pessoal, salvo se, excepcionalmente, o seu tratamento puder repercutir na esfera pessoal de seu titular. Entretanto, essa avaliação não pode ser conduzida apenas no campo teórico, pois, em tese, se a imagem facial se refere a uma pessoa natural que existe, ou existiu, no mundo real, então o seu titular poderá ser identificado de algum modo; portanto, se assim fosse, qualquer informação relacionada a uma pessoa natural seria considerada como um dado pessoal, pois qualquer pessoa é abstratamente passível de identificação, com maior ou menor grau de dificuldade.

Desse modo, a aferição da possibilidade ou não de identificação do titular, a partir do processamento de atributos extraídos da imagem facial, deve ser conduzida dentro do contexto em que se encontra o responsável pelo tratamento desses dados, considerando fatores como custo, tempo e tecnologia, razoavelmente disponíveis e ao seu alcance:

> A análise do potencial de identificação de certa informação pelo agente de tratamento ou por outro sujeito – conforme a orientação objetiva – não pode ser feita em abstrato apenas, como se bastasse uma possibilidade puramente hipotética. No direito europeu, desde a Diretiva 95/46/CE vigora o critério dos meios suscetíveis de ser razoavelmente utilizados, que busca ser balizado por fatores objetivos como custos e tempo de trabalho exigidos para a identificação, o estado da arte da tecnologia existente no período de duração do tratamento e os riscos de falhas técnicas, por exemplo. Trata-se de critério dependente de aspectos contextuais – v. g., estágio de desenvolvimento das tecnologias de rastreamento de comportamento online e

> de algoritmos de aprendizado de máquina – que, em última análise, faz da caracterização como dado pessoal um estado dinâmico.[41]

Essa possibilidade razoável de identificação ou não do titular deve ser aferida não apenas em relação ao agente de tratamento de dados faciais, mas também em relação a qualquer outro agente. Assim, não é imprescindível que os dados necessários para a identificação do titular estejam sob controle ou na posse do mesmo agente de tratamento, bastando que os dados efetivamente existam e possam ser processados por qualquer meio razoavelmente aceitável para que o titular seja considerado uma pessoa natural identificável, ainda que o responsável pelo tratamento de dados faciais não disponha isoladamente de todos os dados necessários à identificação.

Apesar de adotar expressamente o conceito amplo de identificação do titular do dado pessoal, ao não se restringir à pessoa natural identificada, mas também incluir a pessoa natural identificável, a LGPD, ao menos de forma expressa, não indica os critérios e as balizas que possibilitam considerar uma pessoa natural identificável. Não obstante, o princípio da razoabilidade é expressamente invocado pela Lei em inúmeras passagens, inclusive para dispor acerca de meios técnicos e esforços razoáveis, além de trazer fatores objetivos para a determinação do que seja razoável: tempo, custo e tecnologia, muito em linha com os preceitos do GDPR da União Europeia, a partir dos quais a legislação brasileira buscou inspiração. A propósito, o Considerando 26 do GDPR esclarece os critérios aplicáveis para identificação da pessoa natural, os quais podem ser adotados no país para interpretação normativa:

> […] Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. […][42]

Sendo assim, o agente de tratamento de dados que conduz o processamento de análise facial, e não de reconhecimento facial, apesar de não pretender coletar informações que visem à identificação do titular, não escapa do campo de incidência da LGPD, se a identificação, ainda que não pretendida, seja razoavelmente possível

[41] MACHADO, Diego. Considerações iniciais sobre o conceito de dado pessoal no ordenamento jurídico brasileiro. **Civilistica**, [*S. l.*], v. 12 n. 1, 2023, p. 11. Disponível em: https://www.researchgate.net/publication/371577468_Consideracoes_iniciais_sobre_o_conceito_de_dado_pessoal_no_ordenamento_juridico_brasileiro. Acesso em: 27 mar. 2026.

[42] UNIÃO EUROPEIA, *op. cit.*

por qualquer meio ou agente, nas circunstâncias concretas em que ocorre o tratamento de dados. Mesmo que a efetiva identificação se mostre inviável, no contexto do processamento de dados faciais e, portanto, em regra, não se trate de dados pessoais, nos termos da LGPD, não significa necessariamente que o tratamento desses dados seja absolutamente livre, uma vez que o regime protetivo da dignidade humana não se restringe a uma norma específica, mas conta com todo o ordenamento jurídico, interpretado sistemicamente.

6. DISCRIMINAÇÃO ALGORÍTMICA

A expressão facial humana é um poderoso veículo de comunicação não verbal e de relacionamento interpessoal. Essa capacidade reflete a própria complexidade dos agrupamentos sociais e, nesse sentido, discute-se a invariabilidade e a universalidade das expressões faciais da emoção através das culturas. Além disso, emergem novos desafios quando se analisam as pesquisas sobre a relação entre emoção e comportamento facial, que apontam principalmente para a consideração de dialetos emocionais específicos de cada cultura e para a influência dos aspectos sociais e comunicativos no comportamento facial, para além da emoção[43]. Dessa forma, a expressão ou comportamento facial é uma aproximação da emoção humana, que pode ser modulado por reações involuntárias ou intencionais, a depender de aspectos culturais e circunstanciais em que o indivíduo está inserido.

Algumas emoções humanas podem ser mais facilmente reconhecidas por expressões ou comportamentos faciais, como a alegria e a surpresa. Entretanto, outras podem ser mais complexas, como a surpresa feliz e a surpresa triste, justamente em razão da combinação de expressões faciais comuns. Estudos sobre as expressões faciais da emoção, conduzidos por Du, Tao e Martinez[44], demonstram que as emoções podem ser classificadas em dois grupos. O primeiro se refere à categoria de emoções básicas, que inclui alegria, surpresa, raiva, tristeza, medo e aversão. Apesar de se empregar o termo "básico", isso não significa que se tratem de emoções mais básicas do que outras, mas que se referem a categorias que não podem ser decompostas em termos semanticamente menores, além de serem prevalentes na literatura especializada. Por outro lado, o segundo grupo corresponde às emoções compostas, no sentido de que as categorias são construídas a partir da combinação de duas categorias de emoções básicas; nem todas as combinações fazem necessariamente sentido, mas,

[43] SOUSA, Cristina de. Emoção e expressão facial: novos desafios. **Psicologia**, Lisboa, v. 24, n. 2, p. 17-41, 2010. Disponível em: https://revista.appsicologia.org/index.php/rpsicologia/article/view/303/65. Acesso em: 27 mar. 2026.

[44] DU, Shichuan; TAO, Young; MARTINEZ, Aleix M. Compound facial expression of emotion. **Proceedings of the National Academy of Sciences**, Washington, v. 111, n. 15,p. E1454-E1462, 2014, p. 1454. Disponível em: https://www.pnas.org/doi/epdf/10.1073/pnas.1322355111. Acesso em: 27 mar. 2026.

além das seis básicas, outras 15 categorias foram identificadas como típicas e distintas entre si, totalizando 21 expressões faciais da emoção, sem contar a expressão neutra.

Considerando esses desafios, a análise facial computacional procura classificar ou associar as inúmeras expressões ou comportamentos faciais, a partir da identificação de atributos físicos capturados das imagens digitais, a emoções ou sentimentos humanos. Segundo Vemou e Horvath[45], o reconhecimento de emoções faciais opera por meio de três etapas: (i) a detecção facial; (ii) a detecção de expressões faciais; e (iii) a classificação dessas expressões em estados emocionais. A detecção de emoções é baseada na análise de pontos de referência da face humana (como ponta do nariz, sobrancelhas etc.). Além disso, em vídeos, variações desses pontos também são analisadas, com o objetivo de identificar contrações em grupos de músculos faciais e, dependendo do algoritmo, as expressões faciais podem ser classificadas em emoções básicas ou emoções compostas e, em outros casos, podem ser relacionadas a estados mentais ou psicológicos (como cansaço ou tédio). Em razão do uso de dados biométricos e de tecnologias de inteligência artificial, o reconhecimento de emoções faciais compartilha alguns dos riscos do uso de sistemas de reconhecimento facial e dessas tecnologias: apesar de a identificação do indivíduo não ser o objetivo primordial, riscos relacionados à precisão da interpretação da emoção são relevantes.

Nesse sentido, a imprecisão da interpretação da emoção pode advir de diversos fatores: se o comportamento facial é uma aproximação do estado emocional humano, então pode ocorrer a situação em que determinada expressão facial de um indivíduo não corresponda à sua emoção naquele momento, seja porque intencionalmente consegue modificar sua expressão por meio do controle de alguns músculos faciais, ou, a revés, alguma anomalia o impede de movimentá-los, ou até mesmo por questões culturais, em que expressões de sentido comum em alguns grupos sociais podem não ter o mesmo significado em outros. Também a imprecisão pode decorrer de erro na identificação de atributos físicos da face digitalizada, ou na classificação equivocada pelo algoritmo, caso em que a categoria não representa o humor do indivíduo naquele momento. Essas imprecisões não se restringem ao reconhecimento automatizado de emoções humanas, mas também podem ocorrer na categorização de gênero e faixa etária, uma vez que atributos físicos faciais podem não ser suficientes em quantidade e qualidade para prevenir desvios de generalização.

Por outro lado, não seria razoável exigir a precisão absoluta como parâmetro de aceitação ou rejeição de um sistema automatizado de análise facial, seja para o reconhecimento de emoções, seja para o reconhecimento de características demográficas, como gênero e idade. Em algumas circunstâncias, o algoritmo poderia não apresentar uma resposta adequada, mas, se esses casos forem estatisticamente

[45] VEMOU, Konstantina; HORVATH, Anna. Facial Emotion Recognition. **TechDispatch**, v. 1, p. 1-5, 2021. Disponível em: https://www.edps.europa.eu/system/files/2021-05/21-05-26_techdispatch-facial-emotion-recognition_ref_en.pdf. Acesso em: 27 mar. 2026.

desprezíveis, poder-se-ia afirmar que, dentro de determinada margem de erro aceitável ou de confiança razoável, o algoritmo de análise facial seria suficientemente preciso para a aplicação que se pretenda.

Entretanto, justamente por não objetivar a identificação do indivíduo, mas a sua classificação em grupos previamente definidos, como humor (alegria, surpresa, raiva, tristeza, medo, aversão), gênero (masculino, feminino) e faixa etária (jovem, adulto, idoso), e por estar sujeito a erros estatísticos, sistemas automatizados de análise facial estão mais intensamente sujeitos à discriminação algorítmica do que os de reconhecimento facial. Embora a identificação e a autenticação de indivíduos a partir de atributos físicos faciais mensuráveis sejam passíveis de erros estatísticos, muitas vezes decorrentes de vieses algorítmicos oriundos de bases de dados de treinamento insuficientes ou pouco representativas, o reconhecimento facial usualmente não opera com generalizações de atributos ou agregação de indivíduos em classes ou categorias.

Embora o termo viés algorítmico, em diversas circunstâncias, possa ser empregado de forma intercambiável com o termo discriminação algorítmica, não sem razão, pois o comportamento tendencioso do algoritmo pode não raramente produzir resultados discriminatórios; a distinção é relevante em razão de objetivos diferentes dos sistemas de reconhecimento facial e de análise facial, conforme apontado anteriormente. Segundo Alves e Andrade[46], o viés algorítmico decorre do comprometimento da neutralidade do sistema em razão do "treinamento incorreto do algoritmo ou por desdobramentos inesperados do aprendizado de máquina", em que tendências refletem a "predileção humana por determinados valores, devido a fatores sociais e culturais preexistentes à programação e que circundam os projetistas". Assim sendo, falhas dos sistemas de reconhecimento facial estariam mais associadas a vieses algorítmicos.

Por outro lado, os sistemas de análise facial não estariam expostos apenas ao comprometimento da neutralidade, mas também ao fato de, genericamente, associarem indivíduos a categorias de estados emocionais e demográficos incompatíveis com a realidade, por ignorar características e convicções individualizadas. Nesse sentido, o conceito de discriminação algorítmica proposto por Mattiuzzo e Mendes[47] parece mais adequado para retratar os riscos dos algoritmos de análise facial:

---

[46] ALVES, Marco Antonio Sousa; ANDRADE, Otávio Morato de. Da "caixa-preta" à "caixa de vidro": o uso da explainable artificial intelligence (XAI) para reduzir a opacidade e enfrentar o enviesamento em modelos algorítmicos. **Direito Público**, Brasília, v. 18, n. 100, 2022, p. 355. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5973. Acesso em: 27 mar. 2026.

[47] MATTIUZZO, Marcela; MENDES, Laura Schertel. Discriminação algorítmica: conceito, fundamento legal e tipologia. **Revista Direito Público**, Porto Alegre, v. 16, n. 90, p. 39-64, nov./dez. 2019, p. 51. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766/Schertel%20Mendes%3B%20Mattiuzzo%2C%202019. Acesso em: 27 mar. 2026.

> Feitas essas observações, vale esclarecer que o termo "discriminação algorítmica" é utilizado, neste artigo, para englobar tanto cenários que envolvem afirmações estatisticamente inconsistentes quanto cenários em que as afirmações, embora estatisticamente lógicas, de alguma forma tomam os indivíduos que dela são objeto não de forma efetivamente individualizada, mas apenas como parte de um grupo. Isso porque, a nosso ver, uma classificação, ainda que consistente sob o ponto de vista estatístico, pode em alguns casos se mostrar injusta.

Em termos de tipologia, as autoras sugerem a sistematização em quatro tipos principais de discriminação algorítmica: (i) a discriminação por erro estatístico; (ii) a discriminação por generalização; (iii) a discriminação pelo uso de informações sensíveis; e (iv) a discriminação limitadora do exercício de direitos. Apesar de a tipologia se revelar um poderoso instrumento para a mitigação de riscos e o desenvolvimento de salvaguardas, na medida em que especifica o potencial discriminatório em cada situação, importa ressaltar que, enquanto a primeira categoria se aproxima do viés algorítmico, por se tratar basicamente de erro de projeto do algoritmo ou de base de dados tendenciosa de treinamento, as demais categorias se referem ao potencial tratamento discriminatório em razão da decisão automatizada decorrente do enquadramento do indivíduo em determinada classe ou grupo que não o representa adequadamente.

Nesse sentido, por exemplo, se um sistema de análise facial operar com precisão estatística satisfatória para determinado agrupamento social, em detrimento de outros, em razão da tendenciosidade da base de dados de treinamento, é possível que o algoritmo classifique o comportamento facial de um indivíduo como alegria ou satisfação, quando na realidade sua emoção é neutra ou de aversão e, como consequência, tome decisões inadequadas na oferta de produtos ou provimento de serviços. Seria o caso de tratamento discriminatório, uma vez que indivíduos em situações similares são tratados de modo distinto por viés algorítmico, e não por razões isonômicas.

Em outra situação exemplificativa, o algoritmo de análise facial procura classificar o indivíduo em categorias de gênero previamente estabelecidas, possivelmente masculino e feminino, a partir do processamento de atributos faciais mensuráveis, para tomar decisões automatizadas. Sabe-se que a identificação de gênero não se restringe aos aspectos fisionômicos do indivíduo, tornando-se impraticável determinar o gênero de alguém apenas observando a pessoa, sem interagir com ela, conforme Silva[48]:

[48] SILVA, Heloísa Helena. Algoritmos de reconhecimento facial e as discriminações contra pessoas transexuais. **Revista InternetLab**, São Paulo, v. 2, n. 2, dez. 2021. Disponível em: https://revista.internetlab.org.br/algoritmos-de-reconhecimento-facial-e-as-discriminacoes-contra-pessoas-transexuais/. Acesso em: 27 mar. 2026.

> O pesquisador Keyes assim definiu a problemática da questão "identificar o gênero de alguém olhando para uma pessoa e não falando com ela é como perguntar qual o sabor do cheiro do azul", ou seja, a questão não é nem tanto o erro ou o acerto da resposta, mas sim entender que a pergunta em si não faz nenhum sentido. A conformação física é apenas um dos marcadores de gênero e não o único, e os algoritmos de reconhecimento facial, no estágio em que estão hoje, ainda não estão aptos a dar um passo além da aparência como fator determinante para indicação de gênero. A União Europeia, inclusive, já conta com um movimento que intenta o banimento do reconhecimento automatizado de gênero e de orientação sexual, visando a proteção desses dados sensíveis e da população LGBTQ+, vulnerável à discriminação sob esse aspecto.

Nesse caso, não se trata de viés algorítmico, mas da limitação do modelo binário de categorização de gênero, em que o indivíduo é classificado em desacordo com sua identificação de gênero ou com sua orientação sexual, produzindo um resultado automatizado potencialmente discriminatório. Aqui, especificamente, a situação tende a ser ainda mais grave, uma vez que a atitude discriminatória recai sobre grupos historicamente mais vulneráveis e a decisão automatizada tende a reforçar essas desigualdades.

Por fim, pode também ocorrer a situação em que não há viés algorítmico e o sistema de análise facial associa a expressão facial do indivíduo a uma determinada classe ou categoria de acordo com sua emoção ou sentimento, entretanto, contra a sua vontade. É possível admitir que há indivíduos capazes de simular ou representar comportamentos faciais que não condizem necessariamente com suas emoções, por exemplo, no caso de artistas ou atores profissionais. Por outro lado, há também reações faciais involuntárias que representam de forma fidedigna emoções ou sentimentos que, por razões de foro íntimo, o indivíduo não tenha intenção de revelar em determinadas situações. É o caso, por exemplo, da pessoa que tem a sua satisfação ou aversão revelada por sua expressão facial e capturada por um algoritmo de análise facial diante de determinada situação, mas contrária às suas convicções ideológicas e, portanto, isso pode representar uma violação à sua honra subjetiva. Trata-se, enfim, de invasão à privacidade ou à intimidade mental.

7. *NEURODIREITOS*

A face mais alarmante da insuficiência normativa para a "proteção jurídica da mente", expressão cunhada por Pintarelli[49], está associada aos avanços da neurociência e da neurotecnologia, que podem ser assim compreendidas:

[49] PINTARELLI, Camila. A proteção jurídica da mente. **Revista de Direito da Saúde Comparado**, São Paulo, v. 1, n. 1, 2022, p.104. Disponível em: https://periodicos.unisa.br/index.php/direitosaude/article/view/396/458. Acesso em: 27 mar. 2026.

> A neurociência é o campo da ciência responsável por estudar o cérebro humano e o sistema nervoso, como eles funcionam. Enquanto a neurotecnologia é um ramo da neurociência, no qual tecnologias são aplicadas ou usadas para registrar e interpretar informações da atividade cerebral. Se a neurociência tenta entender, por exemplo, as causas por trás do Parkinson, a neurotecnologia busca a aplicação de tecnologias no cérebro que ajudem a superar ou prevenir essa doença[50].

Em termos de categorização, as neurotecnologias podem ser classificadas em invasivas e não-invasivas, cujo critério principal de diferenciação é a localização dos sensores que monitoram a atividade do cérebro. Assim, dispositivos invasivos são aqueles inseridos dentro do corpo do indivíduo para interagir diretamente com os impulsos neurais. Por outro lado, os dispositivos não-invasivos buscam viabilizar a leitura de atividades neurais sem a necessidade de implantes cerebrais.[51]

Os riscos e as preocupações surgem com a ampliação da produção desses dados neurais, associada ao desenvolvimento de tecnologias correlatas, como a inteligência artificial, o *Big Data*, a internet das coisas, a computação em nuvem e a realidade aumentada. Não se trata apenas da proteção de dados pessoais, mas do acesso e da interferência alheia em informações que dizem respeito à mais íntima cognição humana, à autodeterminação, ao autodesenvolvimento e, portanto, trata-se da proteção da própria dignidade humana.

A lacuna normativa deverá ser preenchida, ou integrada, enquanto não houver legislação própria, mas sem deixar de reconhecer os benefícios trazidos por esses avanços tecnológicos e menos ainda impedir o seu contínuo desenvolvimento. Entretanto, a tutela jurídica, em boa medida, é necessária para proteger o homem de si mesmo:

> Vimos que o intenso desenvolvimento da neurotecnologia, com a evolução das técnicas de interface conectiva entre o cérebro e a máquina, estão expandindo as fronteiras da ação humana, gerando esperança e expectativa sobre seus impactos positivos na economia e, na área da saúde, no tratamento e na cura de doenças. Embora sejam avanços que devam ser celebrados, não podemos perder de vista os limites éticos envolvidos em tais procedimentos, pois trata-se de escalada evolutiva que diz respeito à própria integridade psíquica do ser humano, no que inserimos, também,

---

[50] BARROSO, Eliana. Os neurodireitos diante dos avanços da neurociência e da neurotecnologia. **Jusbrasil**, 13 mar. 2023. Disponível em: https://www.jusbrasil.com.br/artigos/os-neurodireitos-diante-dos-avancos-da-neurociencia-e-da-neurotecnologia/1778772576. Acesso em: 1 mar. 2024.

[51] POSSA, Alisson Alexsandro. **A concretização da dignidade humana na era das neurotecnologias**: o direito à liberdade cognitiva como neurodireito na ordem constitucional brasileira. 2022. Dissertação (Mestrado Acadêmico em Direito) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2022, p.15-16. Disponível em: https://repositorio.idp.edu.br/handle/123456789/4688. Acesso em: 27 mar. 2026.

> as preocupações relativas à sedimentação dos processos automatizados de tomada de decisão via interação algorítmica, que também impactam a mente humana e demandam tutela jurídica específica.[52]

Nesse contexto, no âmbito das iniciativas de proteção de neurodireitos, discute-se quais seriam esses direitos e, ainda, se, de fato, se tratariam de novos direitos não abarcados pela ordem jurídica estabelecida. Não se pretende aqui explorar essa discussão, uma vez que, embora relevante, escapa do objetivo desta investigação. Contudo, vale mencionar que o direito à privacidade mental tem sido invariavelmente considerado nas diversas propostas legislativas de neurodireitos, os quais, em linhas gerais, podem ser entendidos como o direito à proteção da segurança e da privacidade de dados neurais obtidos por neurotecnologias e, eventualmente, potencializados quando associados a tecnologias de inteligência artificial[53].

Exemplo concreto dessa produção legislativa é a aprovação da emenda constitucional (Reforma Constitucional nº 21.383) que introduziu formalmente a neuroproteção no âmbito do direito à vida e à integridade física e psíquica da pessoa, na Constituição do Chile[54]. Outro é a EC nº 85/2023, que alterou o parágrafo único do art. 235 da Constituição Estadual do Rio Grande do Sul[55], para incorporar a integridade mental do ser humano como pressuposto da política e da pesquisa científica e tecnológica no Estado.

Ainda em termos de atividade legislativa brasileira, a PEC 29/2023, em tramitação no Senado Federal, pode ser considerada um marco ao propor a alteração da Constituição Federal para incluir, entre os direitos e garantias fundamentais, a proteção à integridade mental e à transparência algorítmica[56]. Outras iniciativas estão em curso no parlamento brasileiro, como o PL 522/2022, que busca modificar a LGPD para conceituar dado neural e regulamentar a sua proteção[57];

---

[52] PINTARELLI, *op. cit.*, p. 117-118.

[53] LOPES, Ana Maria D'Ávila. Neurotecnologia: quando a tecnologia ameaça a dignidade humana. In: LOPES, Ana Maria D'Ávila *et al.* (org.). **Neurodireito, neurotecnologia e direitos humanos**. Porto Alegre: Livraria do Advogado, 2022, p. 21. Disponível em: https://www.researchgate.net/publication/368128401_Neurodireito_Neurotecnologia_e_Direitos_Humanos. Acesso em: 27 mar. 2026.

[54] CHILE. **Constitución Política de La República de Chile**. Santiago: Cámara de Diputadas y Diputados, 1980. Disponível em: https://www.camara.cl/camara/doc/leyes_normas/constitucion.pdf. Acesso em: 27 mar. 2026.

[55] RIO GRANDE DO SUL. **Constituição do Estado do Rio Grande do Sul**. Porto Alegre: Assembleia Legislativa do Estado do Rio Grande do Sul, 1989. Disponível em: https://ww2.al.rs.gov.br/dal/LinkClick.aspx?fileticket=AixRs5bbgtw%3d&tabid=3683&mid=5359. Acesso em: 27 mar. 2026.

[56] BRASIL. **Proposta de Emenda à Constituição nº 29, de 2023**. Brasília, DF: Senado Federal, 2023b. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9386685&ts=1733680966436&rendition_principal=S&disposition=inline. Acesso em: 27 mar. 2026.

[57] BRASIL. **Projeto de Lei nº 522, de 2022**. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2146384&filename=PL%20522/2022. Acesso em: 27 mar. 2026.

o PL 2174/2023, que propõe lei específica para estabelecer normas e princípios para a proteção dos direitos fundamentais relacionados ao cérebro e ao sistema nervoso humano, objetivando garantir a proteção e a promoção de neurodireitos dos indivíduos[58]; e o PL 4/2025, que pretende atualizar o Código Civil, inclusive dispondo de capítulo dedicado à pessoa no ambiente digital, abordando neurodireitos como parte indissociável da personalidade[59].

Feita essa breve contextualização, embora os sistemas de análise facial ou de reconhecimento de emoções faciais não sejam propriamente classificados como neurotecnologias, não há como negar que são capazes de registrar e interpretar informações da atividade cerebral por meio de uma interface homem-máquina não intrusiva: a imagem da face humana. Essa interface remota de captação da atividade mental tem potencial de disseminação similar ao do reconhecimento facial sobre tecnologias concorrentes, como o reconhecimento de íris e o de impressão digital para identificação ou autenticação pessoal.

Nesse sentido, é possível identificar inúmeras situações em que o comportamento facial pode significar, com acurácia, a atividade mental, muitas vezes de forma involuntária, e que se refere exclusivamente à privacidade mental do indivíduo, o qual não cogita que seja livremente revelada a terceiros, por se tratar de matéria do foro íntimo, ou por divergir de sua imagem perante a sociedade, ou por qualquer outra razão individual. Por exemplo, em uma entrevista de emprego, o candidato pode ser exposto intencionalmente a uma situação de segregação racial e, a pretexto de gravar em vídeo a dinâmica da reunião, o algoritmo de reconhecimento de emoções faciais pode captar, registrar e revelar suas convicções mais íntimas, ainda que contrárias à sua postura social e afirmações conscientes. Nesse caso, não parece razoável que a devassa mental seja mais relevante que a sua conduta para qualquer decisão que lhe diga respeito.

Em outra situação hipotética, poderia o algoritmo de reconhecimento de emoções faciais captar, registrar e revelar a satisfação mental de determinada autoridade religiosa, ainda que em lapso insignificante de tempo, diante de uma cena acidental de nudez infantil, ou de repulsa ou de aversão ao presenciar idosos desamparados em condições degradantes. Pode ocorrer ainda a revelação da orientação ou da preferência sexual do indivíduo, a partir da interpretação da reação facial involuntária, que sequer tenha consciência plena dessa condição ou, mesmo a tendo, cuja revelação seja contrária à sua vontade. Vale ressaltar que, em todas as situações

[58] BRASIL. **Projeto de Lei nº 2174, de 2023**. Brasília, DF: Câmara dos Deputados, 2023a. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2264479&filename=PL%202174/2023. Acesso em: 27 mar. 2026.

[59] BRASIL. **Projeto de Lei nº 4, de 2025**. Brasília, DF: Senado Federal, 2025. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9889374&ts=1770318618932&rendition_principal=S&disposition=inline. Acesso em: 27 mar. 2026.

exemplificadas, considera-se revelação o mero acesso não autorizado a informação mental, sendo irrelevante a inexistência de divulgação ou propagação.

Dessa forma, percebe-se que a discussão acerca do tratamento de dados por sistemas de análise facial ou reconhecimento de emoções faciais não se restringe ao âmbito da proteção de dados pessoais, mas alcança o direito à proteção da privacidade mental, não apenas no sentido de impedir o uso indevido de informações representativas da atividade neural, obtidas por sensores implantados dentro ou fora do corpo humano, mas também e, principalmente, no que se refere à intimidade mental. Portanto, parece fazer mais sentido que o debate e a produção legislativa a respeito de neurodireitos sejam desvinculados ou ao menos expandidos para além da neurociência e das neurotecnologias, a fim de propiciar a efetiva tutela da integridade mental, impedindo ameaça ou lesão a direitos e liberdades fundamentais, independentemente da técnica ou dos recursos tecnológicos empregados.

8. CONCLUSÃO

A LGPD refere-se à titularidade da pessoa natural quanto aos dados pessoais que lhe dizem respeito, e não à do agente de tratamento desses dados, ainda que o tratamento seja realizado de acordo com a anuência daquele. Nesse sentido, a titularidade não se transfere, mas apenas a possibilidade temporária de tratamento de dados pessoais, com o objetivo de assegurar ao titular o controle de seus dados.

Esse controle se mostra cada vez mais relevante à medida em que os dados pessoais mais intensamente representam o seu titular e expressam a sua personalidade, muitas vezes para além do que se deseja ou de que se tenha consciência, diante de fenômenos como a datificação e de teorias como a do corpo eletrônico. Assim sendo, a LGPD não visa à proteção de dados pessoais em si, mas os utiliza como via ou instrumento de proteção de seu titular, uma vez que o manejo desses dados afeta direitos da personalidade e alcança a dignidade da pessoa humana.

Por esse raciocínio, a LGPD não inova no campo dos direitos e liberdades fundamentais, mas procura materializar ou dar concretude a fundamentos já lançados constitucionalmente e utiliza meios e instrumentos para atingir esse intento. Um deles é a tipologia ou a classificação de dados em: pessoais, pessoais sensíveis e impessoais; trata-se de tentativa, ainda que sujeita a falhas, de estabelecer balizas ou parâmetros objetivos para viabilizar a aplicação da norma em situações concretas, a fim de tutelar direitos assegurados em abstrato.

No bojo dessa tentativa, surge o argumento de que os sistemas automatizados de análise facial e de reconhecimento de emoções faciais operam em aparente lacuna ou à margem das balizas estabelecidas. Enquanto os algoritmos de reconhecimento facial utilizam atributos da face humana para identificar ou autenticar o seu titular, aqueles sistemas extraem atributos faciais para categorizar o seu titular em classes ou grupos representativos de gênero, faixa etária e humor, em que a

identificação individual, além de não ser um propósito, não seria viável a partir dos atributos coletados. Assim, em interpretação restritiva da LGPD, a impossibilidade de identificação do indivíduo seria argumento suficiente para descaracterizar o atributo facial como dado pessoal ou dado pessoal sensível, uma vez que se trataria de pessoa natural indeterminada e indeterminável, por qualquer meio e agente razoavelmente considerados.

Além disso, a captura não autorizada da face do indivíduo, para fins de análise facial e de reconhecimento de emoções faciais, não representaria necessariamente uma violação ao direito de imagem, porque a *presumptio hominis* de que a captação se destina à posterior divulgação ou à reprodução não se confirmaria nesse caso, esvaziando a lógica civilista. E mais, a impossibilidade de identificação individual tornaria inviável o exercício do direito de imagem e afastaria a necessidade de anuência individualizada, uma vez que eventual oposição pontual cederia ao interesse coletivo, se assim demonstrado pelo uso dessas tecnologias.

No entanto, isso não significa que o tratamento de dados pessoais anônimos seja livremente permitido por algoritmos de análise facial e de reconhecimento de emoções faciais. Ao revés, justamente por operar com a generalização de atributos faciais ou agregação de indivíduos em classes ou categorias, essas tecnologias estão mais intensamente sujeitas à discriminação algorítmica do que as de reconhecimento facial e, portanto, merecem atenção. A propósito, o reconhecimento da existência de uma classe especial de dados pessoais, os dados pessoais sensíveis, insere-se na tentativa de desenvolver salvaguardas antidiscriminatórias aplicáveis ao tratamento dessa espécie de dados pessoais. Desse modo, a desclassificação do dado, como burla instrumental, não pode ser motivo suficiente e legítimo para afastar o objetivo pretendido pela norma.

Também nessa linha de pensamento, o argumento de que os atributos faciais anônimos tratados por sistemas de análise facial e de reconhecimento de emoções faciais não seriam dados pessoais, com o intuito de afastar a incidência da LGPD, não deve prosperar, sem que se considere a repercussão desse tratamento na esfera pessoal de alguém. Nesse sentido, a informação relacionada a uma pessoa natural identificada ou identificável goza de presunção absoluta de afetação da esfera pessoal, portanto, trata-se de dado pessoal por definição e insere-se no campo de incidência da norma. Por outro lado, no caso de informação relacionada a uma pessoa natural anônima, a presunção de afetação da esfera pessoal é relativa, pois, somente diante do caso concreto, será possível aferir se há lesão ou ameaça a direitos e liberdades fundamentais; contudo, se confirmada, o tratamento de atributos faciais anônimos será disciplinado pela LGPD e esses dados anônimos serão considerados pessoais.

Ademais disso, ainda que não se possam classificar como neurotecnologias, os sistemas de análise facial e de reconhecimento de emoções faciais podem captar e registrar remotamente, mesmo que limitadamente, atividades neurais que são expressas nos comportamentos faciais, com a vantagem, ou não, de dispensar o uso

de sensores invasivos ou não-invasivos. Mesmo que anônimos, o tratamento desses dados alcança o direito à proteção da intimidade mental, atingindo outro campo da tutela jurídica, situação em que o anonimato não parece ser o critério mais seguro para dispensar a aplicação da norma.

Em suma, a LGPD desenvolveu um arcabouço normativo para regular o tratamento de dados pessoais, como meio para atingir o objetivo de proteger direitos e liberdades fundamentais de seus titulares. Ainda que se possa legitimamente discutir o enquadramento legal do tratamento de dados dispensado pelos sistemas de análise facial e de reconhecimento de emoções faciais, não se poderá renunciar àquele objetivo, apenas pela desclassificação do dado, que também conta com a tutela de todo o ordenamento jurídico, e não apenas de uma norma, que deve ser interpretada sistemicamente.

REFERÊNCIAS BIBLIOGRÁFICAS

AFFONSO, Filipe José Medon. O direito à imagem na era das deep fakes. **Revista Brasileira de Direito Civil**, Rio de Janeiro, v. 27, n. 1, p. 251-277, 2021. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/438. Acesso em: 27 mar. 2026.

ALVES, Marco Antonio Sousa; ANDRADE, Otávio Morato de. Da "caixa-preta" à "caixa de vidro": o uso da explainable artificial intelligence (XAI) para reduzir a opacidade e enfrentar o enviesamento em modelos algorítmicos. **Direito Público**, Brasília, v. 18, n. 100, 2022. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5973. Acesso em: 27 mar. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Agenda Regulatória para o Biênio 2025-2026**. Brasília, DF: ANPD, 2024a. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/processo_regulatorio/agenda-regulatoria-1. Acesso em: 27 mar. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Radar Tecnológico nº 2 – Biometria e Reconhecimento Facial**. Brasília, DF: ANPD, 2024b. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/. Acesso em: 27 mar. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **ANPD abre Tomada de Subsídios sobre Tratamento de Dados Biométricos**. Brasília, DF: ANPD, 2025a. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-tomada-de-subsidios-sobre-tratamento-de-dados-biometricos. Acesso em: 27 mar. 2026.

AUTORIDADE 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, DF: ANPD, 2025b. 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: 27 mar 2026.

BARROSO, Eliana. Os neurodireitos diante dos avanços da neurociência e da neurotecnologia. **Jusbrasil**, 13 mar. 2023. Disponível em: https://www.jusbrasil.com.br/artigos/os-neurodireitos-diante-dos-avancos-da-neurociencia-e-da-neurotecnologia/1778772576. Acesso em: 1 mar. 2024.

BASTOS, Elísio Augusto Velloso; ESTEVES, Vitória Barros. Tecnologias de reconhecimento facial: um estudo a partir do contexto de vigilância digital e sutil. **Revista Direitos Democráticos & Estado Moderno**, São Paulo, n. 3, p. 216-240, jul./dez. 2021. Disponível em: https://revistas.pucsp.br/index.php/DDEM/article/view/53875/38321. Acesso em: 27 mar. 2026.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. São Paulo: Grupo GEN, 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 27 mar. 2026.

BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 27 mar. 2026.

BRASIL. Decreto Legislativo nº 196, de 2003. Aprova o texto da Convenção sobre o Cibercrime, celebrada em Budapeste, em 23 de novembro de 2001. **Diário Oficial da União**, Brasília, DF, 2003.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 27 mar. 2026.

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/L13709compilado.htm. Acesso em: 27 mar. 2026.

BRASIL. **Projeto de Lei nº 522, de 2022**. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2146384&filename=PL%20522/2022. Acesso em: 27 mar. 2026.

BRASIL. **Projeto de Lei nº 2174, de 2023**. Brasília, DF: Câmara dos Deputados, 2023a. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2264479&filename=PL%202174/2023. Acesso em: 27 mar. 2026.

BRASIL. **Projeto de Lei nº 4, de 2025**. Brasília, DF: Senado Federal, 2025. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9889374&ts=1770318618932&rendition_principal=S&disposition=inline. Acesso em: 27 mar. 2026.

BRASIL. **Proposta de Emenda à Constituição nº 29, de 2023**. Brasília, DF: Senado Federal, 2023b. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9386685&ts=1733680966436&rendition_principal=S&disposition=inline. Acesso em: 27 mar. 2026.

BRASIL. Superior Tribunal de Justiça. **Súmula nº 403**. DJe 24 nov. 2009. Disponível em: https://www.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2014_38_capSumula403.pdf. Acesso em: 27 mar. 2026.

CHILE. **Constitución Política de La República de Chile**. Santiago: Cámara de Diputadas y Diputados, 1980. Disponível em: https://www.camara.cl/camara/doc/leyes_normas/constitucion.pdf. Acesso em: 27 mar. 2026.

DINIZ, Maria H. **Curso de Direito Civil Brasileiro**: teoria geral do direito civil. São Paulo, SP: Saraiva, 2023.

DU, Shichuan; TAO, Young; MARTINEZ, Aleix M. Compound facial expression of emotion. **Proceedings of the National Academy of Sciences**, Washington, v. 111, n. 15,p. E1454-E1462, 2014. Disponível em: https://www.pnas.org/doi/epdf/10.1073/pnas.1322355111. Acesso em: 27 mar. 2026.

EUROPEAN COMMISSION. ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 2/2012 on the concept of personal data**. Bruxelas, 2012. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm. Acesso em: 27 mar. 2026.

LI, Sant Z.; JAIN, Anil K. **Handbook of face recognition**. New York: Springer, 2005.

LOPES, Ana Maria D'Ávila. Neurotecnologia: quando a tecnologia ameaça a dignidade humana. In: LOPES, Ana Maria D'Ávila *et al.* (org.). **Neurodireito, neurotecnologia e direitos humanos**. Porto Alegre: Livraria do Advogado, 2022. Disponível em: https://www.researchgate.net/publication/368128401_Neurodireito_Neurotecnologia_e_Direitos_Humanos. Acesso em: 27 mar. 2026.

LOUREIRO, Henrique Vergueiro. **Direito à imagem**. 2005. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2005. Disponível em: https://repositorio.pucsp.br/jspui/handle/handle/5983. Acesso em: 27 mar. 2026.

MACHADO, Diego. Considerações iniciais sobre o conceito de dado pessoal no ordenamento jurídico brasileiro. **Civilistica**, [*S. l.*], v. 12 n. 1, 2023. Disponível em: https://www.researchgate.net/publication/371577468_Consideracoes_iniciais_sobre_o_conceito_de_dado_pessoal_no_ordenamento_juridico_brasileiro. Acesso em: 27 mar. 2026.

MATTIUZZO, Marcela; MENDES, Laura Schertel. Discriminação algorítmica: conceito, fundamento legal e tipologia. **Revista Direito Público**, Porto Alegre, v. 16, n. 90, p. 39-64, nov./dez. 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direito-publico/article/view/3766/Schertel%20Mendes%3B%20Mattiuzzo%2C%202019. Acesso em: 27 mar. 2026.

PINTARELLI, Camila. A proteção jurídica da mente. **Revista de Direito da Saúde Comparado**, São Paulo, v. 1, n. 1, 2022. Disponível em: https://periodicos.unisa.br/index.php/direitosaude/article/view/396/458. Acesso em: 27 mar. 2026.

POSSA, Alisson Alexsandro. **A concretização da dignidade humana na era das neurotecnologias**: o direito à liberdade cognitiva como neurodireito na ordem constitucional brasileira. 2022. Dissertação (Mestrado Acadêmico em Direito) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2022. Disponível em: https://repositorio.idp.edu.br/handle/123456789/4688. Acesso em: 27 mar. 2026.

RIO GRANDE DO SUL. **Constituição do Estado do Rio Grande do Sul**. Porto Alegre: Assembleia Legislativa do Estado do Rio Grande do Sul, 1989. Disponível em: https://ww2.al.rs.gov.br/dal/LinkClick.aspx?fileticket=AixRs5bbgtw%3d&tabid=3683&mid=5359. Acesso em: 27 mar. 2026.

RODOTÀ, Stefano. A antropologia do homo dignus. Tradução de Maria Celina Bodin de Moraes. **Civilistica.com**, Rio de Janeiro, v. 6, n. 2, 2017. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/08/STEFANO-RODOTA-A-antropologia-do-homo-dignus.pdf. Acesso em: 27 mar. 2026.

SILVA, Heloísa Helena. Algoritmos de reconhecimento facial e as discriminações contra pessoas transexuais. **Revista InternetLab**, São Paulo, v. 2, n. 2, dez. 2021. Disponível em: https://revista.internetlab.org.br/algoritmos-de-reconhecimento-facial-e-as-discriminacoes-contra-pessoas-transexuais/. Acesso em: 27 mar. 2026.

SIQUEIRA, Dirceu Pereira; VIEIRA, Ana Elisa Silva Fernandes. Os limites à reconstrução digital da imagem na sociedade tecnológica. **Revista Eletrônica do Curso de Direito da UFSM**, Santa Maria, v. 17, n. 3, e67299, 2022. Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/67299. Acesso em: 27 mar. 2026.

SOUSA, Cristina de. Emoção e expressão facial: novos desafios. **Psicologia**, Lisboa, v. 24, n. 2, p. 17-41, 2010. Disponível em: https://revista.appsicologia.org/index.php/rpsicologia/article/view/303/65. Acesso em: 27 mar. 2026.

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

THALES. **Facial recognition**: top 7 trends (tech, vendors, use cases). 2021. Disponível em: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition. Acesso em: 27 mar. 2026.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679. Acesso em: 27 mar. 2026.

UNREAL PERSON. **This person does not exist**. [*S. l.*]: Unreal Person, 2023. Disponível em: https://www.unrealperson.com/. Acesso em: 27 mar. 2026.

VEMOU, Konstantina; HORVATH, Anna. Facial Emotion Recognition. **TechDispatch**, v. 1, p. 1-5, 2021. Disponível em: https://www.edps.europa.eu/system/files/2021-05/21-05-26_techdispatch-facial-emotion-recognition_ref_en.pdf. Acesso em: 27 mar. 2026.

WENDEHORST, Christiane; DULLER, Yannic. **Biometric Recognition and behavioural detection**. Policy Department for Citizens' Rights and Constitutional Affairs, PE 696.968 , Aug. 2021. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf. Acesso em: 27 mar. 2026.

ZUK, Ofir. **The State of Facial Recognition Today**. **Datagen.tech**, 2024. Disponível em: https://datagen.tech/blog/the-state-of-facial-recognition-today/. Acesso em: 12 fev. 2024.

Submetido em: 01/12/2024
Aprovado em: 26/09/2025

POLÍTICAS DE INOVAÇÃO DAS ICTS: PERCEPÇÃO DOS PESQUISADORES E DAS ESTRUTURAS DOS NÚCLEOS DE INOVAÇÃO TECNOLÓGICA

Innovation Policies of Stis: Researchers' Perception and the Structures of Technology Transfer Offices

Maria Paula de Oliveira Valadares[1]

SUMÁRIO 1. Introdução; 2. Desenvolvimento; 2.1. Metodologia; 2.2. Referencial teórico; 2.2.1. Arcabouço legal e políticas de inovação; 2.2.2. Núcleos de inovação tecnológica; 2.2.2.1. Modelos de organização e gestão dos núcleos de inovação tecnológica; 2.3. Análise dos dados obtidos por meio do questionário; 3. Conclusão; 4. Agradecimentos; Referências Bibliográficas.

RESUMO O presente artigo aborda a importância das Instituições Científicas e Tecnológicas (ICTs) como propulsoras da inovação, bem como o papel de destaque que essas instituições têm na geração de conhecimento e no desenvolvimento de novas tecnologias. A implementação de políticas de inovação, reguladas pelo Marco Legal da Inovação, entraram em nosso ordenamento jurídico com o objetivo de promover a transferência de tecnologia, proteger a propriedade intelectual e incentivar a colaboração entre os setores público, privado e acadêmico. Assim, esse estudo utiliza uma abordagem metodológica mista, envolvendo métodos quantitativos e qualitativos, o que traduz-se na aplicação de um questionário semiestruturado aos pesquisadores de ICTs e na realização de uma revisão de literatura sobre políticas de inovação e estruturas dos Núcleos de Inovação Tecnológica (NITs). Por meio do questionário aplicado, objetivou-se medir a percepção dos pesquisadores sobre a relevância das políticas de inovação, sobre as oportunidades adicionais para promoção de inovação, sobre a contribuição dos NITs e sobre a adequação das políticas de propriedade intelectual. Por fim, buscou-se investigar o arcabouço legal vigente e as políticas de inovação brasileiras, destacando leis e decretos que regulamentam a inovação nas ICTs e a importância dos NITs na gestão da inovação e da propriedade intelectual, e como esses variam em estrutura e eficácia dependendo dos recursos e da cultura institucional.

Palavras-chave: ICT. NIT. Política de Inovação. Transferência de Tecnologia. Propriedade Intelectual.

ABSTRACT: The present article addresses the importance of Scientific and Technological Institutions (STIs) as drivers of innovation and highlights their prominent role in generating knowledge and developing new technologies. The implementation of innovation policies, regulated by the Innovation Legal Framework, has been incorporated into Brazilian legislation to promote technology transfer, protect intellectual property, and encourage collaboration between public, private, and academic sectors. This study adopts a mixed-methods approach, combining quantitative and qualitative methods, which, in this research, includes applying a semi-structured questionnaire to STI researchers and conducting a literature review on innovation policies and the structure of Technology Transfer Offices (TTOs). The questionnaire aimed to measure researchers' perceptions regarding the relevance of innovation policies, additional opportunities for fostering innovation, the

[1] Perita Criminal da Superintendência da Polícia Técnico-Científica do Estado de São Paulo. Doutora em Ciências pela Universidade de São Paulo (USP).

DOI: 10.22491/*respge*.v16i1.1738

contribution of TTOs, and the adequacy of intellectual property policies. The study sought to investigate the current legal framework and Brazilian innovation policies, highlighting the laws and decrees regulating innovation in STIs, the importance of TTOs in managing innovation and intellectual property, and how their structure and effectiveness vary depending on institutional resources and culture.

Keywords: STI (Scientific and Technological Institutions). TTO (Technology Transfer Offices). Innovation Policy. Technology Transfer. Intellectual Property.

1. INTRODUÇÃO

Atualmente, a inovação tecnológica é um dos principais motores do desenvolvimento econômico e social, sendo que as Instituições Científicas e Tecnológicas (ICTs) são as grandes propulsoras dessa inovação. Nesse sentido, essas instituições desempenham um papel vital na geração de conhecimento, no avanço da pesquisa e no desenvolvimento de novas tecnologias. No Brasil, a implementação de políticas de inovação dentro das ICTs é regulada por um arcabouço legal que visa promover a transferência de tecnologia, proteger a propriedade intelectual e incentivar a colaboração entre o setor público, o privado e o setor acadêmico.

Pode-se definir a Política de Inovação como um conjunto de documentos formais com diretrizes gerais que norteiam a atuação da instituição nas ações ligadas à inovação, à proteção da propriedade intelectual e à transferência de tecnologia[2].

Desde a entrada em vigor da Lei nº 10.973/2004[3], posteriormente aprimorada pela Lei nº 13.243/2016[4], passou a ser exigido que as ICTs estabelecessem suas políticas de inovação. Essas normas fornecem diretrizes para a organização e a gestão dos processos de transferência de tecnologia e geração de inovação, alinhando-se às prioridades das políticas nacionais de ciência, tecnologia e inovação. No entanto, a implementação efetiva dessas políticas ainda enfrenta desafios significativos, como a burocracia, a falta de recursos financeiros e a ausência de uma cultura de inovação consolidada dentro das instituições.

[2] BRASIL. Decreto nº 9.283, de 7 de fevereiro de 2018. Regulamenta a Lei nº 10.973, de 2 de dezembro de 2004, e a Lei nº 13.243, de 11 de janeiro de 2016, para dispor sobre estímulos ao desenvolvimento científico, à pesquisa, à capacitação científica e tecnológica e à inovação. **Diário Oficial da União**, Brasília, DF, 8 fev. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9283.htm. Acesso em: 1 abr. 2026.

[3] BRASIL. Lei nº 10.973, de 2 de dezembro de 2004. Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências. **Diário Oficial da União**, Brasília, DF, 3 dez. 2004. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/l10.973.htm. Acesso em: 1 abr. 2026.

[4] BRASIL. Lei nº 13.243, de 11 de janeiro de 2016. Dispõe sobre o estímulo ao desenvolvimento científico, à pesquisa, à capacitação científica e tecnológica e à inovação. **Diário Oficial da União**, Brasília, DF, 12 jan. 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13243.htm. Acesso em: 1 abr. 2026.

A legislação estabelece que as ICTs devem ter em sua estrutura o Núcleo de Inovação Tecnológica (NIT), órgão interno responsável pela gestão da política de inovação e da propriedade intelectual da instituição. Porém, a primeira tarefa do NIT, e talvez a de maior impacto, foi criar as políticas de inovação e de propriedade intelectual de suas respectivas ICTs. Dessa forma, os NITs tiveram dois trabalhos árduos: elaborar as propostas para a política de inovação e de propriedade intelectual e disseminar essas propostas, sensibilizando todo o ambiente acadêmico sobre a temática, para que a política fosse efetivamente adotada pela instituição[5].

Observa-se que a eficácia dos NITs varia significativamente entre as instituições, sendo influenciada pela estrutura organizacional, pelos recursos disponíveis e pela própria cultura da instituição. Alguns estudos indicam que a falta de autonomia e de recursos, bem como a ausência de uma visão estratégica clara, podem comprometer a eficácia desses núcleos, limitando seu impacto no fomento à inovação.

Diante do exposto, o presente artigo pretende investigar a percepção dos pesquisadores das ICTs sobre as políticas de inovação implementadas em suas instituições, bem como realizar uma revisão de literatura sobre o tema e analisar as estruturas adotadas pelos NITs. A pesquisa busca compreender como essas políticas são vistas pelos pesquisadores, que estão na linha de frente da inovação, e identificar os principais desafios e oportunidades relacionados à sua implementação.

Para alcançar esses objetivos, foi realizada uma coleta de dados por meio de um questionário semiestruturado, composto por três perguntas fechadas e uma pergunta com resposta aberta. Além disso, foi conduzida uma revisão de literatura sobre o tema.

A relevância deste estudo reside em sua tentativa de compreender a eficácia das políticas de inovação nas ICTs e o papel crucial dos NITs. Ao entender as percepções dos pesquisadores e analisar as práticas existentes, espera-se identificar áreas de melhoria para fortalecer a gestão da inovação dentro dessas instituições. Assim, este artigo contribui para o debate sobre como as ICTs podem aprimorar suas políticas de inovação, promovendo um ambiente mais propício à pesquisa, ao desenvolvimento tecnológico e à transferência de conhecimento para o setor produtivo.

2. DESENVOLVIMENTO

2.1. *Metodologia*

Este artigo pretende investigar a percepção dos pesquisadores de ICTs sobre as políticas de inovação implementadas em suas instituições, bem como, realizar uma

[5] ALVES, Vivian Costa; AMARANTE SEGUNDO, Gesil Sampaio; SAMPAIO, Renelson Ribeiro. Reflexões sobre as competências dos núcleos de inovação tecnológica. **Cadernos de Prospecção**, Salvador, v. 8, n. 4, p. 690, out./dez. 2015.

revisão de literatura sobre as políticas e estruturas adotadas pelos NITs. A metodologia adotada é uma combinação de abordagens quantitativa e qualitativa, utilizando um questionário semiestruturado e uma revisão de literatura com foco nas políticas de inovação e nas estruturas organizacionais dos NITs, com o intuito de fornecer um panorama das práticas e dos modelos adotados no Brasil.

A presente pesquisa é de natureza descritiva e exploratória, buscando-se descrever as características de determinada população ou fenômeno, e proporcionar maior familiaridade com o problema, respectivamente, a fim de torná-lo explícito ou de construir hipóteses[6].

Para a coleta de dados, foi elaborado um questionário semiestruturado composto por três perguntas fechadas, cada uma delas contendo um conjunto de opções predefinidas, sem a possibilidade de respostas abertas, e uma pergunta com alternativa aberta. Esse método foi escolhido com o objetivo de padronizar as respostas e facilitar a análise quantitativa dos dados.

O questionário foi desenvolvido após a análise da literatura existente sobre as políticas de inovação das ICTs. As perguntas foram formuladas para abranger a percepção dos pesquisadores sobre a eficácia e a adequação dessas políticas na promoção da inovação e no impacto que elas geram nas atividades de pesquisa e desenvolvimento.

O questionário foi disponibilizado na internet, utilizando a plataforma Google Forms, no mês de junho de 2024, e coletou 22 respostas. O número limitado de respondentes justifica-se pelo perfil restrito do público-alvo do questionário. A escolha de um formulário on-line ocorreu devido à facilidade de distribuição e pela maior capacidade de alcance de participantes de forma eficiente e econômica. O formulário foi divulgado por e-mail e em redes sociais de pesquisadores de ICTs para alcançar o público-alvo.

A amostra foi composta por 22 pesquisadores vinculados a diferentes ICTs no Brasil. Os participantes foram alcançados por meio de redes institucionais e canais de comunicação voltados à inovação, o que possibilitou acessar indivíduos diretamente envolvidos com a utilização e implementação de políticas de inovação em suas respectivas instituições. A estratégia de amostragem adotada favoreceu a obtenção de respostas qualificadas, alinhadas ao perfil do público-alvo da pesquisa.

Este artigo também realizou uma revisão de literatura para analisar as diferentes políticas e estruturas adotadas pelos NITs de ICTs públicas. Foram selecionados artigos científicos, livros, teses, dissertações e documentos oficiais que tratam das políticas de inovação e da estrutura organizacional dos NITs, publicados nos últimos quinze anos. Além disso, foram buscados trabalhos que abordassem diretamente as políticas de inovação de ICTs públicas e as práticas dos NITs.

[6] GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. Barueri: Atlas, 2008.

Os dados coletados foram analisados por meio de técnicas estatísticas descritivas e os dados qualitativos da revisão de literatura foram trabalhados por meio da análise de conteúdo para a identificação de temas e padrões emergentes[7].

2.2. Referencial Teórico

2.2.1. Arcabouço Legal e Políticas de Inovação

No Brasil, as Instituições Científicas e Tecnológicas públicas desempenham um papel fundamental no avanço da pesquisa e do desenvolvimento, impulsionando a inovação e o progresso tecnológico em diversas áreas, desde a biotecnologia até a engenharia aeroespacial. A importância dessas instituições vai além da produção científica, pois são catalisadoras de parcerias estratégicas entre o setor público e o privado e desempenham um papel crucial na formação de recursos humanos altamente qualificados.

A Lei nº 10.973/2004 permitiu uma maior aproximação entre as ICTs e as empresas, estabelecendo a obrigatoriedade de as ICTs instituírem suas políticas de inovação, no entanto, não deu maiores detalhes sobre as possibilidades que as ICTs poderiam explorar. Já a Lei nº 13.243/2016, introduziu novas diretrizes e especifica que a citada política deve dispor sobre a organização e a gestão dos processos de transferência de tecnologia e a geração de inovação no ambiente produtivo em consonância com as prioridades das políticas nacionais de ciência, tecnologia e inovação e com a política industrial e tecnológica nacional[8].

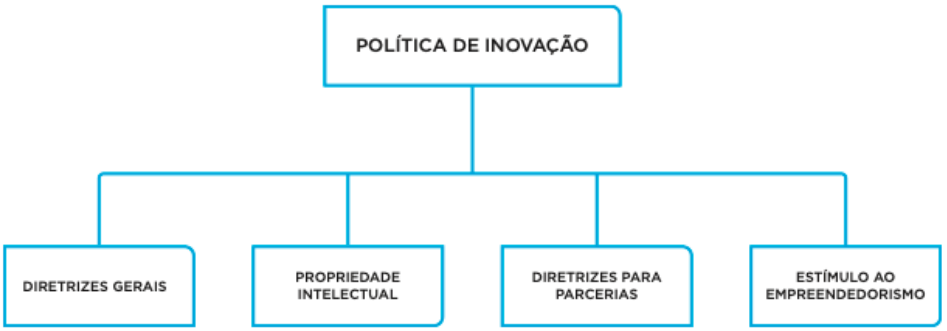
Os tópicos essenciais que devem ser abordados na política da ICT podem ser divididos em quatro categorias principais, a saber: I) Diretrizes Gerais; II) Propriedade Intelectual; III) Diretrizes para Parcerias; e IV) Estímulo ao Empreendedorismo[9], conforme apresentado na Figura 1.

[7] BARDIN, Laurence. **Análise de conteúdo**. Lisboa: Edições 70, 2011.

[8] BRASIL, **Lei nº 13.243, de 11 de janeiro de 2016**, *op. cit*.

[9] BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. Secretaria de Empreendedorismo e Inovação. **Guia de orientação para elaboração da política de inovação nas ICTs**. Brasília, DF: MCTIC, 2019, p. 16. Disponível em: https://www.fortec.org.br/orientacao-politicas-icts. Acesso em: 1 abr. 2026.

Figura 1.
Temas das Políticas de Inovação



Fonte: Brasil, 2019[10].

O Decreto n. 9.283[11], de 2018, trouxe avanços significativos para o ambiente de pesquisa e desenvolvimento, pois regulamentou a Lei de Inovação. A partir dele, permitiu-se que as ICTs públicas celebrem contratos de transferência de tecnologia com empresas privadas, além de serem estabelecidas regras para a participação societária dessas instituições em *startups* e empresas inovadoras. Suas regras também incentivam a criação de ambientes promotores de inovação, como parques tecnológicos e incubadoras de empresas. Além disso, ele regulamenta a transferência de tecnologia, a participação de ICT em projetos internacionais, a simplificação de processos de importação para pesquisa e outros temas.

No âmbito estadual, a Lei Complementar nº 1.049[12], de 19 de junho de 2008, regulamenta medidas para incentivar a inovação tecnológica e a pesquisa no Estado de São Paulo. Ela definiu conceitos como inovação tecnológica e instituiu órgãos e redes para promover essa inovação. Além disso, detalha formas de cooperação entre entidades públicas e privadas. A lei também regulamenta a participação de pesquisadores e inventores no processo de inovação, o compartilhamento de recursos e a formação de parcerias estratégicas. Ademais, institui o Sistema Paulista de

[10] *Ibid.*

[11] BRASIL, **Decreto nº 9.283, de 7 de fevereiro de 2018**, *op. cit.*

[12] SÃO PAULO (Estado). Lei Complementar nº 1.049, de 19 de junho de 2008. Dispõe sobre medidas de incentivo à inovação tecnológica, à pesquisa científica e tecnológica, ao desenvolvimento tecnológico, à engenharia não-rotineira e à extensão tecnológica em ambiente produtivo, no Estado de São Paulo, e dá outras providências correlatas. **Diário Oficial do Estado de São Paulo**, São Paulo, 20 jun. 2008. Disponível em: http://www.al.sp.gov.br/repositorio/legislacao/lei.complementar/2008/lei.complementar-1049-19.06.2008.html. Acesso em: 10 nov. 2023.

Inovação Tecnológica, com o objetivo de promover o desenvolvimento sustentável do Estado por meio da inovação.

As políticas adotadas pelas ICTs são fundamentais para moldar suas direções estratégicas e sua eficácia operacional. No entanto, estas políticas variam significativamente entre si, influenciadas, não apenas por suas missões institucionais, mas também pelos contextos regionais em que estão inseridas e pelas fontes de financiamento disponíveis, quando aplicável. Cada ICT desenvolve abordagens próprias para colaboração com o setor industrial, captação de recursos e comercialização de tecnologias, refletindo sua adaptação às necessidades e capacidades individuais.

O Ministério da Ciência, Tecnologia e Inovações (MCTI) disponibiliza o "Formulário para Informações sobre a Política de Propriedade Intelectual das Instituições Científicas, Tecnológicas e de Inovação" – FORMICT, o qual deve ser preenchido pelas ICTs brasileiras, conforme exigido pela Lei de Inovação, para fornecer dados sobre suas políticas de inovação, propriedade intelectual e transferência de tecnologia (Portaria MCT nº 118[13]). No sítio eletrônico do MCTI, pode-se ter acesso ao relatório do FORMICT, que consolida esses dados; porém, a publicação mais recente é do ano-base 2018, já existindo uma lacuna de 6 anos. Neste documento, pode-se aferir que, das 305 instituições que preencheram o formulário, 71,7% das instituições públicas e 59,4% das instituições privadas detêm uma política de inovação implementada[14]. Portanto, segundo esse dado desatualizado, ainda há cerca de 28,3% das ICTs públicas que não possuem sua política de inovação estabelecida.

A burocracia excessiva, a falta de recursos humanos e financeiros, bem como a ausência de uma cultura de inovação consolidada nas instituições, são barreiras que atrapalham a eficácia das políticas de inovação. Um estudo realizado por Pires e Silva[15] indicou que a implementação de políticas públicas de inovação em nosso país enfrenta desafios relacionados à burocracia e à falta de incentivos claros, o que dificulta a transferência do conhecimento acadêmico para o setor empresarial.

Além disso, durante a pesquisa, observou-se que a avaliação da eficácia das políticas de inovação é frequentemente baseada em indicadores quantitativos, como o número de patentes registradas e de artigos científicos publicados pelas instituições; contudo, esses dados nem sempre refletem o real impacto das políticas de inovação das ICTs no desenvolvimento econômico e social. Assim, seria necessário estabelecer

[13] BRASIL. Portaria MCT nº 118, de 23.02.2010. Aprova o novo formulário para que as Instituições Científicas e Tecnológicas – ICT prestem ao Ministério da Ciência e Tecnologia - MCT, através do Ministério ou do Órgão ao qual a Instituição seja subordinada ou vinculada, […]. **Diário Oficial da União**, Brasília, 23 fev. 2010.

[14] BRASIL, **Decreto n. 9.283, de 7 de fevereiro de 2018**, *op. cit*.

[15] PIRES, Edilson Araújo; SILVA, Karoline Greice Viana Cardoso da. A atuação dos núcleos de inovação tecnológica nas universidades: o caso brasileiro. **Revista de Gestão e Secretariado**, São Paulo, v. 14, n. 9, p. 1596, 2023. Disponível em: https://ojs.revistagesec.org.br/secretariado/article/download/2653/1596. Acesso em: 1 abr. 2026.

indicadores qualitativos que considerem a relevância e a aplicabilidade dos instrumentos estabelecidos pelas políticas no fomento de novas oportunidades de inovação.

Conforme conclui o Relatório FORMICT, ano-base 2018, um dos principais desafios que as instituições ainda enfrentam é a criação e a implementação de suas políticas de inovação, de acordo com as diretrizes do Novo Marco Legal de Ciência, Tecnologia e Inovação.

Com o objetivo de orientar as ICTs a estabelecer suas políticas de inovação, o Fórum Nacional de Gestores de Inovação e Transferência de Tecnologia (FORTEC) e o MCTI construíram em conjunto o *Guia de orientação para elaboração da política de inovação nas ICTs*[16]. Esse documento é um recurso destinado a apoiar os profissionais na criação de Políticas de Inovação para as instituições. Ele aborda aspectos legislativos relevantes e orienta sobre as decisões que as Instituições Científicas e Tecnológicas devem tomar, como a formatação e a quantidade de documentos necessários, além dos níveis de gestão da Política Institucional. O guia inclui exemplos de políticas já atualizadas e outras em discussão, com o objetivo de ser uma contribuição útil para os envolvidos nesse processo.

Dentro do contexto normativo estabelecido pela Lei nº 10.973, e sua reforma pela Lei nº 13.243 de 2016, as Instituições de Ciência e Tecnologia devem adotar uma política de inovação mais proativa. Essa política inclui a formação de alianças estratégicas, encomendas tecnológicas, criação de fundos de investimento e a participação no capital de empresas, por meio do suporte fornecido pelos seus NITs e fundações de apoio robustas. O objetivo é melhorar a infraestrutura, os recursos humanos e o capital intelectual, a fim de enfrentar os desafios de pesquisa e desenvolvimento (P&D), bem como da transferência de tecnologia e inovação.

As ICTs devem seguir um modelo de gestão estratégica de P&D e inovação, baseado no modelo da tríplice hélice, expandido para a quinta hélice, consolidando ecossistemas locais de inovação. Além disso, devem estabelecer parcerias com agências, universidades e empresas para estratégias de internacionalização de P&D e inovação. A consolidação das políticas de inovação pode acelerar a transferência de tecnologia, aumentar as parcerias estratégicas e reposicionar os projetos de pesquisa das ICTs[17].

Um exemplo de boas práticas na formulação da política de inovação é a Universidade Federal do ABC (UFABC), que construiu um documento inicial de sua política de inovação e o submeteu às áreas-chave da instituição, o que permitiu uma visão das demandas e dos processos da universidade que, inicialmente, não haviam

[16] BRASIL, 2019, *op. cit*.

[17] PEDRO, Edilson da Silva. A Política Nacional de Inovação e as Instituições de Ciência e Tecnologia (ICTs). **Cadernos de Prospecção**, Salvador, v. 14, n. 1, p. 1-4, mar. 2021.

sido contemplados[18]. Esse processo de criação de uma política com a participação dos pesquisadores permitiu que fosse formulada uma política completa, adequada às necessidades específicas da instituição, isso possibilita que essas normas não sejam apenas uma formalidade exigida pela lei, mas sim um conjunto de regras práticas que permite à ICT materializar todo o seu potencial inovativo.

2.2.2. Núcleos de Inovação tecnológica

O Marco Legal da Inovação determinou que as Instituições de Ciência e Tecnologia nacionais devem estabelecer NITs para administrar as suas políticas de inovação[19], promovendo a transferência de tecnologia e a proteção da propriedade intelectual. Apesar de seu papel central nas ICTs, segundo os dados descritos no relatório FOMICT, observa-se que 80,9% das ICTs públicas e 53,1% das privadas possuem NIT implementados, ou seja, 19,1% das ICTs públicas ainda não estabeleceram seus NITs.

O sucesso da política de inovação está diretamente ligado à eficácia do Núcleo de Inovação Tecnológica da ICT, pois a função principal do NIT é justamente dar suporte à administração e garantir o bom progresso da política[20].

A importância desses núcleos reside na sua capacidade de atuar como ponte entre a pesquisa acadêmica e o setor produtivo, facilitando a transformação de conhecimento científico em produtos, processos e serviços inovadores que beneficiam a sociedade. Entender as dimensões operacionais dos NITs oferece uma base para apreciar o panorama legal que molda suas atividades. A partir dos laços estreitados por meio dos NITs, as universidades foram incentivadas a estabelecer conexões mais próximas com o setor produtivo, aperfeiçoando, assim, a capacitação profissional e reduzindo a endogamia da academia, que resiste em relacionar-se com empresas. No entanto, em alguns casos, a gestão da propriedade intelectual das universidades tornou-se reativa, devido à falta de visão estratégica e experiência[21].

---

[18] VILHA, Anapatrícia Morales *et al*. Política de inovação de instituições públicas de ciência, tecnologia e inovação: o passo a passo para processos de formulação. **Revista de Gestão e Análise**, Fortaleza, v. 9, n. 3, p. 22-34, set./dez. 2020. Disponível em: https://unichristus.emnuvens.com.br/gestao/article/view/3050. Acesso em: 1 abr. 2026.

[19] MACHADO, Hilka Pelizza Vier; SARTORI, Rejane; CRUBELLATE, João Marcelo. Institucionalização de núcleos de inovação tecnológica em instituições de ciência e tecnologia da região sul do Brasil. **REAd – Revista Eletrônica de Administração**, Porto Alegre, v. 23, n. 3, p. 5-31, set./dez. 2017, p. 7.

[20] BRASIL, 2019, *op. cit*.

[21] SANTOS, Luan Tolentino dos; SANTOS, Glícia Vieira dos. Gestão estratégica da propriedade intelectual em núcleos de inovação tecnológica de universidades públicas brasileiras: desafios e oportunidades. **Revista Tecnológica da Fatec Americana**, Americana, v. 6, n. 2, p. 1-19, abr./set. 2017, p. 1.

Os NITs têm tarefas mais complexas a serem executadas para viabilizar as políticas institucionais de inovação do que as previstas pela legislação vigente[22]. Inicialmente, os NITs foram concebidos para controle e gestão, mas essas funções não são suficientes para cumprir suas atribuições com qualidade.

Lotufo[23] descreve os Núcleos de Inovação Tecnológica (NITs) sob três perspectivas distintas: legal, administrativa e empresarial. A dimensão legal, primeira abordagem, é centrada na regulamentação e formalização das atividades, apoiada pelo setor jurídico da ICT, responsável por avaliar a viabilidade do registro de patentes, bem como por estabelecer convênios com cláusulas específicas, parcerias de colaboração, entre outros. Esta área deveria ser composta principalmente por advogados e especialistas em propriedade intelectual, pessoas qualificadas para interpretar e propor contratos.

Além de lidar com aspectos legais e regulatórios, os NITs também desempenham um papel administrativo fundamental, configurando a segunda dimensão, a qual trata do gerenciamento dos processos de aprovação e encaminhamento necessários para efetivar os convênios e contratos entre as ICTs e as empresas. Enquanto as dimensões legal e administrativa garantem a conformidade com a legislação e a organização, a perspectiva empresarial dos NITs concentra-se em catalisar a conversão de inovações acadêmicas em aplicações comerciais viáveis, desenvolvendo negócios a partir dos resultados de pesquisas. Essa dimensão envolve profissionais que compreendem a dinâmica da inovação, conhecem o mercado e os desafios relacionados à criação e crescimento de empresas baseadas em conhecimento, considerando tanto a perspectiva acadêmica quanto empresarial.

Scott[24] estabelece três pilares na teoria institucional contemporânea: os pilares regulativo, normativo e cognitivo. O pilar regulativo diz respeito às leis, regulamentos e políticas que formalizam comportamentos por meio de regras coercitivas, que para o NIT incluem a legislação brasileira sobre inovação tecnológica, que define os direitos e responsabilidades dos atores envolvidos e regula as parcerias entre ICTs e o setor privado, bem como o cumprimento da própria política de inovação de sua instituição e, também, de normas técnicas e de segurança.

O pilar normativo envolve as normas, valores e expectativas que definem metas apropriadas de desempenho e comportamento, podendo incluir padrões éticos na pesquisa, normas de colaboração entre pesquisadores e empresas e expectativas sobre como os resultados da pesquisa devem ser transformados em inovações práticas. Além disso, reflete a pressão social e cultural que influencia as práticas e estratégias de inovação.

---

[22] ALVES ; AMARANTE SEGUNDO ; SAMPAIO, *op. cit.*, p. 690.

[23] LOTUFO, Roberto de Alencar. A Institucionalização de Núcleos de Inovação Tecnológica e a Experiência da Unicamp. In: SANTOS, Marli Elizabeth Ritter; TOLEDO, Patrícia Tavares Magalhães de; LOTUFO, Roberto de Alencar (orgs). **Transferência de Tecnologia**: estratégias para a estruturação e gestão de Núcleos de Inovação Tecnológica. Campinas, SP: Komedi, 2009, p. 55.

[24] SCOTT, William Richard. **Institutions and Organizations**. London: Sage, 1995.

Por fim, o pilar cultural-cognitivo abrange os modelos mentais que membros da organização compartilham e que moldam suas percepções e interpretações da realidade, incluindo a própria cultura enraizada na instituição. No contexto de um NIT, esse pilar se manifesta na forma como novas tecnologias são percebidas, na disposição para adotar novas abordagens ou tecnologias, e na maneira como o conhecimento e a inovação são valorizados na instituição.

2.2.2.1. *Modelos de Organização e Gestão dos Núcleos de Inovação Tecnológica*

Os modelos dos NITs adotados por ICTs brasileiras variam bastante. Essa diversidade se deve à estrutura de cada ICT, aos recursos disponíveis, às áreas de atuação da instituição e também ao seu contexto regional, sendo adaptáveis às realidades das instituições.

Alguns NITs foram estruturados como unidades autônomas, com equipes dedicadas exclusivamente à gestão da inovação da instituição. Outros possuem personalidade jurídica própria, e também existem os que funcionam de forma integrada a outras unidades administrativas da instituição, compartilhando com elas seus recursos e funcionários.

Tem-se na Agência de Inovação da Universidade Estadual de Campinas (INOVA Unicamp) um exemplo de NIT organizado como unidade autônoma, que, embora não detenha personalidade jurídica própria, tem uma equipe dedicada exclusivamente à gestão da inovação, atuando na proteção da propriedade intelectual, na transferência de tecnologia e no apoio ao empreendedorismo. A INOVA Unicamp é reconhecida por suas parcerias com empresas e pelo apoio a *startups*, e vem contribuindo significativamente para a criação de empresas de base tecnológica na região de Campinas, segundo informações disponíveis no site da INOVA Unicamp[25].

Também se observa a existência de NITs que adotam abordagens regionais, integrando diversas ICTs e colaborando com diversas instituições e outros órgãos governamentais com o objetivo de fomentar a inovação em áreas específicas do país. O NIT-NE é um exemplo desse formato, sendo composto por uma rede de núcleos de inovação tecnológica das universidades federais do Nordeste. Essa iniciativa colaborativa busca fomentar a inovação regional em determinadas áreas do país, bem como promover a integração de múltiplas instituições e órgãos governamentais para apoiar e facilitar o desenvolvimento tecnológico e a transferência de conhecimento[26].

[25] INOVA UNICAMP. **Agência de Inovação Inova Unicamp**. 2024. Disponível em: https://www.inova.unicamp.br/. Acesso em: 2 jun. 2024.

[26] FERNANDES, Cleverton Rodrigues; ATHAYDE FILHO, Petrônio Filgueiras de; CORNÉLIO, Melânia Lopes. A Gestão da Inovação na Universidade Federal da Paraíba. In: ANDRADE, Herlandí de Souza; TORKOMIAN, Ana Lúcia Vitale; CHAGAS JÚNIOR, Milton de Freitas (org.). **Boas práticas de gestão em núcleos de inovação tecnológica**: experiências inovadoras. Jundiaí: Edições Brasil, 2018, p. 58.

Além dos exemplos citados, a Portaria MCTI n. 251, de 12 de março de 2014[27], previu a possibilidade de serem formados "Arranjos de Núcleos de Inovação Tecnológica", que são estruturas organizacionais e colaborativas destinadas a otimizar e coordenar as atividades de inovação, gestão da propriedade intelectual e transferência de tecnologia das ICTs associadas. A finalidade desses arranjos é otimizar e compartilhar recursos, disseminar boas práticas de gestão e facilitar a aplicação da Lei da Inovação e da Política de Inovação das ICTs do MCTI.

Os Arranjos de NITs são compostos pelas ICTs integrantes da estrutura do MCTI, bem como por entidades vinculadas ou supervisionadas pelo Ministério e por ele indicadas. Outras ICTs externas ao MCTI podem se associar aos Arranjos de NITs mediante parecer favorável do Comitê Gestor da Inovação, desde que sua política de inovação esteja em consonância com a do Arranjo de NIT[28].

Exemplos desses Arranjos de NITs são aqueles estabelecidos em 2015, como o NIT Rio, formado por sete ICTs cariocas; o NIT Mantiqueira, formado por seis ICTs de São Paulo e Minas Gerais; o NIT Amazônia oriental, formado por uma ICT paraense; e o NIT Amazônia Ocidental, formado por duas ICTs amazonenses[29].

Os NITs diferem não apenas nesse aspecto, mas também existem ICTs que optam por centralizar seus NITs ou manter um para cada unidade, como é o caso da Agência Paulista de Tecnologia dos Agronegócios (APTA). A APTA é formada por seis institutos: Agronômico, Biológico, de Economia Agrícola, de Pesca, de Tecnologia de Alimentos, e de Zootecnia, além da APTA Regional. Diferentemente da maioria das ICTs, que publicam uma única política de inovação e possuem um NIT centralizado para gestão das demandas de todas as suas unidades, como é o caso da Unicamp e da Universidade Federal de Minas Gerais (UFMG), a APTA publicou sua política e, cada uma de suas unidades também a publicou. Embora com o mesmo conteúdo, cada uma possui o próprio NIT e a própria política. A APTA é um modelo *sui generis*, pois, ao mesmo tempo que manteve uma centralização do conteúdo da política, que é único, ela permite que cada uma de suas ICTs tenha seu NIT e faça a gestão de seus processos.

Esses diferentes modelos refletem a diversidade e a flexibilidade das ICTs brasileiras em responder às demandas locais e setoriais, na tentativa de promover um ecossistema de inovação robusto e dinâmico. Porém, não resta dúvida de que as ICTs precisam assumir e consolidar um papel proativo na gestão da

[27] BRASIL. Portaria MCTI nº 251, de 12.03.2014. Estabelece as Diretrizes para a Gestão da Política de Inovação das Unidades de Pesquisa do Ministério da Ciência, Tecnologia e Inovação – MCTI. **Diário Oficial da União**, Brasília, 13 mar. 2014.

[28] *Ibid*.

[29] BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. **Portaria nº 22, de 30 de janeiro de 2015**. Diário Oficial da União, Brasília, DF, 30 jan. 2015. Seção 1, p. 123-124.

inovação para transformar os avanços do conhecimento em resultados apropriados para a base industrial[30].

É importante refletir que, devido à necessidade de publicar suas políticas rapidamente, em razão da entrada em vigor do Marco Legal da Inovação, a maioria das ICTs não teve tempo suficiente de trabalhar a política de modo a adaptá-la ao perfil específico de cada instituição. Isso resultou em um conjunto de políticas genéricas que seguem a mesma estrutura que foi estabelecida pela lei, embora o próprio arcabouço legal permita uma série de possibilidades a serem exploradas. A diversidade de políticas que poderiam ser criadas, considerando a multiplicidade de ICTs com perfis diferentes que o Brasil possui, possibilitaria grande evolução em nosso ambiente de inovação, abrindo caminhos ainda não explorados.

O sucesso no processo de transferência de tecnologia depende fortemente das pessoas envolvidas. Portanto, para que um NIT, que é o escritório de transferência de tecnologia da ICT, tenha êxito, é essencial contar com uma equipe bem estruturada, tanto em número quanto em qualificação[31]. As pessoas que exercem suas funções nos NITs devem possuir habilidades diferenciadas que não constam nas atuais carreiras das ICTs públicas, o que não se observa, na maioria dos casos, onde os NITs são estabelecidos com servidores em acúmulo de função e sem experiência prévia.

Torkomian[32] já apontava em seu estudo que os NITs eram formados por um número reduzido de servidores e que havia falta de dotação de vagas em concursos específicas para esse fim. Esse panorama permanece ao observarmos os dados constantes no relatório FORMICT, que descreve que em apenas 45,6% dos NITs os recursos humanos são servidores com dedicação integral, evidenciando que na maioria dos NITs, os servidores não são exclusivamente dedicados às suas funções. No mesmo relatório é descrito que 19,1% das ICTs públicas ainda não implementaram núcleos de inovação tecnológica, apesar da obrigatoriedade estabelecida na legislação. Ainda, de acordo com o relatório, a distribuição de profissionais atuando nos NITs é a seguinte: 17 NIT têm apenas um profissional, 206 NIT têm de dois a 10 profissionais, 29 NIT têm de 11 a 20 profissionais, oito NIT têm de

[30] BRANDÃO NETO, Nestor; LEITE, Breno Ricardo de Araújo; MELO, Francisco Cristovão Lourenço de. Model for strategic management of technological innovation in science and technology institutions in the Brazilian aerospace sector: a proposal**. Journal of Aerospace Technology and Management**, São José dos Campos, v. 15, e2123, 2023, p. 1.

[31] SANTOS, Marli Elizabeth Ritter dos. Boas práticas de gestão em Núcleos de Inovação Tecnológica (NIT). In: SANTOS, Marli Elizabeth Ritter dos; TOLEDO, Patricia Tavares Magalhães de; LOTUFO, Roberto de Alencar (orgs.). **Transferência de tecnologia**: estratégias para a estruturação e gestão de Núcleos de Inovação Tecnológica. Campinas: Komedi, 2009, p. 98-99.

[32] TORKOMIAN, Ana Lúcia Vitale. Panorama dos Núcleos de Inovação Tecnológica no Brasil. In: SANTOS, Marli Elizabeth Ritter dos; TOLEDO, Patricia Tavares Magalhães de; LOTUFO, Roberto de Alencar (orgs.). **Transferência de tecnologia**: estratégias para a estruturação e gestão de Núcleos de Inovação Tecnológica. Campinas: Komedi, 2009, p. 29.

21 a 30 profissionais, seis NIT têm 31 a 50 profissionais e quatro NIT contam com mais de 50 profissionais[33].

Seria necessário o empenho do poder público e da gestão das ICTs na formação de equipes responsáveis pela direção e execução dos trabalhos do NIT. Embora a legislação forneça um quadro estrutural, a aplicação prática em diferentes ICTs revela desafios complexos, como mostram os estudos recentes sobre a institucionalização dos NITs no sul do Brasil.

Para ilustrar esses desafios, uma análise mais detalhada dos NITs nas universidades do sul do país destaca problemas significativos de autonomia e cultura empreendedora. Em seu estudo, Machado, Sartori e Crubellate[34] analisaram ICTs do sul do país, e seus resultados mostraram dificuldades significativas na institucionalização dos NITs, devido principalmente à ausência de uma cultura empreendedora, à pouca autonomia e aos entraves burocráticos na contratação de pessoal. As universidades não possuíam um histórico de competitividade ou de relações com o setor privado. A pesquisa conclui que os NITs estão na fase de habitualização, com variações no processo de institucionalização dependendo da instituição, e que há um grau de mimetismo nas ações dos NITs, sugerindo que as práticas ocorrem de maneira a buscar conformidade com os três pilares da teoria institucional de Scott[35], que podem explicar a orientação que os NITs estão seguindo conforme evoluem.

Em muitas instituições, os NITs são vistos como facilitadores da inovação, como promotores da proteção da propriedade intelectual e incentivadores de colaborações com empresas e outras instituições de pesquisa. Essa visão positiva ocorre em instituições onde os NITs são bem estruturados e possuem recursos adequados, demonstrando mais autonomia em seus processos, como nos casos da Unicamp, que estruturou a Inova Unicamp, e da UFMG, que tem a Coordenadoria de Transferência e Inovação Tecnológica (CTIT)[36]. Essa autonomia garante maior eficiência na gestão dos projetos de inovação e na captação de recursos externos. Além disso, na UFMG, as atribuições do NIT são centralizadas na fundação de apoio, a qual mantém a CTIT, o que confere ainda mais flexibilidade em comparação aos demais modelos.

[33] BRASIL, **Decreto nº 9.283, de 7 de fevereiro de 2018**, *op. cit*.

[34] MACHADO; SARTORI; CRUBELLATE, *op. cit*.

[35] SCOTT, *op. cit*.

[36] SANTOS, Elisama Campelo *et al*. Análise comparativa das etapas do processo de transferência de tecnologia em ICTs brasileiras. **Observatorio de la Economía Latinoamericana**, v. 21, n. 5, p. 2453-2470, 2023, p. 2467.

Essa diversidade de perfis dos NITs brasileiros é de extrema relevância, uma vez que permite que as ICTs se adequem às suas realidades regionais e institucionais, aumentando a sua capacidade de adaptação ao ecossistema de inovação.

A relevância do papel dos NITs na construção da cultura de inovação do país é indiscutível. Porém, para que sejam eficazes em suas atribuições, é necessário o apoio de políticas públicas de inovação, somente assim poderão conduzir os processos de inovação adequadamente. A comunidade científica considera de suma importância que haja a profissionalização dos NITs, pois isso permitirá que as ações para promoção da inovação sejam planejadas e direcionadas de maneira mais eficiente, o que aumenta as chances de sucesso das pesquisas realizadas[37].

Porém, inicialmente, é fundamental que haja o reconhecimento da importância dos NITs por parte dos próprios dirigentes das ICTs públicas. A alta gestão da instituição precisa conhecer e valorizar seus núcleos. Conforme esses núcleos forem sendo profissionalizados, espera-se não apenas uma melhoria na gestão da inovação, mas também um aumento substancial na eficácia com que essas instituições contribuem para o ecossistema de inovação do país. Essa transformação pode resultar em uma melhor transferência de conhecimento para o setor produtivo, intensificando a comercialização de inovações e fortalecendo as parcerias estratégicas com o setor privado. Além disso, com equipes mais especializadas e preparadas, os NITs poderão aprimorar as políticas de inovação, influenciando positivamente o ambiente de inovação, uma vez que, com a profissionalização e a eficácia operacional, seria possível acelerar significativamente o progresso científico e tecnológico nacional.

2.3. *Análise dos dados obtidos por meio do questionário*

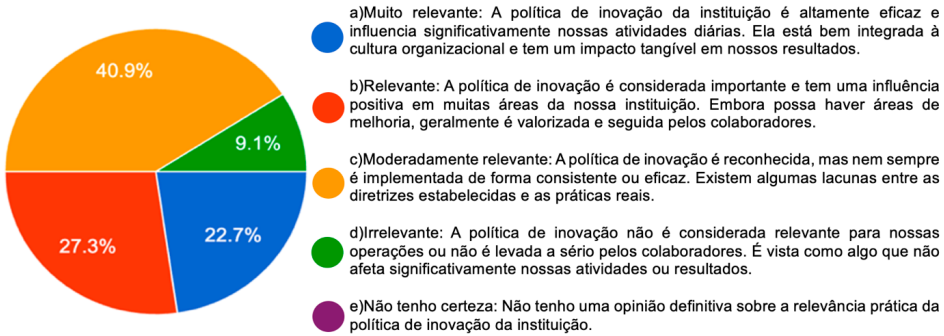
Após o encerramento do prazo para as respostas on-line, foi possível obter uma amostra de 22 pesquisadores. Na sequência, analisaremos as respostas das quatro questões apresentadas em sequência.

Os resultados obtidos na primeira pergunta demonstram que a maioria dos respondentes considera a política de inovação de suas instituições de moderadamente relevante a muito relevante. Isso indica que de maneira geral há uma percepção positiva, embora haja espaço para aumentar a eficácia e a integração dessas políticas na prática diária, conforme a Figura 2:

I) O quão relevante, na prática, é a política de inovação da sua instituição?

[37] NASCIMENTO, Jesusa Vania Bagundes; BELÉM, Adelina do Socorro Serrão; COSTA, Robson Antônio Tavares. Proposta de Política Pública para Fortalecimento dos Núcleos de Inovação Tecnológica no Amapá. **Cadernos de Prospecção**, Salvador, v. 12, n. 5, p. 1244-1256, dez. 2019, p. 1252.

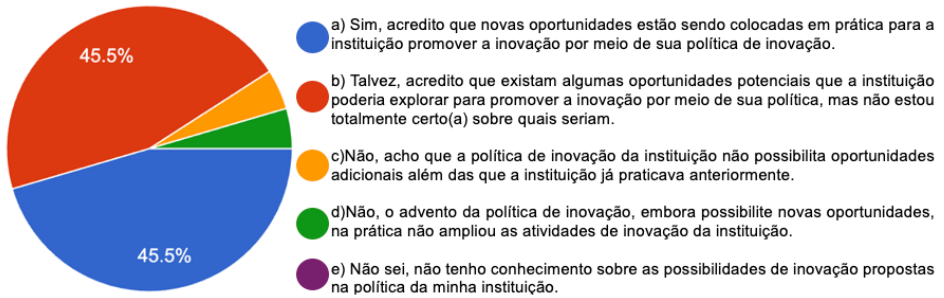
Figura 2.
Gráfico das respostas da primeira questão.



Já na pergunta 2, nota-se uma percepção mista sobre as oportunidades adicionais de inovação por meio da política de propriedade intelectual. Embora a maioria dos respondentes veja potencial, muitos não têm certeza ou desconhecem as especificidades dessas oportunidades, sugerindo que é necessário uma maior divulgação interna e o esclarecimento sobre essas políticas, como seminários sobre o tema.

II) Você acha que há oportunidades adicionais para a instituição promover a inovação por meio de sua política de propriedade intelectual?

Figura 3.
Gráfico das respostas da segunda questão.

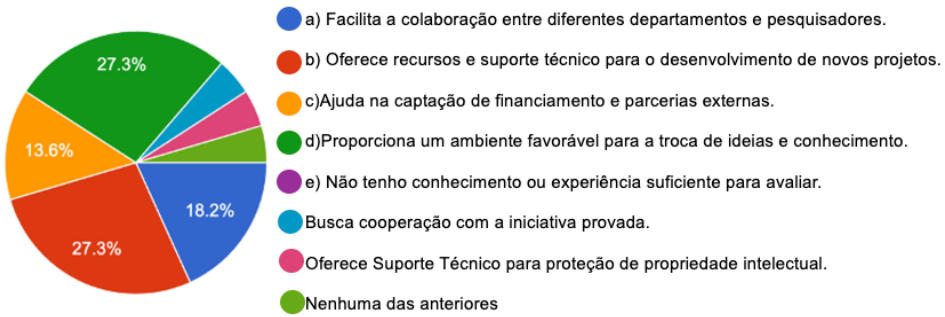


Na pergunta 3, a única que possuía uma opção aberta, fica evidenciado que, embora haja reconhecimento da importância do NIT, uma parte significativa dos respondentes não está familiarizada ou não percebe um impacto significativo do núcleo em novos projetos. Além disso, uma parte dos pesquisadores enxerga o NIT apenas

como suporte no processo de obtenção de patentes. Isso sugere que os NITs poderiam melhorar sua visibilidade e eficácia dentro das instituições. Da mesma forma que na questão 2, a criação de informativos sobre o tema poderia tornar mais claras as possibilidades implementadas pelos NITs para os pesquisadores.

III) O Núcleo de Inovação Tecnológica da sua instituição contribui para o fomento de novos projetos?

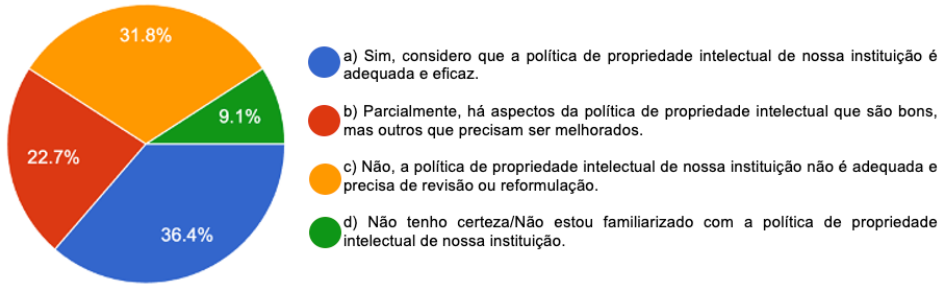
Figura 4.
Gráfico da terceira questão.



Por fim, na quarta questão, observa-se que a adequação das políticas de propriedade intelectual é vista de forma mista. Embora uma parte significativa considere essas políticas adequadas, uma porção quase igual acredita que melhorias são necessárias, indicando áreas específicas onde ajustes podem ser realizados. Isso levanta algumas possibilidades, como a hipótese de que haja um descontentamento por parte dos pesquisadores no que tange à divisão da titularidade das patentes.

IV) A política de propriedade intelectual da minha instituição é adequada?

Figura 5.
Gráfico da quarta questão.



Os dados demonstraram que há uma percepção geral positiva sobre as políticas de inovação e propriedade intelectual. Os resultados indicaram que a maioria dos pesquisadores considera a política de inovação de suas instituições de moderadamente relevante a relevante. Também há uma percepção de que existem oportunidades para promover a inovação por meio da política de propriedade intelectual, embora muitos respondentes não estejam seguros sobre quais seriam estas oportunidades, pois há áreas que necessitam de melhorias e maior clareza. As respostas destacam a necessidade de melhor comunicação e integração dessas políticas nas atividades diárias dos pesquisadores.

O Núcleo de Inovação Tecnológica é percebido como tendo um papel fundamental em alguns casos, mas há uma necessidade de maior familiaridade e clareza sobre suas funções. A política de propriedade intelectual da instituição é considerada adequada por uma parte significativa dos respondentes, mas também há uma percepção de que melhorias são necessárias.

Esses resultados levantam algumas hipóteses sobre o motivo dessa percepção entre os respondentes. Uma delas é a falta de especificidade das políticas das ICTs. Conforme discutido anteriormente, a maioria delas não teve tempo adequado para desenvolver uma política adaptada às particularidades das instituições, resultando em políticas genéricas, muito parecidas entre si. Os pesquisadores podem sentir que esse documento é apenas uma formalidade, sem aplicabilidade prática.

Outra hipótese é que os pesquisadores das ICTs talvez enxerguem a política de inovação e os NITs apenas como uma forma de facilitar seus processos de proteção da propriedade intelectual, atuando como auxiliares nos trâmites de geração de patentes de seus projetos. Porém, as possibilidades de parcerias com empresas privadas, o compartilhamento de instalações e o estabelecimento de incubadoras de empresas de base tecnológica (*spin-offs* universitários), são menos aproveitados e mais obscuros para a maioria dos pesquisadores. Isso se deve a uma cultura arcaica, segundo a qual as instituições públicas não estabelecem parcerias com o setor privado, ou quando o fazem é um processo complexo e demorado, e de que os servidores públicos seguem regime de exclusividade a seus cargos. Essas possibilidades previstas nas políticas deveriam ser melhor aproveitadas. As universidades, principalmente, veem-se apenas como um ambiente de propagação de conhecimento, mas com o Marco Legal da Inovação, já seria hora de experimentar novos caminhos como agentes de inovação e desenvolvimento econômico. Este estudo não contemplou esses aspectos, mas eles poderiam ser investigados em pesquisas futuras.

Alguns caminhos podem ser tomados pelas ICTs, como:

- Melhorar a comunicação: aumentar a transparência e comunicação sobre as políticas de inovação e propriedade intelectual, destacando suas oportunidades e benefícios. Isso pode ser feito realizando seminários sobre o tema, com apresentação de casos de sucesso, bem como pelo aumento da visibilidade dos Núcleos de Inovação Tecnológica, divulgando suas funções e como eles podem contribuir com os pesquisadores na elaboração e gestão de novos projetos.

- Aprimorar a integração das políticas: trabalhar para que as políticas de inovação sejam mais integradas nas atividades diárias dos pesquisadores, aumentando sua relevância na prática profissional.
- Fortalecer os NITs: reforçar os NITs com recursos humanos qualificados e em número adequado. A falta de servidores treinados e em dedicação exclusiva à promoção das políticas institucionais é, certamente, um dos principais pontos fracos das ICTs.
- Revisar as políticas de propriedade intelectual: realizar uma revisão dessas políticas, ouvindo os pesquisadores sobre o tema e solicitando a validação nas novas propostas. Dessa forma, será possível identificar e corrigir aspectos que necessitam de melhorias, aumentando sua adequação e eficácia.
- Adequar a política a realidade da instituição: a maioria das políticas de inovação é genérica e limita-se a copiar a lei com algumas alterações. Uma política construída sob medida para as peculiaridades de cada ICT seria muito mais eficaz.

3. CONCLUSÃO

As políticas de inovação são as pedras fundamentais da atuação das ICTs, pois são elas que moldam as direções estratégicas e a eficácia operacional das instituições. A Lei nº 10.973/2004 e a Lei nº 13.243/2016 estabeleceram a obrigatoriedade dessas políticas para as ICTs, que devem ser implementadas com diretrizes claras e bem estruturadas[38]. Embora, segundo os dados coletados em 2018 pelo FORMICT, mais de 70% das instituições públicas já tenham publicado suas políticas de inovação, e, possivelmente, este número seja ainda maior atualmente, não há informação de quantas destas políticas estão, de fato, sendo adequadamente efetivadas no dia a dia das ICTs.

Os dados do questionário caminham na mesma direção da análise bibliográfica, ao mostrarem que a maioria dos respondentes considera as políticas de inovação de moderadamente a muito relevantes. No entanto, a percepção de irrelevância por uma minoria (9,09%) aponta para desafios na implementação eficaz dessas políticas, como a burocracia e a escassez de recursos humanos e orçamentários.

A literatura analisada é unânime em afirmar a importância da interação entre a universidade, a indústria e o governo para a promoção da inovação, nesse diapasão as políticas de inovação e de propriedade intelectual das ICTs são cruciais para proteger as inovações e incentivar colaborações estratégicas. Os dados obtidos mostram que a maioria dos respondentes acredita que a política de inovação gera

[38] Brasil, **Lei nº 13.243, de 11 de janeiro de 2016**, *op. cit*.

oportunidades adicionais para as atividades das ICTs, o que está alinhado com a teoria da hélice tríplice de Etzkowitz e Leydesdorff[39]; no entanto, a expressiva porcentagem de incerteza (22,73%) indica a necessidade de maior clareza e comunicação sobre as políticas de inovação no ambiente interno das ICTs. Um estudo realizado ano anterior com 49 ICTs concluiu que boa parte delas não acredita possuir uma comunicação interna eficaz voltada a dar suporte ao processo de construção de cultura da inovação[40].

Além disso, a obrigatoriedade da construção da política trazida pela Lei de Inovação levou as ICTs a se apressarem em suas edições, resultando em políticas muito genéricas, que acabaram sendo reproduzidas entre as instituições e não ousaram fugir da fórmula dada, como um protocolo repetido a exaustão. Isso parece um contrassenso quando pensamos que é o estabelecimento de regras que vão guiar os caminhos da inovação das ICTs.

Os NITs são os responsáveis pela gestão das políticas de inovação, facilitando a transferência de tecnologia e a proteção da propriedade intelectual[41]. Contudo, a implementação dos NITs ainda enfrenta muitos desafios, como a falta de autonomia e de recursos. A percepção de que os NITs são fundamentais para novos projetos por uma minoria (22,73%) e a incerteza expressa por alguns respondentes (9,09%) refletem os desafios mencionados na literatura. Isso sugere que os NITs precisam melhorar seu protagonismo dentro das ICTs.

Uma maneira de iniciar esse processo de fortalecimento é aumentar sua visibilidade, inclusive perante a própria gestão institucional da ICT, o que pode facilitar a obtenção de recursos humanos. Com mais servidores, o núcleo torna-se mais eficiente, permitindo o início de um círculo virtuoso, no qual o NIT poderá de destacar progressivamente, sendo reconhecido pela instituição e cumprindo seu papel no ecossistema de inovação.

A eficácia das políticas de propriedade intelectual depende de diretrizes claras e suporte institucional. O FORMICT relata que muitas ICTs ainda não implementaram adequadamente essas políticas. A percepção mista sobre a adequação das políticas de propriedade intelectual reflete os desafios mencionados no referencial teórico. A necessidade de revisão e melhoria das políticas é evidente, com uma parcela significativa dos respondentes apontando inadequação (31,82%). Um exemplo que poderia ser seguido é o da UFABC, que submeteu sua proposta de política de inovação aos setores principais da instituição e somente a implementou após discussões

[39] ETZKOWITZ, Henry; LEYDESDORFF, Loet. The dynamics of innovation: from national systems and "Mode 2" to a triple helix of university-industry-government relations. **Research Policy**, Amsterdam, v. 29, n. 2, p. 109-123, Feb. 2000.

[40] MOURA FILHO, Silvio Liberato de, *et al*. Ecossistema de inovação: métricas para ICTs brasileiras. **Revista de Gestão e Secretariado**, v. 14, n. 7, 11589-11606, 2023.

[41] MACHADO; SARTORI; CRUBELLATE, *op. cit*.

com usuários desses instrumentos, o que permitiu uma visão das demandas e processos da universidade que inicialmente não haviam sido observados[42].

Os dados do questionário confirmam várias das conclusões presentes no referencial teórico. A importância das políticas de inovação e dos NITs é reconhecida, mas a eficácia dessas políticas e a clareza sobre as oportunidades adicionais de inovação ainda precisam ser aprimoradas. A revisão das políticas de propriedade intelectual e a melhoria da comunicação interna são passos essenciais para aumentar a eficácia e a integração dessas políticas nas ICTs.

Para superar esses desafios, é essencial que as ICTs adotem uma abordagem mais proativa na gestão da inovação. É necessário desenvolver uma visão estratégica, adequando suas políticas de forma mais individualizada, seguindo a legislação, mas adaptada à missão e às características da instituição, ouvindo seus pesquisadores e investindo no aprimoramento da comunicação interna sobre as oportunidades e benefícios trazidos por essas políticas. Além disso, é imprescindível que a gestão das ICTs estruture seus NITs, alocando recursos e equipes qualificadas em dedicação exclusiva. Dessa forma, as ICTs poderão assumir seu papel como protagonistas da inovação no país.

4. AGRADECIMENTOS

Gostaria de expressar minha gratidão a todos que gentilmente dedicaram seu tempo para responder ao questionário, contribuindo de maneira essencial para o desenvolvimento deste trabalho.

Agradeço à minha família, cujo apoio e encorajamento contínuo foram fundamentais ao longo desta jornada acadêmica.

Em especial, dirijo meus sinceros agradecimentos ao meu orientador, Dr. Rafael Carvalho de Fassio. Sua orientação perspicaz, atenção dedicada e, sobretudo, paciência inabalável, foram cruciais para o meu progresso e sucesso. Suas valiosas dicas e orientações foram verdadeiramente indispensáveis e inspiradoras.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, Vivian Costa; AMARANTE SEGUNDO, Gesil Sampaio; SAMPAIO, Renelson Ribeiro. Reflexões sobre as competências dos núcleos de inovação tecnológica. **Cadernos de Prospecção**, Salvador, v. 8, n. 4, p. 688-696, out./dez. 2015.BARDIN, Laurence. **Análise de conteúdo**. Lisboa: Edições 70, 2011.

BRANDÃO NETO, Nestor; LEITE, Breno Ricardo de Araújo; MELO, Francisco Cristovão Lourenço de. Model for strategic management of technological innovation in science and technology institutions in the Brazilian aerospace sector: a proposal**. Journal of Aerospace Technology and Management**, São José dos Campos, v. 15, e2123, 2023.

[42] VILHA *et al*., *op. cit.*, p. 31.

BRASIL. Decreto n. 9.283, de 7 de fevereiro de 2018. Regulamenta a Lei nº 10.973, de 2 de dezembro de 2004, e a Lei nº 13.243, de 11 de janeiro de 2016, para dispor sobre estímulos ao desenvolvimento científico, à pesquisa, à capacitação científica e tecnológica e à inovação. **Diário Oficial da União**, Brasília, DF, 8 fev. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9283.htm. Acesso em: 1 abr. 2026.

BRASIL. Decreto n. 10.534, de 28 de outubro de 2020. Institui a Política Nacional de Inovação e dispõe sobre a sua governança. **Diário Oficial da União**, Brasília, DF, 28 out. 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10534.htm. Acesso em: 1 abr. 2026.

BRASIL. Lei nº 10.973, de 2 de dezembro de 2004. Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências. **Diário Oficial da União**, Brasília, DF, 3 dez. 2004. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/l10.973.htm. Acesso em: 1 abr. 2026.

BRASIL. Lei nº 13.243, de 11 de janeiro de 2016. Dispõe sobre o estímulo ao desenvolvimento científico, à pesquisa, à capacitação científica e tecnológica e à inovação. **Diário Oficial da União**, Brasília, DF, 12 jan. 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13243.htm. Acesso em: 1 abr. 2026.

BRASIL. Portaria MCT nº 118, de 23.02.2010. Aprova o novo formulário para que as Instituições Científicas e Tecnológicas – ICT prestem ao Ministério da Ciência e Tecnologia - MCT, através do Ministério ou do Órgão ao qual a Instituição seja subordinada ou vinculada, […]. **Diário Oficial da União**, Brasília, 23 fev. 2010.

BRASIL. Portaria MCTI nº 251, de 12.03.2014. Estabelece as Diretrizes para a Gestão da Política de Inovação das Unidades de Pesquisa do Ministério da Ciência, Tecnologia e Inovação – MCTI. **Diário Oficial da União**, Brasília, 13 mar. 2014.

BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. Portaria n. 22, de 30 de janeiro de 2015. **Diário Oficial da União**, Brasília, DF, 30 jan. 2015. Seção 1, p. 123-124.

BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. Secretaria de Empreendedorismo e Inovação. **Guia de orientação para elaboração da política de inovação nas ICTs**. Brasília, DF: MCTIC, 2019. Disponível em: https://www.fortec.org.br/orientacao-politicas-icts. Acesso em: 1 abr. 2026.

MOURA FILHO, Silvio Liberato de, *et al*. Ecossistema de inovação: métricas para ICTs brasileiras. **Revista de Gestão e Secretariado**, v. 14, n. 7, 11589-11606, 2023.

ETZKOWITZ, Henry; LEYDESDORFF, Loet. The dynamics of innovation: from national systems and "Mode 2" to a triple helix of university-industry-government relations. **Research Policy**, Amsterdam, v. 29, n. 2, p. 109-123, Feb. 2000.

FERNANDES, Cleverton Rodrigues; ATHAYDE FILHO, Petrônio Filgueiras de; CORNÉLIO, Melânia Lopes. A Gestão da Inovação na Universidade Federal da Paraíba. In: ANDRADE, Herlandí de Souza; TORKOMIAN, Ana Lúcia Vitale; CHAGAS JÚNIOR, Milton de Freitas (org.). **Boas práticas de gestão em núcleos de inovação tecnológica**: experiências inovadoras. Jundiaí: Edições Brasil, 2018, p. 55-74.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. Barueri: Atlas, 2008.

INOVA UNICAMP. **Agência de Inovação Inova Unicamp**. 2024. Disponível em: https://www.inova.unicamp.br/. Acesso em: 2 jun. 2024.

LOTUFO, Roberto de Alencar. A Institucionalização de Núcleos de Inovação Tecnológica e a Experiência da Unicamp. In: SANTOS, Marli Elizabeth Ritter; TOLEDO, Patrícia Tavares Magalhães de; LOTUFO, Roberto de Alencar (orgs). **Transferência de Tecnologia**: estratégias para a estruturação e gestão de Núcleos de Inovação Tecnológica. Campinas, SP: Komedi, 2009.

MACHADO, Hilka Pelizza Vier; SARTORI, Rejane; CRUBELLATE, João Marcelo. Institucionalização de núcleos de inovação tecnológica em instituições de ciência e tecnologia da região sul do Brasil. **REAd – Revista Eletrônica de Administração**, Porto Alegre, v. 23, n. 3, p. 5-31, set./dez. 2017.

NASCIMENTO, Jesusa Vania Bagundes; BELÉM, Adelina do Socorro Serrão; COSTA, Robson Antônio Tavares. Proposta de Política Pública para Fortalecimento dos Núcleos de Inovação Tecnológica no Amapá. **Cadernos de Prospecção**, Salvador, v. 12, n. 5, p. 1244-1256, dez. 2019.

PEDRO, Edilson da Silva. A Política Nacional de Inovação e as Instituições de Ciência e Tecnologia (ICTs). **Cadernos de Prospecção**, Salvador, v. 14, n. 1, p. 1-4, mar. 2021.

PIRES, Edilson Araújo; SILVA, Karoline Greice Viana Cardoso da. A atuação dos núcleos de inovação tecnológica nas universidades: o caso brasileiro. **Revista de Gestão e Secretariado**, São Paulo, v. 14, n. 9, p. 1596, 2023. Disponível em: https://ojs.revistagesec.org.br/secretariado/article/download/2653/1596. Acesso em: 1 abr. 2026.

SANTOS, Luan Tolentino dos; SANTOS, Glícia Vieira dos. Gestão estratégica da propriedade intelectual em núcleos de inovação tecnológica de universidades públicas brasileiras: desafios e oportunidades. **Revista Tecnológica da Fatec Americana**, Americana, v. 6, n. 2, p. 1-19, abr./set. 2017.

SANTOS, Marli Elizabeth Ritter dos. Boas práticas de gestão em Núcleos de Inovação Tecnológica (NIT). In: SANTOS, Marli Elizabeth Ritter dos; TOLEDO, Patricia Tavares Magalhães de; LOTUFO, Roberto de Alencar (orgs.). **Transferência de Tecnologia**: estratégias para a estruturação e gestão de Núcleos de Inovação Tecnológica. Campinas: Komedi, 2009, p. 75-108.

SANTOS, Elisama Campelo *et al*. Análise comparativa das etapas do processo de transferência de tecnologia em ICTs brasileiras. **Observatorio de la Economía Latinoamericana**, v. 21, n. 5, p. 2453-2470, 2023.

SÃO PAULO (Estado). Lei Complementar nº 1.049, de 19 de junho de 2008. Dispõe sobre medidas de incentivo à inovação tecnológica, à pesquisa científica e tecnológica, ao desenvolvimento tecnológico, à engenharia não-rotineira e à extensão tecnológica em ambiente produtivo, no Estado de São Paulo, e dá outras providências correlatas. **Diário Oficial do Estado de São Paulo**, São Paulo, 20 jun. 2008. Disponível em: http://www.al.sp.gov.br/repositorio/legislacao/lei.complementar/2008/lei.complementar-1049-19.06.2008.html. Acesso em: 10 nov. 2023.

SÃO PAULO (Estado). Secretaria de Agricultura e Abastecimento. Portaria APTA-226, de 15 de junho de 2018. Reorganiza o Núcleo de Inovação Tecnológica da Agência Paulista de Tecnologia dos Agronegócios – NIT APTA. **Diário Oficial do Estado de São Paulo**, São Paulo, 16 jun. 2018, seção I, p. 27-28.

SCOTT, William Richard. **Institutions and Organizations**. London: Sage, 1995. TORKOMIAN, Ana L**úcia** Vitale. Panorama dos Núcleos de Inovação Tecnológica no Brasil. In: SANTOS, Marli Elizabeth Ritter dos; TOLEDO, Patricia Tavares Magalhães de; LOTUFO, Roberto de Alencar (orgs.). **Transferência de tecnologia**: estratégias para a estruturação e gestão de Núcleos de Inovação Tecnológica. Campinas: Komedi, 2009, p. 21-37.

UNIVERSIDADE FEDERAL DE MINAS GERAIS. Resolução nº 05/2022, de 5 de maio de 2022. Regulamenta a Política de Inovação da Universidade Federal de Minas Gerais, no âmbito do Marco Legal de Ciência, Tecnologia e Inovação. **Boletim UFMG**, Belo Horizonte, 9 jun. 2022. Disponível em: https://ufmg.br/comunicacao/publicacoes/boletim/edicao/2115. Acesso em: 23 nov. 2023.

VILHA, Anapatrícia Morales *et al*. Política de inovação de instituições públicas de ciência, tecnologia e inovação: o passo a passo para processos de formulação. **Revista de Gestão e Análise**, Fortaleza, v. 9, n. 3, p. 22-34, set./dez. 2020. Disponível em: https://unichristus.emnuvens.com.br/gestao/article/view/3050. Acesso em: 1 abr. 2026.

Submetido em: 07/01/2025
Aprovado em: 25/02/2026