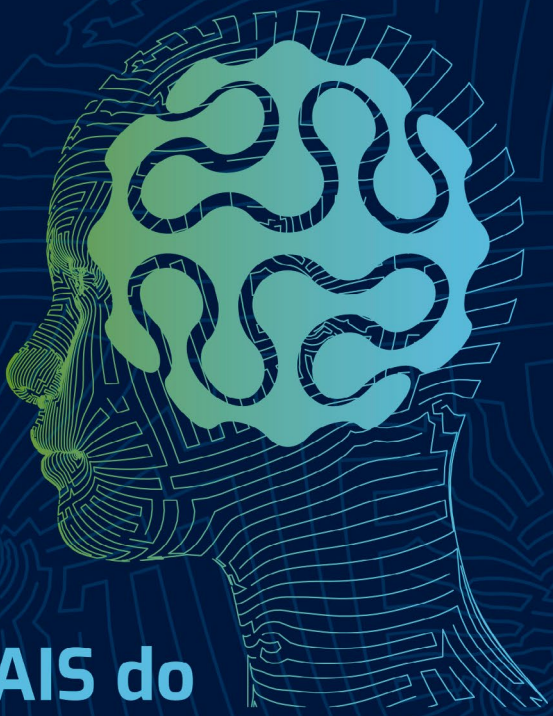


ANAIS do LAWinSUMMIT 3.0

Sociedade Conectada, Democracia e Tecnologias Emergentes

Volume 1

EXPERT
EDITORA DIGITAL

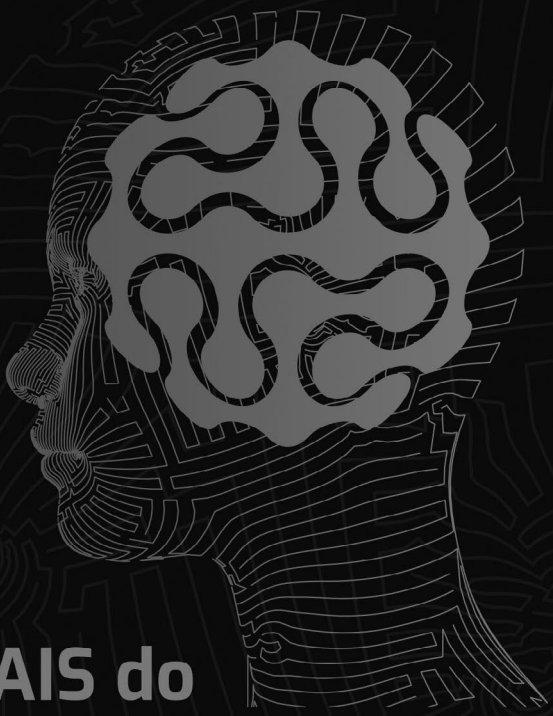
Sociedade conectada, democracia e tecnologias emergentes: este é o eixo que orienta o *LAWin Summit 3.0*, espaço de convergência entre Direito, Tecnologia e Inovação. O presente livro reúne os resumos dos trabalhos apresentados no evento, refletindo a diversidade de olhares acadêmicos e profissionais sobre os desafios e possibilidades que emergem na era digital.

Com uma seleção criteriosa de pesquisas, avaliadas por pareceristas ad hoc, a obra consolida um mosaico de temas contemporâneos: inteligência artificial, proteção de dados, governança digital, impactos sociais dos algoritmos, cidadania digital, democracia em rede e os novos contornos das relações de trabalho, consumo e participação política.

Mais do que um registro científico, este livro é também um convite ao diálogo interdisciplinar. Nele, estudantes, pesquisadores e profissionais compartilham reflexões críticas, propostas regulatórias e experiências práticas que iluminam os dilemas éticos, jurídicos e sociais do nosso tempo.

O *LAWin Summit 3.0* reafirma, assim, o compromisso de construir pontes entre universidade, instituições públicas e sociedade, valorizando a ciência aberta, o pensamento crítico e a inovação responsável. Cada resumo publicado aqui representa não apenas uma contribuição acadêmica, mas também uma peça fundamental no esforço coletivo de compreender e transformar a realidade em direção a um futuro mais democrático, inclusivo e sustentável.

EXPERT
EDITORA DIGITAL



ANAIS do
LAWinSUMMIT 3.0

Sociedade Conectada, Democracia e Tecnologias Emergentes

Volume 1

Direção Executiva: Luciana de Castro Bastos
Direção Editorial: Daniel Carvalho
Diagramação: Editora Expert
Capa: Franklin Carioca Cruz
A regra ortográfica usada foi prerrogativa do autor

Dados Internacionais de Catalogação na Publicação (CIP)

SOUZA, Alcian Pereira de. CRUZ, Franklin Carioca. SILVA, Raisa Albuquerque da. Anais do LAWinSUMMIT 3.0: Sociedade Conectada, Democracia e Tecnologias Emergentes Vol.1 / organizado por Alcian Pereira de Souza, Franklin Carioca Cruz, Raisa Albuquerque da Silva. – Belo Horizonte, MG: Editora Expert, 2025.
322 p.
ISBN:
Tecnologia da informação – Direito – Congressos. 2. Inteligência artificial – Aspectos jurídicos. 3. Proteção de dados – Brasil. 4. Democracia – Inovações tecnológicas. 5. Direito e tecnologia – Congressos. I. Souza, Alcian Pereira de, org. II. Cruz, Franklin Carioca, org. III. Silva, Raisa Albuquerque da, org. IV. Título.
CDD: 343.0999 CDU: 34:004
Modo de acesso: https://experteditora.com.br

Índices para catálogo sistemático:

Direito e Tecnologia / Inteligência Artificial / Proteção de Dados – 343.0999 / 34:004

experteditora.com.br
contato@editoraexpert.com.br

ORGANIZAÇÃO

Alcian Pereira de Souza

Advogado e Professor Adjunto da Universidade do Estado do Amazonas-UEA, lotado na Escola de Direito (ED/UEA). Pós-Doutorando em Neurociências pela UFMG. Possui o Título de Doutor em Ciências pela Universidade de São Paulo-USP, de Mestre em Direito Ambiental pela UEA. É Professor do Programa de Mestrado e Doutorado em Direito Ambiental da UEA (PPGDA/UEA). É Pesquisador Líder do Grupo de Pesquisa do Núcleo de Direito, Tecnologia e Inovação-LAWin/UEA, o qual atua nos eixos de Incentivos à PDI, compliance, proteção de dados e Direito 4.0. Atualmente é Diretor da Escola de Direito da UEA (ED/UEA) e Coordenador dos Cursos de Especialização em Direito 4.0 e Inteligência Artificial e de Direito, Compliance e Mecanismos Anticurrupção da UEA. Assessor Jurídico do Conselho Deliberativo Estadual do SEBRAE/AM.

Franklin Carioca Cruz

Possui mais de 25 anos de experiência atuando como designer. Nos últimos 8 anos vem conciliando sua atuação também como professor e pesquisador. Possui mestrado em Administração Pública pela Universidade Federal de Viçosa - UFV, onde também ingressou para o doutorado. Na sua dissertação desenvolveu um modelo conceitual e prático intitulado Design Thinking for Law Learning, uma abordagem baseada em design thinking capaz de apoiar o aprendizado de forma ativa e a criação de soluções para problemas jurídicos complexos.

Raisa Albuquerque da Silva

Mestre pelo Programa de Pós-Graduação em Administração da Universidade Federal de Viçosa (UFV), Graduada em Direito pela Universidade Federal do Amazonas (UFAM). Professora de Direito Civil e Direito e Inovações Tecnológicas no Instituto Amazônico de Ensino Superior. Técnica em administração da Universidade do Estado do Amazonas, exercendo função de assessoria no Núcleo de

Direito, Tecnologia e Inovação da Escola de Direito (LAWin/UEA). Tem experiência na área de Direito, com ênfase em Direito Privado, Previdenciário, Pesquisa, Desenvolvimento e Inovação (PDI).

COMITÊ CIENTÍFICO

Os resumos publicados neste caderno de resumos passaram para avaliação e aprovação as cegas de dois ou mais pareceristas ad hoc.

Os resumos publicados, bem como as opiniões neles emitidas são de inteira responsabilidade de seus autores.

AUTORES

Adriana Almeida Lima
Albefredo Melo de Souza Júnior
Alcian Pereira de Souza
Alcemir Filomeno Pinto
Ana Carolina Moreira Fernandes
Ana Clara Mendonça Silva
Ana Cristina de Melo Batista
Ana Karoline Farias Barros
Ana Lívia Figliuolo Bezerra de Menezes
Ana Raquel Monassa Dantas
Andrezza Letícia Oliveira Tundis Ramos
Bernardo Silva de Seixas
Camily Figueiredo dos Santos
Carlos Augusto da Silva
Carlos Henrique Everton Machado
Carolina Postigo Silva
Denison Melo de Aguiar
Emilly Victória Batista Dos Santos
Fernando José Ribeiro Feitoza
Franklin Carioca Cruz
Françoyne Martins de Souza
Helder Brandão Goés
Hillary Vitória Brasil Gomes
Joan Bohadana Barroso
João Victor de Almeida Grangeão
Juliana Victória Araújo de Amorim
Karina Lopes Cidade
Katy Any Lopes da Silva
Kelly Borges de Almeida Rocha
Lucas Gabriel Pessoa de Aragão
Lucas Nunes Figueiredo Cavalcante
Luiz Felipe de Farias Leite Borges
Luiz Gustavo Negro Vaz
Lydia de Jesus Azêdo Neta
Maíza Thayná Pereira Ribeiro
Marcela Dorneles Sandrini
Maria Clara Santana Barros de Oliveira
Maria Fernanda Sousa Rodrigues
Myracelle dos Santos da Silva
Nelcy Renata Silva de Souza
Neuton Alves de Lima
Pablo Oliva Souza
Paula Mércia Coimbra Brasil
Priscila Farias dos Reis Alencar
Rebeca de Lima Nogueira
Renato Ferreira Ribeiro Matta
Rhedson Francisco Fernandes Esashika
Rochelle Monteiro Brito
Roberta Carolaine Lira Lopes
Rodrigo de Almeida Grangeão
Ruan Patrick Teixeira da Costa
Stella Maris Barconte
Taís Batista Fernandes
Taís Viga de Albuquerque Oliva Souza
Tayna Lanay Carvalho Veloso de Almeida
Thiago Snaider Nunes da Cruz
Tiago Esashika Crispim
Vitor Luiz Maia da Silva Xavier

Lincy Ester da Silva Parente
Luana Caroline Nascimento Damasceno
Lucas Almeida da Silva
Viviane de Oliveira Rocha
Yara Queiroz Freitas
Yasmim Ferreira Derzi

APRESENTAÇÃO

É com imensa alegria que apresento esta segunda obra coletiva que nasce no coração do **LAWin Summit 3.0**, congresso que, ano após ano, vem se consolidando como um espaço de debate acadêmico, reflexão crítica e construção de pontes entre o Direito e as tecnologias emergentes.

Este livro é o reflexo desse esforço coletivo. Ele reúne não apenas os resultados de pesquisas que iluminam diferentes facetas da sociedade hiperconectada, mas também a energia criativa e a pluralidade de vozes que marcaram o evento.

Entre os principais temas abordados pelos autores estão: a democracia digital; a discriminação algorítmica e seus efeitos na reprodução de desigualdades sociais; a justiça climática e o capacitismo ambiental e algorítmico; os desafios da governança digital e da esfera pública diante da colonização algorítmica; a radicalização online e a educação digital como resposta; o analfabetismo digital e a inclusão social; os dilemas da governança algorítmica e dos marcos regulatórios da inteligência artificial; a aplicação de tecnologias inteligentes na governança climática e no direito ambiental; os desafios das audiências virtuais e do processo eletrônico para o acesso à justiça; além de reflexões críticas sobre a explicabilidade e a *accountability* algorítmica no Poder Judiciário.

É motivo de orgulho constatar o papel do Lawin (Núcleo de Direito, tecnologia e inovação), enquanto Grupo de Pesquisa/CNPQ, somado com o Programa de pós graduação em Direito Ambiental PPGDA e o PPG da UFMG, para o fortalecimento da cultura da produção acadêmica na região amazônica, especialmente no campo do Direito e das novas tecnologias. A obra reafirma que pensar criticamente o presente e, fazê-lo a partir do Amazonas, é também um ato de resistência e inovação.

Por fim, o leitor encontrará o conteúdo estruturado a partir da divisão temática dos cinco Grupos de Trabalho (GTs) do evento, refletindo a riqueza e diversidade das discussões. Que este livro inspire,

provoque e ajude a consolidar um ecossistema acadêmico cada vez mais comprometido com os desafios do nosso tempo.

Prof. Dr. ALCIAN PEREIRA DE SOUZA
Coordenador Geral do Lawin Summit

SUMÁRIO

DEMISSÕES AUTOMATIZADAS E DESATIVAÇÕES INJUSTAS: DESAFIOS JURÍDICOS DA GESTÃO ALGORÍTMICA NAS RELAÇÕES DE TRABALHO

Alcemir Filomeno Pinto

Aluno especial de Mestrado em Direito Ambiental pelo Programa de Pós-Graduação em Direito Ambiental (PPGDA) da Universidade do Estado do Amazonas (UEA). Pós-graduado em Direito: Gestão e Business Law pela Fundação Getúlio Vargas (FGV-SP). Professor do curso de Direito na Escola Superior Batista do Amazonas (ESBAM). Advogado. Lattes: http://lattes.cnpq.br/7417243712907907.ORCID: 0009-0005-6421-2656. E-mail: alcemir.contato@gmail.com.

Katy Any Lopes da Silva

Mestre em Administração pela Universidade Federal de Viçosa (UFV), com ênfase na linha de pesquisa em Inovação, Desenvolvimento e Indústria. Atualmente, é servidora pública na Escola de Direito da Universidade do Estado do Amazonas (UEA) e membro do LAWin - Núcleo de Direito, Tecnologia e Inovação da UEA. Lattes: http://lattes.cnpq.br/5950634094366707. E-mail: klopes@uea.edu.br.

Palavras-chave: Gestão algorítmica; Subordinação digital; Demissões automatizadas; Automação do trabalho; Desenvolvimento Sustentável.

1. OBJETIVOS

O presente trabalho tem como objetivo analisar os impactos da gestão algorítmica nas relações de trabalho mediadas por plataformas digitais, com ênfase nas demissões automatizadas, à luz dos direitos fundamentais previstos na Constituição Federal de 1988 e na Lei Geral de Proteção de Dados Pessoais (LGPD), destacando as lacunas regulatórias existentes no ordenamento jurídico brasileiro.

Busca-se compreender como a lógica da gestão algorítmica influencia a autonomia e a subordinação dos trabalhadores no contexto da Quarta Revolução Industrial, investigar as consequências jurídicas e sociais das decisões automatizadas que resultam em desligamentos sem intervenção humana, bem como examinar os limites da legislação nacional frente a essas novas formas de controle e organização do trabalho.

2. METODOLOGIA

A metodologia adotada será o método dedutivo, partindo-se da análise de normas constitucionais, infraconstitucionais e princípios jurídicos, como o direito à explicação e à proteção de dados pessoais, para examinar os casos concretos de desativações de trabalhadores por sistemas automatizados. Quanto aos meios, a pesquisa será bibliográfica e documental, com base em literatura especializada, além de documentos oficiais, decisões judiciais e reportagens jornalísticas que evidenciam a precarização decorrente da gestão algorítmica, especialmente o exemplo de desativação de motorista da Uber noticiado pela jornalista Sarah O'Connor (2025). Quanto aos fins, trata-se de uma pesquisa qualitativa, voltada à compreensão crítica das consequências jurídicas, sociais e humanas do uso de inteligência artificial no desligamento de trabalhadores.

3. DESENVOLVIMENTO

3.1. TRANSFORMAÇÕES DO TRABALHO NA ERA DIGITAL: A GESTÃO ALGORÍTMICA

A emergência da Quarta Revolução Industrial, impulsionada pela integração de tecnologias digitais, automação, inteligência artificial (IA) e big data, tem promovido transformações profundas nas estruturas produtivas e nas relações de trabalho contemporâneas. Nesse novo cenário tecnológico, destaca-se o fenômeno da gestão

algorítmica: uma forma de controle laboral que utiliza sistemas automatizados para monitorar, avaliar e tomar decisões sobre os trabalhadores, substituindo progressivamente a figura tradicional do empregador-diretor por mecanismos computacionais.

Embora os avanços tecnológicos tragam consigo ganhos de eficiência, também levantam sérias preocupações no campo dos direitos fundamentais. A problemática central que motiva este estudo reside na crescente utilização de decisões automatizadas para desativar ou demitir trabalhadores de plataformas digitais, sem transparência, contraditório ou intervenção humana significativa, prática que tem sido denunciada como forma de desumanização do trabalho e violação de garantias constitucionais e legais, como a ampla defesa (art. 5º, LV, CF/88) e o direito à explicação das decisões automatizadas (art. 20, §1º, LGPD). Soma-se a isso a constatação de que esses trabalhadores, frequentemente classificados como autônomos, encontram-se submetidos a uma forma de subordinação algorítmica, marcada por dependência econômica e controle operacional exercido por inteligência artificial.

A Quarta Revolução Industrial, marcada pela integração de tecnologias digitais, automação, inteligência artificial e big data, impacta diretamente as estruturas produtivas e as relações de trabalho. No cenário laboral, isso se materializa na chamada gestão algorítmica, uma forma de controle operacional dos trabalhadores baseada em dados, por meio de sistemas automatizados de tomada de decisão (PARENTONI, 2024, p. 21-22;34). Segundo Miziara (2024, p. 236), essa sub-revolução tecnológica desafia as estruturas clássicas do Direito do Trabalho, exigindo sua ressignificação. A gestão algorítmica substitui a figura humana tradicional do empregador-diretor por algoritmos que, com base em predições e análises de comportamento, distribuem tarefas, monitoram desempenho e até definem punições ou desligamentos.

Além disso, recaímos na discussão da existência do vínculo empregatício entre esses trabalhadores e as plataformas (não reconhecido pela legislação pátria, até então) pois, a subordinação

jurídica é o critério clássico para configuração do vínculo empregatício, definido pela sujeição do trabalhador às ordens do empregador. Nas plataformas digitais, esse controle é exercido por meio de algoritmos que monitoram, avaliam e punem comportamentos, criando um novo tipo de subordinação algorítmica. Apesar de a aparência ser de autonomia, já que os trabalhadores podem escolher quando se conectar, na prática, a dependência econômica, a ausência de negociação e a imposição unilateral de condições evidenciam subordinação. A jurisprudência de países europeus como Espanha e Portugal já reconhece essa relação, atribuindo vínculo de emprego com base na lógica de comando indireto das plataformas (PARENTONI, 2024, p. 80, 97).

3.2. DEMISSÕES AUTOMATIZADAS, VIOLAÇÃO DE DIREITOS FUNDAMENTAIS E DESUMANIZAÇÃO

As demissões automatizadas consistem na ruptura do vínculo de trabalho decidida exclusivamente por sistemas de IA, com pouca ou nenhuma intervenção humana. Miziara (2024, p. 246) aponta que tais práticas violam frontalmente o art. 20 da Lei Geral de Proteção de Dados (LGPD), que assegura ao titular dos dados o direito à explicação das decisões automatizadas. Esse tipo de desligamento compromete garantias constitucionais como a ampla defesa e o contraditório (art. 5º, LIV e LV, CF/88), além de afetar a dignidade do trabalhador. Zuboff (2019, Cap. III) denomina esse modelo de gestão como *Surveillance Capitalism*, ou capitalismo de vigilância', no qual os dados dos trabalhadores são utilizados como insumo de controle e monetização. Ajunwa (2024, p. 22) utiliza a expressão 'trabalhador quantificado' para descrever a nova lógica em que a força de trabalho é tratada como uma série de métricas e probabilidades calculáveis.

O slogan 'avance rápido e quebre coisas', popularizado pelo Vale do Silício, representa a ideologia da inovação desenfreada, sem considerar as consequências sociais e jurídicas de suas aplicações.

No contexto do trabalho, essa lógica ignora o impacto das decisões automatizadas sobre os trabalhadores, tratando erros algorítmicos como colaterais inevitáveis. No entanto, como cita O'Connor (2025), as 'coisas' quebradas são, na realidade, pessoas como os motoristas desativados injustamente por um algoritmo e ignorado por canais de atendimento humano. Essa desumanização dos processos produtivos demanda resposta institucional urgente, com regulação firme e responsabilidade civil pelos danos causados.

3.3. LIMITES DA REGULAÇÃO BRASILEIRA DIANTE DAS DEMISSÕES AUTOMATIZADAS

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), em seu art. 20, §1º, assegura aos titulares o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais. Essa previsão representa um avanço no reconhecimento do impacto da inteligência artificial sobre os direitos individuais, especialmente em contextos laborais. Contudo, como destaca Miziara (2024, p. 233; 246; 248), o ordenamento jurídico brasileiro ainda carece de regulamentação específica para operacionalizar esse direito no âmbito das relações de trabalho. A prática mostra que trabalhadores desativados por algoritmos enfrentam inúmeras barreiras para acessar a justiça, especialmente em razão da opacidade dos sistemas, da assimetria informacional e da ausência de canais efetivos de contestação. Além disso, em contextos de alta precarização, muitos trabalhadores sequer compreendem que a decisão foi automatizada, o que os impede de exercer seu direito à revisão. A ausência de amparo coletivo e de representação sindical organizada agrava ainda mais essa vulnerabilidade, colocando o trabalhador em uma posição de absoluta desvantagem diante das plataformas digitais (PARENTONI, 2024, p. 32-37).

CONCLUSÃO

A pesquisa identificou que a utilização de algoritmos para gerir trabalhadores em plataformas digitais vem crescendo, sem que haja regulamentação específica no ordenamento jurídico brasileiro. Foi constatado que a ausência de transparência e explicabilidade nas decisões automatizadas compromete o exercício de direitos fundamentais dos trabalhadores. Além disso, observou-se que a jurisprudência e a doutrina ainda enfrentam dificuldades para enquadrar juridicamente a subordinação algorítmica, embora Portugal e outros países da União Europeia já tenham avançado nesse sentido.

Diante dos riscos identificados, é urgente a adoção de medidas legislativas e institucionais que protejam os trabalhadores contra os abusos da gestão algorítmica. Com o exemplo a ser adotado na legislação pátria local, destaca-se a União Europeia, com o art. 22 do Regulamento Geral sobre a Proteção de Dados (GDPR), o qual proíbe decisões baseadas unicamente em tratamento automatizado que produzam efeitos jurídicos relevantes, sem a devida intervenção humana. Para o Brasil, propõem-se as seguintes medidas: (i) reconhecimento da subordinação algorítmica, com base no controle exercido por sistemas digitais; (ii) instituição de mecanismos obrigatórios de revisão humana em decisões que afetem direitos trabalhistas; (iii) promoção de normas que garantam a transparência e auditabilidade dos sistemas algorítmicos utilizados pelas empresas; e (iv) fortalecimento da atuação sindical, por meio de incentivos à organização coletiva dos trabalhadores de plataformas e ampliação do acesso à justiça por meio de ações coletivas. Somente por meio de uma abordagem sistêmica e intersetorial será possível assegurar uma justiça algorítmica verdadeiramente comprometida com os direitos humanos e com a dignidade do trabalhador.

REFERÊNCIAS

AJUNWA, Ifeoma. The Quantified Worker. Cambridge: Cambridge University Press, 2023.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 mai. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 mai. 2025.

MIZIARA, Raphael. A proteção contra despedida algorítmica no contexto laboral: consequências pelo descumprimento do direito à explicabilidade previsto no art. 20 da LGPD. *Revista do Tribunal Superior do Trabalho,* Porto Alegre, v. 90, n. 1, p. 230-249, jan./mar. 2024.

O'CONNOR, Sarah. What can workers do if they're fired by AI? *Financial Times,* Londres, 17 abr. 2025. Disponível em: https://www.ft.com/content/6ca668c6-60a8-4215-857b-491e74f9599a. Acesso em: 9 mai. 2025.

PARENTONI, Thaís de Souza. *Trabalho em plataformas digitais: uma análise da subordinação jurídica nas aplicações de transporte de passageiros e entregas ao domicílio*. 2024. Dissertação (Mestrado em Direito e Ciência Jurídica) – Faculdade de Direito, Universidade de Lisboa, Lisboa, 2024.

ZUBOFF, Shoshana. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. New York: PublicAffairs, 2019.

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, L 119, p. 1-88, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679. Acesso em: 12 mai. 2025.

O NATIVO DIGITAL E A SUPEREXPOSIÇÃO EM REDES SOCIAIS: IMPLICAÇÕES À PROTEÇÃO DOS DIREITOS E GARANTIAS FUNDAMENTAIS

Alcemir Filomeno Pinto

Aluno especial de Mestrado em Direito Ambiental pelo Programa de Pós-Graduação em Direito Ambiental (PPGDA) da Universidade do Estado do Amazonas (UEA). Pós-graduado em Direito: Gestão e Business Law pela Fundação Getúlio Vargas (FGV-SP). Professor do curso de Direito na Escola Superior Batista do Amazonas (ESBAM). Advogado. Lattes: http://lattes.cnpq.br/7417243712907907.ORCID: 0009-0005-6421-2656. E-mail: alcemir.contato@gmail.com.

Viviane de Oliveira Rocha

Graduanda em Direito pela Escola Superior Batista do Amazonas – ESBAM. Mestre em Serviço Social e Sustentabilidade na Amazônia pela Universidade Federal do Amazonas – UFAM. Assistente Social da Marinha do Brasil. ORCID: https://orcid.org/0000-0001-9239-7006. Email:vivianerochass@hotmail.com.

Palavras-chave: Nativos digitais; Direitos fundamentais; Plataformas digitais; Criança e Adolescente.

1. OBJETIVOS

Este estudo tem como objetivo analisar as implicações sociais, jurídicas e éticas do uso de plataformas digitais por crianças e adolescentes, à luz da proteção dos direitos e garantias fundamentais assegurados pelo ordenamento jurídico brasileiro. Busca-se, ainda, investigar de que forma o Marco Legal de Ciência, Tecnologia e Inovação contempla a proteção de populações vulneráveis no acesso às tecnologias, examinar os impactos jurídicos, éticos e psicossociais decorrentes da superexposição digital infantojuvenil, especialmente

no contexto do *sharenting*, e refletir sobre os desafios enfrentados por pais e responsáveis na mediação do uso das redes sociais, destacando a importância da cidadania digital e do letramento tecnológico como instrumentos essenciais para a construção de um ambiente virtual mais seguro e inclusivo.

2. METODOLOGIA

A pesquisa adotará o método dedutivo, com abordagem qualitativa e caráter exploratório. Serão utilizados procedimentos bibliográficos e documentais, com base em legislações nacionais, doutrina especializada e estudos interdisciplinares que tratam dos direitos das crianças e adolescentes no ambiente digital. O objetivo é analisar criticamente os impactos jurídicos, sociais e éticos da exposição infantojuvenil nas plataformas digitais, identificando lacunas normativas e propondo diretrizes para políticas públicas de proteção e cidadania digital.

3. DESENVOLVIMENTO

A infância e a adolescência, fases fundamentais para o desenvolvimento físico, emocional e social do ser humano, vêm sendo profundamente impactadas pelas transformações tecnológicas das últimas décadas. A atual geração de crianças e adolescentes cresce imersa em um universo digitalizado, sendo reconhecida como "nativos digitais", sujeitos que, desde os primeiros anos de vida, interagem naturalmente com dispositivos móveis, redes sociais e plataformas virtuais.

De acordo com Tezani (2017), esses nativos digitais se caracterizam pelo uso constante das Tecnologias Digitais da Informação e Comunicação (TDIC), o que molda suas formas de aprender, se relacionar e perceber o mundo. Franco (2013) complementa ao destacar que, para esses sujeitos, o ciberespaço é também espaço de

convivência, lazer e formação de identidade. Como lembra Prensky (2001), eles estão acostumados a receber informações rapidamente, realizando múltiplas tarefas ao mesmo tempo. Em contrapartida, seus pais e responsáveis, em sua grande maioria os chamados "imigrantes digitais", segundo Mattar (2014), são aqueles que cresceram em um contexto analógico e, por isso, muitas vezes se mostram despreparados para acompanhar e mediar essa nova realidade.

A inserção precoce e intensa de crianças nas plataformas digitais representa, ao mesmo tempo, uma possibilidade de inclusão social e de desenvolvimento, mas também um risco à integridade física, emocional e jurídica desses indivíduos. Diante dessa dualidade, surge o desafio de articular o direito de acesso à tecnologia com os princípios da proteção integral, previstos na Constituição Federal de 1988 e no Estatuto da Criança e do Adolescente (ECA).

No cenário normativo, destaca-se o Marco Legal de Ciência, Tecnologia e Inovação (Lei nº 13.243/2016), regulamentado pelo Decreto nº 9.283/2018. Este conjunto legal visa fomentar a pesquisa, a inovação e o desenvolvimento tecnológico no Brasil. Contudo, apesar de representar avanço em termos de incentivo à produção científica, o marco carece de mecanismos específicos que garantam a proteção de crianças e adolescentes no ambiente digital. Lôbo e Mól (2022) apontam que o Estado brasileiro tem sido omisso na formulação de políticas públicas que assegurem o acesso justo e seguro às inovações tecnológicas como um direito fundamental, o que aprofunda desigualdades sociais, digitais e geracionais.

Nesse cenário, um fenômeno social que tem chamado atenção é o *sharenting*, termo que designa a prática de pais ou responsáveis compartilharem rotineiramente a vida de seus filhos nas redes sociais. Conforme analisado por Ribeiro e Oliveira Filho (2024), essa exposição, muitas vezes motivada por afeto ou por objetivos comerciais, pode configurar violação de direitos da personalidade, como privacidade, honra e imagem, sem que a criança tenha compreensão ou consentimento sobre sua própria presença digital.

Os impactos dessa superexposição ultrapassam os limites jurídicos. Do ponto de vista psicossocial, essa prática pode afetar diretamente a formação da identidade da criança, submetendo-a a padrões irreais de validação social, a julgamentos públicos e à vigilância constante. Do ponto de vista ético, questiona-se a autonomia dos pais para decidir sobre a imagem dos filhos, especialmente em contextos em que há monetização ou exploração de sua imagem.

Além disso, o ambiente digital, em sua forma mais perversa, também abriga ameaças silenciosas e graves. O acesso de crianças e adolescentes a jogos e desafios online perigosos, como os que induzem à automutilação ou simulação de asfixia, evidencia o quanto o ambiente digital pode ser hostil e desregulado. Estudos como os de Lindsey et al. (2019) e Guilheri, Andronikof e Yazigi (2017) mostram que desafios como o "jogo da asfixia" são atraentes justamente por seus efeitos fisiológicos intensos, comparáveis ao uso de substâncias psicoativas, e por promoverem uma suposta "coragem" social diante de seus pares.

Esse fenômeno pode revelar uma grave lacuna no campo da saúde e na atuação preventiva do Estado na garantia dos direitos fundamentais. Apesar dos riscos evidentes, ainda há pouca mobilização institucional e educacional para lidar com os impactos físicos e emocionais dessas práticas. A adolescência, por si só, é uma etapa da vida marcada por transformações, construção de identidade e busca por pertencimento. A presença constante no ambiente virtual, sem o devido acompanhamento, potencializa vulnerabilidades emocionais e pode levar à alienação das relações familiares e comunitárias (RIBEIRO; OLIVEIRA FILHO, 2024).

Diante de tal cenário, o papel da família torna-se crucial. Contudo, muitos pais e responsáveis ainda não possuem o letramento digital necessário para compreender os mecanismos de funcionamento das plataformas, os riscos algorítmicos, os impactos da exposição de dados e a manipulação de conteúdo. Essa despreparação reforça a urgência da criação de políticas públicas voltadas à educação digital parental e à formação de uma cultura de cidadania digital crítica e responsável.

A cidadania digital deve ser compreendida não apenas como o direito de acessar tecnologias, mas como a capacidade de usá-las de forma ética, segura e consciente. A proteção dos direitos fundamentais de crianças e adolescentes no ambiente digital é, portanto, uma tarefa compartilhada entre Estado, famílias, plataformas e sociedade civil.

Frente às limitações atuais, legais, institucionais e culturais, é necessário repensar a governança digital e consolidar políticas intersetoriais que unam os campos do direito, da tecnologia, da educação e da psicologia, do serviço social. A promoção de um ambiente digital mais justo e seguro depende do reconhecimento efetivo de crianças e adolescentes como sujeitos de direitos, e da atuação ativa e coordenada de todos os agentes sociais na garantia de sua proteção.

Assim, os limites e possibilidades do uso digital na infância precisam ser debatidos sob uma perspectiva interdisciplinar. A construção de um ambiente digital saudável e inclusivo passa pelo reconhecimento das crianças e adolescentes como sujeitos de direitos e pela consolidação de um modelo de governança que respeite, eduque e proteja esses sujeitos em sua trajetória digital.

CONCLUSÃO

O uso das tecnologias por crianças e adolescentes deve ser compreendido como um fenômeno social e jurídico complexo, que exige uma abordagem intersetorial e integradora. O reconhecimento do acesso à tecnologia como direito fundamental impõe ao Estado o dever de formular políticas inclusivas, ao passo que cabe à sociedade civil e às famílias a corresponsabilidade pela proteção de sujeitos em desenvolvimento.

Diante da crescente digitalização da infância e dos riscos decorrentes da superexposição de crianças e adolescentes nas plataformas virtuais, torna-se indispensável repensar os marcos

normativos e institucionais que regem os direitos da população infantojuvenil no ambiente digital.

A pesquisa evidencia que, embora o acesso às tecnologias represente uma importante ferramenta de inclusão e desenvolvimento, sua utilização sem a devida regulação, mediação parental e suporte estatal pode comprometer direitos fundamentais relacionados à dignidade, à privacidade e à formação da identidade. É necessário, portanto, repensar os limites da liberdade de expressão e da autonomia parental à luz da proteção integral da criança e do adolescente, propondo medidas que equilibrem inovação, acesso e garantia de direitos fundamentais.

O acesso de crianças e adolescentes à internet é uma realidade e lidar com isso é uma exigência da qual responsáveis não podem escapar. Diante de tantos desafios, é importante ter em mente princípios que podem ajudar tanto na orientação aos filhos quanto na definição de regras. É nesse sentido que os aspectos podem ser considerados: não confundir vivência digital com maturidade digital; cuidar para a prática da fantasia não seja tomada por práticas de engano; tratar a imagem da criança com respeito e segurança.

Ademais, é urgente consolidar políticas públicas intersetoriais que promovam o letramento digital das famílias, responsabilizem plataformas, fortaleçam a atuação do Estado e reconheçam crianças e adolescentes como sujeitos de direitos, assegurando-lhes uma cidadania digital crítica, segura e emancipatória.

REFERÊNCIAS

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 mai. 2025.

BRASIL. Estatuto da Criança e do Adolescente: Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre a proteção integral à criança e ao adolescente. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 18 mai. 2025.

BRASIL. Lei nº 13.243, de 11 de janeiro de 2016. Dispõe sobre estímulos ao desenvolvimento científico, à pesquisa, à capacitação científica e tecnológica e à inovação. Diário Oficial da União: seção 1, Brasília, DF, 12 jan. 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13243.htm. Acesso em: 18 mai. 2025.

BRASIL. Decreto nº 9.283, de 7 de fevereiro de 2018. Regulamenta dispositivos da Lei nº 10.973/2004 e da Lei nº 13.243/2016. Diário Oficial da União: seção 1, Brasília, DF, 8 fev. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9283.htm. Acesso em: 18 mai. 2025.

RIBEIRO, Bruna Eduarda Araújo; OLIVEIRA FILHO, Ênio Walcácer de. A exposição de crianças em redes sociais à luz dos direitos humanos: uma análise de proteção da privacidade e do desenvolvimento infantil. Revista JRG de Estudos Acadêmicos, v. 7, n. 15, 2024.

BOYD, Danah; ELLISON, Nicole. Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, v. 13, n. 1, p. 210–230, 2007.

DECRETO nº 9.283, de 7 de fevereiro de 2018. Regulamenta dispositivos da Lei nº 10.973/2004 e da Lei nº 13.243/2016.

FRANCO, C. de P. Understanding digital natives learning experiences. Revista Brasileira de Linguística Aplicada, Belo Horizonte, v.13, n.3, p.643-658, 2013. Disponível em: https://www.scielo.br/j/rbla/a/pPL56WH7zHMLzBgzBZBDRyL/?format=pdf&lang=en.Acesso em: 24 mai. de 2025.

GABARDO, Emerson; REIS, Luciano Elias. Ciência, tecnologia e inovação como deveres públicos relativos ao Estado e à sociedade civil no Brasil. Revista do Direito, Santa Cruz do Sul, v. 2, n. 52, p. 38–59, 2017.

GUILHERI, J.; ANDRONIKOF, A.; YAZIGI, L. "Brincadeira do desmaio": uma nova moda mortal entre crianças e adolescentes. Características psicofisiológicas, comportamentais e epidemiologia dos 'jogos de asfixia'. *Ciência & Saúde Coletiva*, Rio de Janeiro, v. 22, n. 3, p. 867–878, mar. 2017. Disponível em: https://www.scielosp.org/article/csc/2017.v22n3/867-878/. Acesso em: 18 mai. 2025.

LINDSEY, M. A.; SHEFTALL, A. H.; XIAO, Y.; JOE, S. Trends of suicidal behaviors among high school students in the United States: 1991–2017. *Pediatrics*, v. 144, n. 5, nov. 2019. Disponível em: https://pmc.ncbi.nlm.nih.gov/articles/PMC7299440/pdf/nihms-1597441.pdf. Acesso em: 18 mai. 2025.

LÔBO, Edilene; MÓL, Ana Lúcia Ribeiro. O direito fundamental de acesso às inovações tecnológicas e a omissão do Estado brasileiro na adoção de políticas públicas para sua proteção. Revista Direito UFMS, v. 8, p. 146–165, 2022.

MATTAR, J. Games em Educação: apostila para o curso de Pós-Graduação em Inovação e Gestão em EaD pela USP. São Paulo: USP, 2014. Não publicado.

PALFREY, J.; GASSER, U. Nascidos na era digital: entendendo a primeira geração dos nativos digitais. Porto Alegre: ARTMED, 2011.

PRENSKY, M. Aprendizagem baseada em jogos digitais. São Paulo: Senac, 2001.

RIBEIRO, Bruna Eduarda Araújo; OLIVEIRA FILHO, Ênio Walcácer de. A exposição de crianças em redes sociais à luz dos direitos humanos: uma análise de proteção da privacidade e do desenvolvimento infantil. Revista JRG de Estudos Acadêmicos, v. 7, n. 15, 2024.

TEZANI, Thaís Cristina Rodrigues. Nativos digitais: considerações sobre os alunos contemporâneos e a possibilidade de se (re)pensar a prática pedagógica. Doxa: Rev. Bras. Psicol. Educ., Araraquara, v.19, n.2, p. 295-307, jul./dez. 2017. e-ISSN: 2594-8385.

ENTRE A CAIXA-PRETA E A FUNDAMENTAÇÃO: EXPLICABILIDADE E ACCOUNTABILITY ALGORÍTMICA NO PROCESSO JUDICIAL

Albefredo Melo de Souza Júnior

Advogado. Professor efetivo da Escola de Direito da Universidade do Estado do Amazonas (ED/UEA). Membro do Núcleo de Direito, Tecnologia e Inovação - LAWin/UEA. Mestre em Direito (UniLasalle/RS). albefredo@uea.edu.br

Ana Carolina Moreira Fernandes

Graduanda do 9º período do curso de Direito pela Universidade do Estado do Amazonas.

PALAVRAS-CHAVE: Inteligência Artificial; Poder Judiciário; Explicabilidade; Responsabilidade Algorítmica; Fundamentação das Decisões.

1. OBJETIVOS

A presente pesquisa tem como objetivo examinar os desafios jurídicos e democráticos resultantes da utilização da Inteligência Artificial no âmbito do Poder Judiciário, destacando a importância da explicabilidade das decisões automatizadas e da responsabilização dos agentes envolvidos. Ademais, busca-se compreender como os algoritmos podem influenciar os princípios do contraditório, da ampla defesa e da fundamentação das decisões judiciais, com base na análise das implicações éticas e legais da "caixa-preta algorítmica".

2. METODOLOGIA

Com o intuito de atingir o objetivo primordial deste estudo, foram utilizados os métodos dedutivo e bibliográfico, com base em artigos científicos, legislações brasileiras, documentos de órgãos oficiais, como o CNJ e a Estratégia Nacional de Inteligência Artificial, e casos concretos relacionados à aplicação de IA no sistema de justiça, especialmente no contexto brasileiro. Além disso, foram considerados estudos teóricos sobre a ética digital. Quanto aos fins, a pesquisa foi qualitativa, com abordagem exploratória e analítica.

3. DESENVOLVIMENTO

3.1. A "CAIXA-PRETA" ALGORÍTMICA E OS RISCOS À TRANSPARÊNCIA

A adoção de sistemas de inteligência artificial pelo Poder Judiciário brasileiro vem crescendo, principalmente em tarefas como triagem de processos, verificação de litispendência e auxílio à elaboração de decisões. No entanto, esse crescimento está acompanhado de preocupações quanto à transparência, à fundamentação das decisões automatizadas e à responsabilização dos envolvidos. Diante disso, o presente estudo propõe-se a investigar os limites jurídicos e éticos da utilização desses sistemas à luz dos direitos fundamentais do processo.

Em uma análise inicial, a chamada "caixa-preta" — ou *black box* — representa um dos maiores desafios ao uso da IA no Judiciário. Trata-se de sistemas cujo funcionamento interno é opaco: apenas suas entradas e saídas são visíveis, enquanto o processo decisório permanece inacessível e incompreensível, dificultando a transparência exigida no processo judicial.

3.2. IMPACTOS DA OPACIDADE ALGORÍTMICA NOS PRINCÍPIOS PROCESSUAIS

Diferentemente das decisões humanas, que consideram não apenas informações, mas também conhecimento e julgamento,

permitindo que o raciocínio seja investigado, os algoritmos de aprendizado de máquina muitas vezes produzem resultados inexplicáveis em termos humanos, pois tais sistemas operam com base em padrões extraídos de dados existentes, sem, no entanto, possuírem conhecimento real sobre o assunto tratado.

Nesse sentido, isso é um problema para o Direito, na medida em que o ordenamento jurídico gira em torno de princípios que são base para todo processo existente no judiciário como, por exemplo, o devido processo legal no art. 5º, inciso LIV, da CRFB/88, a ampla defesa e o contraditório, no art. 5º, inciso LV, da CRFB/88, a motivação das decisões judiciais, no art. 93, IX, da CRFB/88 e art.489, §1º do CPC e a responsabilidade pelas decisões, também conhecida como accountability, a qual refere-se à necessidade de indivíduos, organizações e governos prestarem contas por suas ações, decisões e resultados, assumindo a responsabilidade pelos seus impactos.

Por essa razão e de modo a tentar contornar esse obstáculo, o Conselho Nacional de Justiça, através da Resolução nº 665/2025 dispõe em seu artigo 1º que o objetivo dessa regulamentação é promover a inovação tecnológica e a eficiência dos serviços judiciários de modo seguro, transparente, isonômico e ético, em benefício dos jurisdicionados e com estrita observância de seus direitos fundamentais. Portanto, observa-se que a transparência é uma preocupação presente para os operadores do direito quando se trata do uso da IA no âmbito do Poder Judiciário.

3.3. INTELIGÊNCIA ARTIFICIAL EXPLICÁVEL COMO FERRAMENTA DE LEGITIMAÇÃO

A Inteligência Artificial explicável deve ser entendida como um componente essencial para garantir a transparência desses sistemas, pois exerce um papel fundamental no enfrentamento da opacidade algorítmica, ao transformar os "modelos de caixa-preta" em estruturas mais acessíveis e compreensíveis, semelhantes a

"caixas de vidro". Nesse contexto, é fundamental que a criação de sistemas de IA mais transparentes e interpretáveis seja considerada e incentivada no desenvolvimento de políticas públicas, a fim de fortalecer a legitimidade das decisões geradas por essas tecnologias, principalmente no âmbito do sistema judiciário, uma vez que o desenvolvimento de todas as Inteligências Artificiais utilizadas no Poder Judiciário devem passar pelo processo de deep learning resultado de entradas e saídas supervisionadas no momento de aprendizado da máquina ou "machine learning".

Isso porque quando existe um cuidado maior com a forma como a IA aprende tudo que entra em sua base de dados, torna-se mais fácil entender como ela chegou a resposta dos comandos que recebeu. Dessa forma, a "caixa-preta" perde a opacidade e chega mais perto de uma "caixa de vidro", evidenciando a transparência e a explicabilidade de seus resultados. Além disso, é fundamental entender que a IA é um instrumento criado para pensar como o ser humano, contudo, ela ainda não é equivalente a um cérebro humano, de modo que possui limitações de uso, principalmente no que se refere a sua utilização em atividades com criação de decisões judiciais, as quais precisam respeitar princípios constitucionais do direito e da dignidade da pessoa humana.

Ademais, em que pese a IA ser um sistema extraordinário e extremamente tecnológico em vários aspectos, é imprescindível destacar que a Inteligência Artificial pode falhar, produzindo resultados imprecisos, incompletos ou tendenciosos. Sendo assim, quando a IA falha, o erro pode afetar diretamente os direitos individuais e gerar uma cadeia de decisões judiciais viciadas, sem a devida supervisão ou correção. Esse cenário evidencia os riscos sociais da opacidade algorítmica no Judiciário.

3.4. A INDISPENSÁVEL CENTRALIDADE DO SER HUMANO

Assim, para garantir o respeito aos princípios constitucionais e processuais, é fundamental manter o ser humano no centro das decisões. A ideia de "human-in-the-loop", ser humano na tomada de decisão tem sido defendida como indispensável no contexto jurídico, justamente para garantir que as decisões automatizadas possam ser revistas, interpretadas e corrigidas quando necessário. De forma que, o papel do magistrado, nesse cenário, deve ser ressignificado: não como mero executor do que o sistema recomenda, mas como agente crítico, capaz de analisar os dados produzidos pela IA sob a ótica do Direito e da justiça material. Isso reforça a ideia de que a IA deve atuar como uma ferramenta de apoio à decisão, e não como substituta da função jurisdicional.

Contudo, percebe-se que o uso da inteligência artificial pelo Judiciário brasileiro ainda carece de transparência, conforme demonstra o Painel de Projetos de IA do CNJ. De modo que, apenas 22% dos tribunais divulgam publicamente os algoritmos utilizados, o que significa que menos de um quarto dos sistemas de IA em operação podem ser auditados, o que contraria os objetivos implementados pela Resolução do CNJ nº 615/2025 no art. 1º, §2º que dispõe sobre a auditoria e o monitoramento das soluções de IA, os quais serão realizados com base em critérios proporcionais ao impacto da solução, garantindo que os sistemas sejam auditáveis ou monitoráveis de forma prática e acessível, sem a obrigatoriedade de acesso irrestrito ao código-fonte, desde que sejam adotados mecanismos de transparência e controle sobre o uso dos dados e as decisões automatizadas.

Outrossim, o cuidado com a transparência também está presente na Resolução 615/2025 do CNJ, a qual estabelece que a transparência no uso de IA será promovida por meio de indicadores claros e relatórios públicos, que informem o uso dessas soluções de maneira compreensível e em linguagem simples, garantindo que os jurisdicionados tenham ciência do uso de IA, quando aplicável, sem que isso prejudique a eficiência ou credibilidade dos processos e decisões judiciais.

3.5. ACCOUNTABILITY ALGORÍTMICA E A DIFICULDADE DE ATRIBUIR RESPONSABILIDADE

Um ponto ainda controverso é a definição de quem deve responder por eventuais falhas, omissões ou abusos cometidos por sistemas automatizados no Judiciário, tendo em vista que a responsabilidade pode recair sobre o desenvolvedor do sistema, a instituição pública que o implementa, o magistrado que o utiliza ou uma combinação desses atores. Essa multiplicidade de agentes envolvidos levanta questionamentos sobre a eficácia dos modelos tradicionais de responsabilidade civil e administrativa. Ademais, a ausência de previsões normativas específicas para lidar com esse cenário revela um vácuo legislativo, o que fragiliza os mecanismos de accountability. Nesse contexto, é imprescindível que a verificação de compatibilidade com os direitos e garantias fundamentais ocorra em todas as fases do processo de resposta da IA, através da supervisão humana, garantindo que exista uma autorização para que o resultado final ao comando seja aplicado.

Diante desses desafios, é necessário que o Brasil avance na criação de um marco regulatório específico para a utilização de IA no Poder Judiciário. Iniciativas como o Projeto de Lei nº 2338/2023, que institui o Marco Legal da Inteligência Artificial, devem ser debatidas à luz das particularidades do sistema de justiça, com destaque para a necessidade de garantir transparência, revisão humana obrigatória, proteção de dados e mecanismos de controle externo.

Além disso, a regulamentação atual deve ser ampliada, prevendo auditorias obrigatórias, relatórios de impacto algorítmico e a criação de instâncias permanentes de supervisão ética e jurídica das ferramentas utilizadas pelos tribunais. Tais medidas são essenciais para preservar a integridade do sistema judicial e evitar que decisões tecnicamente bem executadas resultem em injustiças ou violem garantias constitucionais, comprometendo sua legitimidade jurídica.

4. CONCLUSÃO

Diante da análise dos impactos da "caixa-preta" na explicabilidade e responsabilização algorítmica nas decisões judiciais automatizadas, é imprescindível a necessidade de regulação clara e específica para o uso da IA no Poder Judiciário, visando garantir que exista um procedimento de revisão humana em cada processo de resposta aos comandos dados a IA, além de criar uma definição precisa sobre a responsabilidade das decisões judiciais que utilizam a IA em seu processo de formação. Portanto, conclui-se que, embora a inteligência artificial possa representar um avanço significativo na eficiência do sistema de justiça, sua aplicação exige limites normativos rigorosos que assegurem transparência, controle humano e respeito aos princípios constitucionais do processo.

5. REFERÊNCIAS

ALVES, M. A. S.; ANDRADE, O. M. 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, [S. l.], v. 18, n. 100, 2022. DOI: 10.11117/rdp.v18i100.5973. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5973. Acesso em: 31 maio. 2025.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). Resolução nº 615, de 11 de março de 2025. Dispõe sobre a governança, a gestão e o uso da inteligência artificial no Poder Judiciário. Brasília, DF, 2025.

KOSINSKI, Mateus. O que é inteligência artificial (IA) de caixa preta? IBM, 24 de outubro de 2024. Disponível em: https://www.ibm.com/think/topics/black-box-ai. Acesso em: 31 maio 2025.

NUNES, D. José Coelho; ANDRADE, Oswaldo Morato de. O uso da inteligência artificial explicável enquanto ferramenta para compreender decisões automatizadas: possível caminho para aumentar a legitimidade e confiabilidade dos modelos algorítmicos? Revista Eletrônica do Curso de Direito da UFSM, Santa Maria, v. 18, n. 1, p. e69329, 2023. DOI: 10.5902/1981369469329. Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/69329. Acesso em: 31 maio 2025.

OLIVEIRA, Rafael Tomaz de. O uso de inteligência artificial na tomada de decisão judicial. *Revista Internacional Consinter de Direito*, São Paulo, v. 8, n. 15, p. 300–324, jul./dez. 2022. Disponível em: https://www.scielo.br/j/rinc/a/qRC4TmVXVDJ8Wkv7Ns49jxH. Acesso em: 31 maio 2025.

TOLEDO, Cláudia; PESSOA, Daniel. O uso de inteligência artificial na tomada de decisão judicial. *Revista de Investigações Constitucionais*, Curitiba, v. 10, n. 1, e237, jan./abr. 2023. Disponível em: https://revistas.ufpr.br/rinc/article/view/e237. Acesso em: 31 maio 2025.

CONTROLE ALGORITMO E VIGILÂNCIA DIGITAL: "*FORTUNE TIGER*" E SEUS IMPACTOS SOCIAIS

Ana Clara Mendonça Silva

Mestranda do Programa de Pós-Graduação em Direito Ambiental da Universidade do Estado do Amazonas. Advogada

Lattes: http://lattes.cnpq.br/1792755283327702

ORCID: https://orcid.org/0009-0001-6791-7388

Ana Raquel Monassa Dantas

Mestranda do Programa de Pós-Graduação em Direito Ambiental da Universidade do Estado do Amazonas. Advogada

Lattes: https://lattes.cnpq.br/5595071271859992

ORCID: https://orcid.org/0009-0008-7740-7198

OBJETIVOS

O objetivo da pesquisa é analisar o controle algoritmo e a vigilância digital frente às plataformas de jogos de azar, "*fortune tiger*", haja vista todo o impacto social negativo em torno delas.

METODOLOGIA

A metodologia utilizada nessa pesquisa foi a do método dedutivo, uma vez que se partiu de um conceito amplo do que seria algoritmo, controle e vigilância digital, para se chegar ao fim específico de analisar de que forma estes são exercidos através das plataformas de jogos de azar, e como isso impacta a vida das pessoas. Quanto aos meios, a pesquisa utilizou-se de produções bibliográficas, bem como

documentos dispostos em bibliotecas científicas. Quanto aos fins, a pesquisa foi qualitativa.

Palavras – chave: controle social; vigilância digital; plataformas de azar.

CONTROLE ALGORITMO E VIGILÂNCIA DIGITAL

O avanço da tecnologia trouxe inovações para diversas áreas da vida, como estudos, notícias, informações, trabalho, política, entretenimento e outras. Não se pode questionar que o referido avanço, em muitos aspectos, facilitou a vida da população, como a otimização do trabalho e dos estudos. No que tange ao "entretenimento", tem-se as famosas plataformas de jogos de azar, que se tornaram um grande risco à saúde mental, financeira e social das pessoas, tendo em vista o constante controle e vigilância digital que estas estão submetidas, exatamente como preveem os algoritmos. Diante disso, faz-se necessário a priori entender o que seriam os algoritmos e como ocorre o controle e a vigilância digital.

Algoritmo é uma sequência de ações que devem ser tomadas para se chegar em determinado resultado. No mundo virtual, o conceito de algoritmo decorre de todos os passos que devem ser tomados para entregar o resultado desejado ao usuário. Segundo Fava (2015, p. 40) esse resultado só é possível porque o usuário deixa rastros que fazem com que o algoritmo entenda o que deve fazer. A partir desses rastros, o usuário começa a se tornar previsível, o que alimenta o sistema com suas preferências, gerando o famoso *feedback*.

Os algoritmos exercem um controle social, como um instrumento de poder, filtrando informações e "ditando" comportamentos. Nesse sentido, Silva (2024, p.3) faz uma diferenciação entre as noções de controle de Foucault (1975) e Deleuze (1992):

> Enquanto Foucault (1975) discute a sociedade disciplinar – caracterizada pela regulação da vida via instituições como prisões, escolas e hospitais

> –, Deleuze (1992) argumenta que as sociedades contemporâneas operam por um controle mais difuso e virtual.

Ainda segundo Silva (2024), o controle social defendido por Deleuze (1992) possui uma ideia de hegemonia algorítmica, ou seja, seria uma forma de manipulação exercida pelos algoritmos, que determina quais informações o indivíduo vai receber. Nesse sentido, os algoritmos têm como parâmetro os conteúdos mais vistos e de maior engajamento, influenciando diretamente no desenvolvimento da construção de opiniões.

Dal Castel (2025), esclarece que o controle social está diretamente ligado às tecnologias, uma vez que é exercido mediante as mídias sociais, serviços de segurança via câmeras, pelas publicidades de vendas realizadas por aplicativos de interação social e outros. No âmbito das publicidades, é possível verificar que os algoritmos influenciam os usuários em diversos aspectos da vida, que vão muito além de meras aquisições de produtos, visto que também influenciam no modo de pensar e de agir daqueles que consomem e que alimentam as plataformas digitais. Sobre isso, Silva (2025, p. 16) esclarece que:

> É visto que os algoritmos que direcionam a publicidade não apenas influenciam decisões de compra, mas também moldam percepções, opiniões e comportamentos em escala social. A coleta massiva e contínua de dados permite às plataformas não apenas reagir a preferências existentes, mas ativamente moldá-las, criando um ciclo de retroalimentação onde o consumo de conteúdo e a exposição à publicidade se reforçam mutuamente.

Dessa forma, verifica-se que o Autor reforça a ideia de que o controle social é exercido por meio de inúmeros meios, o que leva à

sociedade a uma constante vigilância. Nesse sentido, Silva et al (2024, p. 9) corroboram que:

> Apesar das aparentes vantagens proporcionadas pelo capitalismo de vigilância, as atividades das plataformas digitais são altamente controversas. Muitas vezes, essas atividades ultrapassam os limites da legalidade, desafiando a capacidade de intervenção das autoridades jurídicas. Silva et al (2024, p. 9)

Assim, segundo essa afirmação, depreende-se que a vigilância digital está presente em inúmeras plataformas, e que diversas atividades realizadas por essas plataformas não possuem respaldo jurídico, deixando os consumidores vulneráveis. Diante disso, é possível identificar que o controle, antes exercido de forma física, agora é exercido por meios digitais, onde as pessoas não percebem que se encontram em situação de manipulação constante por inúmeras plataformas, sendo as plataformas de jogos de azar o mais "novo" meio de vigilância.

PLATAFORMAS DE JOGOS DE AZAR E SEUS IMPACTOS SOCIAIS

As plataformas de jogos de azar são locais virtuais onde uma pessoa aposta dinheiro contando com a sorte de que pode ganhar mais, são chamadas também de "Bets". Mendieta e Queiroz (2024, p. 9) esclarecem que o termo "Bets" significa aposta, e que engloba o Fortune Tiger (jogo do tigrinho), jogo do Aviator e os jogos desportivos, que dependem de resultados de outros jogos.

Os jogos de azar sempre foram uma presença constante na sociedade brasileira, entretanto, com o advento das plataformas online, e mais especificamente das "bets", os jogos ganharam um destaque exacerbado. Segundo Fazolin e Almeida (2024, p. 5), as plataformas se propagaram em 2023, ano em que o povo brasileiro demonstrou o quão vulnerável é quando se trata de apostas.

Fazolin e Almeida (2024, p. 5) ainda complementam que, antes do advento da internet, havia a possibilidade de se controlar os vícios em relação aos jogos de azar, entretanto, com a plataformização desses jogos, controlar as apostas se tornou impossível. Diante disso, é possível verificar que as pessoas ficam à mercê dos jogos, uma vez que o acesso virtual a eles facilita a disseminação.

Assim, diante da facilidade de se inserir nas plataformas, a população fica exposta a um controle virtual absurdo, que só acarreta prejuízos. Fazolin e Almeida (2024, p. 6) entendem que essa facilidade à inserção nas plataformas, aliada às publicidades realizadas por digitais influencers, acarretam vício e perdas patrimoniais incontáveis. Em um relatório realizado em agosto de 2024 por Cherman e Duarte (2024), para o Departamento de Pesquisa Macroeconômica do Itaú, foi elucidado que:

> Se desconsiderarmos os valores recebidos pelos apostadores quando ganham, teríamos uma estimativa exagerada dos gastos do consumidor com apostas. Para ilustrar, estimamos que o gasto total excluindo os valores recebido por apostadores vitoriosos seja de R$ 68,2 bilhões, valor substancialmente acima de nossa estimativa para o gasto líquido, de R$ 23,9 bilhões (acumulado de doze meses até junho)

Dessa forma, depreende-se que os brasileiros gastam muito mais do que ganham. Esse vício é fruto de um controle social exercido através de certos estímulos ao apostador, que possui a ilusão que o jogo lhe trará recompensa financeira, e mesmo quando não ganha as apostas continuam.

Ademais, o modo de cadastro nas plataformas enseja uma vigilância sobre o usuário sem precedentes, tendo em vista que a inserção dos dados pessoais nas referidas plataformas expõe o apostador a uma constante observação pelas empresas, iniciando ali

uma modelagem de comportamento, onde a pessoa passa a ter suas decisões influenciadas e manipuladas.

À vista disso, uma medida política capaz de mitigar os prejuízos causados pelo vício nessas plataformas é a conscientização da população quanto aos riscos trazidos pelos jogos. Martins et al (2024, p. 11) entendem que:

> É necessário que o poder público se empenhe no desenvolvimento de políticas públicas em prol da conscientização, campanhas educativas, linhas de apoio e prevenção, assim como é primordial que se elaborem regras de restrições ao marketing de jogos de azar direcionado a jovens e populações vulneráveis.

Importante mencionar que, o público que mais sofre com os prejuízos causados pelo vício nas plataformas é a população de baixa renda, uma vez que o "objetivo" do jogo seria a percepção de renda através de ganhos, caso o usuário venha a obter êxito. Ocorre que, essas plataformas são programadas para dar "um gostinho" aos seus usuários no início, e após isso são perdas atrás de perdas, causando danos graves à saúde. Nesse sentido, Ribas et al (2025, p.4) apontam que:

> A acessibilidade a plataformas digitais de apostas tem ampliado o alcance dos jogos de azar, aumentando o risco de vícios, especialmente entre jovens. Perdas financeiras podem levar ao endividamento, enquanto o estigma social e a sensação de fracasso frequentemente resultam em isolamento e problemas de saúde mental, como depressão e ansiedade.

Portanto, a implantação de políticas públicas para conscientizar a população se torna tão importante, sobretudo para a classe vulnerável,

sendo a que mais precisa de amparo, pois entram na furada que são as plataformas em busca de uma renda, muitas vezes até mesmo para comprar um alimento, o que acaba sendo um mal inenarrável para o usuário e toda a sua família.

CONCLUSÃO

A problemática que instigou essa pesquisa foi a de se verificar de que forma as plataformas de jogos de azar exercem o controle social e vigilância digital sobre a população brasileira. O objeto foi cumprido, a medida em que se verificou os impactos que os jogos causam na vida das pessoas. O resultado dessa pesquisa foi o de o controle social e a vigilância digital são exercidos através de inúmeros "canais", como redes sociais, sistemas de vigências e outros. Com o advento das plataformas de jogos de azar, as chamadas "Bets" acabaram por se tornar mais um meio de controle e vigilância, ao passo em que os usuários agem conforme o algoritmo do jogo prevê, além de que dados pessoais destes ficam registrados nos sistemas, auxiliando as empresas na famosa vigilância digital. Entretanto, os prejuízos vão muito além disso, uma vez que famílias estão sendo destruídas e pessoas estão adoecendo psicologicamente, haja vista que o vício pelo jogo enseja atitudes que colocam em risco a integridade física, mental e financeira daqueles que utilizam as plataformas. Diante disso, foi observado que há a possibilidade de conscientizar a população através de políticas públicas que destaquem os perigos presentes nas plataformas, e que as inúmeras divulgações feitas por influenciadores não passam de publicidade enganosa para lucrar de forma fácil.

REFERÊNCIAS

DAL CASTEL, M.; CHIARI GONÇALVES, V. O Controle Social na Era do Capitalismo Digital: Vigilância privada e pública, e seus custos ambientais. **Revista Justiça do Direito**, *[S. l.]*, v. 38, n. 3, p. 162-181, 2025. DOI: 10.5335/rjd.v38i3.15278. Disponível em: https://seer.upf.br/index.php/rjd/article/view/15278. Acesso em: 1 mai. 2025.

DE JESUS-SILVA, T. H. O papel das plataformas digitais na Indústria Cultural sob a perspectiva da Economia Política da Comunicação. **INSÓLITA - Revista Brasileira de Estudos Interdisciplinares do Insólito, da Fantasia e do Imaginário**, *[S. l.]*, v. 4, n. 2, p. 9–27, 2025. Disponível em: https://revistas.intercom.org.br/index.php/insolita/article/view/4950. Acesso em: 1 mai. 2025.

FAVA, Gihana Proba. **O efeito filtro bolha: como dispositivos de vigilância digital convertem usuários em produtos**. 2015. Disponível em: https://repositorio.ufjf.br/jspui/handle/ufjf/1512. Acesso em: 4 de mai. 2025.

SILVA, Thiago Henrique de Jesus. A Reconfiguração da Hegemonia na Era Digital: o Papel dos Algoritmos no Controle da Informação. **Novos Olhares, São Paulo, Brasil, v. 13, n. 2, p. 137–149, 2024**. DOI: 10.11606/issn.2238-7714.no.2024.230401. Disponível em: https://www.revistas.usp.br/novosolhares/article/view/230401. Acesso em: 1 mai. 2025.

MENDIETA, Fábio Henrique Paniagua; QUEIROZ, André Felipe. **Revista Contribuciones a Las Ciencias Sociales, São José dos Pinhais, v.17, n.10, p. 01-21, 2024**. Bets e apostas online: o jogo do Tigrinho e seu efeito tangerina. Disponível em: https://www.researchgate.net/profile/Andre-Queiroz-7/publication/384728888_Bets_e_apostas_online_o_jogo_do_Tigrinho_e_seu_efeito_tangerina/links/67053e38f246af124355f6f7/Bets-e-apostas-online-o-jogo-do-Tigrinho-e-seu-efeito-tangerina.pdf. Acesso em: 17 de mai. 2025.

FAZOLIN, Dayse Karoline Vieira Catellane; ALMEIDA, Andreia Alves de. A IMPORTÂNCIA DA REGULAMENTAÇÃO SOBRE OS JOGOS DE AZAR ONLINE . **Revista Ibero-Americana de Humanidades, Ciências e Educação**, *[S. l.]*, v. 9, n. 12, p. 711–727, 2024. DOI: 10.51891/rease.v9i12.12805. Disponível em: https://periodicorease.pro.br/rease/article/view/12805. Acesso em: 18 mai. 2025.

CHERMAN, Luiz; DUARTE, Pedro. Apostas on-line: estimativas de tamanho e impacto no consumo. **Macro Visão Relatório do Departamento de Pesquisa Macroeconômica do Itaú Unibanco S.A. 13 de agosto de 2024**. Disponível em: https://macroattachment.cloud.itau.com.br/attachments/a77e92d9-319f-45ca-b657-6c721241804b/13082024_MACRO_VISAO_Apostas_on-line.pdf. Acesso em: 18 mai. 2025.

MARTINS, Letícia da Costa Domingues; BONINI, Amanda Maria; STEOLA, Isabella. IMPACTO SOCIAL DOS JOGOS DE AZAR ONLINE E SUAS CONSEQUÊNCIAS DEMOCRÁTICAS. **Anais do Congresso Brasileiro de Processo Coletivo e Cidadania**, *[S. l.]*, v. 12, n. 12, p. 772–791, 2024. Disponível em: https://revistas.unaerp.br/cbpcc/article/view/3487. Acesso em: 18 mai. 2025.

RIBAS, Natália Marcondes *et al.* "Jogo do Tigrinho" e os perigos do jogo patológico. **Debates em Psiquiatria, Rio de Janeiro. 2025;15:1-5**. Disponível em: https://doi.org/10.25118/2763 9037.2025.v15.1393. Acesso: 20 mai. 2025

SILVA, Tiago Luis Schervenski da; OLIVEIRA, P. F. F. A. D.; AMARAL, A. J. D. **Algoritmos, Capitalismo De Plataforma E A Incessante Busca Pelo Estar**. Disponível em: https://repositorioiberojur.com/index.php/catalog/catalog/view/33/465/627. Acesso em: 20 mai. 2025

O IMPACTO DOS AVANÇOS TECNOLÓGICOS E DA INFORMAÇÃO NOS PROCESSOS DENTRO DAS EMPRESAS

Ana Cristina de Melo Batista

Discente do curso de especialização em Direito, Compliance e Mecanismos Anticorrupção da Universidade do Estado do Amazonas - UEA. Bacharela em Administração pela UEA.

Rochelle Monteiro Brito

Mestre em Administração pela Universidade Federal de Viçosa.

PALAVRAS-CHAVE: Avanços tecnológicos; Atividades organizacionais; Organização moderna.

1. OBJETIVOS

O presente trabalho tem como objetivo principal estudar como os avanços tecnológicos mudaram os processos dentro das empresas, tendo em vista que a internet mudou a forma com que as organizações trabalham e executam suas atividades organizacionais, englobando todas as áreas existentes na companhia. Além disso, tem como objetivos específicos analisar os principais impactos dos avanços nas atividades organizacionais e entender os prós e contras desses avanços para as organizações.

2. METODOLOGIAS

A metodologia aplicada foi a abordagem metodológica qualitativa e pesquisa bibliográfica com estudos relacionados ao assunto. Fonseca (2010, p. 96) define que a pesquisa bibliográfica é "o primeiro passo de todo trabalho cientifico, sobretudo pela exploração que se faz em textos".

3. DESENVOLVIMENTO

Atualmente as empresas contam com diversas ferramentas tecnológicas para atingir seus objetivos organizacionais. Independente do ramo de atividade, nas últimas décadas é notável como a expansão das novas tecnologias ao redor do mundo mudaram completamente os processos existentes dentro das empresas. Para Ribeiro (2019) as empresas são parte da sociedade com responsabilidades além do dos resultados financeiros, de que no plano externo – na sociedade – a organização moderna precisa apoiar ações que melhoram os serviços básicos, de forma a expandir o poder aquisitivo da população e atrair consumidores. A forma com que se relacionam, gerenciam pessoas, recrutam e selecionam, treinam, produzem, gerenciam suas finanças, transportam e armazenam seus produtos, o *marketing* e entre outras atividades pertinentes a organização transformaram-se ao passar dos anos.

Gil (2001, p. 39) destaca sobre o impacto das novas tecnologias:

> O ambiente em que se situam as organizações apresenta-se cada vez mais volátil. A cada dia surgem máquinas melhores e *softwares* mais inteligentes. A revolução da informática vem proporcionando com frequência cada vez maior a troca de operadores por computadores e robôs. Como o ritmo de mudança torna-se cada vez mais veloz, logo após a introdução de novas tecnologias já se percebe a necessidade de inovar; por exemplo, um computador de última geração, ao ser adquirido, já começa a tornar-se obsoleto.

O ambiente volátil e o surgimento de recursos mais avançados demonstram a necessidade de as organizações recriarem seus processos, analisando como investir e inserir corretamente. Hoje, muitas empresas contam com equipamentos e máquinas de alto

nível, além de diversos computadores avançados importantes para a execução de suas atividades.

Importante destacar de como os avanços tecnológicos mudam claramente as empresas, e os avanços no domínio da informação e também da comunicação são revolucionários. A internet é transformadora, pois possibilitou não somente a transmissão e recepção de informações, como também transações comerciais e a atuação nas bolsas internacionalmente. (Gil, 2001)

Chiavenato (2016) explica que em um mundo de grandes mudanças, as organizações devem ser rápidas e mudar processos, mudar estratégias, alterar produtos e serviços, buscar utilizar novas tecnologias e entre outros. Destaca ainda, que as pessoas são fundamentais nessas mudanças, é essencial alinhá-los em suas atividades. Seguindo o proposto, uma das áreas mais impactadas pelos avanços tecnológicos e a internet é a de Recursos Humanos. As novas tecnologias necessitam do suporte humano para o eficiente uso nas atividades da empresa, logo é fundamental que as pessoas responsáveis por manusear essas tecnologias sejam qualificadas. Então, devido o investimento nessas novas tecnologias nas organizações, priorizar o recrutamento e seleção, e o treinamento desses trabalhadores é indispensável.

Os processos de recrutamento e seleção passaram por mudanças significativas ultimamente, a tecnologia e a internet contribuíram para que esses processos melhorassem seu desenvolvimento. Ribeiro (2019) comenta que a procura pelo candidato adequado a função determinada, é essencial reservar um espaço no *site* da organização para o preenchimento de ficha ou para o envio do currículo do candidato. As empresas contam com ferramentas online para recrutar e selecionar candidatos com base nos currículos e informações pessoais importantes para a escolha do candidato com o perfil mais adequado. O banco de talentos é uma realidade presente em várias empresas.

Segundo Gil (2001) há um crescimento do setor de serviços, devido a diversos fatores sobretudo os avanços científicos e tecnológicos, que

provocaram a extinção de muitos empregos industriais e mudaram as formas de organização e gestão. Isso requer profissionais com elevados níveis de capacitação técnica, logo, mostra que os processos de seleção deverão tornar-se mais aprimorados para a garantia de pessoal habilitado.

Muitas são as vantagens geradas pelos avanços tecnológicos, praticamente todas as organizações públicas ou privadas incorporaram em suas estruturas tecnologias indispensáveis para a realização de suas atividades. Uso de programas específicos para cada processo, informações compartilhadas, processos seletivos com menos custos e trabalho, automação, gestão financeira ágil e outras.

Chiavenato (2016, p. 2) destaca que

> a Era da Informação colocou o conhecimento como o mais importante recurso organizacional: uma riqueza intangível, invisível, mas fundamental para o sucesso das organizações. E isso trouxe situações completamente inesperadas, como a crescente importância do capital intelectual como riqueza organizacional.

Apesar da necessidade de investir em novas tecnologias, os avanços tecnológicos têm pontos que devem ser observados pelas empresas, na qual podem tornar o investimento e introdução dessas tecnologias na empresa um problema. Para Lacombe (2005) o século XXI inicia com inovações tecnológicas e com o agravamento do desemprego. A chegada de novas tecnologias provoca deslocamentos entre ocupações, o que aumenta a necessidade de qualificação dos trabalhadores.

Ribeiro (2019, p. 26) argumenta que:

> A empresa não deseja restringir a liberdade de ninguém, mas as horas de trabalho devem ser usadas para execução das tarefas. Sem dúvida, as novas

> mídias sociais, os *smartphones* e os computadores são meios usados na comunicação entre familiares e amigos, mas existe uma nova perspectiva: as relações de trabalho, apesar de serem relações sociais como as demais, também são reguladas e sujeitas a regras claras, tanto para a empresa como para o emprego, contratado e pago para executar tarefas durante sua jornada de trabalho.

A questão do uso de celulares ou uso inadequado dos computadores no ambiente de trabalho é uma pauta que deve ser analisada pelos empresários. Outro ponto sobre as novas tecnologias é principalmente a qualificação dos funcionários, pois claramente as empresas deverão buscar trabalhadores qualificados para alinhá-los com as tecnologias presentes. Treinar e desenvolver deve ser visto como uma das prioridades para a empresa, porque a falta de preparo dos responsáveis pelas novas tecnologias pode gerar mais custos do que lucro.

4. CONCLUSÕES

Com base na pesquisa, entende-se que as empresas sofreram grandes impactos gerados pelos avanços tecnológicos mundialmente, com o surgimento de novas máquinas, equipamentos, *softwares*, ferramentas digitais, troca de informações e mudanças no comportamento humano. Ainda, é visível como os impactos atingem diretamente todas as áreas e processos na busca pela melhoria e eficiência. Praticamente todas as organizações utilizam de tecnologias e informática para realizarem suas atividades gerais, algumas com tecnologias de alto nível de performance e lançamento. É evidente que isso contribui para a sociedade como um todo, uma vez que são essenciais para todos os serviços (públicos ou privados).

Com tantas ferramentas disponíveis para as empresas é importante atentar-se para as novas legislações acerca da internet.

A Lei Geral de Proteção de Dados Pessoais – LGPD é um exemplo, pois dispõe de assuntos relacionados ao uso e compartilhamento de dados pessoais e a privacidade dos dados. O grande volume de dados e informações disponibilizadas online devem ser utilizados em conformidade com os regulamentos internos e externos a empresa.

Para tanto, de forma a mitigar os riscos e desafios causados pelos avanços tecnológicos e a informática, recomenda-se atenção perante o investimento em máquinas e equipamentos. Principalmente, definir quem irá ficar responsável pelo manuseio e alimentação, deve-se escolher uma pessoa qualificada para a função. Levando em consideração que a manutenção, muitas vezes, de máquinas e equipamentos de alto nível, é custosa para a organização. Atribuir o uso delas por pessoas despreparadas poderá ocasionar o mal uso, e consequentemente, pode levar à danificação do aparelho.

REFERÊNCIAS

CHIAVENATO, Idalberto. **Treinamento e desenvolvimento de recursos humanos**: como incrementar talentos nas empresas. 8. ed. rev. e atual. Barueri: Manole, 2016.

FONSECA, Luiz Almir Menezes. **Metodologia cientifica ao alcance de todos**. 4. ed. Manaus: Editora Valer, 2010.

GIL, Antonio Carlos. **Gestão de Pessoas**: enfoque nos papéis profissionais. São Paulo: Altas, 2001.

LACOMBE, Francisco José Masset. **Recursos Humanos**: princípios e tendências. São Paulo: Saraiva, 2005.

RIBEIRO, Antonio de Lima. **Gestão de pessoas**. 3. ed. São Paulo: Saraiva Educação, 2019.

O RISCO DE DESUMANIZAÇÃO DO DIREITO DE FAMÍLIA COM O USO DA INTELIGÊNCIA ARTIFICIAL

Ana Lívia Figliuolo Bezerra de Menezes

Graduanda do 7º período do curso de Direito pela Universidade do Estado do Amazonas.

Neuton Alves de Lima

Doutor em Direito pela Universidade Federal de Minas Gerais.

PALAVRAS-CHAVE: Direito de Família. Subjetividade. Inteligência Artificial. Tecnologia.

1. OBJETIVOS

O presente resumo tem como objetivo compreender o motivo pelo qual a aplicação da inteligência artificial na atividade de julgar processos de matéria de Direito de Família não é cabível, em virtude de a valoração humana ser essencial para o entendimento dos sentimentos confusos inerentes às fortes relações formadas pela instituição familiar.

2. METODOLOGIA

Nesta pesquisa, a metodologia é de caráter qualitativa, sendo utilizado o método dedutivo, por meio de fontes bibliográficas, tais como doutrinas, artigos acadêmicos e revistas que se coadunam com a temática abordada, bem como análise de textos legais, a exemplo de Códigos e Resolução do Conselho Nacional de Justiça.

3. DESENVOLVIMENTO

A expressão Inteligência Artificial (IA) foi apresentada por John McCarthy, referindo-se à ideia de uma "conjectura de que todos os aspectos de aprendizagem ou qualquer outra característica da inteligência podem, em princípio, ser descritos com tanta precisão que uma máquina pode simulá-la" (MCCARTHY, 2006, p. 12). Sob essa ótica, entende-se que, para obter os resultados positivos pretendidos, a máquina deve ser alimentada com a maior gama de informações possíveis, amplas e específicas, permitindo, assim, a percepção de padrões, passíveis de serem aplicados em situações reais.

A Inteligência Artificial se faz presente no cotidiano, seja em relação a atividades simples, como estabelecer a comunicação com clientes em um site virtual por meio de *chatbot* (programa simulador de diálogos, escritos ou orais, com indivíduos), seja na elaboração de sistemas complexos em tecnologia, a exemplo de robôs criados à semelhança do homem para substituição da mão de obra humana em empresas. Em razão disso, a IA vem ganhando espaço em diversas áreas do conhecimento, e no Direito não poderia ser diferente.

Marcado pelo acúmulo excessivo de processos (fenômeno denominado de hiperjudicialização), pela morosidade quanto à resolução destes, além dos elevados custos para a manutenção do sistema jurídico, o Poder Judiciário enfrenta dificuldades para promover a real garantia dos direitos materiais e o efetivo acesso à justiça pelos cidadãos. Diante desta problemática, a inteligência artificial se mostra como artifício essencial para aprimorar o desempenho dos servidores, bem como assegurar maior celeridade e dinamicidade às demandas judiciais, uma vez que ela pode ser utilizada para a produção de documentos e na pesquisa de jurisprudência, tendo como base a profunda análise das informações incluídas em seu banco de dados, baseadas em decisões anteriores produzidas pelo próprio juiz ou pelo tribunal em geral. Assim, é possível considerar que a IA viabiliza o aperfeiçoamento do acesso à justiça, tornando-a mais concreta e ágil.

Observando a exposição de motivos da Resolução nº 615 do Conselho Nacional de Justiça (CNJ), que estabelece diretrizes para a aplicação de soluções desenvolvidas com recursos de inteligência artificial no âmbito judiciário, verifica-se que essa tecnologia deve ser utilizada em consonância com os valores éticos fundamentais, a dignidade da pessoa humana, como também com os direitos à segurança da informação e à privacidade. Nesse ínterim, existem determinados institutos os quais necessitam ter uma proteção mais firme em relação ao aproveitamento da IA, dentre eles o Direito de Família, porque apresenta uma conexão notavelmente especial com elementos morais e éticos.

Segundo ensinamentos da doutrinadora Maria Berenice Dias, a família é uma construção cultural na qual cada membro possui uma função determinada, ligados por laços de afeto e respeito, e não necessariamente critérios biológicos. A família é entendida tanto como uma estrutura privada quanto pública, pois é formada a partir das interações íntimas entre seus integrantes, ao mesmo tempo em que é protegida pelo Estado, por considerar que esse núcleo é a base primária de formação de cada pessoa e, em consequência, da própria sociedade (DIAS, 2021, p. 43-45).

A família é o primeiro espaço de socialização do ser e tem a sua importância devidamente reconhecida, inclusive legalmente, conforme art. 226 da Constituição Federal (BRASIL, 1988), uma vez que nela se desenvolvem valores éticos, senso de responsabilidade, solidariedade, laços fraternais, além de trazer a sensação de pertencimento ao indivíduo. Protegendo essa instituição, o Estado incentiva o melhor preparo do cidadão para o convívio em coletividade.

Ademais, a família é um espaço de refúgio e cuidado aos vulneráveis, tais como menores, incapazes e idosos, grupos esses que requerem atenção especial, alcançada, em grande parte, pelas relações de afeto junto aos parentes, garantindo-lhes segurança, proteção e delicadeza no tratamento de seus anseios e necessidades. Destarte, amparar a estrutura familiar é imprescindível para concretizar os direitos fundamentais desses indivíduos.

O Direito de Família é um ramo do direito intrinsecamente ligado ao interior da pessoa, razão pela qual possui caráter personalíssimo. Em se tratando de conflitos surgidos a partir das relações entre parentes, os casos familiares são constituídos por uma carga consideravelmente grande de emoções e, por conta disso, a subjetividade é um elemento fundamental para a tentativa de solucionar as crises afetivas. Nesse viés:

> [...] há que se considerar que em muitas causas em que estão envolvidos os vínculos afetivos, há temores, queixas, mágoas e sentimentos confusos, e nem sempre a resposta judicial é apta para responder aos anseios daqueles que buscam muito mais resgatar danos emocionais do que propriamente obter compensações econômicas (SIQUEIRA, FORNASIER, LARA, 2022, p. 82).

O direito familiar envolve pessoas que estão passando por difíceis momentos na vida pessoal e cujos interesses analisados, em grande parte das hipóteses, são, na verdade, pertencentes a quem não é parte na ação, como o filho menor; motivo pelo qual não estão, em regra, em condições de tomar decisões por si próprios e, por isso, recorrem ao Judiciário, ficando este responsável por realizar julgamentos acerca de aspectos de vida precisamente íntimos dos envolvidos (BELL, 2019, p. 109). Portanto, é inegável que a emoção e a subjetividade são inerentes às relações familiares e, consequentemente, devem ser levadas em consideração no momento de solucionar o conflito de maneira satisfativa.

Em concordância com esse entendimento, faz-se notar a exigência de que os profissionais envolvidos na questão familiar sejam qualificados em quesitos interdisciplinares, ou seja, para o advogado, o magistrado, o promotor e o defensor, não basta o conhecimento jurídico: é imprescindível ter acesso às ciências sociais e psicológicas, a fim de melhor compreender os sentimentos caóticos e a complexidade dos

vínculos entre familiares, bem como destrinchar e decifrar condutas (DIAS, 2021, p. 94-95). Logo, ao entrar em contato com ações de guarda, adoção de menores, alienação parental e interdição, por exemplo, devem ser realizados estudos psicossociais quando as circunstâncias do caso concreto assim o exigirem, com o fito de investigar os potenciais riscos existentes e como essa pesquisa influenciará na decisão final. Desse modo, a interligação multidisciplinar permite a ampliação do conhecimento de determinada situação familiar, sendo considerada uma ferramenta indispensável para o exame real das condições que permeiam a família por trazer um olhar à subjetividade.

Conforme já mencionado anteriormente, a resposta da IA aos *prompts* depende das informações contidas em seu banco de dados, de maneira que, quanto mais elementos são incluídos em seu armazenamento, maior será a probabilidade de constatação de padrões -a partir da pesquisa técnica entre os dados obtidos-, ao passo que o conhecimento escasso gera resultados incompletos. Em decorrência de as ações envolvendo direito de família serem resguardadas por segredo de justiça, verifica-se que há um cuidado maior em relação ao uso dessas informações pela IA, sendo obrigatória, exemplificativamente, a anonimização dos dados de origem, bem como a "efetiva proteção e segurança desses dados e de seus titulares", de acordo com o art. 19, §3º, IV da Resolução nº 615 do CNJ (BRASIL, 2025). Nesse sentido, como a prioridade é promover a proteção ao segredo de justiça, é possível que a máquina careça de elementos suficientes para explorar o seu potencial e, por conseguinte, apresentar uma decisão inteiramente adequada ao caso material.

Ademais, a inteligência artificial, embora criada, desenvolvida e atualizada por pessoas, não apresenta todas as habilidades da mente humana. Consequentemente, a atividade se restringe à investigação de padrões, de modo a compatibilizar a situação atual com os anteriores. Apesar de essa tarefa trazer pontos positivos ao âmbito jurídico, como a possibilidade de prever decisões e evitar determinações contraditórias, nenhum processo, por mais semelhante que seja, será idêntico a outro.

Nesse ínterim, o art. 8º do Código de Processo Civil define que o juiz, ao exercer sua função, deverá atender aos fins sociais e às exigências do bem comum (BRASIL, 2015), incumbência essa incompatível com a IA, uma vez que ela, por ser uma máquina, não faz parte do convívio social. Isso impede, por exemplo, a conclusão de uma ação processual marcada por lacunas legislativas, já que a IA não teria a previsibilidade da lei para solucionar o conflito; empecilho esse não existente com o uso do pensamento humano, pois, a partir dos costumes e da ponderação, pode alcançar uma deliberação especial para a situação omissa. Portanto, torna-se uma ferramenta baseada predominantemente na verificação algorítmica, ou seja, objetiva, sem levar em consideração aspectos sociais e éticos, provenientes da experiência humana.

É possível, então, a utilização de programas tecnológicos para auxiliar na elaboração de sentenças, mas jamais de maneira absolutamente autônoma, em virtude de ser um ato que somente o indivíduo, enquanto cidadão no meio coletivo, é capaz de valorar. Em contrapartida, tarefas essencialmente objetivas, tais como as certidões de vencimento de prazo ou a pauta de audiências, têm a plena possibilidade de serem realizadas pela inteligência artificial, tendo em vista que não há a necessidade de valoração da atividade, por se tratar de uma avaliação precisa e inequívoca. Outrossim, é válido mencionar que, independentemente da circunstância, é obrigatória a revisão e supervisão humana dos resultados obtidos pela IA (BRASIL, 2025).

Como visto, a inteligência artificial não apresenta, em sua formação, traços de sensibilidade, o que impede que a decisão judicial seja produzida exclusivamente por ela. No campo do Direito de Família, o entendimento mencionado é bem mais evidente, uma vez que esse ramo jurídico exige habilidades que não são estritamente técnicas, mas também levam em consideração as experiências de vida (BELL, 2019, p. 109), fator ausente para as tecnologias. Essa característica do Direito de Família é respaldada na ideia de que se deve buscar, sempre que possível, a solução consensual dos conflitos familiares, pois a decisão impactará direta e profundamente as partes envolvidas.

A família apresenta particularidades as quais impõem maior proteção e cuidado no julgamento. É uma estrutura delicada e sensível, voltada para a garantia do bem-estar de grupos vulneráveis, de forma que é inconcebível ignorar os sentimentos e emoções inerentes a essa instituição, pois os vínculos de afetividade são anteriores à relação jurídica processual formada. Em suma, não basta a análise técnico-jurídica do caso apresentado, uma vez que não é capaz de captar a essência do laço familiar, não se adequando à realidade.

Então, proferir decisões que restringem o exame da hipótese a aspectos estritamente objetivos, padronizados e pragmáticos lhe retira a característica substancial do direito de família: a humanidade. Para tanto, é essencial voltar-se a apuração de conhecimentos interdisciplinares, os quais permitem verificar as peculiaridades da relação retratada. Não se nega a relevante contribuição da inteligência artificial no Poder Judiciário, em específico nas varas de família, porém é necessário que a sua atuação seja voltada a atividades mecânicas que fornecem respostas exatas, tais como emissão de certidões e intimações.

4. CONCLUSÃO

Diante do exposto, nota-se que a inteligência artificial tem importante papel em proporcionar celeridade e dinamicidade nas demandas judiciais, em razão da viabilidade de uso em atividades instrumentais, promotoras do andamento processual, trazendo, por conseguinte, maior probabilidade de efetivação dos direitos materiais do cidadão e concretização do acesso à justiça.

Por outro lado, em se tratando de matéria decisória, em especial no Direito de Família, a IA não está capacitada a julgar, uma vez que lhe carece o elemento humano. O ambiente familiar é o primeiro espaço de socialização do homem, sendo formado por cargas emocionais e sensíveis, bem como é indispensável para a proteção e resguardo dos grupos vulneráveis. Nesse sentido, é fundamental o olhar mais

delicado às demandas desse ramo jurídico, por envolver aspectos subjetivos e sentimentais, bem como incorporar ao raciocínio julgador os resultados provenientes das avaliações realizados pelas equipes multidisciplinares: sociais, psicológicas e psiquiátricas.

REFERÊNCIAS

ALCAIDE, Sofia Travassos. **A Aplicabilidade de Sistemas de Inteligência Artificial no Âmbito do Direito de Família e dos Menores**. [S. l.], p. 1-17, 14 dez. 2023. Disponível em: https://hdl.handle.net/1822/88217. Acesso em: 16 maio 2025.

BELL, Felicity. **Family Law, Acess to Justice, and Automation. Macquarie Law Journal**, v. 19, p. 103-132, 2019. Disponível em: https://searchebscohostcom.ez433.periodicos.capes.gov.br/login.aspx?direct=true&db=aph&AN=1413729 69&lang=pt-br&site=ehost-live. Acesso em: 20 maio 2025.

BRASIL. **Constituição (1988).** Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 maio 2025.

BRASIL. **Lei 13.105, de 16 de março de 2015**. Código de Processo Civil. Brasília, DF, Presidência da República, 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 19 maio 2025.

BRASIL. **Resolução nº 615, de 11 de março de 2025 nº 615, de 11 de março de 2025**. Estabelece diretrizes para o desenvolvimento, utilização e governança de soluções desenvolvidas com recursos de inteligência artificial no Poder Judiciário. Brasília, DF: CNJ, 2025. Disponível em: https://atos.cnj.jus.br/files/original1555302025031467d4517244566.pdf. Acesso em: 19 maio 2025.

COVALCHUK, Gabriela Cristina; VIEIRA, Lara Bianca Pinto; ALFONZO, Natália Moritz. **Inteligência Artificial no Direito de Família: Considerações sobre sua Utilização no Cenário Nacional e Internacional**. Revista de Estudos do Vale do Iguaçu, Paraná, v. 1, ed. 42, p. 147-161, 2023.

DIAS, Maria Berenice. **Manual de Direito das Famílias**. 14. ed. rev. atual. e aum. Salvador/BA: Editora JusPodivm, 2021. 1056 p. ISBN 978-65-5680-354-8.

MCCARTHY, John; MINSKY, Marvin L.; ROCHESTER, Nathaniel; SHANNON, Claude E. **A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence**, August 31, 1955. AI Magazine, v. 27, n. 4, 2006.

PAULICHI, Jaqueline da Silva; CARDIN, Valéria Silva Galdino. **A Inteligência Artificial como meio de auxílio ao juiz e a sua capacidade decisória**. Revista Thesis Juris, São Paulo, ano 1, v. 12, p. 147-166, 2023. Disponível em: https://periodicos.uninove.br/thesisjuris/article/view/22102. Acesso em: 23 maio 2025.

SIQUEIRA, Dirceu Pereira; FORNASIER, Mateus de Oliveira; LARA, Fernanda Corrêa Pavesi. **Inteligência artificial e Direito de Família: prenúncio de novos tempos também para esses direitos?** Revista Direitos Culturais, Santo Angelo, v. 17, n.42, p. 71-87, 2022. Disponível em: https://san.uri.br/revistas/index.php/direitosculturais/article/view/752/416. Acesso em: 20 maio 2025.

TOBBIN, Raissa Arantes; CARDIN, Valéria Silva Galdino; VIEIRA, Tereza Rodrigues. **Inteligência Artificial e Prestação Jurisdicional no Âmbito do Direito de Família: Apoio, Substituição e Disrupção à Luz dos Direito da Personalidade**. Revista de Direito de Família e Sucessão, [S. l.], v. 10, n. 1, p. 66-81, 24 ago. 2024. DOI https://doi.org/10.26668/IndexLawJournals/2526-0227/2024.v10i1.10646. Disponível em: https://indexlaw.org/index.php/direitofamilia/article/view/10646. Acesso em: 16 maio 2025.

O IMPACTO DA DIVULGAÇÃO DE INFORMAÇÕES PROCESSUAIS NAS REDES SOCIAIS E OS RISCOS À PRESUNÇÃO DE INOCÊNCIA E AO DEVIDO PROCESSO LEGAL

Camily Figueiredo dos Santos

Acadêmica de Direito na Escola Superior Batista do Amazonas (ESBAM). Lattes: http://lattes.cnpq.br/ 5281672464238114. E-mail: camillyssantos1234@gmail.com.

Renato Ferreira Ribeiro Matta

Mestrando do Programa de Pós-Graduação em Direito Ambiental da Universidade do Estado do Amazonas. Delegado de Polícia Civil. Lattes: http://lattes.cnpq.br/3814728914232176

ORCID: https://orcid.org/0009-0008-3679-462X. E-mail: rfrm.mda25@uea.edu.br

Palavras-chave: presunção de inocência; devido processo legal; redes sociais; exposição midiática; garantias constitucionais.

1. OBJETIVOS

O presente trabalho tem como objetivo analisar os efeitos da divulgação de informações processuais nas redes sociais e seus reflexos sobre a presunção de inocência e o devido processo legal, à luz dos princípios constitucionais e das garantias processuais penais. Busca-se compreender como a exposição midiática precoce de investigados e acusados pode comprometer o contraditório, a ampla defesa e a imparcialidade judicial, além de provocar danos irreversíveis à honra, imagem e dignidade da pessoa humana. A pesquisa propõe, ainda, medidas normativas e educativas voltadas à proteção dos direitos fundamentais na era digital, com vistas à preservação dos pilares do Estado Democrático de Direito.

2. METODOLOGIA

A presente pesquisa adota uma abordagem qualitativa, fundamentada no método dedutivo. O estudo parte da análise dos princípios constitucionais da presunção de inocência, do contraditório, da ampla defesa e do devido processo legal, examinando sua aplicação e violação no contexto contemporâneo das redes sociais e da mídia digital. A investigação adotará pesquisa bibliográfica e documental, doutrina especializada, jurisprudência relevante, legislações nacionais e instrumentos internacionais de proteção aos direitos humanos, além de casos que evidenciem os efeitos da exposição midiática na condução dos processos penais.

3. DESENVOLVIMENTO

3.1. O PRINCÍPIO DA PRESUNÇÃO DE INOCÊNCIA NO ESTADO DEMOCRÁTICO DE DIREITO E O DEVIDO PROCESSO LEGAL

No Estado Democrático de Direito, o princípio da presunção de inocência, devidamente fundamentado na Constituição Federal do Brasil de 1988, assegura em seu art. 5º, LVII, que "Ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória" (BRASIL, 1988). Esse princípio garante, ainda, a realização de um processo justo, imparcial e respeitando a dignidade da pessoa humana (art. 1º, III da CRFB/88) (BRASIL, 1988).

A presunção de inocência, possui duas esferas: interna e externa. A interna está ligada diretamente ao tratamento dado ao acusado dentro do processo penal, aplicando o princípio i*n dubio pro reo*. Na esfera externa, refere-se à proteção dos direitos do acusado, como: a dignidade, honra e a imagem. (CAMPOS, 2022). Este princípio protege os direitos fundamentais do acusado, impedindo que ele seja exposto a preconceitos e sanções sociais antes de uma condenação. Esses julgamentos morais da sociedade, comprometem a imparcialidade do sistema acusatório. Além disso, Pacelli (2017) ressalta que este

princípio vincula o Estado à obrigação de não tratar o acusado como culpado antes do trânsito em julgado. Muito menos atormentar o inocente, pois é inocente, segundo a lei, àquele cujo delito não é provado (BECCARIA, 1999).

Assim, o Tribunal Europeu de Direitos Humanos, bem como a Declaração Universal dos Direitos Humanos (art. 11.1) (ONU, 1948), reforçam a universalidade dessa garantia, que visa proteger o acusado de abusos estatais e midiáticos.

De acordo com a Constituição de 1988, o devido processo legal é indispensável para a aplicação da justiça penal, garante no art. 5º, LIV, que "Ninguém será privado da liberdade ou de seus bens sem o devido processo legal" (BRASIL, 1988); bem como, a plena garantia do contraditório (art. 5º, LV, da CRFB/88), no qual permite que o acusado possa se opor às alegações contrárias, e a ampla defesa, permitindo-lhe de utilizar os meios jurídicos válidos (art. 2º da Lei 9.784/99) (BRASIL, 1999). Somente diante dessas garantias que se poderá considerar alguém culpado. Dessa forma, a autoridade judiciária deve atuar de forma imparcial, impedindo que o processo ocorra de maneira arbitrária.

Tal violação ocorre frequentemente na mídia quando, de forma sensacionalista, são expostas informações antes que os acusados possam exercer seu direto à defesa, caracterizando um linchamento público. No entanto, os linchamentos sempre foram justificados por seus praticantes como uma forma de fazer justiça com as próprias mãos, violando os princípios fundamentais contidos na Constituição de 1988, sem que os praticantes do ato se preocupem com a culpabilidade do agente, ou com a possível inocência (CAMPOS, 2022). Assim, depreende-se que o linchamento possui danos irreversíveis, como a vida do acusado, que muitas vezes é tirada antes da sentença condenatória.

3.2. A DIVULGAÇÃO DE INFORMAÇÕES PROCESSUAIS NAS REDES SOCIAIS: LIBERDADE DE IMPRENSA VS. GARANTIAS INDIVIDUAIS

O fenômeno das mídias digitais gera um ambiente em que a exposição pública de réus e investigados ocorra antes do devido julgamento, promovendo uma tensão constante entre a liberdade de imprensa e as garantias constitucionais, o crime na mídia é frequentemente explorado como uma mercadoria, com um único objetivo: atrair audiência e gerar lucro, na maioria das vezes falhando com a veracidade dos fatos (SILVA, 2024). A produção de notícias, na maioria das vezes, é inteirada por interesses, nos quais a própria agenda de notícias é influenciada por instituições de controle social formal, como a polícia que fornece informações e molda a narrativa midiática em torno do caso (BUDÓ, 2013). Contudo, há um conflito entre a liberdade de imprensa, garantida pelo artigo 220 da Constituição Federal de 1988, e os direitos à honra, imagem e privacidade dos acusados, sendo necessário que se busque harmonizar através do princípio da proporcionalidade.

De acordo com Han (2022), a democracia degenera em infocracia, quando a circulação acelerada e viral de informações substitui os processos deliberativos e racionais próprios da esfera pública democrática. Uma consequência desse fenômeno, é o campo de batalhas narrativas onde a verdade e os critérios objetivos são vencidos pela onda de julgamentos morais. Além disso, quando ocorre a infocracia, a sociedade perde a capacidade de distinguir os fatos diante das informações desprovidas de contexto.

Dito isto, cita-se o caso de Fabiane de Jesus, a qual foi morta após ter sido espancada por moradores, no litoral de São Paulo em 2014. Fabiane foi agredida a partir de um boato gerado por uma página em rede social que afirmava que ela sequestrava crianças para utilizá-las em rituais, entretanto, após a sessão de linchamento, a população constatou que Fabiane havia sido confundida com outra pessoa (G1, 2014). Além disso, o caso de Anthony Ray Hilton, um homem negro que foi preso por um crime que não cometeu, em

1985, após ser confundido com um sequestrador. Ele foi condenado injustamente e passou 30 anos no corredor da morte, até conseguir provar sua inocência em 2015 (HINTON, 2019). Logo, a sociedade não se importa em descobrir o culpado, eles querem um culpado, e os casos apresentados revelam como a mídia e as redes sociais podem trazer consequências irreparáveis na vida pessoal e profissional dos acusados (OLIVEIRA; PAIVA, 2024, p.22).

3.3 CONSEQUÊNCIAS DA EXPOSIÇÃO

A exposição precoce e indevida promovida pela mídia gera fenômenos como o populismo legislativo e o direito penal simbólico, devido à mídia criar a percepção de que o sistema judiciário é ineficaz, transformando o processo penal em uma ferramenta de controle social (OLIVEIRA; PAIVA, 2024). Além disso, a Constituição assegura o direito à indenização por dano moral, bem como a inviolabilidade de honra e imagem, quando a imprensa ou perfis nas redes sociais expõem de maneira prematura e descontextualizada pessoas envolvidas em processos criminais (art. 5º, V e X) (BRASIL, 1988). O dano moral se configura nesses casos, devido a narrativa de culpa ao acusado persistir mesmo após a absolvição.

Trazemos à baila um trecho de extrema importância, referente a um julgado do STJ, sobre a transparência e a proteção dos direitos fundamentais, na ponderação entre o direito à liberdade de imprensa e os direitos da personalidade, especialmente à proteção da dignidade humana, privacidade e intimidade: "Assim, a liberdade de imprensa há de ser analisada a partir de dois paradigmas jurídicos bem distantes um do outro. O primeiro, de completo menosprezo tanto da dignidade da pessoa humana quanto da liberdade de imprensa; e o segundo, o atual, de dupla tutela constitucional de ambos os valores. Nesse passo, a explícita contenção constitucional à liberdade de informação, fundada na inviolabilidade da vida privada, intimidade, honra, imagem e, de resto, nos valores da pessoa e da família, prevista

no art. 220, § 1º, art. 221 e no § 3º do art. 222 da Carta de 1988, parece sinalizar que, no conflito aparente entre esses bens jurídicos de especialíssima grandeza, há, de regra, uma inclinação ou predileção constitucional para soluções protetivas da pessoa humana, embora o melhor equacionamento deva sempre observar as particularidades do caso concreto." (REsp 1.334.097/RJ, Rel. Min. Luis Felipe Salomão, julgado em 15/10/2013).

Sob esse viés, a privacidade e proteção devem ser vistas como um conceito multifacetado que protegem diferentes aspectos da vida pessoal, de maneira indispensável para a dignidade da pessoa humana, sendo um dos pilares do Estado Democrático de Direito.

Diante do cenário abordado, é importante que a regulamentação normativa da publicidade processual seja aperfeiçoada, de forma a limitar a divulgação de informações processuais, especialmente na fase inicial da ação, para fins de que a punição social antecipada não atrapalhe o trâmite processual e viole os direitos fundamentais (LOPES JR., 2017).

Seguindo a narrativa, seria fundamental reforçar o dever de sigilo em casos que envolve a vida privada e que envolvam os direitos da personalidade, estabelecendo punições aos perfis em redes sociais e de imprensa que violem tais restrições. Além disso, é de suma importância que seja investido em políticas públicas que visam a educação midiática e digital, para fins de promover a conscientização da população sobre os riscos do linchamento virtual e do julgamento moral antecipado, educar o consumo crítico da informação e conscientizar sobre a importância das garantias processuais para a preservação do Estado Democrático de Direito (HAN, 2021).

Diante disso, a proteção dos direitos fundamentais na era digital exige uma atuação contínua e vigilante do Estado e da sociedade, para que a dignidade da pessoa humana permaneça como valor supremo. Assim, os protocolos devem buscar o equilíbrio entre o direito à informação e a proteção das garantias processuais (SARLET, 2018).

CONCLUSÃO

A problemática deste pesquisa foi a de analisar o princípio da presunção de inocência, e as garantias do contraditório, da ampla defesa e do devido processo legal como fundamentos inegociáveis do Estado Democrático de Direito a serem preservados mesmo diante das transformações impostas pela era digital. **Os objetivos foram cumpridos à medida que se constatou que a** crescente exposição midiática de investigados e acusados, impulsionada pela lógica das redes sociais e por interesses comerciais, tem gerado verdadeiros linchamentos públicos, promovendo julgamentos morais antecipados e irreversíveis danos à imagem, à honra e à dignidade de pessoas ainda não condenadas. O resultado obtido foi verificar que atis práticas afrontam diretamente o ordenamento jurídico constitucional e revelam a urgência de mecanismos que limitem a divulgação de informações processuais, especialmente na fase pré-processual.

Além disso, torna-se indispensável o fortalecimento da educação midiática e digital como ferramenta de resistência à infocracia e à espetacularização da justiça penal, promovendo uma cultura de respeito às garantias processuais e à dignidade humana. A regulamentação mais precisa da atuação da mídia, aliada ao reforço da responsabilização por abusos informacionais, constitui passo essencial para a construção de uma esfera pública comprometida com os valores constitucionais. Por fim, reforça-se que a defesa das liberdades fundamentais não deve se sujeitar aos anseios populares ou às pressões midiáticas, mas sim se firmar como pilar imprescindível de qualquer sociedade verdadeiramente democrática.

REFERÊNCIAS

BECCARIA, Cesare Bonesana. *Dos delitos e das penas*. Tradução de J. Cretella Jr. e Agnes Cretella. 2. ed. rev. São Paulo: Revista dos Tribunais, 1999.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 maio 2025.

BRASIL. Lei nº 9.784, de 29 de janeiro de 1999. Regula o processo administrativo no âmbito da Administração Pública Federal. Diário Oficial da União: seção 1, Brasília, DF, 1 fev. 1999. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9784.htm. Acesso em: 18 maio 2025.

BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 1.334.097/RJ, Rel. Min. Luis Felipe Salomão, julgado em 15 out. 2013. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/rej.c=pdf&salvar=false. Acesso em: 18 maio 2025.

BUDÓ, Marília de Nardin. *Mídia e controle social: da construção da criminalidade dos movimentos sociais à reprodução da violência estrutural*. Rio de Janeiro: Revan, 2013. (Coleção Questões da Nossa Época, v. 148).

CAMPOS, John Melquyzedek Montenegro. *Da fragilidade da presunção de inocência frente à liberdade de imprensa: análise da proteção penal à honra*. 2022. 57 f. Monografia (Bacharelado em Direito) – Universidade Federal de Campina Grande, Centro de Ciências Jurídicas e Sociais, Sousa, 2022. Orientador: Guerrison Araújo Pereira de Andrade.

G1. Mulher espancada após boatos em rede social morre em Guarujá, SP. G1, Santos e Região, 5 maio 2014. Disponível em: https://g1.globo.com/sp/santos-regiao/noticia/2014/05/

mulher-espancada-apos-boatos-em-rede-social-morre-em-guaruja-sp.html. Acesso em: 18 maio 2025.

HAN, Byung-Chul. *Infocracia: digitalização e a crise da democracia*. 1. ed. São Paulo: Vozes, 2022. *E-book*. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 18 maio 2025.

HINTON, Anthony Ray. *O sol ainda brilha: a história real do homem que passou 30 anos no corredor da morte por crimes que não cometeu*. Tradução de Luis Gil Reyes. 1. ed. São Paulo: Vestígio, 2019.

LOPES JR., Aury. Direito Processual Penal. 21. Ed. São Paulo: SaraivaJur, 2024.

MAFRA, Lígia Kunzendorff. *Presunção de inocência na era digital: o coliseu contemporâneo e os algoritmos de exceção*. 2024. Dissertação (Mestrado em Direitos e Garantias Fundamentais) – Faculdade de Direito de Vitória, Vitória, 2024. Orientador: José Luis Bolzan de Morais. Coorientadora: Mercedes Llorente Sanchez-Arjona.

OLIVEIRA, Ana Paula Ribeiro de; PAIVA, Márcia Pruccoli Gazoni. A influência da mídia no processo penal. *Revista Tópicos*, ISSN 2965-6672, p. 1–7. Disponível em: https://revistatopicos.com.br. DOI: 10.5281/zenodo.13846642. Acesso em: 18 maio 2025.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos. Paris, 1948. Disponível em: https://www.un.org/en/about-us/universal-declaration-of-human-rights. Acesso em: 18 maio 2025.

PACELLI, Eugênio. *Curso de processo penal*. 21. ed. rev., atual. e ampl. São Paulo: Atlas, 2017.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional*. 13. ed. Porto Alegre: Livraria do Advogado, 2018.

SILVA, Péricles Mendes da. Meios de comunicação social, redes sociais, produção de notícias e suas consequências em delitos de grande repercussão. *Revista Processus Multidisciplinar*, v. 5, n. 9, e091130, jan.-jul. 2024. Disponível em: https://periodicos.processus.com.br/index.php/multi/index. Acesso em: 18 maio 2025.

A INTELIGÊNCIA ARTIFICIAL E O COMPORTAMENTO DA COLETIVIDADE: LGPD E OS IMPACTOS NOS MOVIMENTOS SOCIAIS

Carlos Henrique Everton Machado

Pós-Graduando do Curso de Especialização em Direito, Compliance e Mecanismos Anticorrupção, da Escola de Direito (ED) da Universidade do Estado do Amazonas (UEA); Bacharel em Direito pela Escola de Direito (ED) da Universidade do Estado do Amazonas (UEA).

Paula Mércia Coimbra Brasil

Mestranda no Programa de Pós Graduação em Direito na Universidade Federal do Amazonas PPGDir/UFAM; Bacharel em Direito pela Escola de Direito (ED) da Universidade do Estado do Amazonas (UEA).

PALAVRAS-CHAVE: Inteligência Artificial, LGPD, Movimentos Sociais, Psicologia das Multidões.

OBJETIVOS:

Examinar a interseção entre as teorias pertinentes à psicologia das multidões, o uso da inteligência artificial (IA) na análise de comportamentos coletivos e os limites ético-jurídicos impostos pela Lei Geral de Proteção de Dados (LGPD), avaliando como esses elementos se concatenam e influenciam no comportamento dos movimentos sociais.

METODOLOGIAS:

A pesquisa utilizou abordagem qualitativa, com revisão bibliográfica e análise documental de teorias sobre comportamento coletivo, estudos sobre algoritmos de IA aplicados a manifestações

públicas e movimentos sociais, dispositivos legais como LGPD, além de demonstrações práticas envolvendo o fenômeno.

DESENVOLVIMENTO DA PESQUISA:

Partindo da teoria sobre psicologia das multidões, Gustave Le Bon expõe em sua obra "Psicologia das Multidões", alguns conceitos que podem ser averiguados em uma realidade atual, de modo a concatenar com a dinâmica social com as redes sociais e, consequentemente, com as Inteligências Artificiais, para fins deste trabalho denominadas IA's, dos algoritmos destas.

De acordo com Le Bon, uma causa de identificação de caractere de uma multidão é o efeito de contágio, em que, de acordo com o autor, "*todos os sentimentos, todos os atos são contagiosos e são-no a ponto de o indivíduo sacrificar facilmente o seu interesse pessoal ao interesse coletivo*" (Le Bon, 1895). Associando este conceito inicial ao conceito de "a Mente Coletiva", sendo esta na visão do sociólogo "*a personalidade consciente desvanece-se e os elementos e as ideias de todas as unidades são orientados numa direção única*", tem-se uma espécie de coletividade submetida a uma "unidade mental" (Le Bon, 1895).

Deste modo, a suscetibilidade dos indivíduos a guinarem em uma coletividade que possui um único pensamento é gerada por meio da *sugestibilidade e credulidade* das multidões, em que "*a multidão encontra-se quase sempre num estado de atenção expectante que favorece a sua capacidade de se sugestionar*" (Le Bon, 1895).

Neste sentido, os indivíduos componentes se despem da razão individual e "*destituída de espírito crítico, a multidão não pode deixar de ser de uma credulidade excessiva",* onde "*para ela o inverossímil não existe*", facilitando a disseminação de informações falsas e manipulações (Le Bon, 1895).

Como consequência, a multidão cria uma característica de "perda de responsabilidade", pois, de acordo com o autor, "*o indivíduo em multidão adquire, pelo simples fato do seu número, um sentimento de*

poder invencível que lhe permite ceder a instintos que, se estivesse sozinho, teria forçosamente reprimido" (Le Bon, 1895).

Deste forma, a anonimidade da multidão tem como consequência o sentimento de irresponsabilidade por parte dos componentes. Existe um perigo neste comportamento coletivo, pois ele se potencializa de acordo com o tamanho da multidão e o desenvolvimento de um pensamento violento, em que se amplia a ausência de responsabilidade.

Para Gustave, "*o exagero nas multidões incide muitas vezes sobre os maus sentimentos, restos atávicos dos instintos do homem primitivo, que o receio do castigo obriga o indivíduo isolado e responsável a reprimir*", inserido neste local coletivo, os instintos e vontades das pessoas, em que "*para o indivíduo isolado seria perigoso entregar-se a esses instintos, mas, integrado numa multidão irresponsável, onde a impunidade está por consequência assegurada, tem plena liberdade para os satisfazer*" (Le Bom, 1895).

Outro conceito utilizado por Le Bon, muito caro à análise deste trabalho, é o entendimento de "hipnose", pois, após o indivíduo estar mergulhado nesta visão de pensamento coletivo, e pelas consequências que disso se depreende, o ser "*depressa se encontra num estado característico que muito se assemelha com o estado de fascinação do hipnotizado nas mãos do hipnotizador"* (Le Bon, 1895).

Neste ponto, explicitados os conceitos dados pelo autor francês, em um contexto completamente diverso do atual, é notável a associação desta teoria aos tempos atuais, e abarcados à realidade das redes sociais. Desta senda, surgem questionamentos: teria a IA dos algoritmos das redes sociais a capacidade de "sugestionar" e "contagiar" pessoas para vieses específicos, gerando a "multidão" e sua "unidade de pensamento"? Poderia o efeito de hipnose, não ser controlado por um "*hipnotizador*" indivíduo, mas sim por meio do algoritmo, sendo assim, os indivíduos submissos não a uma pessoa, mas a própria IA? Estes são os pontos focais e essenciais para o exame deste trabalho.

Entender o funcionamento dos algoritmos é essencial para compreender os seus efeitos na sociedade. Atualmente, a produção

dos algoritmos passa por constante evolução e desenvolvimento, desembocando em redes neurais complexas, com o advento dos conceitos de *deep learning* e *machine learning*. "*Inspirado no funcionamento do cérebro, por isso também conhecido como redes neurais, o deep learning foi concebido na década de 1980*", oferecendo uma redução no "*tempo de treinamento dos algoritmos*", servindo como uma espécie de "*previsão, com base de dados*" (Kaufman & Santaella, 2020).

De acordo com Kaufman & Santaella, "*redes neurais são funções matemáticas biologicamente inspiradas, formadas por neurônios artificiais que interagem entre si*", complementado a isto, atualmente, "*a maior parte da curadoria é efetivada pelos algoritmos de IA, particularmente pelo processo de deep learning*", onde um de seus efeitos colaterais, de acordo com as autoras, concerne na "*formação de "bolhas" ou "câmara de eco" (clusters)*", que consistem na "*homogeneização que estas promovem das relações sociais ao manter os indivíduos em círculos sociais fechados, formados por iguais*" (Kaufman & Santaella, 2020).

Assim, a aglutinação destes fatores, que explicam de maneira suscinta as redes sociais e seu algoritmo, podem explicitar a razão de interação entre as estruturas atuais das inteligências artificiais e a teoria da Psicologia da Multidão, em que o acesso livre aos dados individuais na rede e a constante evolução das redes neurais, desenvolvem de maneira abissal os algoritmos, que colaboram, porém, afetam de maneira significativa as interações sociais, a segurança e dignidade dos indivíduos.

A "mecânica" da Inteligência Artificial (IA) no monitoramento de manifestações sociais no Brasil, por meio das redes sociais e afins, suscita preocupações significativas quanto à violação de direitos fundamentais. A Constituição Federal de 1988 garante a inviolabilidade da intimidade e da vida privada (Art. 5º, X), a liberdade de expressão (Art. 5º, IV e IX), o direito de reunião (Art. 5º, XVI) e o direito de associação (Art. 5º, XVII-XXI). Entretanto, algoritmos de IA, ao processar dados de manifestações individuais ou coletivas, podem identificar padrões que influenciam ou predizem dinâmicas coletivas,

correndo o risco de reforçar estereótipos, criminalizar movimentos legítimos e fomentar hostilidade devido a vieses algorítmicos.

Nesse cenário, a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) atua como um marco regulatório essencial, exigindo que o tratamento de dados pessoais por IA observe princípios como finalidade (Art. 6º, I), adequação (Art. 6º, II), necessidade (Art. 6º, III), transparência (Art. 6º, VI), não discriminação (Art. 6º, IX) e responsabilização (Art. 6º, X). Além disso, a LGPD estabelece regras específicas para o tratamento de dados pelo Poder Público (Art. 23) e para o uso compartilhado de dados (Art. 26 e 27). A Autoridade Nacional de Proteção de Dados (ANPD) possui o poder de auditar sistemas automatizados para verificar aspectos discriminatórios (Art. 20, §2º).

Assim, para garantir a conformidade legal e a proteção dos direitos em um contexto de monitoramento em tempo real, faz-se imperativa a adoção de medidas robustas de transparência, auditoria e governança ética da IA, assegurando que a tecnologia sirva à sociedade sem comprometer as liberdades democráticas.

CONCLUSÕES:

Depreende-se que uma regulação da IA pela Lei Geral de Proteção de Dados (LGPD) é fundamental para preservar a legitimidade e integridade dos movimentos sociais, garantindo a proteção dos direitos individuais e coletivos em ambientes digitais e físicos.

Auferiu-se a necessidade de implementação de auditorias que analisem a influência algorítmica para sistemas usados em espaços públicos e nas redes sociais, a criação de protocolos que considerem contextos socioculturais para evitar generalizações enviesadas e o fortalecimento da Autoridade Nacional de Proteção de Dados (ANPD) para fiscalizar tecnologias de vigilância, assegurando transparência, responsabilidade e conformidade legal.

Destarte, a integração dos princípios da Psicologia das Multidões com a governança algorítmica e a legislação da LGPD é essencial para garantir uma análise automatizada e atualizada, mas que respeite a diversidade e a legitimidade dos comportamentos coletivos, promovendo uma vigilância responsável e democrática, tão caros à Constituição Federal e ao Estado Democrático de Direito.

REFERÊNCIAS

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal,. 496 p.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF,.

LE BON, Gustave. Psicologia das Multidões. França: Presses Universitaires de France. Tradução de Ivone Moura Delraux. [S.l.], 1895. Disponível em: https://cliqueapostilas.com/Content/apostilas/ab760ba25ab50e911baae2da5959f29a.pdf. Acesso em: 25 mai. 2025.

KAUFMAN, Dora; SANTAELLA, Lucia. O papel dos algoritmos de inteligência artificial nas redes sociais. Revista FAMECOS, [S. l.], v. 27, n. 1, p. e34074, 2020. DOI: 10.15448/1980-3729.2020.1.34074. Disponível em: https://pucrs.emnuvens.com.br/revistafamecos/article/view/34074. Acesso em: 25 mai. 2025.

O RISCO DO USO DA HIPERVIGILÂNCIA URBANA COMO MECANISMO DE CONTROLE SOCIAL: ANÁLISE COMPARADA DA VIOLAÇÃO DE DIREITOS NO BRASIL E NA ARGENTINA

Carolina Postigo Silva

Doutoranda em Ciências Jurídicas pela Pontificia Universidad Católica Argentina. Mestra em Direito Ambiental pelo Programa de Pós-Graduação da Universidade do Estado do Amazonas (PPGDA-UEA). Especialista em Direito Eleitoral pelo Instituto Brasiliense de Direito Público (IDP/DF). E-mail: carolinapostigo@hotmail.com.

Hillary Vitória Brasil Gomes

Pós-Graduanda em Direito Empresarial pela Pontifícia Universidade Católica do Rio Grande do Sul (PUC/RS). Graduada em Direito pela Faculdade La Salle de Manaus. E-mail: hillarybrasil24@gmail.com.

Stella Maris Barconte

Doutoranda em Ciências Jurídicas pela Pontificia Universidad Católica Argentina. Mestrado em Direito do Trabalho pela Pontificia Universidad Católica Argentina. Pós-graduação em prática do direito do trabalho, Advogada pela Universidade de Buenos Aires. E-mail: drabarconte@gmail.com.

Palavras-Chave: Hipervigilância Urbana; Reconhecimento Facial; Controle social; Consentimento Informado; Regulação tecnológica.

OBJETIVOS

Este resumo tem como objetivo analisar a expansão da hipervigilância urbana e o uso tecnologias de inteligência artificial, como o reconhecimento facial, a partir de um estudo comparativo entre Brasil e a Argentina, destacando os impactos nos direitos

fundamentais. A partir das teorias de Foucault e Habermas, investigar os riscos de controle social e a necessidade de regulação. Examina casos emblemáticos para evidenciar abusos e violações, propondo diretrizes para uma regulação democrática alinhada aos princípios constitucionais e o uso ético.

METODOLOGIA

O percurso metodológico será fundado no método dedutivo como abordagem geral; No que tange à análise das fontes legislativas, adotar-se-á o método comparativo, com o intuito de identificar semelhanças, diferenças e particularidades entre os ordenamentos jurídicos do Brasil e da Argentina acerca do tema investigado; quanto aos meios, a pesquisa será bibliográfica com análise da legislação, doutrina e reportagens publicadas em *websites*; quanto aos fins, a pesquisa compreende-se qualitativa e exploratória.

DESENVOLVIMENTO DA PESQUISA

No século XXI, a expansão do uso de tecnologias de vigilância em ambientes urbanos acelerou-se a um ritmo vertiginoso. Sistemas de câmeras interconectadas, algoritmos de análise preditiva, drones e software de reconhecimento facial já fazem parte da paisagem cotidiana de muitas cidades latino-americanas.

Este fenômeno, muitas vezes justificado por razões de segurança pública, levanta sérios desafios sob a perspectiva do direito constitucional e dos direitos humanos. Brasil e Argentina, dois dos países mais relevantes da América Latina, oferecem um marco paradigmático para a análise. Ambos adotaram sistemas de vigilância de alta tecnologia sem um debate legislativo profundo nem mecanismos adequados de controle, gerando situações de abuso, discriminação e afetação de direitos fundamentais.

O conceito de "hipervigilância" implica um sistema intensivo e onipresente de monitoramento contínuo, onde as fronteiras entre a segurança pública e o controle social se tornam difusas. No marco do pensamento foucaultiano, este tipo de vigilância configura um novo "biopoder", para se referir à prática dos estados modernos de "explorar numerosas e diversas técnicas para subjugar os corpos e controlar a população", conceito introduzido em "*La volonté du savoir*", o primeiro volume de sua *Histoire de la sexualité* de Foucault (1976, p. 131-132), que transforma os cidadãos em objetos permanentes de observação, com consequências jurídicas, sociais e subjetivas.

O uso de tecnologias preditivas e sistemas de IA incrementa este fenômeno, posto que não só registram o que ocorre, mas também pretendem antecipar comportamentos futuros, afetando princípios como a presunção de inocência e a autonomia individual.

No âmbito brasileiro, o conceito de reconhecimento facial pode ser definido pela Autoridade Nacional de Proteção de Dados-NAPD (2024, p.6) nos seguintes termos:

> A biometria é a análise técnica, realizada por meios matemáticos e estatísticos, das características fisiológicas (tais como impressão digital, face, íris, geometria da mão, vascularização da mão, DNA e voz) ou comportamentais (voz, expressão facial, assinatura, modo de andar etc.) de um indivíduo. Quanto maior a quantidade de dados presentes na amostra biométrica provenientes de uma ou mais características, maior será a probabilidade de que ela tenha uma correspondência única, ou seja, a amostra apresentará maior qualidade para que a análise seja mais precisa e confiável.

Os Estados como São Paulo, Rio de Janeiro e Bahia adotaram o sistema de reconhecimento facial sob o argumento da segurança pública e especialmente objetivando a identificação de criminosos, a exemplo de foragidos ou com mandados de prisão em aberto.

A Lei nº 13.709/2018 (Lei Geral de Proteção de Dados) consagrou a proteção da dignidade e dos direitos fundamentais, tendo como fundamentos, conforme seu art. 2º, o respeito à privacidade, a autodeterminação informativa, a inviolabilidade da intimidade, da honra e da imagem, além dos direitos humanos e do livre desenvolvimento da personalidade. E ainda, a LGPD em seu art. 5, II, também definiu como dado pessoal sensível, entre outros, o dado biométrico vinculado a pessoa natural.

O uso de reconhecimento facial no Brasil tem revelado os riscos da aplicação indiscriminada da IA em práticas de vigilância urbana, especialmente diante da ausência de critérios técnicos e de mecanismos efetivos de controle institucional. Um caso emblemático foi noticiado pela Globo (2024), quando João Antônio Trindade Bastos, um homem negro, foi preso injustamente pela polícia de Sergipe enquanto assistia a uma partida de futebol, após ser erroneamente identificado por um sistema de reconhecimento facial como sendo um foragido da justiça.

O episódio ganhou ampla repercussão nacional e expôs não apenas as fragilidades técnicas dessas tecnologias, mas também o viés racial presente nos algoritmos, que tendem a reproduzir padrões discriminatórios historicamente enraizados no sistema de segurança pública, contribuindo para transformar a vigilância automatizada em instrumento de controle social seletivo. Ademais, demonstra-se violação ao princípio da dignidade da pessoa humana, previsto no art. 1º, inciso III e viola o art. 5, incisos X, LIV e LVII da Constituição Federal de 1988.

Ademais, a coleta de dados faciais em espaços públicos tem ocorrido sem o consentimento dos cidadãos e sem transparência quanto ao destino e ao tratamento das informações obtidas. Questiona-se: O reconhecimento facial em espaços públicos é apenas para fins de segurança pública ou estamos vulneráveis ao uso do sistema para controle social?

No Brasil, até o momento, o uso de tecnologias de reconhecimento facial permanece sem regulamentação específica, apesar da existência de projetos de lei em tramitação na Câmara dos Deputados.

Por sua vez, na Argentina, a implementação de tecnologias baseadas em IA para a vigilância urbana e outros fins, observa-se igualmente a ausência de um marco normativo atualizado e de mecanismos eficazes de controle institucional, gerando debates cruciais acerca da proteção de direitos fundamentais.

A Lei Nacional de Proteção de Dados Pessoais da Argentina, Lei nº 25.326/2000, constitui o principal marco normativo que rege o tratamento de dados pessoais no país, estabelecendo os princípios gerais para a coleta, armazenamento, uso e transferência de dados, incluindo a necessidade de consentimento informado do titular, a finalidade do tratamento e a segurança da informação. No entanto, sua promulgação é anterior ao auge massivo da IA e dos sistemas de hipervigilância, o que acarreta lacunas significativas e desafios interpretativos em sua aplicação contemporânea.

A vinculação entre a 25.326/2000 e os casos de IA e controle social reside no fato de que, embora a lei estabeleça uma base de proteção, seu alcance é superado pelas capacidades das novas tecnologias. A noção de "consentimento informado" torna-se particularmente problemática quando os cidadãos são monitorados constantemente sem uma clara compreensão de como seus dados biométricos ou de comportamento são coletados, processados e utilizados.

Um caso emblemático na Argentina é o do Sistema de Reconhecimento Facial de Foragidos (SRFP), implementado pelo Governo da Cidade Autônoma de Buenos Aires em 2019. Diversas organizações de direitos humanos, como o Centro de Estudos Legais e Sociais (CELS) e a Associação pelos Direitos Civis (ADC), questionaram a legalidade do sistema, assinalando que operava sem auditorias independentes, sem avaliação de impacto em direitos fundamentais e com sérios riscos de discriminação algorítmica.

A Sentença da Vara de 1ª Instância em Contencioso Administrativo e Tributário nº 4 da Cidade Autônoma de Buenos Aires, de 07 de

setembro de 2022, nos autos intitulados: "OBSERVATORIO DE DERECHO INFORMATICO ARGENTINO O.D.I.A. Y OTROS CONTRA GCBA SOBRE AMPARO - OTROS", EXP 182908/2020-0, abordou a constitucionalidade e convencionalidade do Sistema de Reconhecimento Facial de Foragidos (SRFP) implementado pelo Governo da Cidade Autônoma de Buenos Aires (GCBA). Esta decisão, posteriormente confirmada em sua essência pela Câmara de Apelações, marcou um precedente significativo no debate sobre a hipervigilância urbana e suas implicações para os direitos fundamentais.

A declaração de inconstitucionalidade do Sistema de Reconhecimento Facial de Foragidos (SRFP) em Buenos Aires baseou-se em graves deficiências e irregularidades: (1) ausência de Avaliação de Impacto na Proteção de Dados (EIPD), impedindo a análise dos riscos à privacidade e aos direitos humanos fundamentais dos cidadãos; (2) uso de base de dados (CONARC) com erros e desatualizações, gerando "falsos positivos"; (3) violação de direitos fundamentais, como presunção de inocência, privacidade, intimidade e autodeterminação informativa, ao realizar coleta de dados sensíveis sem consentimento. (4) descumprimento dos mecanismos de controle legal, como a não formação da Comissão Especial prevista na Lei nº 6.339/2020 e (5) Omissão de relatórios da Defensoria Pública. Por fim, perícia judiciais comprovaram o uso ilegal do sistema para buscar milhares de pessoas fora da base autorizada e revelaram manipulação e funcionamento irregular durante a pandemia.

Assim, houve o cumprimento da decisão da juíza Liberatori que suspendeu o uso do SRFP, mantendo os demais sistemas de videovigilância. O caso evidenciou a urgência de regulamentação rigorosa e transparente para tecnologias biométricas, fixando um precedente na Argentina sobre os limites constitucionais da vigilância automatizada. Reafirmou-se que a proteção de direitos fundamentais deve prevalecer sobre inovações tecnológicas, exigindo base legal, consentimento, proporcionalidade e controle efetivo no uso de IA.

A obra de Michel Foucault, intitulada "Vigiar e Punir", descreve uma nova modalidade de poder sobre as pessoas, a qual passa

pela vigilância e disciplina objetivando o exercício de controle da sociedade. Inspirado no modelo do Panóptico de Jeremy Bentham, o Foucault utiliza essa estrutura como metáfora para um sistema em que os indivíduos se comportam como se estivessem constantemente sendo observados, internalizando a vigilância e promovendo a autovigilância. Para Foucault (1975, p. 194), a visibilidade torna-se um mecanismo de dominação: "a visibilidade é uma armadilha".

A necessidade de uma regulação efetiva diante dos riscos do reconhecimento facial - uma forma de IA - tanto no âmbito público quanto privado, encontra um sólido fundamento na teoria da ação comunicativa de Jürgen Habermas.

Habermas postula que a razão não é meramente instrumental ou estratégica, mas que se enraíza na comunicação orientada ao entendimento mútuo. No contexto da hipervigilância e do controle social, a aplicação da IA sem uma base consensual e transparente contradiz diretamente os princípios da ação comunicativa, comprometendo o diálogo público, sem o consentimento informado dos afetados e minando a livre formação da opinião e da vontade.

Habermas argumenta que uma sociedade racionalizada não se baseia apenas na eficiência de sistemas econômicos e administrativos, mas também na vitalidade de um "mundo da vida" que se estrutura comunicativamente. A "colonização do mundo da vida" ocorre quando a lógica instrumental dos sistemas (como o dinheiro e o poder) invade e distorce os âmbitos da comunicação e do entendimento. A hipervigilância urbana e a manipulação algorítmica representam precisamente esta colonização, ao impor lógicas de controle e eficiência sobre a esfera pública e as interações cotidianas, sem um processo comunicativo que legitime seu uso.

Diante do vazio legal e da falta de mecanismos de controle, a perspectiva habermasiana oferece um caminho para a solução: 1- Necessidade de um Marco Normativo Baseado no Consenso: A regulação da IA deve ser fruto de um consenso social amplo, com base em um discurso racional que permita avaliar criticamente a validade das normas; 2- Transparência e Auditoria Independente: A

opacidade dos algoritmos e a falta de transparência exigem auditoria independente para garantir que a sociedade compreenda e controle o uso da IA; 3- Participação Cidadã e Controle Democrático: A teoria de Habermas enfatiza a importância dos procedimentos democráticos que garantam a formação da opinião e da vontade coletiva; 4- Autodeterminação Informativa e Consentimento Informado: A coleta de dados sem consentimento fere a autodeterminação informativa, exigindo um consentimento claro, informado e acessível sobre o uso dos dados e o funcionamento dos sistemas de IA.

CONCLUSÃO

A hipervigilância urbana e o uso não regulado de tecnologias baseadas em IA configuram uma transformação estrutural na forma como o poder é exercido em todo o mundo. Essas se projetam como ferramentas de controle social, com capacidade de intervir sobre comportamentos coletivos, opinião pública e processos democráticos, tal como pudemos contemplar nos casos expostos no Brasil e na Argentina.

A falta de regulamentação específica sobre IA em ambos os países configura um cenário de risco jurídico e ético. Por tal razão, é essencial que os Estados latino-americanos se atentem aos desafios da nova fase da revolução digital, evitando a adoção de sistemas de IA que reproduzam vieses discriminatórios ou violem a dignidade humana.

Uma dimensão inegável no debate sobre IA e vigilância é a necessidade imperiosa de garantir o consentimento informado das pessoas sobre o uso de seus dados pessoais, diante da opacidade dos sistemas de coleta de dados e do desconhecimento sobre os algoritmos.

Assim, é crucial que a implementação de tecnologias, especialmente em contextos públicos ou de impacto social significativo, assegure transparência, acesso à informação, possibilidade de consentimento livre e revogável, e o exercício pleno dos direitos sobre os dados. A soberania informacional deve ser tratada como expressão

dos direitos fundamentais, e não subordinada a interesses corporativos ou estatais.

A ausência de salvaguardas mínimas desvirtua o princípio da autonomia pessoal e permite formas de vigilância incompatíveis com o Estado de direito. A soberania sobre os dados deve ser compreendida como expressão dos direitos fundamentais, e não como concessão técnica sujeita a interesses externos. Além disto, a ausência de um marco regulatório dedicado aos dados biométricos transcende as questões do reconhecimento facial, revelando a existência de riscos equiparáveis nos sistemas de reconhecimento biométrico, incluindo o reconhecimento de marcha, íris, impressões digitais e voz.

Conclui-se que, é imperioso avançar na regulamentação do uso de IA por meio de auditorias algorítmicas independentes, políticas de *accountability*, participação cidadã e revisão das bases de dados sensíveis. Urge harmonizar as legislações segundo o princípio *pro persona* e os padrões interamericanos de direitos humanos, garantindo um uso tecnológico pautado na legalidade, proporcionalidade e transparência. Assim, inspirados pela resiliência e pela visão dos que nos precederam, é imperativo a busca em construir um futuro onde a tecnologia seja um instrumento a serviço da justiça e do bem-estar humano.

REFERÊNCIAS

ARGENTINA. **Ley n.º 25.326, de 4 de octubre de 2000**. Protección de los Datos Personales. *Boletín Oficial*, Buenos Aires, 4 oct. 2000. Disponível em: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto. Acesso em: 23 mai. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (Brasil). **Biometria e reconhecimento facial: estudos preliminares**. 1. ed. n. 2, Brasília: ANPD, 2024.

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/constituicao.htm. Acesso em:13 mai. 2025.

BRASIL. **Lei n° 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 mai. 2025.

CENTRO DE ESTUDIOS LEGALES Y SOCIALES (CELS). Confirman la inconstitucionalidad del uso del sistema de reconocimiento facial. **CELS**, Buenos Aires, 10 abr. 2023. Disponível em: https://www.cels.org.ar/web/2023/04/confirman-la-inconstitucionalidad-del-uso-del-sistema-de-reconocimiento-facial/. Acesso em: 23 mai. 2025.

FOUCAULT, Michel. **Vigiar e Punir: nascimento da prisão**. Tradução de Raquel Ramalhete. 42. ed. Petrópolis, RJ: Vozes, 2014.

FOUCAULT, Michel. **História da sexualidade I: a vontade de saber**. Tradução de Maria Thereza da Costa Albuquerque e J. A. Guilhon Albuquerque. Rio de Janeiro: Graal, 1988. Obra original: *Histoire de la sexualité I: la volonté de savoir*. Paris: Gallimard, 1976.

G1. ‘Medo, frustrado e constrangido’, diz homem detido por engano em estádio após erro do sistema de reconhecimento facial. **Fantástico**, Rio de Janeiro, 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: 27 mai. 2025.

HABERMAS, Jürgen. **Teoria da ação comunicativa: racionalidade da ação e racionalização social.** Tomo I. Tradução de Manuel Jiménez Redondo. São Paulo: Taurus, 1999. Obra original publicada em 1981.

O USO DE DEEPFAKE E A RESPONSABILIDADE CIVIL: A NECESSIDADE DE NOVAS ABORDAGENS JURÍDICAS NA ERA DA INTELIGÊNCIA ARTIFICIAL

Ruan Patrick Teixeira da Costa[1]
Emilly Victória Batista Dos Santos[2]
Lucas Gabriel Pessoa de Aragão[3]

Palavras- chaves: Deepfake; Responsabilidade Civil; Inteligência Artificial

OBJETIVOS

O presente trabalho tem como objetivo analisar os impactos decorrentes da utilização de deepfakes, produzidas por meio de inteligência artificial, com foco na configuração da responsabilidade civil diante da manipulação tecnológica, à luz do ordenamento jurídico brasileiro. Para tanto, busca-se examinar os fundamentos da responsabilidade civil relacionados à proteção da imagem, da honra e da privacidade, além de investigar em um caso concreto nacional

1 Mestre em Direito Ambiental pelo PPGDA da Universidade do Estado do Amazonas (UEA). Analista Jurídico da Defensoria Pública do Estado do Amazonas. Professor de cursos de graduação. Especialista em Direito Penal, Investigação Forense e Perícia Criminal pela Uniasselvi. Bacharel em direito pela Universidade Federal do Pará (UFPA). Orcid: https://orcid.org/0000-0002-1891-3639. E-mail: ruan.teixeiraadv@gmail.com Lattes: http://lattes.cnpq.br/5918316459107517.

2 Graduanda de Direito na Universidade do Estado do Amazonas (UEA). Técnica em Informática pelo Instituto Federal do Amazonas (IFAM). Bolsista de Iniciação Científica PIBIC/CNPQ, pesquisadora vinculada à Escola Superior da Magistratura do Amazonas (ESMAM), membro da Clínica de Estudos Constitucionais (CEC/UEA), integrante do Laboratório de Ciências Criminais (LAB) do Instituto Brasileiro de Ciências Criminais (IBCCRIM) e Membro da Comissão OAB Universitário. Email: emillyvictoriabatistadossantos@gmail.com Lattes: http://lattes.cnpq.br/0027778964063788. Orcid: https://orcid.org/0009-0004-1785-7390.

3 Graduando de Direito na Universidade do Estado do Amazonas (UEA). Escritor. Membro da Clínica de Estudos Constitucionais (CEC/UEA). Membro da Comissão OAB Universitário. Email: pessoadearagao@gmail.com. Lattes: http://lattes.cnpq.br/1161202022230657. Orcid: https://orcid.org/0009-0000-4108-4624.

que envolve o uso de deepfakes e sua consequente responsabilização civil. A proposta é refletir criticamente sobre as soluções normativas existentes e identificar eventuais lacunas diante das novas tecnologias de manipulação de conteúdo.

METODOLOGIA

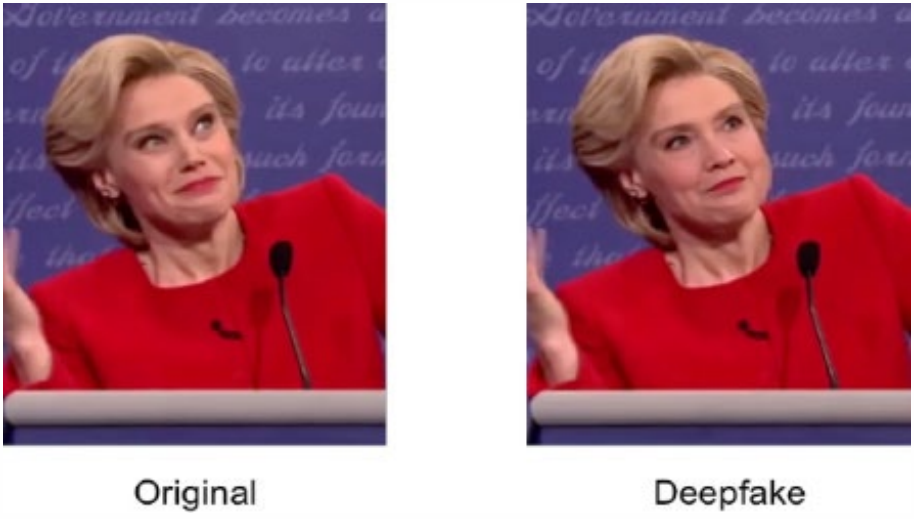
A pesquisa se baseia no método qualitativo, com enfoque analítico-descritivo, ao compreender o fenômeno jurídico criado pelo uso de deepfakes no âmbito jurídico no contexto civil. O procedimento utilizado será a pesquisa bibliográfica com levantamento e análise crítica da doutrina acerca da responsabilidade civil, direitos da personalidade e os impactos do avanço tecnológico das deepfakes e pesquisa documental com base nas legislações aplicáveis no caso, bem como o exame de um caso concreto nacional que evidencia a aplicação prática do direito em situações envolvendo deepfakes.

DESENVOLVIMENTO DA PESQUISA

A era da tecnologia proporcionou a ampliação de utilização de inteligência artificial (IA) na criação de deepfakes que possibilitam a manipulação e criação de conteúdos falsos, seja em forma de imagem, vídeo ou áudio. Mesmo com os benefícios da ampliação de criação pela área de IA, os riscos causados na disseminação de deepfakes distorcidas da verdade causam impactos negativos na sociedade e no ordenamento jurídico.

Os vídeos conhecidos como “Deepfake” oferecem a capacidade de trocar o rosto de uma pessoa por outra em um videoclipe ou imagem, essa tecnologia criada, aprimora e cria os vídeos falsos que imitam as expressões faciais, gestos, voz e variações do indivíduo, tornando-os cada vez mais realistas (Maras & Alexandrou, 2018).

Figura 1- Exemplo de imagem utilizando Deepfake



Fonte: Afchar, Nozick & Yamagishi, 2018

As deepfakes são as maiores influenciadoras da disseminação de Fake News no mundo digital e são estrategicamente utilizadas para atrair a atenção de usuários, e, com o avanço tecnológico se torna cada vez mais difícil distinguir se o conteúdo é real ou não. Segundo um estudo publicado na PLOS One, envolvendo 529 indivíduos, 1 pessoa entre 4 não consegue distinguir um áudio Deepfake de um real. Ainda, o estudo afirma que o resultado é alarmante pois identifica a fragilidade da sociedade ser influenciada por criações falsas.

De acordo com Bunk et al. (2017), o número de imagens digitais tem crescido exponencialmente com o advento de novas câmeras, smartphones e tablets. O uso de mídias sociais como como Facebook, Instagram, WhatsApp e Twitter contribuíram ainda mais para a sua distribuição de informações falsas que tem impactos direto na população.

Um caso real brasileiro envolvendo o uso indevido de IA foi a utilização de deepfakes que envolveram a Havan e o empresário Luciano Hang contra a plataforma Meta (empresa responsável por plataformas como Instagram e Facebook). A vitória ocorreu no

Tribunal de Justiça de Santa Catarina (TJSC) por decisão unanime que proibiram a divulgação de anúncios falsos que envolviam a imagem do empresário.

O caso criou um entendimento sobre a importância de ações judiciais que envolvam crimes digitais e o uso indevido de imagem. Segundo o portal SCTododia (2025), o resultado do caso é inédito e transmite clareza e a responsabilidade de redes sociais em relação à veiculação de anúncios enganosos, especialmente aqueles que utilizam inteligência artificial e técnicas de manipulação digital, como deepfakes, para atrair consumidores e aplicar golpes.

No Brasil ainda não se tem uma legislação específica referente às deepfakes, por enquanto as leis existentes dão amparo a possíveis crimes cometidos. Siqueira (2019) aponta que:

> A Legislação Brasileira não criminaliza especificamente o "DeepFake'. Mas os intérpretes têm buscado amparo em tipos penais abertos descritos na Lei Federal n.º 12.735/2012 (Lei Azeredo), Lei Federal n.º 12.737/2012 popularmente conhecida como Lei Carolina Dickmann, Lei Federal n.º 12.965/2014 (Marco Civil da Internet); Lei Federal n.º 13.718/2018 oriunda do Projeto de Lei n.º 5.555/2013, Lei Federal n.º 13.709/2018 - Lei Geral de Proteção de Dados Pessoais, Lei Federal n.º 13.853/2019. Além dos tipos penais descritos na Lei de Crimes Financeiro (Lei Federal n.º 7.492/86), Lei de Falências (Lei Federal n.º 11.101/2005), Código Eleitoral (Lei Federal n.º 4737/65) e principalmente nos crimes contra a honra (artigos 138/145 do Código Penal) e dignidade sexual (artigos 213/235 'c' do Código Penal).

Por conseguinte, os danos sofridos por uma determinada vítima em razão das deepfakes, implicam na responsabilidade civil dos autores desse infortúnio, que atinge não somente os ofendidos pela criação de conteúdos com inverdades, bem como a ordem pública,

a moral do tecido social e o ordenamento jurídico brasileiro. Para a doutrinadora Maria Helena Diniz a responsabilidade civil consiste na:

> a aplicação de medidas que obriguem uma pessoa a reparar o dano moral ou patrimonial causado a terceiros, em razão de ato por ela mesma praticado, por pessoa por quem ela responde, por alguma coisa a ela pertencente ou de simples imposição legal. (Diniz 2005, p. 32)

A responsabilidade civil consiste em um mecanismo jurídico que objetiva a reparação de danos causados a terceiros, sejam eles morais ou patrimoniais. De modo categórico, a responsabilidade civil é uma obrigação imperativa ao autor de um ato ilícito na sociedade civil. Em concordância, Rui Stoco (2004, p. 46), conceitua que a responsabilidade civil é a obrigação de reparar mediante indenização quase sempre pecuniária ao dano que o fato ilícito causou a outrem.

A lei n° 10.406 de 10 de janeiro de 2002, intitulado Código Civil, é o principal mecanismo normativo que fundamenta a responsabilidade civil em seus artigos 186 e 927 ao definir a obrigação de reparar os danos causados a outrem por atos ilícitos. A saber o texto legal:

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
> Art. 927. Aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo.

Para que se configure a responsabilidade civil, é mister a presença dos elementos que a caracterizam. É indispensável que se comprove o ato ilícito, o dano, e o nexo de causalidade entre o ato ilícito e o dano. O doutrinador Rui Stoco (2004, p. 1665) traz a simples definição de

dano moral na hipótese de que quando o dano não corresponde às características de dano patrimonial se tem a presença do dano moral.

Ademais, em se tratando de violação de direitos por meio das deepfakes, a potencial vítima, poderá alegar violação a seu direito de personalidade, como direito à imagem e à privacidade. O Código Civil Brasiliense trata desses direitos especificamente em seus artigos 20 e 21. A saber o texto legal:

> 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.
> Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

As deepfakes são patentemente uma violação aos dispositivos acima citados, tratando-se da utilização da imagem de alguém para criar um conteúdo falso, o que compromete a dignidade, a reputação e a privacidade das pessoas envolvidas. Também pode ser utilizada para fins comerciais, sem a devida permissão.

O fato de as deepfakes circularem no meio digital, é primordial destacar a responsabilidade civil das plataformas, as quais são os instrumentos de divulgação de tais dissimulações ilícitas pelos seus autores.

Embora as plataformas em que são divulgadas as deepfakes não serem diretamente as criadoras de seus conteúdos, elas podem responder perante a justiça caso não adotem medidas para retirarem de circulação, conteúdos ilícitos, conforme descreve a lei 12. 965 de 23 de abril de 2014 (Marco Civil da Internet).

> 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.

CONCLUSÃO

O âmbito jurídico foi desafiado aos novos desenvolvimentos tecnológicos e pelo uso de inteligência artificial na ascensão do Deepfake pela comunidade, em específico no que diz respeito à responsabilidade civil. A capacidade de desenvolver áudio, imagens e vídeos falsos, mas com graus de verossimilhança ao real gera riscos à imagem, privacidade e dignidade de uma pessoa, exigindo a perspectiva da sua responsabilidade civil.

Por fim, o estudo realizado acerca da responsabilidade civil implica na obrigação do Estado assegurar que as vítimas de conteúdos falsos do Deepfake sejam devidamente amparadas, especialmente por conta da velocidade de compartilhamento existente neste caso. Entretanto, ainda se faz necessário a criação de legislações, com a consequente aplicação de sanções aos que vierem a praticar condutas contrárias ao direito, mas que levem considerem esse novo desenvolvimento jurídico e quais impactos terão na sociedade de uma forma mais eficaz.

REFERÊNCIAS

Afchar, D.; Nozick, V.; Yamagishi, J. **MesoNet: a compact facial video forgery detection network.** *arXiv*, arXiv:1809.00888v1 [cs.CV], 4 set. 2018. Disponível em: https://arxiv.org/abs/1809.00888. Acesso em: 1 jun. 2025.

Bunk, J.; Bappy, J.; Mohammed, T.; Nataraj, L.; Flenner, A.; Manjunath, B.; Chandrasekaran, S.; Peterson, L. **Detection and localization of image forgeries using resampling features and deep learning.** *arXiv*, arXiv:1707.00433v1 [cs.CV], 3 jul. 2017. Disponível em: https://arxiv.org/abs/1707.00433. Acesso em: 1 jun. 2025.

DINIZ, Maria Helena. Curso de Direito Civil Brasileiro - Responsabilidade Civil. Vol.7. São Paulo: Saraiva, 2011.

JUSPODIVM, EDITORA. Vade Mecum JusPODIVM. 17° ed. São Paulo: JusPodivm, 2025.

Mai, K. T.; Bray, S.; Davies, T.; Griffin, L. D. **Warning: Humans cannot reliably detect speech deepfakes.** *PLOS ONE*, v. 18, n. 8, e0285333, 2023. Disponível em: https://doi.org/10.1371/journal.pone.0285333. Acesso em: 1 jun. 2025.

Maras, M.-H.; Alexandrou, A. **Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos.** *The International Journal of Evidence & Proof*, v. 23, n. 3, p. 255-262, 2018. Disponível em: https://doi.org/10.1177/1365712718807226. Acesso em: 1 jun. 2025.

Peck Pinheiro (2022) defende que a manipulação digital ilícita, como nas deepfakes, enseja responsabilidade civil e, eventualmente, penal, por violar direitos personalíssimos e gerar danos à vítima.

PECK, Patrícia. Direito Digital: Internet e os Tribunais. 5ª ed. São Paulo: Saraiva, 2021.

Pecsen, T. **1 a cada 2 brasileiros afirma já ter compartilhado Fake News sem saber.** *dfndr blog*, 2020. Disponível em: https://www.psafe.com/blog/1-a-cada-2-brasileiros-afirma-ja-ter-compartilhado-fake-news-sem-saber/. Acesso em: 1 jun. 2025.

SCTD. **TJSC dá vitória à Havan e a Hang contra Meta Platforms.** *SCTD*, [s.d.]. Disponível em: https://sctd.com.br/cotidiano/tjsc-da-vitoria-a-havan-e-a-hang-contra-meta-platforms/. Acesso em: 1 jun. 2025.

SIQUEIRA, P. A. R. **O 'Deep Fake' e a legislação brasileira: utilização de instrumentos legais para a proteção à imagem.** *Conteúdo Jurídico*, 2019. Disponível em: https://www.jusbrasil.com.br/artigos/o-deep-fake-e-a-legislacao-brasileira-utilizacao-de-instrumentos-legais-para-a-protecao-a-imagem/735209926?msockid=2c05a39fc78a67a02db9b6-9dc6db6652. Acesso em: 1 jun. 2025.

STOCO, Rui**. Responsabilidade Civil e sua interpretação jurisprudencial.** – São Paulo: Editora Revista dos Tribunais, 2004.

O ADVOGADO NA ERA DA INTELIGÊNCIA ARTIFICIAL: O USO DE JURISPRUDÊNCIAS FALSAS E O RISCO ÉTICO AO EXERCÍCIO DA ADVOCACIA.

Ruan Patrick Teixeira da Costa[4]
Nelcy Renata Silva de Souza[5]
Emilly Victória Batista Dos Santos[6]

Palavras- chaves: Inteligência artificial; Advogado; Ética profissional.

OBJETIVOS

O presente trabalho tem como objetivo analisar as recentes notícias sobre o uso de inteligência artificial na elaboração de documentos que se baseiam em alucinações e criações de jurisprudências falsas e são utilizados por advogados em processos judiciais, além dos impactos causados por essa ação e a descredibilidade gerada diretamente sobre a atuação e ética

4 Mestre em Direito Ambiental pelo PPGDA da Universidade do Estado do Amazonas (UEA). Analista Jurídico da Defensoria Pública do Estado do Amazonas. Professor de cursos de graduação. Especialista em Direito Penal, Investigação Forense e Perícia Criminal pela Uniasselvi. Bacharel em direito pela Universidade Federal do Pará (UFPA). Orcid: https://orcid.org/0000-0002-1891-3639. E-mail: ruan.teixeiraadv@gmail.com Lattes: http://lattes.cnpq.br/5918316459107517.

5 Mestra em Direito Ambiental pelo PPGDA da Universidade do Estado do Amazonas (UEA). Advogada. Bacharela em Direito pela UFPA. E-mail: nelcyrenata@gmail.com. ORCID: https://orcid.org/0000-0002-8258-1376 Lattes: http://lattes.cnpq.br/0036764451569275.

6 Graduanda de Direito na Universidade do Estado do Amazonas (UEA). Técnica em Informática pelo Instituto Federal do Amazonas (IFAM). Bolsista de Iniciação Científica PIBIC/CNPQ, pesquisadora vinculada à Escola Superior da Magistratura do Amazonas (ESMAM), membro da Clínica de Estudos Constitucionais (CEC/UEA), integrante do Laboratório de Ciências Criminais (LAB) do Instituto Brasileiro de Ciências Criminais (IBCCRIM) e Membro da Comissão OAB Universitário. Email: emillyvictoriabatistadossantos@gmail.com Lattes: http://lattes.cnpq.br/0027778964063788. Orcid: https://orcid.org/0009-0004-1785-7390.

profissional com base no Estatuto da Advocacia (Lei nº 8.906/1994) e no Código de Ética e Disciplina da OAB.

METODOLOGIA

A abordagem utilizada foi qualitativa e exploratória, pois visa entender o fenômeno social contextualizado sobre o uso de inteligência artificial aplicado ao grupo de advogados com base em pesquisa bibliográfica. O trabalho se concentra na análise de notícias reais, concretas e atuais sobre o uso de IA pelos operadores do direito, em específico na citação de jurisprudências falsas com foco nos riscos e impactos na legislação que abrange a temática, examinando o Estatuto da Advocacia (Lei nº 8.906/1994) e o Código de Ética e Disciplina da OAB.

DESENVOLVIMENTO DA PESQUISA

O uso de inteligência artificial (IA) revolucionou o mundo pela realização rápida e autônoma desde tarefas simples até as mais complexas, fazendo parte da vida cotidiana de um indivíduo ao solucionar dúvidas, criar imagens e outros inúmeros benefícios realizados pelo grande desenvolvimento tecnológico atual. Pelo mecanismo da IA possuir um software capaz de representar o comportamento e pensamento humano para execução de atividades e até escolha de decisão, essa ferramenta tecnológica chegou ao Poder Judiciário e é amplamente utilizada por profissionais do meio jurídico. Segundo Azevedo (2019) o uso de IA influenciou o domínio jurídico por sua capacidade de processar dados, identificar padrões, realizar testes, analisar e avaliar informações para produzir resultados específicos.

O uso desse software não tem como objetivo alterar a essência humana em um trabalho jurídico, nem mesmo substituir os advogados, mas sim permitir que estes se concentrem em tarefas mais cognitivas

e desenvolvimento de argumentos ao invés de atividades rotineiras como redigir um extenso documento (Figueiredo, 2018).

A utilização da IA pode trazer benefícios, entre eles se destacam a redução do tempo e a correção automática de erros humanos em processos, em virtude do vasto acesso a informações em curto espaço de tempo.

Entretanto, essa inovação ainda apresenta várias lacunas e riscos, que incluem falhas tecnológicas que implicam na alucinação e criação imprecisa de fatos jurídicos, o que se evidencia no caso das jurisprudências falsas, as quais afetam a reputação de advogados que se baseiam no software sem a devida pesquisa e confirmação das fontes.

Um caso que exemplifica essa questão foi o registrado sob o número 0002062-61.2025.8.16.0019 na 1º Câmara Criminal do Tribunal de Justiça do Paraná (TJ/PR), que rejeitou recurso com jurisprudência inventada na defesa de um réu pronunciado ao Tribunal do Júri. O excesso de citação de jurisprudências falsas ganhou notoriedade pela grande falha detectada: a criação de 43 precedentes jurídicos inexistentes, o que se evidencia no trecho abaixo:

> Segundo o relator, desembargador Gamaliel Seme Scaff, foi constatado que a peça recursal mencionava 43 precedentes jurídicos inexistentes, muitos deles atribuindo decisões a magistrados que jamais atuaram na Corte. Nomes como "Fábio André Munhoz" e "João Augusto Simões" foram apontados como autores de julgados que, na realidade, nunca existiram. Para completar o cenário de inautenticidade, os números de processos citados seguiam padrões claramente fictícios, como "1234-56" e "3456-78".

Na decisão proferida, o uso de citações falsas foi referido como "criações de alguma (des)inteligência artificial" e "é imprestável, não havendo como ser conhecido". O colegiado ainda repreendeu a ação

do advogado que possuía a obrigação de revisar a peça processual que foi feita pela ferramenta. Tal ação prejudicou o andamento da ação judicial e o exercício da função da respectiva corte.

O caso citado serve como alerta, não apenas aos advogados, mas a todos os usuários que utilizam da ferramenta para suas pesquisas no âmbito processual. É importante lembrar que essas ferramentas são complementares aos advogados e não substituem o papel fundamental que desempenham (Soares et al., 2020).

Outro caso que repercutiu foi a multa por litigância de má-fé no valor de R$2.604,00 (dois mil, seiscentos e quatro reais) a um advogado que fez o ajuizamento de uma petição escrita pelo ChatGPT, uma das mais conhecidas plataformas de inteligência artificial, solicitando se tornar amicus curiae em um processo movido contra o ex-presidente Jair Bolsonaro.

A referida decisão foi tomada pelo ministro Benedito Gonçalves, corregedor-geral de Justiça Eleitoral, que destaca, se tem evidente violação ao dever não deduzir pretensão ciente de que é destituída de fundamento e ainda, classificou a petição como "uma fábula escrita a duas mãos" e "extremamente inadequado".

O uso de IA e citação de jurisprudências falsas não possui lei específica neste caso, mas há várias normas jurídicas que preenchem a lacuna existente para esse caso de avanço tecnológico. No que diz respeito ao advogado e o Código de Ética e Disciplina da OAB, por meio da Resolução CFOAB nº 02/2015 constam as seguintes disposições:

> Art. 2º O advogado, indispensável à administração da Justiça, é defensor do Estado Democrático de Direito, dos direitos humanos e garantias fundamentais, da cidadania, da moralidade, da Justiça e da paz social, cumprindo-lhe exercer o seu ministério em consonância com a sua elevada função pública e com os valores que lhe são inerentes. Parágrafo único. São deveres do advogado: II – atuar com destemor, independência, honestidade, decoro, veracidade,

> lealdade, dignidade e boa-fé; III – velar por sua reputação pessoal e profissional;

Já na Lei nº8.906 de julho de 1994 que dispõe sobre o estatuto da advocacia e a Ordem dos Advogados do Brasil, os seguintes artigos dispõem sobre infrações e sanções disciplinares:

> Art. 34. Constitui infração disciplinar:
> XXV - manter conduta incompatível com a advocacia;
> Art. 35. As sanções disciplinares consistem em:
> I - censura;
> II - suspensão;
> III - exclusão;
> IV - multa.
> Parágrafo único. As sanções devem constar dos assentamentos do inscrito, após o trânsito em julgado da decisão, não podendo ser objeto de publicidade a de censura.

De acordo com a legislação aplicável à errônea conduta de advogados, se o principal objetivo de proteger o respeito às regras éticas e processuais, a preservação da credibilidade e segurança jurídica do ordenamento jurídico e o princípio da boa-fé processual. E para uma análise dos impactos de uso de jurisprudências falsas, devem ser entendidas as atuais sansões impostas para advogados que utilizam do ChatGPT e jurisprudências falsas.

Segundo uma notícia do site G1, No Tribunal de Justiça de Santa Catarina, um advogado que apresentou jurisprudências falsas foi multado ao pagamento de multa de 10% do valor atualizado da causa. Neste caso, mantem-se sigilo a respeito dos valores e o nome do profissional em questão.

Além disso, 6ª Câmara do TJSC determinou que o caso seja comunicado à Ordem dos Advogados do Brasil – Seccional Santa

Catarina (OAB/SC) com encaminhamento do recurso para devida análise.

O papel do advogado, como defensor dos interesses do seu cliente, deve priorizar a verdade no uso informações, incluindo a obrigação de investigar minunciosamente os fatos, apresentar informações verdadeiras no tribunal de forma honesta. A veracidade é uma responsabilidade fundamental que o advogado assume para garantir a justiça e integridade no âmbito jurídico (Rogério, 2024)

CONCLUSÃO

As recentes notícias sobre o uso de inteligência artificial na criação de documentos jurídicos por advogados têm repercutido na mídia, e gerado um impacto negativo sobre o exercício da advocacia como meio de acesso à justiça, afetado pela falta de responsabilidade em averiguar as informações e jurisprudências de um processo.

A tecnologia avança para melhorias e facilitação de ações humanas, entretanto, os princípios basilares de todo o ordenamento jurídicos são os mesmos e devem ser respeitados. O trabalho de um advogado deve observar a veracidade, responsabilidade e ética continuam como pilares de sua atuação. O uso de IA pode ser um grande aliado, mas deve ser usada com consciência e compromisso com a verdade. Os casos reais brasileiros abordados nesta pesquisa evidenciam os valores de um processo jurídico e os cuidados na atuação jurídica.

Portanto, as informações falsas ensejam sanções disciplinares junto à Ordem dos Advogados do Brasil (OAB) por respeito as regras éticas e preservação da credibilidade do profissional de direito e a segurança de um sistema jurídico. Servindo de alerta não só para advogados, mas também para todo o ecossistema jurídico que utilizam da inteligência artificial. Seu uso deve ser criterioso e sempre acompanhado da devida revisão humana, sob pena de graves consequências processuais e éticas.

REFERENCIAS

ÂMBITO JURÍDICO. **Advogado é multado pelo TSE por usar ChatGPT em petição**. Âmbito Jurídico, 24 abr. 2023. Disponível em: https://ambitojuridico.com.br/advogado-e-multado-pelo-tse-por-usar-chatgpt-em-peticao/. Acesso em: 01 junho 2025.

AZEVEDO, Noé. **A justiça e a máquina de escrever.** Revista dos Tribunais, São Paulo, v. 57, n. 306/307, p. 29-30, 2019

FIGUEIREDO, Diana. **Tecnologia muda às exigências na área de direito**, 2018

G1 SANTA CATARINA**. Advogado multado por informações falsas geradas por ChatGPT entra com recurso.** G1, 20 fev. 2025. Disponível em: https://g1.globo.com/sc/santa-catarina/noticia/2025/02/20/advogado-multado-informacoes-falsas-chatgpt-recurso.ghtml. Acesso em: 2 jun. 2025.

MIGALHAS. **Advogado usa ChatGPT em petição e é multado pelo TSE: "fábula".** Migalhas, São Paulo, 19 abr. 2023. Disponível em: https://www.migalhas.com.br/quentes/385080/advogado-usa-chatgpt-em-peticao-e-e-multado-pelo-tse--fabula. Acesso em: 01 junho 2025

MIGALHAS. **TJ/PR rejeita recurso feito por IA que inventou 43 jurisprudências.** Migalhas, São Paulo, 25 abr. 2025. Disponível em: https://www.migalhas.com.br/quentes/429134/tj-pr-rejeita-recurso-feito-por-ia-que-inventou-43-jurisprudencias. Acesso em: 29 maio 2025.

OLIVEIRA, Silvana de**. TJ/PR rejeita recurso feito por IA: 43 jurisprudências falsas e um alerta à advocacia.** Just Arbitration, 26 abr. 2025. Disponível em: https://justarbitration.com.br/2025/04/26/tj-pr-rejeita-recurso-feito-por-ia-43-jurisprudencias-falsas-e-um-alerta-a-advocacia/. Acesso em: 29 maio 2025.

PARANÁ. Tribunal de Justiça. 1ª Câmara Criminal. Recurso em Sentido Estrito n. 0002062-61.2025.8.16.0019, Comarca de Ponta Grossa. Relator: Desembargador Gamaliel Seme Scaff. Julgado em 12 abr. 2025. Publicado em 15 abr. 2025. Disponível em: https://portal.tjpr.jus.br/jurisprudencia/j/4100000031991241/Ac%C3%B3rd%C3%A3o-0002062-61.2025.8.16.0019. Acesso em: 29 maio 2025.

ROGÉRIO, Thiago. **O que é veracidade?** Conferência da Advocacia. Disponível em: https://www.conferenciadaadvocaciars.com.br/glossario/o-que-e-veracidade-na-advocacia/. Acesso em: 2 jun. 2025.

SOARES, Marcelo Negri et al. **Inteligência artificial:impactos no direito e na advocacia.** Direito Público, v. 17, n. 93, 2020.12 SOARES, Marcelo Negri et al. Inteligência artificial: impacto no direito e na advocacia. Direito Público, v. 17, n. 93, 2020.

TRIBUNAL DE JUSTIÇA DE SANTA CATARINA**. TJSC multa autor de recurso por jurisprudência falsa gerada por inteligência artificial.** Imprensa TJSC, 18 fev. 2025. Disponível em: https://www.tjsc.jus.br/web/imprensa/-/tjsc-multa-autor-de-recurso-por-jurisprudencia-falsa-gerada-por-ia. Acesso em: 2 jun. 2025.

VITAL, Danilo. **TSE multa advogado por petição baseada em "fábula" escrita com ChatGPT.** Jurídico, São Paulo, 18 abr. 2023. Disponível em: https://www.conjur.com.br/2023-abr-18/tse-multa-advogado-peticao-baseada-conversa-chatgpt/. Acesso em: 29 maio 2025.

GOVERNANÇA ALGORÍTMICA E *COMPLIANCE* DIGITAL: FUNDAMENTOS PARA A SALVAGUARDA DOS DIREITOS FUNDAMENTAIS NA ERA DA INTELIGÊNCIA ARTIFICIAL

Fernando José Ribeiro Feitoza

Acadêmico em Especialização em Direito, Compliance e Mecanismos Anticorrupção pela Universidade do Estado do Amazonas - UEA /AM.

Albefredo Melo de Souza Junior

Advogado. Professor efetivo da Escola de Direito da Universidade do Estado do Amazonas (ED/UEA). Membro do Núcleo de Direito, Tecnologia e Inovação (LAWin/UEA). Mestre em Direito (Unilasalle/RS). albefredo@uea.edu.br

1. OBJETIVOS

O presente artigo tem por objetivo investigar os fundamentos normativos da governança algorítmica e do compliance digital, a fim de demonstrar sua relevância para a efetivação dos direitos fundamentais na era da inteligência artificial.

2. METODOLOGIA

Sob o prisma metodológico, este trabalho adota abordagem qualitativa, com base em revisão bibliográfica, análise de diplomas legais, notadamente a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e o Projeto de Lei nº 2.338/2023 no cenário brasileiro. A pesquisa pretende-se contribuir para o debate acadêmico-jurídico sobre os desafios e caminhos possíveis para uma regulação democrática e humanizada dos sistemas de inteligência artificial.

3. DESENVOLVIMENTO DA PESQUISA

A ascensão da inteligência artificial (IA) como vetor estruturante das transformações tecnológicas do século XXI tem suscitado intensos debates no campo jurídico, sobretudo no que tange à compatibilização entre o uso de algoritmos e a preservação dos direitos fundamentais. Em uma sociedade cada vez mais moldada por sistemas de decisão automatizada, sejam eles empregados na esfera privada, como no setor financeiro e na gestão de recursos humanos, ou na esfera pública, como na segurança, educação e saúde, torna-se imperiosa a construção de um marco normativo que assegure a governança ética desses sistemas e sua sujeição aos limites constitucionais (Weyermüller, Wedy e Hupffer, 2024, p. 8).

Sob o plano normativo, o tema ainda se encontra pendente de regulação, haja vista que ainda tramita no Congresso Nacional o Projeto de Lei nº 2.338/2023, sobre o desenvolvimento, o fomento e o uso ético e responsável da IA com base na centralidade da pessoa humana com o objetivo de regular a IA no Brasil.

Mesmo diante desse cenário, a governança algorítmica emerge como conceito jurídico-normativo que visa disciplinar a forma pela qual os algoritmos são concebidos, operados, auditados e responsabilizados. Sua finalidade não se esgota na regulação técnica, mas abarca a exigência de mecanismos que garantam a transparência, a equidade e a responsabilização por decisões produzidas por sistemas de inteligência artificial. Tais exigências tornam-se ainda mais prementes quando se observa a crescente incidência de discriminações algorítmicas, violação à autodeterminação informativa e decisões opacas que afetam diretamente a esfera jurídica de indivíduos e coletividades.

A título de compreensão, a governança algorítmica compreende um campo regulatório que objetiva disciplinar o ciclo de vida dos sistemas automatizados, que abrange desde a sua concepção, desenvolvimento, aplicação e supervisão. Trata-se de uma "modalidade

de governo, de si e dos outros, respaldada na própria racionalidade dos algoritmos" (Castro, 2025, p. 1).

Diferentemente da responsabilidade civil, a governança algorítmica propõe um controle de natureza preventiva, incorporando as noções de accountability, explicabilidade e transparência. No plano jurídico, o tema tem suscitado debates jurídicos e relevando-se alvo de preocupação, na medida em que, conforme Souza, Sabbag e Achilles (2024, p. 2), nas novas tecnologias da informação e comunicação encontra-se aderência suficiente para reproduzir uma sociedade incivil, diante da sobreposição de interesses privados homogeneizantes de finalidades públicas. Complementam os autores (2024, p. 2):

> Isso porque essas novas tecnologias são operadas por algoritmos obedientes aos imperativos neoliberais das organizações-empresas – Big Techs –, fazendo com que o mediador das relações simbólicas entre sujeitos e instituições seja engessado por uma linguagem binária redutora da diversidade das relações interpessoais.

Tal premissa é reforçada diante da incidência de eventos envolvendo os sistemas automatizados, que ora revelam a opacidade algorítmica, que impossibilita o cidadão compreender os critérios utilizados para a tomada de decisão produzida pela Inteligência Artificial, comprometendo a capacidade de contraditório e a ampla defesa; ora operam de forma discriminatória, a qual, de acordo com Silva e Barbosa (2023, p. 5-6), pode ser compreendida como:

> a possibilidade de as tecnologias de inteligência artificial replicarem ou até mesmo reforçarem preconceitos já existentes na sociedade, a partir de distinções, preferências ou exclusões capazes de afetar o tratamento entre indivíduos, sobretudo os grupos vulneráveis.

Daí emerge a importância de mecanismos como *accountability* algorítmica, explicabilidade e transparência. A primeira consiste na obrigação de agentes públicos e privados de prestarem contas sobre os critérios de decisão, o funcionamento do sistema automatizado, que deve ocorrer ainda na fase de planejamento, desenvolvimento, operação dos sistemas e os resultados das decisões por eles tomadas. Já a explicabilidade trata "da capacidade de descrever e justificar as decisões tomadas por sistemas de IA, permitindo que sejam entendidas e confiáveis para os humanos" (Pádua e Lorenzetto, 2024, p. 353). E a transparência, por sua vez, consiste no "acesso claro às informações e processos de tomada de decisão, explicando como as decisões são feitas e quais critérios e algoritmos (sequências de instruções lógicas) são aplicados."

Com efeito, são necessários os mecanismos que reforcem a integridade dos sistemas automatizados, sobretudo aqueles utilizados para a produção de decisões na esfera pública, que repercutem nos direitos individuais e coletivos, de modo a garantir que o desenvolvimento e aplicação da Inteligência Artificial (IA) operem de forma segura e benéfica para a sociedade (Sasson e Costa, 2024).

Nesse sentido, surge a *compliance* como resposta, na medida que este instrumento objetiva a prevenção de riscos associados à desconformidade normativa, a segurança operacional e a responsabilidade ética dos agentes envolvidos. Trata-se de movimento recente que vem se consolidando no campo normativo, e desponta como ferramenta complementar e essencial à governança algorítmica, conforme propõe esta pesquisa. De acordo com Carvalho e Rodrigues (2016, p. 9), trata-se de "um conjunto de medidas internas que permite prevenir ou minimizar riscos de violação às leis decorrentes de atividade praticada por um agente econômico e de qualquer um de seus sócios e colaboradores". Assim, o *compliance* digital surge como instrumento complementar e essencial à governança algorítmica, uma vez que não se limita à observância formal da legalidade, mas constitui ferramenta estratégica, assegurando a aderência a valores

fundamentais, tais como a dignidade da pessoa humana, o direito à igualdade e a proteção de dados pessoais (Vieira, Barreto, 2019).

Para fins de ilustração, registre-se que a Lei Geral de Proteção de Dados estabelece princípios, direitos e deveres voltados à proteção de dados pessoais, impondo às organizações a adoção de mecanismos de conformidade voltados à salvaguarda dos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade. E os programas de *compliance*, por sua vez, consistem nos meios pelos quais tais exigências implementadas, sistematizadas e monitoradas, a exemplo do treinamento de colaboradores que manuseiam informações sensíveis, mapeamento de dados. Isso quer dizer, que o *compliance* constitui o instrumento que estrutura os mecanismos de monitoramento contínuo, auditoria e documentação, com vistas a garantir que a organização age em conformidade com o arcabouço legal (Godinho e Faria, 2021).

E o *compliance* digital surge como instrumento complementar e essencial à governança algorítmica. Seu escopo abrange o desenvolvimento de políticas internas, códigos de conduta, práticas de integridade e mecanismos de auditoria contínua voltados à conformidade legal. O *compliance*, portanto, não se limita à observância formal da legalidade, mas constitui ferramenta estratégica de *accountability*, assegurando a aderência a valores fundamentais, tais como a dignidade da pessoa humana, o direito à igualdade e a proteção de dados pessoais (Vieira, Barreto, 2019).

A implementação de *compliance* implica a execução de políticas claras de governança de dados e conformidade com os direitos dos titulares, que se releva essencial para afastar litígios e sanções administrativas, especialmente à luz da Lei Geral de Proteção de Dados (LGPD) (Godinho e Faria, 2021). Já nos órgãos públicos, como secretarias, tribunais, secretarias de saúde ou instituições de segurança, a exigência de *accountability* é ainda maior, em razão da supremacia do interesse público.

Por sua vez, as empresas de tecnologia operam com coleta massiva de dados e perfilamento automatizado, que podem ser

processados sob uma excessiva racionalidade para a realização de reconhecimento facial, crédito automatizado e produção de decisões em políticas públicas, o que, não raras vezes pode ensejar na incidência de discriminação e opacidade algorítmica, reproduzindo ou reforçando preconceitos existentes na sociedade.

Cabe aqui recordar que em 2020, o *Twitter* admitiu na plataforma, em que o algoritmo de reconhecimento fácil constrangeu os usuários pretos que submeteram suas imagens para a aplicação automatizada na remoção de impurezas. Sobre o caso comenta Netto (2022, p. 1293):

> Um exemplo recente desta espécie reside na admissão pública de erro efetuada, ao final de 2020, pelo Twitter, acerca de um algoritmo de reconhecimento facial atuante em tal plataforma. Este se destinava a automatizar a tarefa de cropping, em que se removem as impurezas do fundo de uma imagem, promovendo-se o seu melhor enquadramento. A controvérsia surgiu quando usuários reportaram que, ao submeterem imagens em que constavam uma pessoa negra e uma pessoa branca, a tendência algorítmica consistia em manter a última no enquadramento considerado ideal.

Logo, considerando que os programas de inteligência artificial têm como ponto de partida a sistematização de dados, incluindo os pessoais, não há como negar a intersecção entre LGPD, programas de *compliance* e o uso ético da IA.

Nesse sentido, a aplicação de sistemas *compliance* pode desempenhar um importante papel na consolidação de uma cultura organizacional orientada à ética e à responsabilidade digital, uma vez que constitui uma ferramenta eficaz na contenção de opacidade, abusos e discriminações praticadas pela IA. Além da concepção e operação dos sistemas de automatização, a calibragem dos algoritmos deve orientar-se pelo respeito aos direitos fundamentais (Sasson e Costa, 2024).

Embora o marco regulatório do uso da inteligência artificial no Brasil ainda pende de aprovação no Congresso Nacional, os interesses envolvidos sobre o tema podem prolongar em demasia o processo legislativo. No entanto, como não há como reveter a onipresença dos sistemas de automatização nas diversas esferas decisórias, seja do setor público quanto do privado, os poderes estatais não podam se furtar do dever de garantir que a IA venha subverter no campo digital a ordem jurídica sobre qual se assenta o Estado Democrático de Direito.

4. CONCLUSÕES

Com a pretensão de atender às finalidades aqui propostas, a pesquisa demonstrou a relevância das categorias jurídicas "governança algorítmica", "discriminação algorítmica", "opacidade algorítmica", "*accountability*", "explicabilidade" e "transparência". Embora ainda não haja regulação específica sobre o tema, não se pode ignorar as exigências a serem dirigidas às empresas responsáveis pela mineração de dados, que colocam em risco princípios basilares como a dignidade humana, a igualdade, a não discriminação e a autodeterminação informativa.

A governança algorítmica configura-se como estrutura regulatória do ambiente digital, baseada em mecanismos de controle legítimos e preventivos que garantem transparência, explicabilidade e responsabilização dos agentes envolvidos no uso de sistemas automatizados. Considerando que o compliance digital atua como vetor que operacionaliza esses princípios no cotidiano institucional e empresarial, promovendo políticas de integridade, gestão de riscos e conformidade com a legislação, especialmente a LGPD, emerge como instrumento complementar para reforçar a integridade desses sistemas frente à opacidade, abusos e discriminações promovidas pela IA.

A onipresença desses sistemas e a incidência de práticas algorítmicas discriminatórias e opacas acentuam a preocupação com

a ausência de um marco regulatório no Brasil. Apesar da tramitação do Projeto de Lei nº 2.338/2023, interesses diversos têm dificultado sua celeridade. Ainda assim, remanesce a urgência em buscar soluções normativas e tecnológicas que garantam o desenvolvimento da IA com base na justiça social e nos valores constitucionais, evitando a reprodução de desigualdades históricas por ferramentas tecnocientíficas.

Assim, a governança algorítmica e o compliance digital não devem ser vistos como formalidades institucionais, mas como mecanismos essenciais e interseccionais para a construção de uma inteligência artificial transparente, justa e constitucionalmente adequada. Ambos devem estar comprometidos com a supremacia dos direitos fundamentais diante da transformação digital, reforçando a necessidade de um pacto regulatório que submeta a inovação tecnológica à ética e à dignidade humana, especialmente no âmbito público.

Palavras-chave: Governança algorítmica; *Compliance* digital; Direitos fundamentais; Inteligência artificial; Regulação ética.

REFERÊNCIAS

BRASIL. **Projeto de Lei n. 2.338, de 2023.** Dispõe sobre o uso da inteligência artificial no Brasil. Brasília, DF: Senado Federal, 2023. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9881643&ts=1742240906322& disposition=inline. Acesso em: 29 mai. 2025.

CARVALHO, Vinicius Marques de; RODRIGUES, Eduardo Frade. **Guia para Programa de Compliance: Orientações sobre estruturação e benefícios da adoção dos programas de compliance concorrencial**. Ministério da Justiça. Conselho Administrativo de Defesa Econômica, 2016.

CASTRO, Julio Cesar Lemes de. **A economia libidinal da governança algorítmica**. Revista de Psicologia da Universidade de São Paulo, 2025, vol. 36.

FRANÇA NETTO, Milton Pereira de; EHRHARDT JÚNIOR, Marcos. **Os riscos da discriminação algorítmica na utilização de aplicações de inteligência artificial no cenário brasileiro**. Revista Jurídica Luso Brasileira, v. 8, n. 3, p. 1271–1318, 2022.

GODINHO, Willames José Morais; FARIAS, Emerson Oliveira de. **A atuação da Lei Geral de Proteção de Dados (LGPD) frente Compliance**. Revista Científica Semana Acadêmica, Fortaleza, nº. 000212, 10/09/2021.

PÁDUA, Sérgio Rodrigo de; LORENZENTTO, Bruno Meneses. **O Direito Fundamental à Explicabiliadade da Inteligência Artificial utilizada em decisões estatais**. Revista da AGU, Brasília-DF - v. 23 - n. 02 – jun/2024.

SASSON, Jean Marc; COSTA, Carina Araújo. **O papel do compliance na era da IA: ética e transparência são cruciais para eficiência e**

privacidade em um mercado cada vez mais digital. 2024. Disponível em: https://www.jota.info/opiniao -e-analise/colunas/regulacao-e-novas-tecnologias/o-papel-do-compliance-na-era-da-ia. Acesso em: 02 jun. 2025.

SILVA, Isabela Maria Soares; BARBOSA, Letícia Mendes. **Inov(ação): discriminação algorítmica racial e as inteligências artificiais no Brasil**. Revista do Centro Acadêmico Afonso Pena, Belo Horizonte, Vol. 28, N. 2, 2023.

SOUZA, Gabriel Scudeller de; SABBAG, Deise Maria Antonio; ACHILLES, Daniele. **Governamentalidade Algorítmica, sociedade incivil e capitalismo de vigilância: resistência pela produção do comum**. Revista TransInformação, Campinas, v. 36, 2024.

VIEIRA, James Batista; BARRETO, Rodrigo Tavares de Souza. **Governança, gestão de riscos e integridade**. Brasília: Enap, 2019. 240p.

WEDY, Gabriel; HUPFFER, Haide Maria; WEYERMÜLLER, André Rafael. **Direito e inteligência artificial: perspectivas para um futuro ecologicamente sustentável**/ organização Gabriel Wedy, Haide Maria Hupffer, André Rafael Weyermüller. – São Leopoldo: Casa Leiria, 2024.

JUSTIÇA 4.0 E A TRANSFORMAÇÃO DIGITAL DO JUDICIÁRIO: ENTRE A INOVAÇÃO TECNOLÓGICA E A GARANTIA DE DIREITOS FUNDAMENTAIS

Françoyne Martins de Souza
Joan Bohadana Barroso
Franklin Carioca Cruz

PALAVRAS-CHAVE: Justiça 4.0; Transformação digital; Inovação tecnológica; Direitos fundamentais; Poder Judiciário.

1. OBJETIVOS

O objetivo deste resumo expandido é analisar o impacto da Justiça 4.0 na transformação digital do Poder Judiciário brasileiro, com ênfase na relação entre inovação tecnológica e a garantia dos direitos fundamentais. Busca-se examinar como a adoção de novas tecnologias, como inteligência artificial, automação de processos e plataformas digitais, têm promovido mudanças estruturais no sistema judicial, contribuindo para a eficiência, transparência e acessibilidade dos serviços jurisdicionais. Além disso, pretende-se discutir como as inovações tecnológicas podem coexistir com a preservação dos princípios constitucionais e a proteção dos direitos fundamentais dos jurisdicionados.

2. METODOLOGIA

A metodologia deste estudo fundamentou-se em uma revisão integrativa da literatura, abrangendo artigos científicos, legislações, relatórios institucionais e documentos oficiais relacionados à transformação digital do Poder Judiciário no contexto da Justiça 4.0. Como principal fonte de dados estatísticos e diagnósticos sobre o funcionamento do sistema judicial brasileiro, utilizou-se o relatório

Justiça em Números 2024, elaborado pelo Conselho Nacional de Justiça (CNJ), documento consolidado como referência nacional em transparência e análise da administração judiciária. Foram examinados indicadores de produtividade, movimentação processual, estrutura organizacional, iniciativas digitais e dados sobre a implementação dos Núcleos de Justiça 4.0, permitindo uma análise crítica das tendências, desafios e impactos da inovação tecnológica na garantia dos direitos fundamentais no âmbito do Poder Judiciário brasileiro.

3. DESENVOLVIMENTO

3.1. ORIGEM E CONTEXTUALIZAÇÃO DA JUSTIÇA 4.0

Desde o momento em que o Poder Judiciário assume a incumbência de dirimir os complexos conflitos sociais, impende-lhe adotar instrumentos e metodologias capazes de assegurar a todos os jurisdicionados a efetiva realização de seus direitos. Nessa perspectiva, é imperativo que os sistemas de justiça ofereçam soluções compatíveis com a dinâmica das transformações sociais, em especial as de natureza tecnológica. Em razão disso, intensificam-se os esforços e as pesquisas voltadas à construção de um ecossistema digital que conecte, de maneira segura e transparente, o próprio Judiciário, os cidadãos e os demais atores processuais.

Dados extraídos do relatório *Justiça em Números 2024* evidenciam que o Poder Judiciário tem intensificado significativamente os investimentos em fluxos de inovação, por meio da implementação de programas e iniciativas que impulsionaram, em ritmo inédito, a modernização tecnológica e a transformação dos métodos de trabalho. Esse movimento teve seu marco inicial em 2006, com a promulgação da Lei nº 11.419, que passou a regulamentar a utilização de meios eletrônicos na tramitação de processos judiciais, na comunicação de atos processuais e na prática de atos por meio digital.

O relatório também ressalta que o cenário provocado pela pandemia de COVID-19 foi determinante para a aceleração do

desenvolvimento e da adoção de ferramentas digitais no âmbito do Poder Judiciário. Nesse contexto, destacou-se o Programa Justiça 4.0, responsável por impulsionar uma série de estratégias voltadas à transformação digital do sistema de justiça, com vistas à ampliação do acesso à Justiça, à eficiência processual e à integração tecnológica entre os diversos órgãos jurisdicionais.

Iniciado em 2020, o Programa Justiça 4.0 resulta de um acordo de cooperação entre o Conselho Nacional de Justiça (CNJ) e o Programa das Nações Unidas para o Desenvolvimento (PNUD), com o apoio de diversos tribunais superiores e demais órgãos do sistema de justiça. Seu objetivo central é desenvolver e aprimorar soluções tecnológicas que tornem os serviços jurisdicionais mais acessíveis, eficazes e eficientes para a população.

Além disso, a iniciativa visa otimizar a gestão processual voltada a magistrados, servidores, advogados e demais operadores do Direito, por meio do uso colaborativo de tecnologias digitais e ferramentas baseadas em inteligência artificial. Entre seus principais propósitos destacam-se a celeridade na entrega da prestação jurisdicional, a ampliação do alcance dos serviços forenses e a racionalização dos custos orçamentários no âmbito da Justiça.

De acordo com o Conselho Nacional de Justiça (2024), o Programa Justiça 4.0:

> *é um catalizador da transformação digital que visa a aprimorar a justiça em um serviço (seguindo o conceito de justice as a service), aproximando ainda mais esse Poder das necessidades dos(as) cidadãos(as) e ampliando o acesso à justiça. As inovações tecnológicas têm como propósito dar celeridade à prestação jurisdicional e reduzir despesas orçamentárias decorrentes desse serviço público. (Conselho Nacional de Justiça, 2024, p. 218).*

Entre as ferramentas tecnológicas implementadas no âmbito do Programa Justiça 4.0, destacam-se, notadamente, a Plataforma Digital

do Poder Judiciário Brasileiro (PDPJ-Br), a Plataforma Sinapses, a Plataforma Codex, o Juízo 100% Digital, o Balcão Virtual e os Núcleos de Justiça 4.0.

Essas soluções tecnológicas têm por finalidade não apenas a ampliação da eficiência institucional e o aprimoramento da prestação jurisdicional, mas também a efetivação dos direitos e garantias fundamentais consagrados na Constituição da República Federativa do Brasil de 1988, especialmente no que se refere à promoção do amplo acesso à justiça, à razoável duração do processo e à tutela jurisdicional adequada e efetiva.

3.2. INSTRUMENTOS TECNOLÓGICOS: PLATAFORMAS, INTELIGÊNCIA ARTIFICIAL E PORTAIS

A consolidação do Programa Justiça 4.0 encontra expressão concreta na implementação de um conjunto articulado de ferramentas tecnológicas, concebidas com o propósito de otimizar a tramitação processual, ampliar o acesso à justiça e promover maior eficiência na atuação dos órgãos jurisdicionais. Tais ferramentas são estruturadas de forma a permitir a interoperabilidade entre os sistemas judiciais, a automatização de tarefas repetitivas e o uso de inteligência artificial como suporte à tomada de decisão judicial e administrativa. Conforme destaca o CNJ, "o Programa Justiça 4.0 propõe a adoção de soluções tecnológicas inovadoras para aprimorar a prestação jurisdicional, tornando-a mais acessível, eficiente e transparente".

Dentre essas inovações, destaca-se nas plataformas tecnológicas, instrumentos como o DataJud, a Plataforma Codex e a Plataforma Digital do Poder Judiciário (PDPJ-Br) que constituem a espinha dorsal da infraestrutura digital do Judiciário. O DataJud centraliza e consolida dados processuais provenientes de 91 órgãos, servindo como fonte oficial para o Sistema de Estatísticas do Poder Judiciário e baseando relatórios estratégicos como o Justiça em Números desde 2022. Já a Plataforma Codex atua como um robusto data lake, agregando bases

processuais, estruturando dados e alimentando sistemas de business intelligence e modelos de IA, potencializando a análise e a tomada de decisão. A PDPJ-Br, por sua vez, representa um ambiente colaborativo de desenvolvimento multisserviço, modernizando o Processo Judicial Eletrônico (PJe) ao incorporar conceitos como microsserviços, computação em nuvem e inteligência artificial, promovendo flexibilidade e integração nacional no trâmite processual.

Destaca-se ainda a Plataforma Sinapses, responsável pelo armazenamento, treinamento, versionamento e auditoria de modelos de IA, assegurando governança e transparência no uso dessas tecnologias. Todas essas iniciativas convergem para a efetivação da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), que orienta a evolução tecnológica e a transformação digital no setor.

No campo da inteligência artificial, a introdução da APOIA (Assistente Pessoal Operada por Inteligência Artificial) marca um avanço significativo. Integrada à PDPJ-Br e desenvolvida inicialmente pelo TRF-2, a Apoia utiliza IA generativa para criar conteúdos textuais a partir de comandos, auxiliando magistrados e servidores em tarefas como elaboração de relatórios, ementas, revisão de textos jurídicos, sínteses processuais, triagem temática e detecção de litigância predatória. Com uma arquitetura aberta e colaborativa, a ferramenta oferece uma alternativa institucional segura frente a soluções privadas, promovendo agilidade, precisão e segurança no tratamento de dados sensíveis. Outros projetos de IA, como Oxe (TJBA), Galileu (TRT-4) e Assis (TJRJ), também foram selecionados para compor iniciativas colaborativas, ampliando o ecossistema de inovação.

No que tange ao acesso à Justiça, instrumentos como o Balcão Virtual, o Juízo 100% Digital, os Núcleos de Justiça 4.0, o Domicílio Judicial Eletrônico e os Pontos de Inclusão Digital (PID) têm desempenhado papel fundamental. O Balcão Virtual, acessível nos sites dos tribunais, simula o atendimento presencial por videoconferência, otimizando recursos e ampliando o acesso, embora ainda enfrente desafios relacionados à conectividade e à inclusão digital. Conforme

Rapin e Igreja (2022), "a magistratura atuante concorda em sua maioria (60%) que o balcão virtual tenha se tornado a principal forma de atendimento dos órgãos judiciais em que atuam" (RAPIN; IGREJA, 2022). No mesmo sentido, o Juízo 100% Digital, regulamentado pela Resolução n. 345/2020, permite que todo o processo judicial transcorra de forma remota, enquanto os Núcleos de Justiça 4.0, criados pela Resolução n. 385/2021, concentram-se em matérias especializadas e operam integralmente em ambiente digital, reduzindo custos e promovendo eficiência. O Domicílio Judicial Eletrônico, obrigatório para instituições públicas e empresas, centraliza comunicações processuais em ambiente virtual, otimizando tempo e recursos. Por fim, os Pontos de Inclusão Digital viabilizam o acesso de cidadãos excluídos digitalmente, reforçando o compromisso do Judiciário com a universalização do acesso à Justiça.

3.3. IMPACTOS E DESAFIOS PARA A GARANTIA DE DIREITOS FUNDAMENTAIS

Como relatado por Rapin e Igreja (2022), com a evolução tecnologia veio consigo desafios complexos para a total inclusão ao acesso à justiça:

> *Diante dos novos desafios colocados pela transformação digital da justiça, verificamos que uma gama específica de obstáculos se apresenta. Indagados sobre os desafios enfrentados com o uso de novas tecnologias nas atividades judiciais, as magistradas e os magistrados participantes de nossa pesquisa apontaram, de forma expressiva: a dependência, cada vez maior, do acesso à justiça em relação à qualidade do acesso e da conexão à Internet (1.786 respondentes, de um total de 1.859); a necessidade de reestruturação do trabalho remoto e da gestão do órgão judicial (1.493); a tendência dos espaços físicos do Poder Judiciário perderem sua importância e diminuírem diante do atual processo de desenvolvimento tecnológico (1.456);*

> *a falta de informação à população sobre os possíveis usos da rede digital para acessar à justiça (1.309); a falta de domínio de ferramentas tecnológicas pelos usuários do sistema de justiça (1.304); o cansaço e/ou esgotamento relacionado à quantidade de tempo de conexão (1.161); e a falta de equipamentos e/ou infraestrutura adequados aos usuários do sistema de justiça (1.116).*
> *Assim, podemos considerar que o acesso efetivo à justiça vai além do movimento de entrada nas instituições; é constituir um espaço jurídico não só mais inclusivo, mas mais aberto à "autotransformação" (IGREJA; RAMPIN, 2021, p. 212)*

A transformação digital no âmbito do Poder Judiciário impõe impactos e desafios significativos para a garantia de direitos fundamentais, especialmente no que tange ao acesso efetivo à justiça. O avanço das tecnologias da informação e comunicação alterou profundamente as relações jurídicas, tornando-as mais dinâmicas, massivas e desterritorializadas, ao mesmo tempo em que exigiu do sistema judicial brasileiro uma rápida adaptação para acompanhar tais mudanças. Nesse contexto, a Constituição Federal de 1988, ao consagrar o acesso à justiça e a proteção de dados como direitos fundamentais, estabelece parâmetros normativos que orientam a atuação estatal e privada frente às inovações tecnológicas.

A digitalização dos processos judiciais, a automação por meio de inteligência artificial e a adoção de ferramentas como blockchain e contratos inteligentes trouxeram ganhos de eficiência, celeridade e transparência ao sistema judiciário. Lunardi (2019) avalia que "mecanismos de gestão judicial, administração da justiça, gestão da inovação e inovações tecnológicas têm trazido esperança de que o processo judicial possa se tornar mais célere e efetivo". A possibilidade de consultas e acompanhamento processual online, audiências por videoconferência e a simplificação de procedimentos são exemplos de avanços que potencializam o exercício do direito fundamental de acesso à justiça. No entanto, tais benefícios não se distribuem de forma

homogênea na sociedade brasileira. Persistem obstáculos estruturais, como a desigualdade no acesso à internet de qualidade, a carência de equipamentos adequados e a falta de domínio das ferramentas tecnológicas por parte de usuários e operadores do direito. Esses fatores acentuam a exclusão digital e comprometem a universalidade do acesso à justiça, especialmente para populações vulneráveis e economicamente desfavorecidas.

Outro desafio relevante reside na necessidade de reestruturação do trabalho remoto e na redefinição dos espaços físicos do Poder Judiciário, que tendem a perder centralidade diante do desenvolvimento tecnológico. A ausência de informação adequada à população sobre os usos da rede digital para acessar a justiça, aliada ao cansaço e esgotamento decorrentes do tempo excessivo de conexão, revela a complexidade da transição para o ambiente digital. Além disso, a dependência crescente de sistemas digitais aumenta a exposição a riscos de segurança cibernética e à violação de dados sensíveis, tornando imprescindível a observância rigorosa das normas de proteção de dados, como a Lei Geral de Proteção de Dados Pessoais e o artigo 5º, inciso LXXIX, da Constituição Federal.

No plano ético e jurídico, a automação de decisões judiciais por algoritmos suscita questionamentos sobre transparência, responsabilidade e respeito aos princípios do contraditório e da ampla defesa, exigindo regulamentação adequada e constante atualização dos profissionais do direito. Dessa forma, o desafio contemporâneo consiste em promover a inclusão digital, garantir infraestrutura adequada, capacitação contínua e regulamentação eficiente, de modo a assegurar que a transformação digital seja instrumento de efetivação e não de restrição dos direitos fundamentais, em conformidade com os preceitos constitucionais e com a dignidade da pessoa humana.

CONCLUSÃO

A transformação digital do Poder Judiciário brasileiro, impulsionada pelo Programa Justiça 4.0, representa um marco na modernização institucional e na busca por maior eficiência, transparência e acessibilidade dos serviços jurisdicionais. A incorporação de plataformas digitais, inteligência artificial e novas formas de atendimento remoto trouxe avanços concretos, como a redução de custos, a celeridade processual e a ampliação do acesso à justiça, especialmente para populações geograficamente distantes dos grandes centros.

Contudo, o estudo evidencia que tais inovações não estão isentas de desafios. A exclusão digital, a necessidade de infraestrutura adequada, a capacitação dos usuários e a garantia de transparência e governança dos sistemas automatizados são questões centrais que exigem respostas contínuas e políticas públicas efetivas. A digitalização, para além de modernizar procedimentos, precisa ser acompanhada de um compromisso com a inclusão social e com a proteção dos direitos fundamentais, evitando o aprofundamento das desigualdades históricas e assegurando que todos possam usufruir dos benefícios das novas tecnologias.

Diante disso, conclui-se que a Justiça 4.0 inaugura um novo paradigma para o Judiciário brasileiro, mas seu pleno êxito depende do equilíbrio entre inovação tecnológica e respeito aos princípios constitucionais. O futuro da justiça digital exige o fortalecimento de estratégias inclusivas, o monitoramento constante dos impactos das inovações e a atuação proativa do Estado na promoção do acesso universal às ferramentas digitais. Somente assim será possível garantir que a transformação digital contribua, de fato, para a efetivação dos direitos fundamentais e para a construção de uma justiça mais acessível, eficiente e democrática.

REFERÊNCIAS

CONSELHO NACIONAL DE JUSTIÇA (CNJ). Justiça 4.0 – Tecnologia da Informação e Comunicação. Disponível em: https://www.cnj.jus.br/tecnologia-da-informacao-e-comunicacao/justica-4-0/. Acesso em: 25 maio 2025.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). Tribunais de todo o país já podem utilizar primeira IA generativa integrada à PDPJ-Br. Disponível em: https://www.cnj.jus.br/tribunais-de-todo-o-pais-ja-podem-utilizar-primeira-ia-generativa-integrada-a-pdpj-br/. Acesso em: 25 maio 2025.

SILVA, A. C. da; et al. Inteligência artificial no sistema judicial brasileiro: desafios e oportunidades. Revista P2P & Inovação, v. 7, n. 1, 2024. Disponível em: https://revista.ibict.br/p2p/article/view/7341/7068. Acesso em: 25 maio 2025.

RAPIN, Talita, IGREJA, Rebecca Lemos. Acesso à Justiça e Transformação Digital: um Estudo sobre o Programa Justiça 4.0 e Seu Impacto na Prestação Jurisdicional. *Revista Brasileira de Direito Público*, Brasília, v. 19, n. 102, p. 120–153, abr./jun. 2022. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6512/2694. Acesso em: 27 maio 2025.

CONSELHO NACIONAL DE JUSTIÇA. Justiça em números 2024. Brasília: CNJ, 2024. 448 p. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2024/05/justica-em-numeros-2024.pdf. Acesso em: 26 maio 2025.

FERRAZ, Taís Schilling; CARACAS, Jaqueline Reis; BAGGIO, Cristhiane Trombini Puia. Programa Justiça 4.0: a perspectiva inovadora da prestação jurisdicional sob o enfoque da celeridade e da transparência. Brazilian Journal of Development, Curitiba, v.8, n.10, p.67590-67610,

oct, 2022. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/53190/39575. Acesso em: 28 maio 2025.

O USO ÉTICO DA INTELIGÊNCIA ARTIFICIAL NA ELABORAÇÃO DE ARTIGOS CIENTÍFICOS

Denison Melo de Aguiar

Advogado. Doutor em Direito pelo PPGD-UFMG. Professor da Escola de Direito da UEA. Contato: daguiar@uea.edu.br

Adriana Almeida Lima

Advogada. Doutora em Direito pelo PPGD-UFMG. Professora da Escola de Direito da UEA. Contato: allima@uea.edu.br

Helder Brandão Goés

Advogado. Mestrando em Direito pelo PPGDA-UEA. Contato: heldergoes9780@gmail.com

Palavras-chave: ética; inteligência artificial; artigos científicos; ética científica aplicada.

1. OBJETIVOS

O objetivo geral deste resumo é descrever como pode ocorrer o uso ético da inteligência artificial (IA) na elaboração de artigos científicos. Os objetivos específicos são: 1. Dissertar sobre a ética no uso de inteligências artificiais e 3. Aplicar esse uso ético na elaboração de artigos científicos.

2. METODOLOGIA

A metodologia empregada é a qualitativa com o foco em pesquisa bibliográfica (Marconi e Lakatos, 2004). A pesquisa qualitativa se configura com o uso de lei, doutrinas, em especial artigos científicos que tratam de temática central e adjacentes. Foi feito levantamento bibliográfico no google acadêmico, com revisão bibliográfica de

temática para se centrar, não no que o objeto de pesquisa se apresenta, qual seja, a relação entre ética, inteligência artificial e artigos científicos, mas, como é possível a utilização ética das inteligências artificiais na elaboração de artigos científicos, por meio de diálogo com a inteligência artificial copilot (2025), em forma de questionamentos. Portanto, a parte procedimento é importante pois mostra a aplicação e desenvolvimento da utilização instrumental da Inteligência artificial como instrumento ético na prática.

3. DESENVOLVIMENTO

A utilização das Inteligências artificiais na elaboração de artigos científicos já é uma realidade do meio científico no Brasil e no mundo, onde não há retorno, a questão principal é se pensar na sua utilização ética. Assim sendo, é relevante que a ética, nesta utilização, seja o primeiro parâmetro na elaboração de manuscritos, dentro deste contexto, se questiona: como pode ocorrer o uso ético da inteligência artificial na elaboração de artigos científicos? Para esta questão, pode-se ter a seguinte hipótese: Não é possível garantir um uso ético da inteligência artificial, como um procedimento, na elaboração de artigos científicos, pois sempre poderá haver o uso antiético da IA; a manipulação de dados, a indução antética dos dados e tratamentos; e ausência de transparência no processo. As boas práticas vão depender das diretrizes éticas claras utilizadas e da regulamentação que garanta a transparência e integridade na utilização da IA em pesquisas acadêmicas (Pithan e Vidal, 2013).

Ao se tratar de pesquisas científicas o grande desafio ético está no plágio, noutros termos, a reprodução não autorizada de obras protegidas por direitos autorais (Brasil, 1998). Ao se utilizar uma IA copiando e colando um texto elaborado por esta, se estar fazendo plágio, mesmo que não pela IA não replique o texto, assim, não se trata de meta-autoria, tão pouco de autorias (Marcelo Araujo, 2017), mas da utilização de má-fé de IA, o que se leva por conta questionar,

como se pode fazer um uso ético, sem se comete o crime de plágio. O plágio é, sem de dúvidas, um problema na formação dos profissionais, na orientação entre professor-aluno e um atraso ao desenvolvimento intelectual aplicado à ética.

Um profissional que dependa de IA para fazer um manuscrito pode ter uma deficiência na sua formação, para além da má-fé, nos termos de Rosado, *et al* (2012, p. 212):

> Apesar de todos os esforços que o meio jurídico tem feito para combater esse tipo de ato que é o plágio, o fato de o ser humano almejar conseguir tudo rápido, supera essa expectativa de ordem que a lei quer impor, é quase uma questão incontrolável, só aquelas pessoas que tem o bom senso e que querem realmente aprender é que vão fazer a coisa do jeito certo. É interessante afirmar também que, lá na frente, quando o estudante concluir seu curso superior, aí sim, é que veremos a diferença entre o profissional bom e aquele que se enganou a si mesmo. Por isso, a lei tem realmente que ser rigorosas quanto ao plágio, devendo haver por parte do governo uma divulgação maior quanto essa questão, pois ainda hoje se fala muito pouco no assunto, ou quase nada.

Portanto, o problema ético na utilização da IA, não está nela, mas em quem a utiliza. Entretanto, no meio científico no Brasil as cobranças de produção científicas podem colocar em xeque a saúde mental dos pesquisadores (MENEZES, *et al*, 2018), o que pode ser um meio de incentivo para a utilização indevida da IA, além disso, houve a atualização do uso da plataforma sucupira como parâmetro de produção científica, o que se pode centrar pela produção científica com alta qualidade da produção em citações de fator de impacto, da qual , talvez esse seja um sinal ou uma tendência para se repensar o fazer da pesquisa no Brasil. Logo, os profissionais pesquisadores, devem, como parâmetro primordial ter a utilização da ética não como

um parâmetro coercitivo ou coesivo, mas sim, como um parâmetro coerente na prática ética da pesquisa.

A aplicação do uso ético na elaboração de artigos científicos está na formação técnica e humanista de cada profissional. A formação técnica é muito importante, mas sem que tenha uma formação ética e humanística pode fazer a aplicação da má-fé na pesquisa e consequentemente nas políticas públicas e sociais. Nestes termos, a formação ética, durante toda a formação continuada dos profissionais, como pedagogia, talvez seja a melhor maneira para se consolidar o uso ético das IAs.

Partindo-se desta perspectiva, pode-se ter algumas orientações relevantes no sentido do uso ético na elaboração de artigos científicos. O uso transparente pode ser uma conduta ética, em especial, quando na metodologia, os autores fazem declaração do uso de IA, mas deve-se ter cuidado em se mostrar como fez o tratamento de dados, não basta citar que utilizou, o mais comum é informar que o fez em forma de perguntas e respostas; a verificação dos dados e informações disponibilizadas pelas IAs, em que pese os textos gerados serem convincentes, os pesquisadores devem validar os dados para evitar imprevisões, confirmando os dados elencados pelas IAs; uso da proteção dos dados sensíveis, para que haja o uso das normas de privacidade e segurança, em prol a proteger informações confidencias; compromisso ético dos pesquisadores no desenvolvimento de suas pesquisas; o incentivo ao reconhecimento do autoria humana, onde se utilizou a IA como instrumento auxiliar na escrita, quando a formulação de ideias e conclusões foram desenvolvidas pelos pesquisadores; detecção de plágio, ou seja, usar a IA como uma ferramenta para investigação de plágios, o que pode garantir a originalidade dos trabalhos acadêmicos; correção de língua vernácula; tradução a transcrição dos textos, quando a IA pode contribuir na tradução de artigos e transcrição de entrevistas, facilitando o acesso às informações. Elaboração de dados quantitativos em forma de estatística descritiva ou inferencial, dentre outros (Copilot, 2025). A IA não deve fazer a pesquisa pelos

pesquisadores, mas sim auxiliar na otimização da elaboração e revisão feitas pelos pesquisadores.

4. CONCLUSÕES

Ao se retornar ao questionamento: como pode ocorrer o uso ético da inteligência artificial na elaboração de artigos científicos? pode-se validar a hipótese. A hipótese: Não é possível garantir um uso ético da inteligência artificial, como um procedimento, na elaboração de artigos científicos, pois sempre poderá haver o uso antiético da IA; a manipulação de dados, a indução antética dos dados e tratamentos; e ausência de transparência no processo, é confirmada, pois os parâmetros de má-fé sempre serão possíveis, dependendo da decisão dos pesquisadores. Com isso, se coloca em xeque a qualidade e a idoneidade das pesquisas.

Um fator muito importante a ser destacado é a citação de IAs no manuscrito. Quando há a possibilidade de se criar um link descrevendo como foi o tratamento de dados pela IA, pode ser uma postura, de decisão a sua utilização, mesmo assim, não poderá se ter a pseudo replicação, ou confirmação dos dados, o que pode ser um risco para pesquisa de média e alta complexidades. Por fim, cabe aos pesquisadores o bom senso do uso das IAs na elaboração do manuscrito, de forma transparente, responsável, íntegra, ética para manter a originalidade e ser um caso bem-sucedido de produção científica.

A ética deve ser o primeiro parâmetro de quaisquer pesquisas. Dessa forma, pode-se concluir que o uso ético das IAs é determinante na elaboração de artigos científicos como uma questão fundamental da integridade da pesquisa acadêmica, onde as IAs podem ser um instrumento poderoso para otimização da escrita e revisões de artigos, desde que sua utilização respeite os princípios da transparência, responsabilidade e autoria humana. O desafio está na postura do ser humano e não a IA em si.

A utilização humana de IA deve ser ética. Haverá o risco de plágio e manipulação de dados, o que exige um compromisso sólido com boas práticas acadêmicas podem assegurar a IA, na condição de um recurso auxiliar e não um substituto do pensamento crítico e da originalidade cientificas, somando-se a isso, há de se ter regulamentações e diretrizes bem estabelecidas como meios essenciais para evitar o uso indevido da IA, o que pode proteger a credibilidade das produções científicas, bem como, formando profissionais éticos. Portanto, ser a aplicação ética da IA, uma forma de envolver a educação continuada ética, com formação humanística e técnica dos pesquisadores, para atuarem de forma transparente e responsável. A jornada para a aplicação ética de IA na pesquisa envolve educação com o uso consciente e ético da IA, o que não deve ser vislumbrado como uma restrição, mas sim como uma oportunidade para fortalecer a qualidade e confiabilidade do conhecimento científico.

REFERÊNCIAS

ARAUJO, Marcelo. O uso de inteligência artificial para a geração automatizada de textos acadêmicos: plágio ou meta-autoria? **Logeion**: filosofia da informação, v. 3, n. 1, p. 89-107, 2016. Disponível em: http://revista.ibict.br/fiinf/article/view/3012 Acesso em: 02 jun. 2025.

BRASIL. **Lei n. 9.610, de 19 de fevereiro de 1998.** Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9610.htm Acesso em: 02 jun. 2025.

COPILOT. **Coplitot**. 2025. Disponível em: https://copilot.microsoft.com/chats/MKsZ7EijNb9dkGkLVVCAr Acesso em: 02 jun. 2025.

MARCONI, M. de A.; LAKATOS, Eva Maria. **Metodologia científica**. São Paulo: Atlas, 2004. Disponível em: https://soniaa-arq.prof.ufsc.br/arq1001metodologiacinetificaaplicada/2013/grupo2/06.pdf Acesso em: 02 jun. 2025.

MENEZES, Alice Lopes do Amaral et al. Paralelos entre a produção científica sobre saúde mental no Brasil e no campo da Saúde Mental Global: uma revisão integrativa. **Cadernos de Saúde Pública**, v. 34, p. e00158017, 2018. Disponível em: https://www.scielo.br/j/csp/a/5SxHG9MTjW655YWY6kZpp7M/ Acesso em: 02 jun. 2025.

PITHAN, Lívia Haygert; VIDAL, Tatiane Regina Amando. O plágio acadêmico como um problema ético, jurídico e pedagógico. **Direito & Justiça**, v. 39, n. 1, 2013. Disponível em: https://revistaseletronicas.pucrs.br/fadir/article/view/13676 Acesso em: 02 jun. 2025.

ROSADO, Wesley et al. **Plágio, o crime desconhecido**. **Cadernos do CNLF**, v. 17, n. 11, 2013. Disponível em: http://www.filologia.org.br/xvii_cnlf/cnlf/11/16.pdf Acesso em: 02 jun. 2025.

INTELIGÊNCIA ARTIFICIAL E TRIBUTAÇÃO: A TRANSPARÊNCIA FISCAL E A PROTEÇÃO DOS DIREITOS CONSTITUCIONAIS

Juliana Victória Araújo de Amorim

Graduanda em Direito pela Universidade do Estado do Amazonas (UEA)

Prof. Dr. Neuton Alves Lima

Doutor em Direito pela Universidade Federal de Minas Gerais (UFMG)
Mestre em Segurança Pública, Cidadania e Direitos Humanos pela Universidade do Estado do Amazonas (UEA),
Graduado em Direito pela Universidade de Fortaleza (UNIFOR),
Professor efetivo da Universidade do Estado do Amazonas (UEA)

PALAVRA-CHAVE: Inteligência Artificial. Tributação. Direitos Fundamentais. Transparência Fiscal.

1 OBJETIVOS

O presente trabalho busca analisar o avanço e crescente uso da tecnologia, em especial a inteligência artificial (IA), no campo da administração pública voltada à seara tributária. É importante reconhecer que parte dos processos de arrecadação e fiscalização dos contribuintes está em constante transformação. Com a utilização dessas ferramentas, sistemas automatizados podem analisar dados e cruzar informações, permitindo a auditoria digital e facilitando o trabalho da gestão tributária. Nesse contexto, deve-se ter como princípio fundamental a proteção da transparência fiscal e dos direitos constitucionais dos contribuintes, conforme previsto na Constituição Federal de 1988.

2 METODOLOGIA

Para a metodologia deste resumo, adotou-se uma abordagem qualitativa, de caráter exploratório, utilizando-se o procedimento técnico de pesquisa bibliográfica e documental. Foram analisados artigos científicos que abordam os institutos relacionados à problemática aqui investigada.

3 DESENVOLVIMENTO

Inicialmente, é notório que nos dias atuais a sociedade vive em torno das tecnologias, e essas por sua vez, influenciam em torno de todo o ordenamento em que estamos inseridos. De certo, que, servem como auxílio e instrumentos para acrescer nas ações humanas, neste viés, o que antes era difícil e lento para identificar, hoje torna-se menos complexo e rápido com a utilização de um simples comando, *prompt*, por meio da IA.

Nessa perspectiva, a atividade de fiscalização tem passado por transformações profundas, acompanhando as mudanças da sociedade, principalmente ao adotar ferramentas digitais e tecnologias como a inteligência artificial, que simula processos cognitivos humanos para apoiar os fiscais em suas tarefas (Engelmann e Lietz, 2020). Assim, órgãos como a Receita Federal e Secretarias das Fazendas investem em tecnologias para aprimorar a detecção de fraudes, sonegação e planejamentos para analisar e controlar os recursos financeiros provenientes da arrecadação.

Sabe-se que essas ferramentas oferecem avanços notáveis; no entanto, suscitam sérios questionamentos quanto à compatibilidade dessas tecnologias com os princípios constitucionais que regem a administração pública. Nesse sentido, é importante salientar que o Direito Tributário — na concepção das ações do fisco — não deve ser pautado apenas pela necessidade de financiamento estatal, mas

também pelo compromisso de garantir a relação do contribuinte com a sociedade, à luz dos direitos fundamentais.

Outrossim, o cruzamento automático de dados fiscais e o comportamento do contribuinte permite ao algoritmo buscar a eficiência na arrecadação. A coleta e a criação de grandes bancos de dados, por exemplo, o SPED acumula dados de transações desde 2007, sendo que os relacionados a importação acumulam dados desde 1997 (Jambeiro Filho, 2016). No entanto, é preciso que haja uma rede de proteção as questões jurídicas e éticas, no tocante à transparência dos critérios que são adotados pela ferramenta do algoritmo, garantindo um ideal aos direitos dos contribuintes.

Nesse contexto, insta salientar que a transparência fiscal não se limita apenas à clareza das informações sobre os ganhos e investimentos públicos, mas abrange também as regras, diretrizes e critérios utilizados na tributação. Dessa forma, surge a necessidade da transparência algorítmica, ou seja, a definição dos meios e dos modos pelos quais a inteligência artificial estabelece os parâmetros para decisões que impactam os contribuintes.

Nessa linha, deve ser entender os princípios constitucionais e as consequências da fiscalização algorítmica. O princípio da legalidade (art. 5°, II da CF/88) estabelece que nenhum cidadão será obrigado a fazer ou deixar de fazer algo senão em virtude de lei. De modo amplo, quando as decisões tomadas por IA se fundam sem a devida fiscalização, sem base legal ou sem clareza nos critérios utilizados, gera uma violação a este princípio.

De igual modo, o princípio da Isonomia tributária (art. 150, II da CF/88) pode elucidar sobre a base de informações e o treinamento que o algoritmo passou, com dados históricos da sua equipe de treinamento, que podem ter vieses discriminatórios, reforçando estigmas contra grupos sociais, como pequenos empreendedores, microempresas ou cidadãos de regiões periféricas.

À luz dos princípios do devido processo legal e da ampla defesa, observa-se a ausência de explicabilidade nos algoritmos, o que dificulta o exercício pleno desses direitos. Com frequência, os contribuintes

não compreendem os motivos pelos quais foram selecionados para auditoria, tampouco têm acesso aos critérios que fundamentaram a decisão. Além disso, é sabido que, para os contribuintes de baixa renda, essas informações são ainda menos acessíveis, e o processo administrativo para contestar tais decisões demanda esforços físicos, temporais e financeiros significativos.

Por conseguinte, a ausência desses parâmetros dos sistemas utilizados desencadeia violações ao princípio da legalidade tributária, uma vez que, segundo o art. 150, I, da Constituição Federal de 1988, estabelece que nenhum tributo pode ser exigido sem que exista uma lei que o institua.

Sob esse prisma, cita-se o art. 5o, XXXV da Constituição da República Federativa do Brasil, que dispõe "a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça de direito". Diz respeito, então, de um direito munido de fundamentalidade formal e material (SARLET, 2010). Portanto, se o contribuinte é autuado com base em decisão formulado pelo sistema de algoritmos em que os critérios possam estar sem a base legal, resultará em uma violação potencial ao princípio da motivação das decisões, ampla defesa e contraditório.

Desse modo, a esfera jurídica de proteção do contribuinte modifica-se na medida que a forma de exercício das competências da administração tributária também se modifica pelo uso da inteligência artificial, acompanhando aquela as alterações ocorridas aos direitos fundamentais (Engelmann e Lietz, 2020). Assim, embora o uso da inteligência artificial na administração pública traga ganhos significativos, é importante ressaltar que a segurança jurídica dos direitos e garantias constitucionais exige um planejamento mais rigoroso por parte da gestão fiscal.

4 CONCLUSÃO

Diante do estudo apresentado, constata-se que o uso da Inteligência Artificial na área tributária proporciona benefícios significativos, como maior eficiência e agilidade na fiscalização e na arrecadação. Contudo, é essencial que sua aplicação seja pautada por estratégias que garantam equilíbrio funcional e observância aos preceitos éticos, especialmente no tocante à transparência fiscal e à proteção dos direitos constitucionais. Ressalta-se, ainda, a necessidade de assegurar o respeito aos princípios da igualdade tributária, da privacidade e do acesso à justiça durante a implementação e operação da IA nos processos fiscais.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Constituição da República Federativa do Brasil. Brasília: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/ constituicao.htm>. Acesso em 12 mai. 2024.

ENGELMANN, Débora; LIETZ, Bruna; DAHLEM, João Pedro. DIREITOS FUNDAMENTAIS DOS CONTRIBUINTES, ADMINISTRAÇÃO TRIBUTÁRIA E INTELIGÊNCIA ARTIFICIAL. 2020.

JAMBEIRO FILHO, Jorge Eduardo de Schoucair. SISAM - Sistema de Seleção Aduaneira por Aprendizado de Máquina. Disponível em: http://receita.economia.gov.br/sobre/institucional/memoria/concurso-historias-de-trabalho-darfb/arquivos-pdf/arquivos-6a-edicao/historia-de-sisam-com-a-vivi-parte2.pdf. Acesso em: 09 jul 2020.

PAULSEN, Leandro. Curso de Direito Tributário. São Paulo: Saraiva, 2019.

SARLET, Ingo Wolfgang. A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional. Porto Alegre: Livraria do Advogado, 2010.

A DUPLA FACE DA INTELIGÊNCIA ARTIFICIAL NO JUDICIÁRIO: POTENCIALIDADES, RISCOS E A URGÊNCIA DE UMA GOVERNANÇA ROBUSTA

Lydia de Jesus Azêdo Neta

Especialista em Proteção de Dados Pessoais (LGPD/GDPR)

Lattes: http://lattes.cnpq.br/6945443553102290

Pablo Oliva Souza

Mestre em Criminologia e Investigação Criminal - ISCPSI/Interpol

Lattes:http://lattes.cnpq.br/0957944434439946

Taís Viga de Albuquerque Oliva Souza

Especialista em Marketing Empresarial – Universidade Federal do Amazonas

Lattes: http://lattes.cnpq.br/0489140053208770

PALAVRAS-CHAVE: Equidade. Governança de IA. Inteligência Artificial. Poder Judiciário. Viés Algorítmico**.**

1. OBJETIVOS

O presente artigo teve por objetivo analisar criticamente o desafio central da distorção algorítmica na implementação da Inteligência Artificial (IA) no sistema judicial. Para além da análise diagnóstica deste risco específico, buscou-se identificar, discutir e propor os elementos-chave constitutivos de um robusto *framework* de governança focado em prevenir, mitigar e remediar má interpretações, assegurando a equidade e a justiça, com especial enfoque nas diretrizes éticas, requisitos técnicos para o uso de dados, mecanismos de segurança, e na garantia da rastreabilidade e auditoria humana voltadas à detecção de discriminação.

2. METODOLOGIA

O presente estudo emprega uma metodologia de abordagem qualitativa. O método de procedimento adotado será o dedutivo e quanto aos meios será de caráter descritivo, bibliográficos, uso da doutrina, consultadas publicações acadêmicas especializadas em algorítmicos e ética da IA, relatórios de instituições de referência, legislação pertinente e diretrizes éticas emergentes, com foco particular nas implicações da dupla face da IA no sistema judicial e documentos disponíveis na rede mundial de computadores.

3. DESENVOLVIMENTO DA PESQUISA

A pesquisa inicia com uma sucinta contextualização do potencial transformador da IA no sistema judicial (Seção 1). Subsequentemente, a segunda seção, um dos focos centrais, aprofunda-se no campo algorítmico como o principal risco ético-legal, detalhando suas origens, manifestações e o potencial impacto discriminatório e na perpetuação de injustiças. A seção explora como a falta de transparência e a complexidade da responsabilização agravam o problema do viés (Seção 2). A terceira seção, cerne do estudo, apresenta e discute detalhadamente os elementos essenciais de um arcabouço de governança especificamente desenhado para combater a questão algorítmica e promover a equidade na IA judicial (Seção 3). Finalmente, a quarta seção, outro pilar da discussão, aborda os desafios práticos para a implementação efetiva dessa governança anti-viés e aponta perspectivas futuras para pesquisa, regulação e monitoramento contínuo focados na mitigação de vieses (Seção 4).

A Inteligência Artificial (IA) desponta como uma força transformadora no sistema judicial. Contudo, sua implementação suscita um debate: a exploração de seu potencial exige um rigoroso arcabouço de governança, notadamente sob o aspecto do aperfeiçoamento dos sistemas de informação, com escopo de

assegurar a sua aplicação responsável, a integridade dos dados e a auditabilidade humana dos resultados. A celeridade da IA não pode eclipsar a urgência desta discussão, pois a natureza sensível dos dados judiciais e o impacto sobre direitos fundamentais demandam uma análise criteriosa dos riscos de discriminação algorítmica e a necessidade de uma ação regulatória proativa focada na equidade.

3.1 PRIMEIRA SEÇÃO - BREVE CONTEXTUALIZAÇÃO DO POTENCIAL DA IA NO SISTEMA JUDICIAL

A IA no domínio jurídico sinaliza uma mudança potencial de paradigma, com aplicações em otimização de fluxos de trabalho (automação de tarefas administrativas), suporte à decisão (pesquisa jurisprudencial avançada) e ampliação do acesso à justiça (*chatbots*). Iniciativas como o projeto "Victor" do STF e a plataforma "Sinapses" do CNJ ilustram esse potencial. Contudo, mesmo essas aplicações promissoras não estão imunes aos riscos que serão o foco deste artigo, notadamente o viés algorítmico, que pode comprometer a justiça pretendida por tais avanços (ANGWIN et al., 2016).

3.2 SEGUNDA SEÇÃO - O "DEBATE CRUCIAL": O VIÉS ALGORÍTMICO COMO AMEAÇA CENTRAL À JUSTIÇA E A NECESSIDADE DE GOVERNANÇA

Enquanto a IA oferece um horizonte de transformações, sua implementação no Judiciário é indissociável de um "debate crucial" centrado nos riscos que pode acarretar. Dentre eles, o viés algorítmico emerge como a ameaça mais significativa à equidade e legitimidade do sistema de justiça. Esta seção resume a natureza deste desafio, suas implicações ético-legais e a urgência de uma governança robusta.

O viés algorítmico, frequentemente originado em dados históricos que refletem e podem amplificar preconceitos sociais, raciais, de gênero ou econômicos, representa uma ameaça insidiosa.

Tais dados, como destacado por Barocas e Selbst (2016), não são meros reflexos neutros, mas construções que podem perpetuar injustiças sistêmicas ao treinar algoritmos para replicar padrões discriminatórios passados. A integridade dos dados, portanto, vai além da proteção, exigindo qualidade, representatividade e um tratamento crítico de vieses inerentes, sendo a diversidade nas equipes de desenvolvimento um fator mitigador.

A complexidade aumenta com a opacidade de muitos modelos de IA ("caixas-pretas", conforme Adadi & Berrada, 2018), que dificulta a identificação de como o viés opera. No contexto judicial, a falta de transparência e explicabilidade (*XAI*) impede a contestação de decisões algorítmicas potencialmente enviesadas e compromete a auditabilidade humana, sendo a *XAI* uma ferramenta crucial para expor e combater o viés.

Adicionalmente, a questão da responsabilidade por decisões enviesadas é premente: estabelecer cadeias claras de *accountability* (desenvolvedor, instituição, operador) é fundamental para reparação e incentivo de sistemas justos, transparentes e técnicos. Finalmente, o viés algorítmico pode corroer garantias fundamentais como o devido processo legal e o direito de defesa, especialmente se sistemas de avaliação de risco ou dosimetria da pena operarem com vieses não corrigidos, minando a presunção de inocência e o direito a um julgamento individualizado. A análise desses riscos reforça a necessidade de uma governança específica para promover equidade e mitigar discriminação na IA judicial.

3.3 TERCEIRA SEÇÃO - GOVERNANÇA PARA MITIGAÇÃO DE VIÉS ALGORÍTMICO E PROMOÇÃO DA EQUIDADE NA IA JUDICIAL

Diante da ameaça central representada pela questão algorítmica, um robusto arcabouço de governança não é apenas desejável, mas imperativo. Esta seção resume os pilares desse framework de governança anti-viés, que deve ser proativo e especificamente

orientado para prevenir, detectar e mitigar vieses, assegurando que a IA no Judiciário promova justiça e equidade. No cerne dessa governança residem **princípios éticos fundamentais com foco na equidade**, como justiça, não discriminação, transparência para detecção de viés, e responsabilidade por resultados enviesados. O **uso responsável de frameworks de IA** é crucial, exigindo diretrizes éticas para desenvolvimento e aquisição que priorizem a mitigação de viés, a realização de avaliações de impacto algorítmico e de direitos humanos com ênfase em discriminação, e testes rigorosos de viés com validação contínua. A **governança de dados** emerge como linha de frente, demandando políticas claras para coleta e tratamento de dados sensíveis (conforme LGPD), o uso de técnicas de pré-processamento para mitigar desbalanceamentos e a auditoria contínua da qualidade.

Complementarmente, são essenciais **mecanismos de rastreabilidade e auditoria humana focados em equidade**. Isso inclui sistemas de *logging* detalhados para análise de viés, interfaces de *XAI* que auxiliem na investigação de como características influenciam predições de forma desproporcional, a atuação de comitês de ética multidisciplinares com mandato anti-viés, e processos claros para contestação de decisões potencialmente enviesadas.

Por fim, a **capacitação, formação e uma cultura de consciência sobre viés** são indispensáveis, envolvendo treinamento específico para todos os atores do sistema judicial e o fomento à pesquisa sobre detecção e mitigação de viés no contexto judicial. Tal construção é um processo dinâmico, a consolidar a IA como aliada de uma justiça eficiente e equitativa.

3.4 QUARTA SEÇÃO – DESAFIOS: IMPLEMENTAR GOVERNANÇA ANTI-VIÉS E PERSPECTIVAS FUTURAS

A implementação efetiva da governança anti-viés depara-se com dificuldades práticas que demandam recursos especializados escassos e competem com outras prioridades orçamentárias. Soma-se

a isso o desafio técnico e filosófico de mensurar "justiça" e "equidade" algorítmica, dado que múltiplas métricas podem ser mutuamente exclusivas (KLEINBERG et al., 2016).

Nesse contexto, a regulação da IA no Judiciário com foco em anti-discriminação é vital. Legislação existente, como a LGPD, precisa ser detalhada para sistemas algorítmicos, com o CNJ desempenhando um papel relevante na expedição ágil de resoluções. As perspectivas futuras exigem investimento contínuo em pesquisa e monitoramento. Isso inclui o desenvolvimento de métodos mais robustos de detecção e mitigação de viés contextualmente apropriados ao Judiciário brasileiro (como *fairness-aware machine learning*), o aprimoramento da XAI para explicar vieses de forma compreensível, estudos sobre o impacto do viés na confiança pública no sistema de justiça, e a implementação de monitoramento contínuo de métricas de equidade para identificar desvios ("fairness drift"). Superar esses desafios é fundamental para que a IA seja uma força para a equidade.

4. CONCLUSÃO

Este estudo focou no desafio primordial do viés algorítmico na Inteligência Artificial aplicada ao sistema judicial e na imperativa necessidade de um arcabouço de governança robusto e direcionado para mitigar esse risco. A promessa de eficiência da IA não pode ser realizada à custa da justiça e da equidade.

Reafirma-se que apenas uma governança proativa, centrada na detecção, mitigação e correção de vieses, pode assegurar que a IA sirva como um instrumento para proteger direitos fundamentais e não para aprofundar desigualdades existentes. Os elementos de governança propostos, desde princípios éticos focados na não discriminação até mecanismos técnicos de auditoria de equidade e capacitação específica, são vitais. Os desafios para implementar tal governança são consideráveis, mas não intransponíveis. Exigem

compromisso institucional, investimento em pesquisa e diálogo contínuo e multidisciplinar.

A jornada de integração da IA no Judiciário deve ser guiada pela busca incessante por uma justiça que, ao se modernizar tecnologicamente, reforce seu compromisso fundamental com a equidade e a dignidade humana, combatendo ativamente qualquer forma de discriminação, seja ela humana ou algorítmica.

REFERÊNCIAS

ADADI, A.; BERRADA, M. Peeking Inside the Black-Box: **A Survey on Explainable Artificial Intelligence (XAI**). Disponível em: https://ieeexplore.ieee.org/document/8466590. Acesso: 27 mai. 2025.

ANGWIN, J. et al. Machine Bias: **There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks. ProPublica**, May 23, 2016. Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Acesso: 27 mai. 2025.

BAROCAS, S.; SELBST, A. D. **Big Data's Disparate Impac**t. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://courts.ca.gov/sites/default/files/courts/default/2024-12/btb24-2l-2.pdf. Acesso: 27 mai. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/. Acesso: 27 mai. 2025.

EUROPEAN COMMISSION. High-Level Expert Group on Artificial Intelligence. **Ethics Guidelines for Trustworthy AI**. Brussels, 2019. Disponível em: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. Acesso: 27 mai. 2025.

KLEINBERG, J.; MULLAINATHAN, S.; RAGHAVAN, M. **Inherent Trade-Offs in the Fair Determination of Risk Scores.** Disponível: https://cs.emis.de/LIPIcs/volltexte/2017/8156/pdf/LIPIcs-ITCS-2017-43. Acesso: 27 mai. 2025.

A RESPONSABILIDADE CIVIL DO *DISCORD* POR ASSÉDIO VIRTUAL: UMA ANÁLISE JURÍDICA À LUZ DO ORDENAMENTO BRASILEIRO

Lucas Nunes Figueiredo Cavalcante

Pós-graduando – UEA – Escola de Direito

Rochelle Monteiro Brito

Mestre em Administração pela Universidade Federal de Viçosa – UFV

Palavras-chave: *Discord*; Assédio Virtual; Responsabilidade Civil; digital.

1. OBJETIVO

O presente estudo busca analisar a responsabilidade civil da plataforma *Discord* diante de atos de assédio virtual praticados em seus servidores, considerando o ordenamento jurídico brasileiro bem como compreender o funcionamento jurídico da plataforma e seus mecanismos de moderação. Além disso busca também analisar os dispositivos aplicáveis como por exemplo o Marco Civil da Internet, a LGPD e o Código Civil, avaliar se os termos de uso e as políticas de *compliance* da plataforma estão adequados à legislação brasileira e propor sugestões ou diretrizes jurídicas para aprimorar a proteção dos usuários brasileiros.

2. METODOLOGIA

O presente estudo de forma exploratória, busca aprofundar o entendimento acerca da responsabilidade civil da plataforma *Discord* frente aos atos de assédio virtual praticados em seus

servidores, bem como as práticas adotadas pela plataforma. Também é adotada uma metodologia de natureza qualitativa, uma vez que busca compreender, interpretar e analisar os aspectos jurídicos relacionados à responsabilidade civil da plataforma no contexto de atos de assédio virtual à luz do ordenamento jurídico brasileiro e para tanto, adotou-se a pesquisa bibliográfica com consulta a documentos, reportagens, livros, normas e estudos científicos, dessa forma permitindo uma compreensão crítica sobre os limites e possibilidades da responsabilização da plataforma *Discord*

3. DESENVOLVIMENTO

Recentemente, especialmente no Brasil, tem-se visto o crescente uso de plataformas digitais de comunicação, dentre elas está o *Discord*, que trouxe benefícios de integração social, mas também desafios jurídicos relevantes, especialmente sobre práticas ilícitas de assédio virtual, ameaças e discursos de ódio A plataforma possui, dentre outras, uma característica que permite aos usuários a criação de servidores privados e semiprivados o que dificulta o controle a investigação e a responsabilização por práticas abusivas. Conforme um artigo publicado na editora acadêmica *SageJournals* dos EUA diz que, *"No entanto, esses mesmos recursos de privacidade pelos quais o Discord é celebrado atraíram supremacistas brancos para o site e permitiram que prosperassem."* (HESLEP; BERGE, 2024, p. 536).

O *Discord*, em suas diretrizes, veda expressamente práticas de assédio, que compreende atos de intimidação, assédio sexual, perseguição, evasão de bloqueios e organização de invasões a servidores com a finalidade de hostilizar usuários. Ademais, proíbe qualquer forma de ameaça, seja direta, indireta ou velada, contra indivíduos ou grupos, visando à manutenção de um ambiente digital seguro e respeitoso.

Umas das principais regulamentações no Brasil para a responsabilidade civil das plataformas é o Marco Civil da Internet,

Lei nº 12.965/2014, que condiciona essa responsabilidade em relação a remoção de conteúdo somente após ordem judicial configurando uma responsabilidade subjetiva. Bem como menciona Dra. Patrícia Peck, PhD em Direito Internacional e especialista em Direito Digital e Cibersegurança:

> Devido à importância de se garantir o direito à informação e a proteção da liberdade de expressão, foi promulgada uma lei específica no Brasil para tratar de algumas destas questões chamada de Marco Civil da Internet. A análise deste recente marco legal demonstra a difícil missão de legislar sobre a matéria. Com pouco mais de 30 artigos, tentou-se estabelecer uma carta de princípios para uma Internet mais inclusiva e justa para os brasileiros. São eles: neutralidade, acesso à Internet como direito essencial para o exercício da cidadania, liberdade de expressão e permanência do conteúdo e sua remoção só em casos excepcionais e com ordem judicial [...]. (PECK, 2021, p. 57)

Do outro lado, tem-se a Lei nº 13.709/2018, Lei Geral de Proteção de Dados que impõe deveres de dados e segurança impactando também na atuação dessas empresas diante de crimes virtuais.

De forma complementar, o Código Civil Brasileiro, através dos artigos 186 e 927, permite a responsabilização por omissão, sobretudo quando a plataforma, podendo evitar o dano, se torna omissa. Entretanto, a aplicação das normas brasileiras enfrenta impedimentos práticos, pois se trata de uma empresa estrangeira americana, gerando obstáculos de jurisdição para a efetividade da aplicação da lei. Da mesma forma, relata Dra. Patrícia Peck:

> A privacidade dos usuários da Internet é um tema de extrema relevância para ser discutido não apenas em nível nacional, nas leis de cada país,

> mas principalmente em nível internacional, já que a natureza da Internet é global.

Em que pese a importância da LGPD e do Marco Civil da Internet, é difícil dar um adequado tratamento sobre privacidade apenas com leis nacionais, sem que seja estabelecido um compromisso internacional sobre a matéria. (PECK, 2021, p. 63)

Além disso, o STJ decidiu que a responsabilidade dos provedores de aplicações de internet por conteúdos gerados por terceiros é subjetiva, tornando-se solidária com o autor do conteúdo ofensivo a partir do conhecimento da lesão e não tomando as providências necessárias para a remoção do conteúdo. Disse o Relator e Ministro do STJ, Marco Buzzi:

> Independentemente da legislação aplicável, como entende o STJ, nas situações em que há afronta à intimidade física e sexual, o provedor de conteúdo de internet será responsabilizado se for notificado, ainda que extrajudicialmente, e não retirar de imediato o material moralmente ofensivo. [...] No entanto, se a empresa é comunicada acerca do conteúdo ilícito e não reage de forma rápida para retirá-lo, configura-se a sua responsabilidade subjetiva, e ela responderá solidariamente com o autor do dano pela reparação à vítima. (STJ, 2020)

Essa orientação demonstra que há um dever de diligência mínima imposto às plataformas, principalmente quando informadas acerca de conteúdos lesivos, como casos de assédio, ameaças ou perseguições, não sendo necessário em todos os casos a devida notificação da plataforma para a remoção do conteúdo.

4. CONCLUSÃO

Diante da análise realizada, verifica-se que, embora o *Discord* adote políticas de moderação e termos de uso voltados à prevenção de práticas do assédio virtual, tais medidas nem sempre são suficientes para assegurar a efetiva proteção dos usuários brasileiros, pois mostram-se significativos os desafios no que diz respeito à aplicação extraterritorial das leis brasileiras e à efetividade das medidas judiciais em face da plataforma estrangeira que não possui representação formal no Brasil.

Logo, são relevantes as lacunas na legislação brasileira para lidar com crimes virtuais ocorridos na plataforma evidenciando a necessidade de evolução normativa, bem como a adequação plena às práticas de *compliance* brasileiras para que seja possível garantir um ambiente digital mais seguro, além de se mostrarem necessárias discussões jurídicas mais aprofundadas e a proposição de diretrizes específicas que fortaleçam os mecanismos de proteção dos usuários no ambiente digital brasileiro sem que se comprometa seus direitos fundamentais.

Portanto, uma das soluções viáveis seria o fortalecimento de acordos internacionais de cooperação jurídica voltados especificamente para o enfrentamento de ilícitos praticados nos ambientes digitais, de forma a viabilizar a responsabilização civil de plataformas estrangeiras como o *Discord*, bem como uma alternativa concreta seria exigir, por meio de legislação específica, que empresas de tecnologia que ofereçam serviços em território brasileiro mantenham representação jurídica no país, como já ocorre em legislações de outros países, como na União Europeia, com o *Digital Services Act (DSA)* de 2022. Essa medida facilitaria a aplicação das leis nacionais, além de tornar mais célere a responsabilização civil em casos de omissão na prevenção de crimes virtuais.

Além disso, é indispensável o investimento na educação digital dos usuários e na conscientização sobre segurança online, aliado à criação de canais institucionais de apoio às vítimas de crimes virtuais.

Como destaca Castells: *"O poder é exercido antes de tudo em torno da produção e difusão de nós culturais e conteúdos de informação. O controle sobre redes de comunicação torna-se a alavanca pela qual interesses e valores são transformados em normas condutoras do comportamento humano"*. (Castells, 2003, p. 224)

Como bem diz, o empoderamento dos usuários por meio da informação deve ser tão relevante quanto as normas jurídicas, é necessário que os usuários tenham uma educação e um pensamento crítico acerca do âmbito digital para que não sejam manipulados.

5. REFERÊNCIAS

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília: Presidência da República, [2002]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 28 maio 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República, [2014]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 28 maio 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Presidência da República, [2018]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 28 maio 2025.

BRASIL. Superior Tribunal de Justiça. **Responsabilização de provedor de aplicação por conteúdo ofensivo independe de notificação judicial.** Brasília, 04 dez. 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04122020-Responsabilizacao-de-provedor-de-aplicacao-por-conteudo-ofensivo-independe-de-notificacao-judicial.aspx. Acesso em: 1 jun. 2025.

CASTELLS, Manuel. *A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade.* Tradução Maria Luiza X. de A. Borges; revisão técnica Paulo Vaz. Rio de Janeiro: Jorge Zahar, 2003. Disponível em: https://dlivros.com/livro/galaxia-internet-manuel-castells. Acesso em: 1 jun. 2025.

DISCORD. *Bullying, Harassment, and Threats Policy Explainer.* Discord Inc., [2024]. Disponível em: https://discord.com/safety/bullying-harassment-threats-policy-explainer. Acesso em: 28 maio 2025.

DISCORD. *Terms of Service.* São Francisco, CA: Discord Inc., [2025]. Disponível em: https://discord.com/terms. Acesso em: 28 maio 2025.

HESLEP, D. G.; **BERGE,** P. S. *Mapping Discord's darkside: Distributed hate networks on Disboard. New Media & Society,* v. 26, n. 1, p. 534-555, 2024. Disponível em: https://doi.org/10.1177/14614448211062548. Acesso em: 1 jun. 2025.

PECK, Patricia. *Direito digital.* 8. ed. São Paulo: Saraiva Educação, 2021. Disponível em: https://pdfcoffee.com/direito-digital-patricia-peck-pinheiro-2021-pdf-free.html. Acesso em: 1 jun. 2025.

IA E RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA: DESAFIOS AOS DIREITOS FUNDAMENTAIS NO BRASIL

Luiz Felipe de Farias Leite Borges[7]
Lucas Almeida da Silva[8]

Palavras-chave: Inteligência Artificial. Reconhecimento Facial. Segurança Pública. Direitos Fundamentais. Discriminação Algorítmica.

1. INTRODUÇÃO

O uso de tecnologias de reconhecimento facial na segurança pública brasileira tem avançado sem regulamentação específica, gerando riscos diretos aos direitos fundamentais. Embora apresentada como solução tecnológica eficiente, essa ferramenta impacta negativamente a privacidade, a dignidade e a não discriminação, sobretudo de populações negras e periféricas.

Estudos, como o do **National Institute of Standards and Technology (NIST, 2019)**, mostram que esses sistemas apresentam até **100 vezes mais falsos positivos para pessoas negras, asiáticas e indígenas**, especialmente em operações do tipo **1:N**, comuns na segurança pública. No Brasil, esses riscos são concretos, evidenciados em casos documentados em **Salvador, Rio de Janeiro, Campinas e Sergipe**, onde houve prisões equivocadas, abordagens indevidas e erros operacionais. A escolha desses casos decorre da implementação efetiva da tecnologia, da repercussão pública e dos registros de violações de direitos.

Além disso, a legislação brasileira — como a **Lei Geral de Proteção de Dados (Lei nº 13.709/2018)** — não oferece instrumentos suficientes,

7 Pós-graduando em Direito 4.0 e Inteligência Artificial pela Universidade do Estado do Amazonas (UEA). E-mail: luizborges937@gmail.com

8 Mestre em Informática pela Universidade Federal do Amazonas (UFAM). E-mail: lucas.alsilva01@gmail.com

como avaliações de impacto, auditorias, transparência algorítmica e controle social. O país se distancia de práticas internacionais, como o **AI Act (2024)** da União Europeia e legislações municipais nos Estados Unidos, que já impuseram restrições ou até baniram o uso da tecnologia.

Diante desse cenário, este trabalho analisa os impactos jurídicos, sociais e tecnológicos do uso do reconhecimento facial na segurança pública brasileira, defendendo que, nas condições atuais, sua aplicação viola direitos fundamentais e demanda a construção urgente de um marco regulatório robusto e centrado na proteção desses direitos.

2. OBJETIVOS

O presente trabalho tem como objetivo geral analisar os impactos jurídicos, sociais e tecnológicos do uso de reconhecimento facial na segurança pública brasileira, destacando os riscos à proteção de dados, à não discriminação, à privacidade e à dignidade da pessoa humana.

De forma específica, busca-se:

- Mapear casos concretos no Brasil que evidenciam riscos, como Salvador, Rio de Janeiro, Campinas e Sergipe;
- Avaliar as fragilidades do ordenamento jurídico brasileiro frente ao uso do reconhecimento facial na segurança pública;
- Investigar modelos internacionais de regulação, como o **AI Act (2024)** da União Europeia e legislações de cidades dos Estados Unidos;
- Discutir os principais desafios técnicos, como viés algorítmico, falsos positivos e limitações operacionais;
- Propor diretrizes jurídicas para regulamentação do uso do reconhecimento facial no Brasil, com foco na proteção dos direitos fundamentais.

3. METODOLOGIA

A pesquisa adota abordagem qualitativa, exploratória e analítica, de caráter interdisciplinar, integrando fundamentos do direito, da ciência de dados e dos estudos críticos sobre tecnologia. A análise foi organizada em três etapas.

A primeira corresponde à revisão bibliográfica e documental, baseada em literatura acadêmica, marcos normativos e relatórios técnicos nacionais e internacionais. Os materiais foram selecionados por sua relevância teórica, atualidade e aderência direta ao tema, priorizando estudos entre 2018 e 2024, como o relatório do NIST (2019), a pesquisa de Buolamwini e Gebru (2018) e o AI Act (2024).

A segunda etapa é o estudo de casos concretos no Brasil, focando nas experiências de Salvador, Rio de Janeiro, Campinas e Sergipe. A escolha dessas cidades considerou a existência de registros públicos de erros operacionais, repercussão social e disponibilidade de dados que evidenciam impactos do reconhecimento facial sobre direitos fundamentais.

A terceira etapa consiste na análise comparada internacional, tomando como referência os modelos adotados na União Europeia, especialmente o AI Act (2024), e nas cidades norte-americanas de São Francisco, Boston, Portland e Oakland, que estabeleceram restrições ou baniram o uso da tecnologia na segurança pública.

Essa abordagem permite compreender os riscos jurídicos, técnicos e sociais associados ao uso do reconhecimento facial no Brasil e discutir caminhos regulatórios alinhados à proteção dos direitos fundamentais.

4. DESENVOLVIMENTO DA PESQUISA

O reconhecimento facial na segurança pública brasileira avança sem regulamentação específica, gerando riscos concretos à privacidade, proteção de dados e não discriminação. Embora

apresentado como solução tecnológica, essa ferramenta reproduz desigualdades estruturais, falsos positivos e violações de direitos, afetando desproporcionalmente populações negras e periféricas.

Os sistemas operam por meio de **redes neurais convolucionais (CNNs)**, que processam imagens faciais identificando padrões — como distância entre olhos, formato do nariz e contorno do rosto —, convertendo essas informações em vetores matemáticos para comparação com bancos de dados.

Apesar da sofisticação, há limitações estruturais associadas ao viés algorítmico. O estudo de **Buolamwini e Gebru (2018)** revelou que, enquanto a taxa de erro para **homens brancos foi de 0,8%**, para **mulheres negras chegou a 34,7%**, um aumento de **4.237%**. O relatório do **NIST (2019)**, que avaliou **189 algoritmos**, confirmou que, nos sistemas do tipo **1:N**, comuns na segurança pública, a taxa de falsos positivos para **homens brancos varia de 0,08% a 0,3%**, enquanto para **pessoas negras chega a 8% a 30%, até 100 vezes mais**. Resultados semelhantes foram observados para **asiáticos (5% a 25%)** e **indígenas (6% a 28%)**.

Estudo	Grupo	Erro (%)	Diferença Relativa
Buolamwini & Gebru (2018)	Homens Brancos	**0,80%**	Base de referência
	Mulheres Negras	**34,70%**	**+4.237% (43 vezes mais)**
NIST (2019)	Homens Brancos	**0,08% a 0,3%**	Base de referência
	Pessoas Negras	**8% a 30%**	**+7.900% a +9.900% (até 100x mais)**
	Pessoas Asiáticas	**5% a 25%**	**+6.150% a +8.250% (até 80x mais)**
	Pessoas Indígenas	**6% a 28%**	**+7.400% a +9.300% (até 90x mais)**

Esses riscos se materializam em casos concretos no Brasil. Em **Salvador (BA)**, levantamento da **Agência Pública (2019)** apontou que **90,5% dos presos por reconhecimento facial eram negros**, com destaque para a prisão equivocada de uma mulher no **Carnaval de**

2020, identificada como um homem procurado. No **Rio de Janeiro (2019)**, um homem foi detido após erro do sistema e só liberado após horas de privação de liberdade (**UOL Notícias**). Em **Campinas (SP)**, testes operacionais em terminais urbanos resultaram em abordagens equivocadas (**Rede Cidade Digital, 2020**). Em **Sergipe (2024)**, um torcedor foi detido por erro do sistema, levando o governo estadual a suspender temporariamente o uso da tecnologia.

Esses episódios confirmam que o reconhecimento facial, longe de ser neutro, funciona como mecanismo de vigilância seletiva, com impacto desproporcional sobre corpos negros e periféricos. Além disso, fatores como má iluminação, baixa qualidade de câmeras e ângulos desfavoráveis agravam ainda mais as taxas de erro.

O atraso regulatório brasileiro é evidente frente às medidas adotadas por outros países. Na **União Europeia**, o **Artificial Intelligence Act (2024)** classifica o reconhecimento facial como tecnologia de **altíssimo risco**, impondo restrições severas e, em muitos casos, **proibição total**, salvo exceções rigorosamente justificadas.

Nos **Estados Unidos**, cidades como **São Francisco, Boston, Portland e Oakland** proibiram completamente o uso do reconhecimento facial por órgãos públicos. O **Canadá**, por meio do seu órgão de proteção de dados, considerou ilegal o uso da tecnologia sem consentimento ou base legal robusta, suspendendo projetos em cidades como Toronto e Calgary. Na **Austrália**, órgãos de proteção à privacidade interromperam projetos públicos após constatar violações às leis locais. Na **Índia**, cresce a pressão da sociedade civil e do Judiciário pela suspensão desses sistemas, devido à ausência de uma lei nacional de proteção de dados.

Enquanto esses países avançam na regulação, priorizando a proteção dos direitos fundamentais, o **Brasil segue utilizando o reconhecimento facial na segurança pública sem marco legal específico, sem avaliações de impacto, governança algorítmica, auditorias ou controle social.**

Portanto, sua continuidade nas condições atuais representa **risco concreto e violação direta dos princípios constitucionais**

da dignidade da pessoa humana, privacidade, igualdade, não discriminação e devido processo legal.

5. CONCLUSÕES

A análise demonstra que o uso de tecnologias de reconhecimento facial na segurança pública brasileira, nas condições atuais, representa risco concreto e desproporcional aos direitos fundamentais, especialmente à privacidade, dignidade, igualdade e devido processo legal. Dados técnicos e casos concretos confirmam que esses sistemas operam com vieses estruturais, afetando desproporcionalmente populações negras, indígenas, asiáticas e grupos marginalizados, reforçando práticas discriminatórias e seletivas.

O cenário brasileiro evidencia grave defasagem normativa frente às práticas internacionais, onde restrições, suspensões e proibições já são adotadas diante dos riscos associados. Nesse contexto, a suspensão do uso do reconhecimento facial na segurança pública não é apenas recomendável, mas juridicamente necessária à proteção dos direitos fundamentais.

Admite-se, de forma excepcional e condicionada, sua utilização em ambientes privados e controlados, mediante consentimento e submetida a critérios rigorosos de governança, transparência e auditoria. Entretanto, sua aplicação em operações de segurança pública e monitoramento de espaços deve ser imediatamente suspensa, uma vez que carece de respaldo normativo e afronta preceitos constitucionais e compromissos internacionais.

O reconhecimento facial, na configuração atual, não apenas carece de efetividade e segurança técnica, mas amplia desigualdades e viola garantias fundamentais, resultando em riscos que não podem ser ignorados. A ausência de transparência, de mecanismos de auditoria e de controle social, agrava ainda mais os impactos dessa tecnologia no contexto brasileiro. Assim, a continuidade de seu uso, sem um marco regulatório robusto e instrumentos como avaliações

de impacto, transparência algorítmica e auditorias independentes, configura violação direta aos direitos fundamentais, reafirmando a urgência de sua suspensão.

REFERÊNCIAS

AGÊNCIA PÚBLICA. 90% das pessoas presas com reconhecimento facial na Bahia são negras. 2019. Disponível em: https://apublica.org/. Acesso em: 21 maio 2025.

BENJAMIN, R. *Race after technology: abolitionist tools for the new Jim code.* Cambridge: Polity Press, 2019.

BIONI, B. R. *Proteção de dados pessoais: a função e os limites do consentimento.* São Paulo: Thomson Reuters, 2021.

BUOLAMWINI, J.; GEBRU, T. Gender shades: intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, v. 81, p. 1-15, 2018.

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

CRAWFORD, K. *Atlas of AI: power, politics, and the planetary costs of artificial intelligence.* New Haven: Yale University Press, 2021.

EUROPEAN UNION. *Artificial Intelligence Act.* Brussels: European Commission, 2024.

INTERNETLAB. *Vigilância biométrica no Brasil: riscos, regulação e direitos.* São Paulo, 2022.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST. *Face recognition vendor test (FRVT) part 3: demographic effects.* 2019. Disponível em: https://doi.org/10.6028/NIST.IR.8280. Acesso em: 21 maio 2025.

REDE CIDADE DIGITAL. Campinas testa câmera de reconhecimento facial como a que flagrou procurado no carnaval. 2020. Disponível em: https://redecidadedigital.com.br/. Acesso em: 21 maio 2025.

UOL NOTÍCIAS. Homem é preso por engano após ser identificado por reconhecimento facial no Rio. 2019. Disponível em: https://noticias.uol.com.br/. Acesso em: 21 maio 2025.

UOL NOTÍCIAS. Reconhecimento facial leva à prisão equivocada de torcedor em Sergipe. 2024. Disponível em: https://noticias.uol.com.br/. Acesso em: 21 maio 2025.

ZUBOFF, S. *The age of surveillance capitalism.* New York: Public Affairs, 2020.

INTELIGÊNCIA ATIVA: ENTRE O INTELECTO UNIVERSAL E A INTELIGÊNCIA ARTIFICIAL CONTEMPORÂNEA.

Luiz Gustavo Negro Vaz

Mestre em Sociedade e Cultura na Amazônia pela Universidade Federal do Amazonas UFAM.
Especializando em Compliance e Mecanismos Anticorrupção, UEA, Manaus – AM,
E-mail: luiz.vaz@trt11.jus.br
Lattes: http://lattes.cnpq.br/5654194505900566

PALAVRAS-CHAVE: Inteligência Ativa; Intelecto Universal; Inteligência Artificial (IA); Filosofia Islâmica; Consciência.

1. OBJETIVOS

O presente trabalho tem como principal objetivo comparar a "Inteligência Ativa" da filosofia islâmica medieval (Avicena e Averróis) com a inteligência artificial contemporânea, visando explorar os limites epistemológicos, ontológicos e éticos da replicação da cognição humana por sistemas não biológicos. Este resumo propõe uma análise comparativa entre os conceitos clássicos de intelecto e os desenvolvimentos contemporâneos da inteligência artificial, explorando os limites epistemológicos, ontológicos e éticos da replicação artificial da mente humana, construindo um diálogo entre tradição filosófica e inovação tecnológica.

O avanço da inteligência artificial (IA) na contemporaneidade tem levantado questões fundamentais sobre a natureza do intelecto, a consciência e a possibilidade de replicação da cognição humana por sistemas não biológicos. Nesse contexto, a tradição filosófica islâmica, em especial as contribuições de Avicena (Ibn Sīnā) e Averróis (Ibn

Rushd), oferece fundamentos teóricos relevantes para pensar a inteligência como um princípio ativo, universal e metafísico.

Avicena introduz a ideia de uma Inteligência Ativa como uma substância incorpórea responsável pela iluminação do intelecto humano, permitindo a compreensão das formas universais. Averróis desenvolve a teoria do intelecto único e eterno, compartilhado por toda a humanidade. Tais concepções contrastam fortemente com as bases computacionais e estatísticas da IA atual, que opera por simulações de padrões e dados massivos, sem consciência reflexiva ou intuição metafísica.

2. METODOLOGIA

Com o intuito de atingir o objetivo proposto, a abordagem adotada é filosófico-comparativa, baseada na análise textual de fontes primárias e secundárias. O estudo estabelece um diálogo entre a concepção filosófica de inteligência ativa desenvolvida nos tratados de Avicena, principalmente no Kitāb al-Nafs (Livro da Alma), e no Tahāfut al-Tahāfut (Incoerência da Incoerência) de Averróis, confrontando-as com as noções operacionais de inteligência artificial concebidas por autores como Alan Turing (1950), Norbert Wiener (1948), John Searle (1980) e Luciano Floridi (2014).

A investigação orienta-se por três eixos principais: (1) A estrutura do conhecimento e sua origem no sujeito ou na máquina; (2) O problema da universalidade e da individuação do intelecto; (3) Os limites éticos e ontológicos da inteligência artificial em relação ao ideal clássico de sabedoria.

A recuperação do conceito de inteligência ativa, ainda que anacrônica em termos tecnológicos oferece subsídios críticos relevantes para o debate sobre IA, especialmente quanto à responsabilidade moral, à subjetividade e ao valor intrínseco do conhecimento.

3. DESENVOLVIMENTO

3.1 AVICENA E A INTELIGÊNCIA ATIVA

A teoria do intelecto ativo (ʿaql faʿāl) de Avicena representa uma síntese entre aristotelismo e neoplatonismo. Este intelecto não é apenas uma faculdade cognitiva, mas uma substância metafísica separada que ocupa o décimo nível na hierarquia das inteligências emanadas do Uno necessário, associando-se ao anjo Gabriel na tradição islâmica.

O processo epistemológico aviceniano fundamenta-se na iluminação dos dados sensíveis pelo intelecto agente, tornando-os inteligíveis à mente humana. Esta operação assemelha-se à luz que torna visíveis os objetos aos olhos: sem a atuação do intelecto ativo, a alma permanece em potência, incapaz de abstrair universais das imagens sensíveis (maḥsūsāt).

A estrutura hierárquica da inteligência aviceniana progride da apreensão sensível à união com o inteligível puro, transcendendo o âmbito cognitivo para abarcar dimensões éticas e espirituais. O filósofo que alcança a ciência verdadeira realiza simultaneamente sua perfeição moral e ontológica.

3.2 AVERRÓIS E O INTELECTO UNIVERSAL

Averróis desenvolve uma teoria revolucionária que postula a existência de um único intelecto agente universal, comum a toda humanidade. Sua concepção tripartite distingue: (i) O intelecto material (receptáculo individual das formas inteligíveis); (ii) O intelecto agente (substância separada, eterna e universal) e (iii) O intelecto adquirido (produto da união entre os anteriores).

Diferentemente de Avicena, Averróis defende que o intelecto agente não se particulariza em cada alma, mas existe como entidade única compartilhada por toda espécie humana, fundamentando a universalidade da ciência.

A radicalidade desta posição reside em sua inversão ontológica: não é o indivíduo quem pensa, mas o intelecto universal que pensa no indivíduo. Esta perspectiva provocou forte reação entre escolásticos como Alberto Magno e Tomás de Aquino, culminando na condenação do averroísmo latino em 1277.

3.3 INTELIGÊNCIA ARTIFICIAL: FUNDAMENTOS E PARADIGMAS COGNITIVOS

A inteligência artificial surgiu em meados do século XX como tentativa de simular a cognição humana através de sistemas computacionais, baseando-se na hipótese funcionalista de que processos mentais podem ser formalmente descritos e algoritmizados. Alan Turing (1950) estabeleceu as bases teóricas ao propor o "teste de Turing" como critério para determinar a capacidade de uma máquina "pensar".

John McCarthy cunhou o termo "inteligência artificial" em 1956 durante a conferência de Dartmouth, estabelecendo a IA como disciplina interdisciplinar. Desde então, a área passou por ciclos de entusiasmo e decepção até a recente explosão promovida pelo aprendizado de máquina, big data e redes neurais profundas.

Sistemas contemporâneos como GPT, AlphaGo e DALL-E realizam tarefas antes consideradas exclusivamente humanas, funcionando com base em estruturas estatísticas e lógicas formais. No âmbito jurídico, por exemplo, a IA já é utilizada para analisar vastos volumes de jurisprudência e legislação, auxiliando advogados na identificação de precedentes relevantes e na previsão de desfechos processuais, aperfeiçoando a tomada de decisões e a eficiência operacional em um cenário de crescente complexidade informacional e digitalização. Como destacaram Stuart Russell e Peter Norvig (2020), os modelos atuais são predominantemente "indutivos", inferindo regras a partir da experiência empírica, sem uma metafísica do conhecimento.

John Searle (1980), com seu "argumento do quarto chinês", demonstrou que a IA pode manipular signos sem compreensão semântica. Apesar disso, teóricos como David Chalmers, Nick Bostrom e Ray Kurzweil defendem a possibilidade de uma IA forte, dotada de consciência e subjetividade.

3.4 CONTRAPONTO FILOSÓFICO: TÉCNICA, METAFÍSICA E SUBJETIVIDADE

O contraste entre o *intellectus agens* na tradição filosófica clássica e a inteligência artificial contemporânea revela uma profunda distinção ontológica: de um lado, a inteligência como ato do ser vinculado à verdade e finalidade; de outro, como técnica voltada à eficácia e instrumentalidade.

Para os filósofos medievais, a inteligência é inseparável da estrutura metafísica do real. Em ambos, o conhecimento representa um modo de união com o ser, um caminho da alma rumo à verdade e realização ontológica.

A Inteligência Artificial emerge de um paradigma técnico que rompe com essa tradição metafísica, reduzindo o saber à informação e a inteligência ao cálculo. Como observou Heidegger (1954), a técnica não é apenas instrumental, mas uma forma de "enquadramento" (Gestell) que transforma o ser em recurso disponível.

Esta redefinição acompanha um esvaziamento da subjetividade, pois a IA opera por funções algorítmicas que, embora eficientes, carecem de intencionalidade, autoconsciência e finalidade própria. A inteligência humana envolve julgar, interpretar, errar e duvidar - processos não redutíveis a cálculos.

3.4.1 CONVERGÊNCIAS E DESCONTINUIDADES

Existem algumas analogias funcionais entre a inteligência ativa medieval e a IA contemporânea: (i) Ambas apresentam uma

separação entre o sujeito que recebe a informação e a instância que a processa; (ii) A "inteligência em nuvem" assemelha-se ao intelecto agente averroísta que é único e acessível a todos; (iii) Ambos realizam uma forma de abstração - intelectual no caso filosófico, técnica no caso computacional.

Contudo, as divergências ontológicas são decisivas: (i) A inteligência ativa insere-se em um contexto metafísico onde o ser é teleológico e ordenado; (ii) A IA é um produto técnico-funcional, contingente, temporal e dependente de infraestrutura humana; (iii) A inteligência ativa conhece por assimilação (*intelligere est fieri*), enquanto a IA conhece por modelagem estatística e (iv) A IA carece do contexto, corporeidade e intuição pré-reflexiva essenciais ao conhecimento humano.

4. CONCLUSÕES

Este estudo estabeleceu um diálogo entre os conceitos filosóficos medievais de *intellectus agens* e os paradigmas contemporâneos da inteligência artificial. A comparação revelou que, apesar de analogias superficiais, existem divergências profundas e irredutíveis. A inteligência ativa dos filósofos islâmicos é uma faculdade transcendente, vinculada à natureza racional da alma e orientada ao verdadeiro. Em contraste, a inteligência artificial é um artefato técnico, imanente, desprovido de consciência ou intencionalidade.

Essa distinção carrega implicações epistemológicas, ontológicas e políticas significativas. No plano epistemológico, o conhecimento humano mediado pelo intelecto ativo possui sentido e finalidade, enquanto a IA opera com base em padrões estatísticos frequentemente desprovidos de significado semântico ou contextual.

Retomar Avicena e Averróis não é apenas um exercício erudito, mas uma estratégia filosófica crítica para repensar os fundamentos da "inteligência" em tempos de automação e datificação. Ambos

propõem modelos de racionalidade que valorizam a interioridade, a contemplação e a união com os princípios mais altos da realidade.

Em um mundo cada vez mais orientado por decisões algorítmicas, retomar a noção de inteligência ativa afirma que a racionalidade não se esgota na previsão estatística ou eficácia técnica - pensar é mais que calcular, conhecer é mais que correlacionar, e ser inteligente inclui discernir, julgar, amar, criar e se abrir ao mistério do ser.

REFERÊNCIAS

AVERROÍS (Ibn Rushd). A Decisiva Resposta (Fasl al-Maqal). Tradução, edição e estudo crítico por Charles E. Butterworth. Princeton: Princeton University Press, 2001.

AVICENA (Ibn Sīnā). O Livro da Cura: Lógica, Física e Metafísica. Tradução, Introdução e Notas de S. R. Al-Azmeh. São Paulo: Loyola, 2018.

BOSTROM, Nick. Superintelligence: Paths, Dangers, Strategies. Oxford: Oxford University Press, 2014.

CHALMERS, David J. The Conscious Mind: In Search of a Fundamental Theory. New York: Oxford University Press, 1996.

DAVIDSON, Herbert A. Alfarabi, Avicenna, and Averroes on Intellect: Their Cosmologies, Theories of the Active Intellect, and Theories of Human Intellect. New York: Oxford University Press, 1992.

DREYFUS, Hubert L. What Computers Can't Do: The Limits of Artificial Intelligence. New York: Harper & Row, 1972.

FLICK, Uwe. Introdução à Pesquisa Qualitativa. Porto Alegre: Artmed, 2009.

FLOREDI, Luciano. The Fourth Revolution: How the Infosphere is Reshaping Human Reality. Oxford: Oxford University Press, 2014.

HEIDEGGER, Martin. A questão da técnica. Tradução de Miguel Real. Lisboa: Presença, 1994. (Original publicado em 1954).

JONAS, Hans. O Princípio Responsabilidade: Uma Ética para a Civilização Tecnológica. Rio de Janeiro: Vozes, 1984.

RUSSEL, Stuart; NORVIG, Peter. Artificial Intelligence: A Modern Approach. 4. ed. Upper Saddle River: Pearson, 2020.

SEARLE, John R. Minds, Brains, and Programs. Behavioral and Brain Sciences, v. 3, n. 3, p. 417–424, 1980.

TURING, Alan M. Computing Machinery and Intelligence. Mind, v. 59, n. 236, p. 433–460, 1950.

WIENER, Norbert. Cybernetics: Or Control and Communication in the Animal and the Machine. Cambridge, MA: MIT Press, 1948.

A VIOLAÇÃO DA PRIVACIDADE NO BRASIL DIGITAL: O CASO DOS VAZAMENTOS EM GRUPOS DO TELEGRAM

Karina Lopes Cidade

Acadêmica de Direito na Escola Superior Batista do Amazonas (ESBAM). Lattes: http://lattes.cnpq.br/8283026721159480. E-mail: k.lopescidade@gmail.com.

Maíza Thayná Pereira Ribeiro

Mestranda do Programa de Pós-Graduação em Direito Ambiental da Universidade do Estado do Amazonas. Advogada.
E-mail: maizaribeiro.adv@gmail.com.
Lattes: http://lattes.cnpq.br/4401171125628103.
ORCID: https://orcid.org/0009-0000-9161-2237.

Palavras-chave: dados pessoais; direito à privacidade; LGPD; Telegram; vazamento de dados.

1. OBJETIVOS

Este trabalho tem como objetivo analisar criticamente o recente episódio de vazamento em massa de dados pessoais de brasileiros divulgado em grupos do Telegram, sob a perspectiva da Lei Geral de Proteção de Dados Pessoais (LGPD) e da Constituição Federal de 1988. Busca-se compreender os impactos jurídicos e sociais desse tipo de exposição, discutir a responsabilidade das plataformas digitais e do poder público, e evidenciar as fragilidades na aplicação das normas de proteção de dados no Brasil. Pretende-se, ainda, apontar caminhos para o fortalecimento da autodeterminação informativa e para a efetivação dos direitos fundamentais na era digital.

2. METODOLOGIA

O estudo adota o método dedutivo, partindo-se da análise das normas constitucionais e infraconstitucionais que asseguram o direito à privacidade, à intimidade e à proteção de dados pessoais. Quanto aos meios, trata-se de uma pesquisa bibliográfica e documental, com base em doutrinas jurídicas, legislações nacionais e internacionais, decisões judiciais e reportagens jornalísticas. Quanto aos fins, a pesquisa é qualitativa, voltada à reflexão crítica sobre as consequências da fragilidade da proteção de dados no Brasil, sobretudo em contextos de uso indiscriminado e vazamento criminoso de informações pessoais.

3. DESENVOLVIMENTO

3.1. O DIREITO FUNDAMENTAL À PRIVACIDADE E A EFETIVIDADE DA LGPD

Em um cenário pautado pela tecnologia e pela *interconnected* global, onde o acesso à informação é perpetuamente facilitado, observa-se uma diminuição na capacidade de reflexão consciente por parte do indivíduo. Para Carvalho (2013), isso ocorre porque as pessoas tendem a absorver uma quantidade vasta de informações de forma automática, sem dedicar tempo para analisá-las criticamente ou avaliar sua veracidade, limitando-se a repassá-las de maneira superficial. Esse fluxo intenso de dados, muitas vezes, impede que os usuários questionem a origem, a validade ou as implicações das mensagens recebidas, muitas das quais têm autoria duvidosa. Como resultado, há uma propagação descontrolada de conteúdos potencialmente falsos ou enganosos, bem como dados pessoais vazados e divulgados em questões de segundos, reforçando uma cultura de disseminação de informações sem o devido cuidado ou responsabilidade.

A Constituição Federal brasileira de 1988, em seu artigo 5º, inciso X, assegura a todos os brasileiros e aos estrangeiros residentes no país a inviolabilidade do direito à intimidade e à privacidade, ou

seja, todas as pessoas, independentemente de sua origem, gozam de igualdade perante a lei e têm o direito fundamental à proteção de sua vida pessoal, seus dados e informações pessoais, garantindo que esses dados permaneçam invioláveis e assegurado indenização por dano moral e material em caso de violação (BRASIL, 1988).

A Lei nº 13.709/2018, Lei Geral de Proteção de Dados (LGPD), tem como finalidade principal proteger os direitos relacionados à liberdade, à privacidade e ao desenvolvimento da personalidade das pessoas físicas. Em seu art. 1º e 2º dispõe sobre o tratamento de dados pessoais, incluindo aqueles realizados por meios digitais, feitos por pessoas físicas (indivíduos) ou jurídicas (empresas ou órgãos públicos), além disso, busca estabelecer um ambiente de segurança jurídica, promovendo a padronização de regras e práticas que garantam a proteção dos dados pessoais de todos os indivíduos no Brasil, alinhando-se aos padrões internacionais existentes. Diante disso, a LGPD define o que são dados pessoais e especifica que alguns tipos de informação, como os dados sensíveis e aqueles referentes a crianças e adolescentes, exigem cuidados adicionais. Ela também esclarece que a proteção se aplica a qualquer dado tratado, seja em suportes físicos ou digitais. Outro ponto importante é que, mesmo que a organização esteja sediada fora do Brasil ou o dado seja processado em outro país, se houver tratamento de informações de pessoas que estão no território nacional, a lei deve ser cumprida (BRASIL, 2018).

Leme (2019) explica que a preocupação com a proteção de dados evoluiu ao longo do tempo, sendo que sua origem remonta ao final do século XIX. No entanto, esse tema foi ganhando maior relevância especialmente a partir do início da internet, durante a Guerra Fria, quando diversos países passaram a criar bancos de dados unificados controlados por autorizações, por receio de que as informações pudessem ser usadas de forma opressiva contra a liberdade e privacidade dos cidadãos.

Embora os avanços legislativos e a preocupação com a proteção de dados pessoais não sejam algo recente, ainda enfrentamos obstáculos significativos, como a insuficiência de estruturas eficazes

de fiscalização para combater vazamentos de informações. Isso é especialmente preocupante no contexto das plataformas de acesso digital, como Google, Telegram, e as inteligências artificiais (IA), onde a vulnerabilidade a vazamentos e uso indevido de dados ainda representa um desafio expressivo (ARAUJO, 2023).

3.2. O TELEGRAM COMO MEIO DE VAZAMENTO DE DADOS PESSOAIS

Uma reportagem divulgada no portal Metrópolis (VASCONCELOS, 2022) expõe que "dados pessoais de brasileiros são divulgados em grupos do telegram". A matéria destaca que nos grupos do Telegram os usuários têm acesso a informações sensíveis, como nome completo, data de nascimento, CPF/CNPJ, endereço, e-mail, dados da Receita Federal, além de informações sobre veículos, como placa, chassi e Renavam, mediante o uso de *bots* automatizados, que é um comando específico para realizar a buscar dos dados solicitados pelo usuário. Essa prática, além de ilegal, amplia significativamente os riscos de crimes como fraudes, roubo de identidade e desequilíbrios na segurança pessoal dos indivíduos afetados. A circulação livre dessas informações reveladas de forma clandestina demonstra a fragilidade na fiscalização e a urgência de medidas mais rigorosas para coibir esse tipo de vazamento e proteger os dados dos cidadãos.

A plataforma tem sido utilizada para práticas ilegais, como vazamentos de dados, devido à sua ampla funcionalidade de comunicação entre os usuários e ao fato de possuir um modelo operacional que dificulta a fiscalização e responsabilização (OLIVEIRA E MARQUES, 2024, p. 16).

Segundo decisão do Supremo Tribunal Federal (STF, 2023), no âmbito do Inquérito nº 4933, instaurado para apurar a conduta de diretores do Google e do Telegram no Brasil, especialmente quanto à possível articulação de uma campanha contra o Projeto de Lei nº 2.630/2020, conhecido como "PL das Fake News", apurou-se, por meio

da investigação conduzida pela Polícia Federal, que até o ano de 2023 o Telegram não possuía representante oficial no país. Oliveira e Marques (2024) destacam que o Telegram enfrentou bloqueios judiciais em 2023 devido à ausência de colaboração com as investigações judiciais relacionadas à empresa.

Vazquez (2024) destaca que os riscos cibernéticos, referem-se às ameaças e ataques que vêm se tornando cada vez mais frequentes no ambiente digital, com uma evolução exponencial ao longo dos anos. Esses riscos resultam em prejuízos que podem alcançar bilhões de reais. Tanto empresas como pessoas físicas são vulneráveis aos riscos cibernéticos, principalmente ao adotarem práticas inseguras, como o uso de senhas fracas ou a ausência de autenticação de dois fatores. Para Silva (2025) as ameaças que atingem sistemas físicos conectados às tecnologias digitais, como infraestruturas e dispositivos, também têm aumentado, o que impõe novos desafios na área da segurança cibernética e na proteção de dados pessoais, especialmente no que diz respeito às aplicações e adequações do Direito brasileiro diante dessas novas realidades.

O Brasil ainda enfrenta dificuldades na construção de uma estrutura robusta de governança digital. Essa fragilidade institucional impede a implementação de regras eficazes de controle, de responsabilização e de cooperação internacional, essenciais para lidar com a complexidade e o alcance das plataformas digitais globais. (VAZQUES, 2024). Portanto, a falta de uma governança digital forte reforça o desafio de proteger os dados pessoais e a vida privada dos cidadãos, das práticas criminosas de grupos por meio das empresas tecnológicas estrangeiras, como o Telegram (SILVA, 2025).

3.3. CONSEQUÊNCIAS DO VAZAMENTO

O Brasil, assim como outros países, enfrenta um elevado volume de vazamentos de dados por meio das plataformas digitais. Diante dessa realidade, o país foi compelido a estabelecer legislações específicas

que regulamentam as políticas de proteção de dados pessoais, visando garantir maior segurança e privacidade aos usuários (GOMES *et al.*, 2025).

O vazamento de dados pessoais não é algo meramente abstrato ou teórico; ele tem consequências extremamente concretas e graves para os indivíduos afetados. Dados vazados podem ser utilizados para cometer fraudes financeiras, realizar golpes, aplicar chantagens, promover assédio e até discriminação, seja no mercado de trabalho, na busca por moradia ou em outros aspectos sociais, causando danos irreparáveis à vítima (PETRI; GIOLA JUNIOR, 2023).

No contexto brasileiro, diversas medidas podem ser adotadas para prevenir vazamentos de dados e proteger a privacidade dos cidadãos. Primeiramente, a implementação e fiscalização rigorosa da LGPD são essenciais, pois ela estabelece princípios fundamentais para o tratamento de dados pessoais, como necessidade, transparência, segurança e responsabilização. No entanto, embora a LGPD seja um passo importante, sua eficácia depende de uma aplicação concreta, com fiscalização efetiva e penalizações severas para infrações, reforçando que a lei seja aplicada com mais força e agilidade (SAMPAIO, 2021).

Para garantir a proteção eficaz dos dados pessoais e responsabilizar adequadamente terceiros pelo uso indevido, são medidas essenciais: implementação de medidas técnicas robustas, como criptografia ponta a ponta, firewalls avançados, autenticação de múltiplos fatores, controle de acesso rigoroso e auditorias frequentes de processos de armazenamento, transmissão e uso de informações; promoção de campanhas educativas que capacitem os cidadãos a compreenderem melhor seus direitos e os riscos envolvidos no compartilhamento de dados; e elaboração de normativas complementares à LGPD, especialmente no âmbito do uso de inteligência artificial e Big Data, de modo a garantir que os avanços tecnológicos não comprometam os direitos fundamentais dos indivíduos (ARAUJO, 2023).

CONCLUSÃO

Diante da análise realizada, conclui-se que o vazamento massivo de dados pessoais no Brasil, especialmente por meio de plataformas como o Telegram, evidencia a fragilidade estrutural da proteção de dados no país. Embora a Constituição Federal de 1988 e a LGPD reconheçam e assegurem o direito à privacidade e à autodeterminação informativa, a prática revela um descompasso entre a norma e sua efetiva aplicação. A atuação limitada das plataformas digitais frente às determinações judiciais, aliada à ausência de um sistema de governança digital eficaz, aprofunda a vulnerabilidade dos cidadãos diante de riscos cibernéticos cada vez mais sofisticados. O caso do Telegram mostra como a arquitetura dessas plataformas, aliada à insuficiência de mecanismos regulatórios e de responsabilização, potencializa a violação de direitos fundamentais. Para enfrentar essa realidade, torna-se indispensável o fortalecimento institucional dos órgãos reguladores, a promoção de medidas de educação digital, a adoção de tecnologias de segurança da informação e a elaboração de normativas específicas para os novos desafios da era da inteligência artificial e do Big Data. Apenas com um esforço coordenado entre poder público, sociedade civil e setor privado será possível assegurar a proteção efetiva dos dados pessoais no Brasil e garantir que os direitos fundamentais não sejam continuamente violados em nome da conectividade.

REFERÊNCIAS

ARAUJO, Leandro Barbosa de. Danos morais e materiais por vazamento de dados pessoais em ambiente digital sob a ótica do ordenamento jurídico brasileiro e da jurisprudência. **Revista Jurídica UNIGRAN.** Dourados, MS. v. 25,n. 49, Jan./Jun. 2023. Disponível em: https://l1nq.com/UDFLb. Acesso em: 29 mai. 2025.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 29 mai. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 29 mai. 2025

BRASIL. Supremo Tribunal Federal. **Inquérito 4.933 Distrito Federal**. Decisão. 2023. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/INQ493321despacho.pdf. Acesso em: 29 mai. 2025.

CARVALHO, Solange. Os Impactos Da Banalização Da Informação Nas Redes Sociais. **Revista (Com) Textos Linguísticos**. v.7, n.8.1. Edição Especial. 2013. Disponível em: https://periodicos.ufes.br/contextoslinguisticos/article/view/6020. Acesso em: 29 mai. 2025.

GOMES, Patrícia Guedes Gomide Nascimento, et al. Vulnerabilidades: Panorama Das Legislações De Proteção De Dados Pessoais Gdpr, Ccpa, Lgpd E Pipl. **Revista Direito UNIFACS**. n.297, p.1-24. 2025. Disponível em: file:///C:/Users/Usu%C3%A1rio/Downloads/9520-37879-1-PB.pdf. Acesso em: 30 mai. 2025.

LEME, Carolina da Silva. Proteção e tratamento de dados sob o prisma da legislação vigente. **Revista Fronteiras Interdisciplinares do Direito**. v.1, n.1, p.178-197. 2019. Disponível em: https://revistas.pucsp.br/fid/article/view/41960. Acesso em: 29 mai. 2025.

OLIVEIRA, Débora Ferreira de.; MARQUES, Rodrigo Moreno.O ataque das plataformas digitais contra o projeto de lei das fake news: Uma análise sob as lentes do colonialismo digital e do colonialismo de dados. **Revista Tendências da Pesquisa Brasileira e Ciência da Informação**. v. 17, p. 1-26, 2024. Disponível em: https://revistas.ancib.org/index.php/tpbci/article/view/693. Acesso em: 29 mai. 2025.

PETRI, Giovanna Perobon; GIOLA JUNIOR, Cildo. A (In)Efetividade da LGPD ante o consumidor virtual: Uma análise acerca do vazamento de dados pessoais nas vendas de marketplaces. **Revista de Iniciação Científica e Extensão da Faculdade de Direito de Franca.** v.8, n.1, dez. 2023. Disponível em: https://www.revista.direitofranca.br/index.php/icfdf/article/view/1456. Acesso em 29 mai. 2025.

SILVA, Lucas Lima. **Tensões entre as Big techs e o Estado brasileiro: Uma análise sobre o descumprimento de decisões judiciais pelo Telegram e pelo X/Twitter e sobre a interferência no processo legislativo pelo Google**. 2025. Trabalho de Conclusão do Curso (Bacharelado em Direito) - Universidade Federal do Tocantins, Arraias, 2025.

SAMPAIO, José Adércio Leite. Capitalismo de vigilância e a ameaça aos direitos fundamentais da privacidade e da liberdade de expressão. **Revista Jurídica**. Curitiba. vol. 01, n°. 63, p. 89 – 113. 2021.

VASCONCELOS, Thalita. **Dados pessoais de brasileiros são divulgados em grupos do Telegram**. METROPÓLIS. Distrito Federal, 2022. Disponível em: https://www.metropoles.com/distrito-federal/dados-pessoais-de-brasileiros-sao-divulgados-em-grupos-do-telegram. Acesso em: 29 mai. 2025.

VAZQUEZ, Fabio José Buchedid. Política de resposta a incidentes cibernéticos e estratégias de aderência à legislação brasileira. Revista Dataset Reports. v.3, n.1. 2024. Disponível em: https://journals.royaldataset.com/dr/article/view/108. Acesso em 29 mai. 2025.

RECONHECIMENTO FACIAL E TECNOLOGIAS DE VIGILÂNCIA: LIMITES CONSTITUCIONAIS

FACIAL RECOGNITION AND SURVEILLANCE TECHNOLOGIES: CONSTITUTIONAL LIMITS

Marcela Dorneles Sandrini

Advogada. Mestra em Constitucionalismo e Direitos na Amazônia do Programa de Pós- Graduação em Direito (PPGDir) da Universidade Federal do Amazonas – UFAM. Email: marcela.sandrini@hotmail.com.

Maria Fernanda Sousa Rodrigues

Advogada. Graduada em Direito pela Universidade do Estado do Amazonas (UEA). Email: sousamariafernanda3@icloud.com

Palavras-chave: Tecnologias de vigilância. Direitos Fundamentais. Privacidade.

RESUMO

O avanço das tecnologias de reconhecimento facial tem transformado práticas de vigilância pública e privada em diversos contextos, como segurança urbana, controle de acesso e monitoramento em tempo real. Apesar de seus benefícios potenciais, esse uso crescente levanta sérias preocupações constitucionais. Aplicada em espaços públicos, sistemas de segurança e até instituições educacionais, essa tecnologia vem sendo adotada sob a justificativa de promover eficiência e segurança. Este trabalho analisa os limites jurídicos do uso dessa tecnologia à luz da Constituição Federal de 1988, especialmente quanto à proteção da privacidade, igualdade e liberdade. A ausência de uma legislação específica no Brasil e os riscos de discriminação algorítmica, vigilância em massa e violações

de direitos fundamentais são destacados, apontando-se a necessidade de uma regulação robusta e democrática para proteger os cidadãos.

OBJETIVO GERAL

Esse resumo propõe analisar os riscos constitucionais e os impactos sociais do uso de tecnologias de reconhecimento facial, propondo limites jurídicos que garantam a proteção dos direitos fundamentais no Brasil.

OBJETIVOS ESPECÍFICOS

- Investigar os principais usos atuais do reconhecimento facial no Brasil e no mundo.
- Identificar os direitos fundamentais potencialmente violados por essa tecnologia.
- Avaliar a eficácia da LGPD na proteção de dados biométricos no contexto da vigilância estatal.
- Analisar experiências internacionais que estabeleceram restrições ao uso de reconhecimento facial.

METODOLOGIA

A pesquisa é de natureza qualitativa, com abordagem exploratória e analítica. Utiliza-se revisão bibliográfica e documental, com base em legislações nacionais (como a Constituição de 1988 e a LGPD), além de obras acadêmicas que tratam da proteção de dados e da atuação estatal, como Lei Geral de Proteção de Dados: Comentários à Lei nº 13.709/2018 (CAVALCANTI, 2019). O estudo também examina casos concretos de uso da tecnologia no Brasil e no exterior, a fim de comparar modelos regulatórios e práticas institucionais. A análise parte do entendimento de que, embora a tecnologia represente um avanço significativo no campo da segurança pública, sua aplicação irrestrita pode gerar

violações graves, como a discriminação algorítmica e o cerceamento das liberdades individuais.

DESENVOLVIMENTO

Nas últimas décadas, os avanços tecnológicos têm transformado profundamente a forma como o Estado e as empresas interagem com a sociedade, sobretudo no campo da segurança e da vigilância. Nesse contexto, o uso de tecnologias de reconhecimento facial tem se expandido de maneira acelerada, sendo aplicado em aeroportos, espaços públicos, transporte coletivo e até em instituições de ensino. Essa expansão, no entanto, tem gerado intensos debates sobre seus impactos nos direitos fundamentais garantidos constitucionalmente.

Este trabalho busca analisar os principais riscos constitucionais envolvidos na adoção de tecnologias de reconhecimento facial, destacando a importância de se estabelecer limites jurídicos claros que preservem os direitos fundamentais. Parte-se do pressuposto de que tais tecnologias, apesar de apresentarem potenciais benefícios em termos de segurança pública, podem gerar efeitos colaterais graves quando utilizadas de forma indiscriminada ou sem o devido controle legal.

O reconhecimento facial é uma tecnologia biométrica que identifica e verifica a identidade de uma pessoa a partir da análise de suas características faciais. Com o avanço da inteligência artificial, os sistemas passaram a ser capazes de processar grandes volumes de imagens em tempo real, o que permitiu sua aplicação em diversas esferas sociais.

Entre os principais usos estão a identificação de suspeitos em câmeras de segurança, o controle de acesso a edifícios, a organização de eventos com grandes públicos e o monitoramento de fronteiras. No entanto, além da promessa de maior segurança e eficiência, o uso indiscriminado dessas ferramentas levanta questionamentos éticos, políticos e jurídicos.

Em países como os Estados Unidos e a China, essa tecnologia tem sido empregada para vigilância em massa, muitas vezes sem o conhecimento ou o consentimento da população. No Brasil, ainda não há uma legislação específica que regule de forma ampla o uso dessas ferramentas, o que gera um vácuo normativo preocupante.

O uso de tecnologias de vigilância baseadas em reconhecimento facial representa uma ameaça direta a diversos direitos fundamentais garantidos pela Constituição Federal de 1988. Um dos principais riscos é a violação do direito à privacidade (art. 5º, inciso X), uma vez que a coleta e o tratamento de dados biométricos frequentemente ocorrem sem o consentimento dos indivíduos.

Outro ponto crítico refere-se à possibilidade de discriminação algorítmica. Estudos mostram que sistemas de reconhecimento facial apresentam taxas de erro significativamente maiores para pessoas negras, indígenas e asiáticas, além de mulheres, do que para homens brancos. Isso reforça desigualdades históricas e pode contribuir para abordagens policiais abusivas e injustiças no sistema penal.

Além disso, o uso dessa tecnologia pode comprometer a liberdade de expressão e de reunião (art. 5º, incisos IV e XVI), pois indivíduos monitorados constantemente podem se sentir inibidos em exercer seus direitos civis e políticos. A sensação de vigilância constante configura um ambiente de autocensura e opressão, especialmente em contextos de protesto ou manifestação política.

A Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709/2018 – estabelece princípios e obrigações para o tratamento de dados sensíveis, como os biométricos. Contudo, a ausência de uma legislação específica voltada para o uso estatal dessas tecnologias de vigilância torna a proteção insuficiente, já que não há critérios claros para o uso de tais dados por órgãos públicos de segurança.

A ausência de um marco legal robusto no Brasil permite que essas tecnologias sejam adotadas de maneira opaca e desproporcional, sem mecanismos eficazes de controle, fiscalização e responsabilização. Embora a LGPD represente um avanço importante, ela ainda é

insuficiente para lidar com os desafios específicos da vigilância biométrica em larga escala.

Países como a Bélgica e cidades como São Francisco, nos Estados Unidos, optaram por banir temporariamente o uso do reconhecimento facial por autoridades públicas, justamente devido à ausência de garantias constitucionais mínimas. No Brasil, experiências como a do Carnaval de Salvador, onde essa tecnologia foi utilizada para identificar foragidos da Justiça, mostraram a eficácia do sistema, mas também levantaram dúvidas sobre a proteção de dados e os critérios de seleção dos alvos.

O desafio, portanto, é criar uma legislação que concilie os potenciais benefícios da tecnologia com a efetiva proteção dos direitos fundamentais. É necessário que essa regulação estabeleça princípios como: o uso restrito e proporcional da tecnologia, a obrigatoriedade de consentimento, a transparência dos algoritmos, o direito à explicação das decisões automatizadas e a responsabilização em caso de erro ou abuso.

CONCLUSÃO

O reconhecimento facial, embora possa representar uma ferramenta útil em determinadas circunstâncias, carrega consigo riscos relevantes aos direitos e garantias fundamentais consagrados pela Constituição de 1988. A falta de regulamentação específica e a opacidade dos sistemas utilizados expõem a sociedade a práticas de vigilância potencialmente abusivas, que comprometem a privacidade, a igualdade e a liberdade dos cidadãos.

Dessa forma, é urgente que o debate sobre o uso dessas tecnologias seja pautado por critérios constitucionais e democráticos, com ampla participação da sociedade civil, do Judiciário, da academia e dos órgãos reguladores. Somente assim será possível garantir que os avanços tecnológicos não sejam utilizados como instrumentos de

opressão, mas como ferramentas a serviço da dignidade humana e da justiça social.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 22 mai. 2025.

BORELLI, Alessandra et al. **Direito digital: debates contemporâneos**. São Paulo: Revista dos Tribunais, 2019. 299 p. Disponível em: <http://biblioteca2.senado.gov.br:8991/F/func=direct&doc_number=001160830&local_base=SEN01>. Acesso em 19 mai. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Senado Federal, 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 22 mai. 2025.

CAVALCANTI, Danilo Doneda; PINHEIRO, Renato Opice Blum. **Lei Geral de Proteção de Dados: Comentários à Lei nº 13.709/2018**. São Paulo: Thomson Reuters, 2019.

COTS, Márcio. **Lei geral de proteção de dados pessoais: comentada**. São Paulo: Revista dos Tribunais, 2018. 303 p. Disponível em: <http://biblioteca2.senado.gov.br:8991/F/func=direct&doc_number=001134775&local_base=SEN>. Acesso em 22 mai. 2025.

CRAVO, Daniela Copetti. **Direito à portabilidade na Lei geral de proteção de dados.** Indaiatuba, SP: Foco, 2020. x, 109 p. Disponível em: <http://biblioteca2.senado.gov.br:8991/F/func=direct&doc_number=001179382&local_base=SEN01>. Acesso em 20 mai. 2025.

DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes. **LGPD & administração pública: uma análise ampla dos impactos**. São Paulo: Revista dos Tribunais, 2020. 991 p. Disponível em: <https://proview.

thomsonreuters.com/launchapp/title/rt/monografias/246338257 /v1>. Acesso em 18 mai. 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei geral de proteção de dados.** 3. ed. São Paulo: Revista dos Tribunais, 2021. 368 p. Disponível em: <https://proview.thomsonreuters.com/launchapp/title/rt/monografias/215543393/v3>. Acesso em 18 mai. 2025.

FRAZÃO, Ana et al. (coord.). **Inteligência artificial e direito: ética, regulação e responsabilidade.** São Paulo: Revista dos Tribunais, 2019. 716 p. Disponível em: <http://biblioteca2.senado.gov.br:8991/F/?func=direct&doc_number=001155559&local_base=SEN01>. Acesso em 18 mai. 2025.

JUNQUEIRA, Thiago. **Tratamento de dados pessoais e discriminação algorítmica nos seguros.** 1. ed. São Paulo: Revista dos Tribunais, 2020. E book. Disponível em: <https://proview.thomsonreuters.com/launchapp/title/rt/monografias/243330264 /v1/page/1>. Acesso em 17 mai. 2025.

RAMOS, Rafael. **Lei Geral de Proteção de dados e o Poder Público.** Porto Alegre: Centro de Estudos em Direito Municipal. 2021. Disponível em: <https://lproweb.procempa.com.br/pmpa/prefpoa/pgm/usu_doc/ebook_lgpd_e_poder_publico_23052021.pdf>. Acesso em 19 mai. 2025.

O DIREITO FUNDAMENTAL À PRIVACIDADE MENTAL NO AMBIENTE DE TRABALHO E OS DESAFIOS DAS TECNOLOGIAS INTRUSIVAS

Myracelle dos Santos da Silva

Aluna especial do Programa de Pós-Graduação em Direito Ambiental da Universidade do Estado do Amazonas (PPGDA/UEA). Pós-graduanda em Direito Eleitoral e em Gestão Pública pela Universidade do Estado do Amazonas – UEA. Especialista em Cuidados de Usuários de Álcool e Outras Drogas pelo Centro Educacional Novas Abordagens em Saúde Mental. Especialista em Direito Civil e Processual Civil pelo Instituto de Especialização do Amazonas – ESP. Graduada em Direito pela Universidade Paulista – UNIP.

Alcian Pereira de Souza

Professor Adjunto da Escola de Direito da Universidade do Estado do Amazonas. Doutor em Ciências pela FEA/USP, Mestre em Direito pela UEA. Pesquisador Líder do Grupo de Pesquisa CNPQ "Direito, Tecnologia e Inovação". Coordenador Geral do Núcleo de Direito, Tecnologia & Inovação- LAWin/UEA

PALAVRAS-CHAVE: Privacidade mental; Neurodireitos; Inteligência artificial; Direitos fundamentais; Ambiente de trabalho.

OBJETIVOS

Analisar o direito fundamental à privacidade mental no ambiente de trabalho diante dos desafios impostos pelas tecnologias cognitivas intrusivas — como neurotecnologias, softwares de vigilância emocional e sistemas de gestão algorítmica — à luz da evolução normativa nacional e internacional. O estudo visa destacar os riscos da coleta de dados neuroinformacionais e do assédio algorítmico, propondo o reconhecimento dos neurodireitos como garantia fundamental do

trabalhador. A partir da análise da Constituição Federal, da Lei Geral de Proteção de Dados (LGPD), da PEC nº 29/2023 e da Lei nº 14.831/2024, objetiva-se demonstrar a urgência de uma regulamentação específica que assegure a compatibilidade entre inovação tecnológica, saúde psíquica e dignidade da pessoa humana no ambiente laboral.

METODOLOGIA

A pesquisa adota abordagem quali-quantitativa, de natureza exploratória e bibliográfica, com análise de dispositivos normativos nacionais e internacionais, estudos acadêmicos e documentos institucionais. São examinadas legislações comparadas de países como Chile, França, Estados Unidos e da União Europeia, que tratam da proteção da privacidade mental e da regulação das neurotecnologias. O referencial teórico é fundamentado nos neurodireitos, propostos como Marcello Ienca, Roberto Andorno e Rafael Yuste, que defendem a proteção da identidade psíquica e da liberdade cognitiva frente aos avanços tecnológicos no ambiente de trabalho.

DESENVOLVIMENTO DA PESQUISA

A privacidade é um direito consagrado no art. 5º, inciso X, da Constituição Federal de 1988, sendo um desdobramento da dignidade da pessoa humana (art. 1º, III). Contudo, a evolução tecnológica tem desafiado esse princípio fundamental, exigindo um novo olhar sobre a proteção da esfera íntima e psíquica dos indivíduos. Em 2021, o Chile tornou-se o primeiro país a consagrar os neurodireitos em sua Constituição. A Lei nº 21.383 modificou a Carta Fundamental para estabelecer que o desenvolvimento científico e tecnológico deve estar a serviço das pessoas, protegendo a integridade física e psíquica dos indivíduos. Essa reforma visa garantir a privacidade mental e a identidade pessoal frente ao avanço das neurotecnologias (Biblioteca do Congresso do Chile, 2021). A França, desde 2017, implementou o

direito à desconexão por meio da Lei nº 2016-1088, conhecida como "Loi Travail". Essa legislação obriga empresas com mais de 50 funcionários a estabelecerem horários nos quais os trabalhadores não devem ser contatados por meios digitais, visando preservar o equilíbrio entre vida profissional e pessoal e proteger a saúde mental dos empregados (Cielolaboral, 2020). A União Europeia aprovou o AI Act, a primeira legislação abrangente sobre inteligência artificial. O regulamento classifica os sistemas de IA conforme o risco que apresentam e proíbe práticas como o uso de IA para manipular emoções de trabalhadores ou para vigilância biométrica sem consentimento. O objetivo é garantir que o desenvolvimento e uso da IA respeitem os direitos fundamentais e a dignidade humana (Parlamento Europeu, 2023).

Diferentemente de países como Chile ou França, os Estados Unidos não possuem uma legislação federal unificada que reconheça os neurodireitos ou o direito à desconexão. A proteção da privacidade mental no país é fragmentada e frequentemente limitada a iniciativas estaduais ou setoriais.. Nos EUA, empresas líderes em tecnologia vêm desenvolvendo ferramentas capazes de mapear padrões neurológicos com fins de produtividade, como é o caso de softwares que analisam a atenção, o engajamento e o humor de funcionários durante o expediente. Essa prática levanta sérias preocupações éticas sobre consentimento e autonomia, sendo criticada por autores como Farah (2021), que advertem para os riscos de exploração cognitiva e manipulação comportamental sem a devida regulação. No campo legislativo, há propostas de leis como o "Neuro-Rights Initiative" liderado por pesquisadores da Universidade de Columbia, que visa influenciar políticas públicas a reconhecerem a liberdade cognitiva, a integridade mental e a autodeterminação como direitos humanos fundamentais (Yuste et al., 2017). As chamadas tecnologias cognitivas intrusivas têm ganhado espaço nas organizações com a promessa de elevar os níveis de produtividade, eficiência e segurança. No entanto, essas ferramentas também têm sido utilizadas como instrumentos de vigilância que, quando mal regulamentados, podem promover assédio algorítmico, discriminação, pressão psicológica e invasão da

intimidade mental do trabalhador. Nesse contexto, três conceitos inter-relacionados emergem com destaque: as neurotecnologias, os dados neuroinformacionais e o assédio algorítmico. As neurotecnologias referem-se a dispositivos e sistemas capazes de captar, interpretar ou manipular a atividade cerebral, como capacetes com sensores EEG (eletroencefalograma) ou softwares que medem níveis de atenção e estresse. Tais tecnologias vêm sendo testadas em ambientes corporativos para fins de gestão de desempenho e seleção de pessoal, suscitando preocupações quanto à violação da privacidade mental e da autonomia psíquica (Yuste et al., 2017).

Essas tecnologias coletam dados neuroinformacionais, ou seja, dados derivados da atividade cerebral que revelam pensamentos, emoções, intenções e estados mentais (Ienca & Andorno, 2017). Assim, os dados, em sua profundidade e sensibilidade, representam um novo patamar de risco à integridade subjetiva, uma vez que são extraídos de forma não verbal e muitas vezes involuntária. Quando tais ferramentas são combinadas a sistemas automatizados de controle, emerge o fenômeno do assédio algorítmico: uma forma de assédio moral caracterizada pela atuação opressiva de algoritmos que cobram metas inalcançáveis, envia alertas constantes de desempenho, punem o trabalhador por pausas ou falhas e promovem um ambiente de constante vigilância e autocensura. Como destacam De Stefano e Wouters (2020), o controle algorítmico intensifica a precarização e compromete a saúde mental ao substituir o julgamento humano por decisões automáticas desprovidas de empatia. Essas tecnologias oferecem às empresas a possibilidade de automatizar decisões e acelerar processos internos, resultando em ganhos econômicos e aumento da produtividade. Contudo, o uso excessivo e generalizado de mecanismos de vigilância no ambiente corporativo, tais como câmeras com captação de áudio, rastreamento de pegadas digitais na internet, controle por meio de crachás eletrônicos, leitura de e-mails corporativos e até a fiscalização de aplicativos internos de mensagens, levanta sérias preocupações quanto aos limites éticos e jurídicos dessa prática. Quando utilizadas de forma abusiva, tais práticas podem

configurar violação grave ao direito fundamental à privacidade, gerando repercussões emocionais relevantes, instaurando um estado permanente de vigilância e contribuindo diretamente para o adoecimento psíquico dos trabalhadores.

Diante desse contexto, é fundamental destacar a figura do empregado como parte hipossuficiente na relação de trabalho, cuja vulnerabilidade se manifesta em múltiplas dimensões: econômica, técnica e jurídica. Enquanto o empregador detém os meios de produção, maior poder econômico e suporte jurídico qualificado, o trabalhador depende do vínculo empregatício para sua subsistência e, muitas vezes, não possui recursos ou conhecimento técnico suficientes para contestar imposições empresariais. Essa assimetria justifica a prerrogativa prevista no art. 2º da Consolidação das Leis do Trabalho (CLT), que confere ao empregador o chamado poder diretivo, desdobrado em: a) poder de organização; b) poder de controle; e c) poder disciplinar. Ainda que legítimo, o exercício desse poder encontra limites nos princípios constitucionais da dignidade da pessoa humana, boa-fé objetiva e respeito aos direitos fundamentais, devendo ser exercido com proporcionalidade e razoabilidade, a fim de evitar abusos. A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) representa um importante marco normativo ao regulamentar o tratamento de dados sensíveis, exigindo consentimento, finalidade legítima e medidas de segurança. No entanto, a LGPD ainda não aborda de forma específica os chamados dados neuroinformacionais, o que evidencia a urgência de avanços legislativos e da ampliação da doutrina sobre o tema. Paralelamente, a Declaração Universal sobre Bioética e Direitos Humanos da UNESCO (2005) reconhece a integridade mental como dimensão essencial da autonomia e da dignidade humana.

É nesse contexto que emergem os neurodireitos, como a liberdade cognitiva, a proteção da identidade psíquica e a não manipulação de pensamentos, que precisam ser reconhecidos no ordenamento jurídico brasileiro. Países como o Chile já aprovaram emendas constitucionais que incorporam tais garantias. No Brasil, tramita a PEC nº 29/2023, que propõe o reconhecimento da proteção

mental como direito fundamental explícito. Além disso, a recente sanção da Lei nº 14.831/2024, conhecida como Lei da Saúde Mental no Trabalho, estabelece diretrizes para a promoção, prevenção e cuidado com a saúde mental dos trabalhadores, reforçando a necessidade de uma abordagem preventiva e integrada da saúde psíquica no contexto laboral. A preocupação com a saúde mental também tem sido alvo de atenção por parte de organismos nacionais e internacionais. A Organização Mundial da Saúde (OMS) tem registrado um crescimento significativo nos índices globais de transtornos mentais relacionados ao trabalho. No Brasil, dados do Instituto Nacional do Seguro Social (INSS) revelam que os transtornos mentais e comportamentais já figuram entre as principais causas de afastamento do trabalho e concessão de aposentadoria por invalidez. Apenas entre 2018 e 2023, o número de afastamentos por essas causas passou de 119.400 para 230.100 casos — um aumento de 92,7%. Esse dado evidencia o impacto direto das condições psíquicas na capacidade laboral e no sistema previdenciário. Diante disso, é imperativo estabelecer limites éticos e jurídicos para o uso de tecnologias intrusivas no ambiente de trabalho, assegurando que a busca por eficiência empresarial não se sobreponha ao respeito aos direitos fundamentais, à dignidade e à saúde mental dos trabalhadores.

CONCLUSÕES

A privacidade mental pode ser considerada uma extensão dos direitos da personalidade, protegida implicitamente pela dignidade da pessoa humana. Autores como Luigi Ferrajoli defendem que os direitos fundamentais devem evoluir para incluir novas dimensões da liberdade individual, como a liberdade cognitiva. Norberto Bobbio destaca que os direitos humanos são históricos e se expandem conforme as transformações sociais e tecnológicas. Ingo Sarlet, por sua vez, argumenta que a proteção da integridade psíquica é essencial para a efetivação da dignidade humana no contexto contemporâneo.

O Projeto de Lei nº 2.338/2023, conhecido como Marco Legal da Inteligência Artificial, está em tramitação no Congresso Nacional. O PL estabelece princípios para o desenvolvimento e uso responsável da IA, como a centralidade da pessoa humana e o respeito aos direitos fundamentais. No entanto, especialistas apontam que o projeto ainda carece de disposições específicas sobre a proteção da privacidade mental e os neurodireitos, indicando a necessidade de aprimoramento legislativo. Relatório da Organização Internacional do Trabalho (OIT) de 2023 analisa o impacto da gestão algorítmica no ambiente de trabalho. O estudo revela que o uso de sistemas automatizados para monitorar e avaliar o desempenho dos funcionários pode levar à intensificação do trabalho, perda de autonomia e aumento do estresse, afetando negativamente a saúde mental dos trabalhadores (ILO, 2023). A emergência das tecnologias cognitivas intrusivas no ambiente de trabalho impõe um novo desafio ao Direito: assegurar a proteção da privacidade mental dos trabalhadores frente à atuação cada vez mais invasiva de empregadores. É necessário reconhecer a privacidade mental como um direito fundamental implícito, cuja salvaguarda é essencial para a preservação da dignidade, da autonomia e da saúde psíquica do indivíduo. A regulamentação do uso dessas tecnologias deve estar ancorada em princípios constitucionais, na LGPD e em tratados internacionais de direitos humanos, promovendo um equilíbrio entre inovação tecnológica e proteção de direitos.

REFERÊNCIAS

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988.

BRASIL. Consolidação das Leis do Trabalho. Decreto-Lei nº 5.452, de 1º de maio de 1943.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais – LGPD.

BRASIL. Lei nº 14.831, de 27 de março de 2024. Estabelece diretrizes para a saúde mental no trabalho.

PEREIRA, Rodrigo Carelli. Direito à desconexão e novas tecnologias de controle. São Paulo: DLTR, 2022.

BRASIL, Marina. Neuro direitos e privacidade mental: uma nova fronteira dos direitos humanos. Revista Brasileira de Bioética, v. 19, n. 1, p. 123–138, 2023.

DALLARI, Dalmo de Abreu. O direito à intimidade no Estado Democrático de Direito. Revista dos Tribunais, v. 89, n. 792, p. 45–52, 2010.

NOMADISMO DIGITAL: DESAFIOS DA SAÚDE MENTAL E ESTRATÉGIAS DE PROTEÇÃO NO TRABALHO REMOTO

Andrezza Letícia Oliveira Tundis Ramos

Mestranda no Programa de Pós-Graduação Stricto Sensu em Direito Ambiental (PPGDA) pela Universidade do Estado do Amazonas. Analista Judiciário do Tribunal Regional do Trabalho da 11ª Região. E-mail: andrezzatundis@hotmail.com. Lattes: http://lattes.cnpq.br/3113091738233741. Orcid: https://orcid.org/0009-0003-0680-0578.

Luana Caroline Nascimento Damasceno

Mestranda no Programa de Pós-Graduação Stricto Sensu em Direito Ambiental (PPGDA) pela Universidade do Estado do Amazonas. Pesquisadora do Grupo de Pesquisa - OSPPA (Observatório Social de Políticas Públicas na Amazônia) - UEA/AM. Advogada. E-mail: lcndamasceno@gmail.com. Lattes: http://lattes.cnpq.br/1392385777508283. Orcid: 0009-0006-9994-538X.

Priscila Farias dos Reis Alencar

Mestranda no Programa de Pós-graduação Stricto Sensu em Direito Ambiental na Universidade do Estado do Amazonas (PPGDA). Agente Técnico-Jurídico do Ministério Público do Estado do Amazonas. E-mail: pri.freis@gmail.com. Lattes: https://lattes.cnpq.br/8820755769778357. Orcid: 0009-0008-7422-3342.

PALAVRAS-CHAVE: Nomadismo Digital; Saúde Mental; Sobretrabalho; Flexibilidade no Trabalho; Direito à Desconexão.

OBJETIVO GERAL

O objetivo geral desta pesquisa é analisar como a cultura do trabalho digital influencia a saúde mental dos nômades digitais e

quais estratégias podem ser implementadas para mitigar os riscos associados ao sobretrabalho.

OBJETIVOS ESPECÍFICOS

Os objetivos específicos incluem:

1. Investigar as características que favorecem o sobretrabalho entre nômades digitais.
2. Identificar os principais riscos psicossociais relacionados a essa prática.
3. Analisar diretrizes e regulamentações adequadas para proteger esses profissionais.

METODOLOGIA

A pesquisa adota uma abordagem dedutiva, iniciando com uma análise conceitual e teórica do nomadismo digital e suas implicações. A metodologia será qualitativa, utilizando revisão bibliográfica de artigos científicos e livros relevantes, além da análise documental das legislações nacional e internacional pertinentes ao tema.

1. CARACTERÍSTICAS DA CULTURA DO TRABALHO DIGITAL

A flexibilidade e a autonomia no trabalho digital são frequentemente vistas como os principais benefícios para os nômades digitais, permitindo que trabalhem de qualquer lugar e gerenciem seus horários. No entanto, essas vantagens também podem levar a uma tendência ao excesso de trabalho, uma vez que os limites entre trabalho e lazer podem se tornar confusos. A conectividade constante e a pressão para estar sempre disponível exacerbam esses problemas, resultando em estresse, ansiedade e solidão.

Os nômades digitais desfrutam de altos níveis de flexibilidade e autonomia, facilitados por tecnologias digitais. Essa flexibilidade

permite que escolham suas horas de trabalho e locais, teoricamente promovendo um melhor equilíbrio entre vida pessoal e profissional (Wood et al., 2019; Popma, 2013). Contudo, a falta de limites claros entre trabalho e lazer frequentemente leva à sobrecarga de trabalho, pois esses profissionais lutam para separar suas vidas profissionais e pessoais (Cook, 2020).

2. RISCOS PSICOSSOCIAIS ASSOCIADOS AO SOBRETRABALHO

O excesso de trabalho entre nômades digitais apresenta riscos significativos à saúde mental, como estresse tecnológico e dependência de plataformas digitais. A solidão gerada pelo trabalho remoto intensifica esses riscos, tornando essencial a implementação de estratégias que promovam o equilíbrio entre vida pessoal e profissional. A pressão constante para estar conectado e produtivo pode levar a uma diminuição na satisfação com a vida e ao aumento de problemas como ansiedade e depressão (Glavin & Schieman, 2021; Salvagioni et al., 2017).

3. DIRETRIZES E REGULAMENTAÇÕES

A promoção do direito à desconexão é uma medida crucial para proteger os nômades digitais. Países como França e Itália já implementaram leis que permitem que os trabalhadores se desconectem fora do horário de trabalho. A Organização Internacional do Trabalho (OIT) pode desempenhar um papel importante na criação de diretrizes que abordem os riscos psicossociais do trabalho remoto, garantindo acesso a recursos de saúde mental (Pons, 2021).

Além disso, a Convenção 190 da OIT reconhece o assédio moral digital como uma forma de violência e assédio no trabalho, estendendo a definição de violência e assédio ao âmbito das comunicações relacionadas ao trabalho (OIT, 2019). A adaptação dos regulamentos de saúde e segurança ocupacional é essencial para enfrentar os desafios

do trabalho remoto, considerando questões ergonômicas e a falta de um local de trabalho definido (Popma, 2013; Nilsen et al., 2022).

CONCLUSÕES

A pesquisa evidencia a inter-relação entre a cultura do trabalho digital e a saúde mental dos nômades digitais. A normalização do sobretrabalho e a falta de limites claros entre trabalho e vida pessoal são fatores que contribuem para o aumento de riscos à saúde mental. A implementação de práticas que promovam a separação entre trabalho e vida pessoal é fundamental para garantir o bem-estar desses profissionais. A promoção do direito à desconexão e a adoção de normativas que considerem as particularidades do trabalho remoto são essenciais para garantir um ambiente laboral saudável.

REFERÊNCIAS

BARZOTTO, Luciane Cardoso; ALLES, Matheus Soletti. As relações de trabalho e o nomadismo digital: uma nova cultura de controle laboral e o sobretrabalho. **Revista Tribunal Regional do Trabalho da 3ª Região**, Belo Horizonte, v. 68, n. 106, p. 27-44, jul./dez. 2022. Disponível em: https://as1.trt3.jus.br/bd-trt3/bitstream/handle/11103/87394/revista-106-27-44.pdf?sequence=. Acesso em: 28 abr. 2025.

BRAGA, Simony. O futuro do trabalho e o protagonismo dos nômades digitais: aspectos jurídicos sob a ótica do Direito do Trabalho. **Migalhas**. Disponível em: https://www.migalhas.com.br/depeso/337867/futuro-do-trabalho-e-o-protagonismo-dos-nomades-digitais--aspectos-juridicos-sob-a-otica-do-direito-do-trabalho. Acesso em: 30 abr. 2025.

OIT. ORGANIZAÇÃO INTERNACIONAL DO TRABALHO. C190 - Convenio sobre la violencia y el acoso, 2019 (núm. 190). Disponível em: https://normlex.ilo.org/dyn/nrmlx_es/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C190. Acesso em: 30 abr. 2025.

POPMA, Jan. The Janus face of “New Ways of Work”: rise, risks and regulation of nomadic work. **Social Science Research Network**, 2013. Disponível em: https://pure.uva.nl/ws/files/2318140/136113_Janus_Face_of_New_Ways_of_Work.pdf . Acesso em: 30 abr. 2025.

SALVAGIONI, Denise Albieri Jodas; MELANDA, Francine Nesello; MESAS, Arthur Eumann; et al. Physical, psychological and occupational consequences of job burnout: A systematic review of prospective studies. **PLOS ONE**, v. 12, n. 10, p. 1–29, 2017. Disponível em: https://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0185781&type=printable . Acesso em: 29 abr. 2025.

A INTELIGÊNCIA ARTIFICIAL COMO INSTRUMENTO DE FORTALECIMENTO DO *COMPLIANCE* AMBIENTAL

Vitor Luiz Maia da Silva Xavier

Mestrando em Direito Ambiental do Programa de Pós-Graduação em Direito Ambiental da Universidade do Estado do Amazonas – PPGDA/UEA. vitor.luiz2107@gmail.com;

Priscila Farias dos Reis Alencar

Mestranda no Programa de Pós-graduação Stricto Sensu em Direito Ambiental na Universidade do Estado do Amazonas (PPGDA). Agente Técnico-Jurídico do Ministério Público do Estado do Amazonas. E-mail: pri.freis@gmail.com. Lattes: https://lattes.cnpq.br/8820755769778357. Orcid: 0009-0008-7422-3342.

PALAVRAS-CHAVE: *Compliance* Ambiental; Inteligência Artificial; Sustentabilidade; Governança Ambiental; Conformidade Legal.

OBJETIVOS

O presente resumo tem como objetivo analisar o uso da inteligência artificial (IA) como instrumento de fortalecimento do *compliance* ambiental no Brasil. Busca-se, de forma específica, compreender os fundamentos do *compliance* e do compliance ambiental; identificar os marcos normativos nacionais relevantes; e demonstrar como as tecnologias baseadas em IA podem ser integradas às estratégias de prevenção e controle de danos ambientais, promovendo uma governança mais eficaz e sustentável.

METODOLOGIA:

A pesquisa adota uma abordagem qualitativa, de natureza exploratória e explicativa, com base em levantamento bibliográfico e documental. Foram analisadas obras doutrinárias, artigos científicos, legislações e documentos normativos. Complementarmente, foram examinados estudos recentes sobre a aplicação da inteligência artificial em processos de monitoramento ambiental e gestão de riscos, com o intuito de estabelecer uma correlação entre tecnologia e conformidade ambiental.

DESENVOLVIMENTO DA PESQUISA:

1. CONCEITO DE *COMPLIANCE*

O termo *compliance* deriva do verbo inglês *to comply*, que significa "agir em conformidade com uma norma, diretriz ou comando". Segundo Mendes (2017, p. 23), trata-se da adoção de mecanismos e instrumentos que assegurem o cumprimento eficaz das normas aplicáveis. Originado no setor corporativo dos Estados Unidos, o instituto ganhou força a partir de eventos marcantes, como a crise de 1929 e a necessidade de regulamentações mais rígidas no sistema financeiro, consolidando-se como ferramenta de gestão de riscos (Bragato, 2017).

Embora inicialmente vinculado à iniciativa privada, o compliance passou a ser adotado também na esfera pública. Oliveira, Costa e Silva (2018, p. 7) destacam que, diante da complexidade da sociedade pós-industrial, a governança pública também se beneficia desse conjunto de práticas, o que amplia sua aplicabilidade às funções legislativa, administrativa, jurisdicional e de fiscalização do Estado.

No Brasil, a disseminação do *compliance* se intensificou a partir da década de 1990, mas foi com a promulgação da Lei nº 12.846/2013 (Lei Anticorrupção) que o instituto ganhou reconhecimento jurídico explícito. O art. 7º, inciso VIII, da referida norma prevê a adoção

de mecanismos internos de integridade, auditoria, incentivo à denúncia de irregularidades e aplicação de códigos de conduta como atenuantes na responsabilização de pessoas jurídicas por atos lesivos à administração pública.

Importa mencionar que, por se tratar de vocábulo estrangeiro, autores como Melo (2023) defendem a utilização do termo "política de integridade" como equivalente mais apropriado no contexto jurídico nacional. Ainda assim, o uso de compliance permanece amplamente aceito, sobretudo na doutrina e nos documentos institucionais.

Portanto, o *compliance*, enquanto programa de integridade, configura-se como um instrumento essencial para prevenir práticas ilícitas e promover a cultura de conformidade. Segundo Oliveira, Costa e Silva (2018), trata-se de uma estratégia relevante tanto para a governança pública quanto para a privada, ao contribuir para a promoção de uma gestão ética e transparente.

2. COMPLIANCE AMBIENTAL

A preocupação com a proteção ambiental ganhou contornos institucionais a partir da Conferência de Estocolmo (1972) e foi consolidada com a publicação do Relatório Brundtland (1987), que introduziu o conceito de desenvolvimento sustentável, posteriormente ratificado na ECO-92, no Rio de Janeiro. No ordenamento jurídico brasileiro, a Lei nº 6.938/1981 inaugurou a Política Nacional do Meio Ambiente, reforçada pela Constituição Federal de 1988, que, em seu art. 225, reconhece o direito de todos a um meio ambiente ecologicamente equilibrado e impõe ao Estado e à coletividade o dever de preservá-lo para as presentes e futuras gerações.

Nesse contexto, o *compliance* ambiental emerge como resposta à crescente demanda por mecanismos eficazes de adequação à legislação ambiental. Trata-se da integração de normas, procedimentos e diretrizes que asseguram a conformidade das atividades empresariais e institucionais com os princípios do desenvolvimento sustentável.

O primeiro marco regulatório específico nesse sentido foi a Resolução nº 4.327/2014 do Banco Central, que estabeleceu diretrizes para a Política de Responsabilidade Socioambiental (PRSA) nas instituições financeiras, posteriormente substituída pela Resolução nº 4.945/2021, que ampliou o escopo para incluir também a dimensão climática, consolidando a Política de Responsabilidade Social, Ambiental e Climática (PRSAC).

Além disso, tramita no Congresso Nacional o Projeto de Lei nº 5.442/2019, que visa regulamentar os programas de conformidade ambiental. Em seu art. 2º, define-os como o conjunto de mecanismos internos destinados à auditoria, incentivo à denúncia de irregularidades e aplicação de códigos de conduta, com o objetivo de detectar, prevenir e corrigir práticas lesivas ao meio ambiente.

Ainda que não aprovado, o projeto sinaliza uma tendência normativa importante, estimulando o setor produtivo a adotar voluntariamente práticas de compliance ambiental. Diversas empresas já vêm incorporando essas diretrizes, antecipando obrigações legais futuras e demonstrando compromisso com a sustentabilidade e a prevenção de riscos socioambientais.

3. INTELIGÊNCIA ARTIFICIAL E O *COMPLIANCE* AMBIENTAL

Turing (1950) propôs pela primeira vez "que os computadores e a inteligência poderiam inspirar a inteligência artificial (IA) a replicar a cognição humana e as habilidades de aprendizagem". Nota-se o como essa frase de 1950 é aplicável atualmente. A inteligência artificial conforme mencionado, é uma tecnologia que simula a inteligência humana, como o raciocínio, etc, atualmente temos o Chatgpt, Copilot, Germini, dentre outras e estão sendo usadas em diversas áreas da ciência, inclusive a jurídica, trazendo respostas em segundos.

Callejón (2024, p.230) comenta que "os aplicativos da IA, como o Chatgpt, movem-se dentro dos parâmetros culturais próprios da

sociedade digital, permitem poupar tempo, o bem mais escasso da nossa sociedade".

Posto isso, podem ser usadas como uma ferramenta de *compliance* ambiental, Predanzini, Nishina, Freiria (2024, p.16) lecionam que:

> Destaca-se como prioridade máxima a prevenção de queimadas, que e do desmatamento ilegal, situações em que a IA pode ser implementada para monitorar áreas vulneráveis por meio de imagens de satélite e sistemas de vigilância inteligentes, permitindo uma resposta rápida para conter atividades clandestinas ou acidentes. Dessa forma, áreas com dimensões continentais como a floresta amazônica, cuja fiscalização por métodos tradicionais é pouco factível, poderão ser vistoriadas de forma massiva e inteligente. Além disso, recomenda-se a incorporação da IA na agricultura de precisão, visando otimizar o uso do solo, reduzir a necessidade de expansão agrícola em áreas de floresta e tornar a produção mais sustentável. No setor energético, a IA poderá desempenhar um papel crucial na maximização da geração de energia renovável, e pode ser considerada uma aceleradora para a transição energética total. Recomenda-se a utilização dessa tecnologia durante o planejamento urbano e destaca-se sua relevância para a otimização do sistema de distribuição de energia. Outro destaque importante é a grande capacidade de análise de dados da IA que viabiliza a otimização dos processos industriais e empresárias. A análise sistemática da cadeia produtiva de diferentes setores traz como resultado maior eficiência energética e minimização de desperdícios de recursos.

Do mesmo modo, Pengyu, Zhongzhu e Miao (2024) comentam que "a IA ajuda as empresas a identificar as demandas do mercado, otimizar processos operacionais e alcançar a otimização da alocação de recursos processando e analisando big data. além disso, os aplicativos

de ia podem ajudar as empresas a identificar riscos potenciais, incluindo riscos ambientais, riscos da cadeia de suprimentos e riscos de segurança. além disso, a ia pode ajudar as empresas a entender as demandas das partes interessadas externas, incluindo consumidores, fornecedores e investidores, melhorando assim sua imagem social".

Diante do exposto, é evidente que a inteligência artificial tem se consolidado como uma ferramenta poderosa e versátil, ainda irá existir vieses algorítmicos; desigualdades regionais no acesso, contudo, a tecnologia é capaz de transformar profundamente os processos empresariais e institucionais, inclusive na esfera ambiental. Ao incorporar essa tecnologia, empresas e governos não apenas ganham em eficiência e prevenção de danos, como também reforçam seu compromisso com a responsabilidade socioambiental e com os princípios do desenvolvimento sustentável.

CONCLUSÃO

Constata-se que a inteligência artificial, apesar de desafios, configura-se como uma ferramenta promissora para o aprimoramento do *compliance* ambiental. Sua capacidade de processar grandes volumes de dados, identificar padrões, antecipar riscos e otimizar processos contribui diretamente para a prevenção de danos ambientais e o cumprimento de normas legais. A incorporação da IA em setores como agricultura, energia, planejamento urbano e fiscalização ambiental pode potencializar a eficiência das políticas públicas e privadas, consolidando uma cultura de sustentabilidade e responsabilidade socioambiental. Assim, reforça-se a necessidade de políticas regulatórias que incentivem e orientem o uso ético e eficaz dessa tecnologia no contexto da governança ambiental.

REFERÊNCIAS

Brasil. Lei nº 6.938, de 31 de agosto de 1981. **Dispõe sobre a Política Nacional do Meio Ambiente, seus fins e mecanismos de formulação e aplicação, e dá outras providências**. 1981. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l6938.htm . Acesso em: 02/06/2025.

Brasil. **Constituição da República Federativa do Brasil**. Brasília, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 02/06/2025.

Banco Central do Brasil. **Resolução nº 4.327, de 25 de abril de 2014**. Estabelece diretrizes para a elaboração e a implementação da Política de Responsabilidade Socioambiental pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Diário Oficial da União: seção 1, Brasília, DF, n. 78, p. 101-102, 28 abr. 2014. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/normativo.asp?numero=4327 . Acesso em: 02/06/2025.

Banco Central do Brasil. **Resolução nº 4.945, de 15 de setembro de 2021.** Estabelece diretrizes para a Política de Responsabilidade Social, Ambiental e Climática (PRSAC). Diário Oficial da União: seção 1, Brasília, DF, n. 177, p. 92-94, 16 set. 2021. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/resolucao4945prsac . Acesso em:02/06/2025.

Bragato, Adelita Aparecida Poadera Bechelani. **O compliance no Brasil: a empresa entre a ética e o lucro./** Dissertação (Mestrado) – Universidade Nove de Julho – Uninove, São Paulo, 2017.Disponivel: https://bibliotecatede.uninove.br/bitstream/tede/1646/2/Adelita%20Aparecida%20Podadera%20 Bechelani%20Bragato.pdf. Acesso em: 02/06/2024.

Callejón, Francisco Balaguer. **A Constiuição do Algoritmo.** Editora Forense, 2023.

Comissão Mundial sobre Meio ambiente e desenvolvimento. **Nosso Futuro Comum.** Editora da Fundação Getúlio Vargas. Rio de Janeiro,1.991.

Mendes, Francisco Schertel. **Compliance :concorrência e combate à corrupção.** São Paulo: Trivisan Editora, 2017.

Melo, Celso Antônio Bandeira de. **Curso de Direito Administrativo** - Belo Horizonte Fórum.

Oliveira, Marcio Luis; Costa, Beatriz Souza; Silva, Cristiana Fortini Pinto e. **O instituto do compliance ambiental no contexto da sociedade plurissistêmica**. Veredas do Direito, Belo Horizonte, v. 15, n. 33, p. 51–71, set./dez. 2018. Disponível em: http://www.domhelder.edu.br/revista/index.php/veredas/article/view/1396 . Acesso em: 02/06/2025.

Organização das Nações Unidas . **Declaração de Estocolmo sobre o Meio Ambientem Humano**. Disponível em : https://www.nescon.medicina.ufmg.br/biblioteca/registro/referencia/0000001728#:~:text=Refer%C3%AAncia%3A,Unidas%20sobre%20Meio%20Ambiente%20Humano. Acesso em : 02/06/2024.

Predranzini, Helena Nogueira; Nishina, Isabella Ferraz; Freiria, Rafael Costa. **A inteligência artificial como ferramenta para contenção da crise climática no Brasil.** Homa Publica – Revista Internacional de Derechos Humanos y Empresas, Juiz de Fora, v. 8, n. 1, p. 1–20, jan./jul. 2024. Disponível em: https://homacdhe.com/index.php/revista/article/view/126. Acesso em: 02/06/2025.

Turing, Alan M. Computing machinery and intelligence. Mind, Oxford, v. 59, n. 236, p. 433–460, 1950. Disponível em: https://academic.oup.com/mind/article/LIX/236/433/986238. Acesso em:02/06/2025.

Wu, Yulin; Zhang, Jiahui; Cai, Xinyu. **Impact of regional artificial intelligence development on corporate environmental information**.

Finance Research Letters, [S.l.], v. 80, 107413, 2025. Disponível em: https://doi.org/10.1016/j.frl.2025.107413. Acesso em: 02/06/2025.

A EXPLICABILIDADE DOS SISTEMAS DE IA COMO DIREITO FUNDAMENTAL: UMA ANÁLISE EM TEMPOS DE IA GENERATIVA

Rebeca de Lima Nogueira

Bacharel(a) em Direito, Universidade do Estado do Amazonas

Taís Batista Fernandes

Doutor(a), Docente da Universidade do Estado do Amazonas

OBJETIVOS

1. Analisar como a explicabilidade dos sistemas de IA garante a proteção e a promoção dos direitos fundamentais, em especial, diante do desenvolvimento da IA generativa.

1.1.Identificar os conceitos iniciais relacionados à IA.

1.2.Identificar os principais conceitos relacionados à explicabilidade em sistemas de IA.

1.3.Analisar a explicabilidade em sistemas de IA como direito fundamental e seus benefícios.

PALAVRAS-CHAVE: explicabilidade, inteligência artificial, direito fundamental.

METODOLOGIAS

A presente pesquisa tem como finalidade verificar a importância da explicabilidade dos sistemas de IA para a proteção e a promoção dos direitos fundamentais, em especial, diante do crescente avanço da IA generativa. Nesse âmbito, os dados necessários à realização da presente pesquisa serão obtidos por meio da pesquisa bibliográfica-documental. Tais como artigos científicos, dissertações, teses,

documentos normativos, dentre outros. Assim, para busca de tais fontes, empregaremos o Google Acadêmico, Portal de Periódicos da CAPES, Elsevier, dentre outras revistas eletrônicas.

Ademais, em relação à forma como serão analisados os dados encontrados na pesquisa, será utilizada a abordagem predominantemente qualitativa, com foco na natureza e na essência do conteúdo coletado. Por último, quanto aos seus objetivos, o presente resumo terá como base a pesquisa exploratória-descritiva. Isso porque se busca compreender e descrever melhor o fenômeno da explicabilidade aplicada ao sistema de IA e sua relação com os direitos fundamentais.

INTRODUÇÃO

Hodiernamente, uma das subáreas das Tecnologias de Informação e de Comunicação (TIC´s) que tem sido amplamente desenvolvida é a da inteligência artificial (IA). Por meio dela, contemporaneamente, é possível a automatização de processos, bem como a tomada de decisões de forma precisa baseada em IA. Sob esse âmbito, conforme o relatório "Nossa vida com IA: da inovação à aplicação", promovido pela Google em parceira com a Ipsos, no ano de 2024, o Brasil ultrapassou a média global do uso de IA generativa (GOOGLE; IPSOS, 2025, p. 5). Esse cenário ocorre, pois, os sistemas artificialmente inteligentes têm sido incorporados de forma cada vez mais expressiva no dia a dia da sociedade. Assim, eles têm auxiliado desde a identificar trajetos mais eficientes até realizar recomendações de produtos no mercado on-line.

Entretanto, à medida que esses sistemas se tornam mais complexos, se discute o quão compreensível é o processo de tomada de decisão adotado por tais ferramentas. Isso porque, segundo, por vezes, os sistemas de IA operam de maneira opaca, não só do ponto de vista dos provedores, mas também daqueles que os implementam e dos indivíduos que interagem com tais ferramentas, os usuários externos

(EDPS, 2023, p. 3). Tal fenômeno é conhecido como efeito "caixa-preta" ou, em inglês, *black box*. Assim, é diante desse cenário que surge a necessidade de assegurar mecanismos mínimos de explicabilidade para os sistemas de IA, visando à promoção e à proteção dos direitos fundamentais. Dentre eles, do direito fundamental à explicação livre e esclarecida, além da transparência e do não enviesamento das decisões adotadas, de modo a propiciar o desenvolvimento de uma IA responsável, ética e segura.

CONCEITOS INICIAIS SOBRE IA

Os primeiros passos dados em direção à IA que se conhece hoje ocorreram ainda na década de 50, quando o matemático e cientista da computação, Alan Turing, propôs o jogo da imitação, o qual possuía como finalidade desenvolver um programa computacional capaz de se relacionar com pessoas externas como se fosse um ser humano (TURING, 1950, p. 433-460). Posteriormente, em 1956, pela primeira vez, foi utilizada a expressão *Artificial Intelligence (AI)* para se referir a sistemas capazes de resolver problemas tal como se fossem humanos e de se aperfeiçoarem.

Desse modo, observa-se que a definição de IA é ampla e diversa, abarcando tanto a IA simbólica, baseada no aprendizado de máquina (*machine learning*), quanto a IA baseada em redes neurais e no aprendizado profundo (*deep learning*), além de outros tipos que possam surgir. Nesse sentido, com o crescente desenvolvimento de pesquisas na área da aprendizagem de máquina, além da maior disponibilidade de dados e do aumento do poder computacional, surgiu a área da IA Generativa. Esse tipo de IA é baseada em redes neurais artificiais, as quais são modelos matemáticos que imitam o processo de aprendizagem do cérebro humano.

É diante desse cenário que emerge o campo da IA intitulado Inteligência Artificial Explicável (*Explainable Artificial Intelligence - XAI*). Tal subcampo tem como objetivo analisar ferramentas e técnicas

para desmembrar as soluções de IA, notadamente as que envolvem caixa preta, gerando explicações claras, perspicazes e transparentes das decisões adotadas por IA.

EXPLICABILIDADE EM SISTEMAS DE IA

Por conseguinte, em relação à explicabilidade aplicada aos sistemas de IA, cumpre destacar que, embora ela não esteja claramente positivada no ordenamento jurídico brasileiro, já existem um conjunto de documentos nacionais e internacionais que destacam a importância de se garantir tal princípio. Em âmbito internacional, por exemplo, o Regulamento do Parlamento Europeu e do Conselho da União Europeia n. 2024/1689, também conhecido como *AI Act*, destaca no item 27 que os sistemas de IA devem ser desenvolvidos e utilizados de forma a permitir a sua explicabilidade adequada (UE, 2024, p. 130).

De igual modo, Burle e Cortiz (2020, p.11), ao realizarem um mapeamento de princípios de inteligência artificial em iniciativas internacionais, destacaram que instituições como a Academia de Inteligência Artificial de Pequim e a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) defendem que os sistemas de IA devem ser explicáveis a fim de que "as pessoas entendam os resultados baseados em IA e possam desafiá-los". Por fim, a UNESCO em sua recomendação sobre IA assim esclarece:

> A explicabilidade significa tornar inteligível e fornecer informações sobre o resultado dos sistemas de IA. A explicabilidade desses sistemas também se refere à compreensibilidade sobre a entrada, a saída e o funcionamento de cada bloco de construção dos algoritmos e como ele contribui para o resultado dos sistemas. Assim, a explicabilidade está estreitamente relacionada com a transparência, pois os resultados e os subprocessos que conduzem a resultados devem almejar serem compreensíveis e rastreáveis, conforme o contexto. **Os atores de IA devem se comprometer**

> **a garantir que os algoritmos desenvolvidos sejam explicáveis. No caso de aplicativos de IA que afetam o usuário final de uma forma que não seja temporária, facilmente reversível ou de baixo risco, deve-se garantir que seja fornecida uma explicação significativa para qualquer decisão que resultou na ação tomada, para que o resultado seja considerado transparente** (UNESCO, 2022, p. 23, grifos nossos).

Em síntese, pode-se conceituar a IA explicável como "a capacidade dos sistemas de IA de fornecer explicações claras e compreensíveis para suas ações e decisões" (EDPS, 2023, p. 3). Sob esse âmbito, Arrieta *et al* (2020, p. 84-85) faz uma distinção entre transparência, interpretabilidade e explicabilidade no contexto da IA. A primeira estaria relacionada à capacidade de um modelo específico de ser compreendido por si só por um humano. Já o segundo conceito se refere ao grau de compreensibilidade humana de um determinado modelo de "caixa preta" ou decisão. Dessa forma, existem diversos tipos de abordagem possíveis para a XAI. A primeira delas se refere aos modelos autointerpretáveis ou transparentes, nos quais a interpretabilidade é incorporada no design dos sistemas.

Esses modelos apresentam algoritmos fáceis de compreender que demonstram como os dados de entrada (*inputs*) influenciam as saídas ou as variáveis-alvo (*outputs*). Já nas explicações *post hoc* ou explicabilidade pós-modelagem, o comportamento do sistema é primeiro observado e depois explicado a nível global (fornece uma compreensão geral do comportamento e do processo de tomada de decisão de um modelo de IA) ou local (concentra-se no processo de tomada de decisão de um modelo de IA para uma finalidade específica). Esses tipos de abordagem são recomendados para sistemas mais complexos (ARRIETA *et al,* 2020, p. 87-88). Sendo assim, embora as explicações *post-hoc* tenham suas limitações, elas podem fornecer informações relevantes para auxiliarem os usuários finais a

compreenderem suas saídas usando técnicas textuais, visuais, locais, por exemplo, por simplificação, dentre outras.

DIREITO À EXPLICAÇÃO COMO DIREITO FUNDAMENTAL E SEUS BENEFÍCIOS

Dessa forma, independentemente de qual seja a técnica de explicabilidade adotada para o sistema de IA, observa-se que a sua utilização traz grandes benefícios. Isso porque, segundo uma pesquisa realizada em 2019 pelo MIT Sloan Management Review, entre os gestores do mundo corporativo, por exemplo, uma das principais inquietações que envolve a utilização da IA em suas empresas está relacionada a resultados que não podem ser explicados (MIGUEL, 2020). Nesse sentido, a pesquisa identificou que desenvolver a confiança em IA está diretamente ligada ao entendimento e à comunicação sobre como funciona a lógica de resultados e a tomada de decisões por esses sistemas.

Ademais, verifica-se que a compreensão do seu funcionamento reduz vieses e erros, melhorando a confiança dos usuários em tais modelos. Além disso a explicabilidade em sistemas de IA pode ser benéfica para consecução de padrões regulatórios, de modo a certificar que um produto ou serviço atende às normas legais, ajudando até mesmo em questões de responsabilidade; para avaliação de risco, robustez e vulnerabilidade, bem como em relação à autonomia e atendimento a valores sociais do sistema. Doutro modo, para além dos benefícios de se garantir tal diretriz, nota-se o direito à explicação como um direito fundamental.

Nesse âmbito, Silva e Ehrhardt (202, p. 14) destacam que o próprio Código de Defesa do Consumidor apresenta como direito básico, no seu artigo 6º, inciso III, a informação adequada e clara sobre os diferentes produtos e serviços, incluindo os riscos que apresentem. Dessa forma, embora, por vezes, o dever de informação encontre barreiras pela falta de conhecimento preciso sobre o funcionamento da

IA, especialmente em situações de *black box*, mesmos nesses casos se faz necessário encontrar mecanismos para garantir a explicabilidade desses sistemas. Principalmente, por exemplo, nos órgãos judiciais, em que "uma decisão não pode ser efetivamente contestada sem que se possa auditar a inteligência artificial e compreender, em termos mínimos, o seu funcionamento" (SILVA, EHRHARDT, 2020, p. 11).

Outrossim, cabe esclarecer que a própria Constituição Federal de 1988, em seu artigo 5º, garante o direito à segurança, bem como à proteção dos dados pessoais dos indivíduos no inciso LXXIX (BRASIL, 1988). De igual forma, o Regulamento do Parlamento Europeu e do Conselho da União Europeia n. 2024/1689 assim garante no artigo 86:

> 1. Qualquer pessoa afetada sujeita a uma decisão tomada pelo responsável pela implantação com base nos resultados de um sistema de IA de risco elevado enumerado no anexo III, com exceção dos sistemas enumerados no ponto 2 desse anexo, e que produza efeitos jurídicos ou analogamente afete num grau significativo essa pessoa, de forma que considere ter repercussões negativas na sua saúde, segurança ou direitos fundamentais, **tem o direito de obter do responsável pela implantação explicações claras e pertinentes sobre o papel do sistema de IA no processo de tomada de decisão e sobre os principais elementos da decisão tomada** (UE, 2024, p. 110, grifos nossos).

Ante o exposto, verifica-se que, mais que um mero princípio, a explicabilidade em IA deve ser vista como um direito fundamental dos usuários, independente do tipo de IA adotado. Dessa forma, ela deve funcionar como um mecanismo contra a opacidade em tais sistemas, desafiando cientistas e pesquisadores a desenvolverem métodos eficazes de explicabilidade e de modo a aumentar a confiança dos usuários em tais ferramentas. Ademais, sempre lembrando que tal explicabilidade deve ser adaptada para cada contexto, adequando-se ao

público que se pretender atingir e gerando uma relação participativa do usuário para com a máquina.

CONCLUSÃO

Portanto, é evidente que, diante de um contexto de constante evolução da IA, por vezes, garantir a explicabilidade dos sistemas de IA possa ser um grande desafio para desenvolvedores de tais tecnologias. Contudo, como visto ao longo deste resumo, a explicabilidade tem sido defendida e promovida em diversos âmbitos nacionais e internacionais, já existindo mecanismos para garantir tal diretriz. Porém, para além disso, é necessário que ela seja vista como um direito fundamental de todo o usuário, razão pela qual se requer o devido cuidado e atenção ao ser implementada pelo desenvolvedores e demais participantes de tal ecossistema.

REFERÊNCIAS

ARRIETA, Alejandro Barredo, *et al*. **Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible ai.** [s. n.], [S. l.], v. 58, p. 82 – 115, 2020. ISSN 1566-2535. Disponível em: < https://www.sciencedirect.com/science/article/pii/S1566253519308103>. Acesso em: 20 maio 2025.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988. Brasília, DF: Senado Federal, 1988. Disponível em: < https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 23 maio 2025.

BURLE, Caroline; CORTIZ, Diogo. **Mapeamento de princípios de inteligência artificial.** São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2020. Disponívelem:<https://www.nic.br/media/docs/publicacoes/17/20200721143359/digital_mapeamento_principios_IA_portugues.pdf>. Acesso em 15 out. 2024.

EUROPEAN DATA PROTECTION SUPERVISOR (EDPS). **TechDispatch: explainable artificial intelligence**. #2/2023. Luxembourg: Publications Office, 2023. Disponível em: < https://www.edps.europa.eu/system/files/2023-11/23-11-16_techdispatch_xai_en.pdf>. Acesso em: 25 maio 2025.

GOOGLE; IPSOS. **Our life with AI: from innovation to application**. Janeiro, 2025. Disponível em:<https://static.googleusercontent.com/media/publicpolicy.google/en//resources/ipsos_google_our-life-with-ai_2024_25.pdf >. Acesso em: 23 maio 2025.

MIGUEL, Angela. **A explicabilidade na construção de uma inteligência artificial**. MIT Sloan Management Review Brasil. 2020. Disponível em: < https://mitsloanreview.com.br/a-explicabilidade-na-construcao-de-uma-inteligencia-artificial/#:~:text=A%20explicabilidade%2C%20

portanto%2C%20%C3%A9%20a,a%C3%A7%C3%B5es%20em%20um%20processo%20automatizado>. Acesso em: 15 maio. 2025.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA (UNESCO). **Recomendação sobre a Ética da Inteligência Artificial**. Aprovada 23 de novembro de 2021. 2022. Disponível em: <https://asmetro.org.br/portalsn/wp-content/uploads/2022/08/Recomendacao-sobre-a-Etica-da-Inteligencia-Artificial-UNESCO-Digital-Library.pdf>. Acesso em: 25 maio 2025.

SILVA, G. B. P.; EHRHARDT JÚNIOR, M. **Diretrizes éticas para a Inteligência Artificial confiável na União Europeia e a regulação jurídica no Brasil**. Revista IBERC, Belo Horizonte, v. 3, n. 3, p. 1–28, 2020. DOI: 10.37963/iberc.v3i3.133. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/133. Acesso em: 2 jun. 2025.

TURING. Alan Mathison. **Computing Machinery and Intelligence**. Mind, Volume LIX, Issue 236, October 1950, Pages 433–460, Disponível em: <https://phil415.pbworks.com/f/TuringComputing.pdf>. Acesso em: 7 ago. 2024.

UNIÃO EUROPEIA (UE). **Regulamento do Parlamento Europeu e do Conselho da União Europeia 2024/1689**. 2024. Disponível em: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> . Acesso em: 15 jan. 2025.

INTELIGÊNCIA ARTIFICIAL, EXPLICABILIDADE E ACCOUNTABILITY ALGORÍTMICA NA ADMINISTRAÇÃO PÚBLICA: FUNDAMENTOS JURÍDICOS E DESAFIOS À TRANSPARÊNCIA DEMOCRÁTICA

Rhedson Francisco Fernandes Esashika

Mestrando em Engenharia Elétrica | IOT e IA - Universidade do Estado do Amazonas PPGEEL/UEA, Especialista em Direito Constitucional (ESMAM) e Especialista em Aprendizado de Máquina (IFAM), e-mail: rhedson@gmail.com

Tiago Esashika Crispim

Mestrando em Constitucionalismo de Direitos da Amazônia (UFAM) |, Especialista em Direito Público (UEA), e-mail: ti.esashika@gmail.com

Palavras-chaves: inteligência artificial; explicabilidade algorítmica; accountability pública; transparência administrativa; decisões automatizadas.

1. OBJETIVOS

O presente trabalho tem como objetivo principal analisar os fundamentos jurídicos da explicabilidade e da accountability algorítmica como instrumentos essenciais para a promoção da transparência e do controle democrático no uso de sistemas de Inteligência Artificial pela Administração Pública brasileira. Pretende-se, nesse sentido, investigar o conceito de explicabilidade algorítmica e sua normatividade no ordenamento jurídico nacional, à luz da Constituição Federal, da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e de regulamentações administrativas setoriais. Busca-se, ainda, examinar os mecanismos jurídicos e institucionais de responsabilização aplicáveis à atuação estatal mediada por algoritmos, com ênfase nas decisões automatizadas

que impactam direitos fundamentais. O trabalho também se propõe a discutir os desafios técnicos, normativos e práticos à efetivação da transparência algorítmica no setor público, sobretudo diante das tensões entre segredo comercial e dever de publicidade, das limitações de entendimento dos usuários e da incipiente estrutura institucional de fiscalização. Além disso, objetiva-se refletir sobre a necessária evolução do dever de motivação dos atos administrativos diante do uso crescente de sistemas automatizados, propondo a integração entre motivação e explicabilidade como condição de validade jurídica das decisões públicas e como requisito indispensável à construção de um marco regulatório democrático e eficaz para a inteligência artificial no Brasil.

2. METODOLOGIA.

A pesquisa adota uma abordagem de natureza dedutiva, alicerçada na análise crítica dos fundamentos normativos que regulam a utilização de sistemas algorítmicos pela Administração Pública. O método de procedimento é qualitativo, com ênfase em revisão bibliográfica e documental, abrangendo doutrina especializada, legislação nacional — com destaque para a Constituição Federal, a Lei nº 13.709/2018 (LGPD) e projetos de marco legal da IA —, além de documentos oficiais e relatórios institucionais. A pesquisa contempla, ainda, a análise comparada de referenciais internacionais, como o *Artificial Intelligence Act* da União Europeia (UNIÃO EUROPEIA, 2021), que adota uma abordagem baseada em risco e exige altos padrões de explicabilidade e supervisão humana, e o *Blueprint for an AI Bill of Rights*, publicado pelo governo dos Estados Unidos (ESTADOS UNIDOS, 2022), que propõe princípios orientadores para decisões automatizadas centradas nos direitos dos cidadãos. Foram utilizados repositórios acadêmicos como o Google Scholar e bibliotecas jurídicas digitais, com a aplicação de expressões-chave como "explicabilidade algorítmica", "accountability pública", "governança da IA" e "transparência estatal",

a fim de consolidar uma análise crítica e interdisciplinar sobre os desafios jurídicos da atuação algorítmica estatal.

3. DESENVOLVIMENTO DA PESQUISA

3.1. FUNDAMENTOS DA EXPLICABILIDADE ALGORÍTMICA NO DIREITO BRASILEIRO

A explicabilidade algorítmica consiste na capacidade de um sistema automatizado oferecer razões compreensíveis para suas decisões, sendo elemento essencial à legitimidade da atuação estatal baseada em Inteligência Artificial (IA). Esse dever não se restringe à abertura de códigos-fonte, mas demanda informações claras sobre critérios, dados e lógicas aplicadas, possibilitando o controle público e a proteção de direitos fundamentais.

No ordenamento jurídico brasileiro, o principal fundamento está no artigo 20 da Lei Geral de Proteção de Dados Pessoais (LGPD)[9], que garante ao titular o direito à revisão e à obtenção de explicações sobre decisões automatizadas. O que representa um importante instrumento normativo no contexto da proteção de direitos fundamentais diante do avanço das tecnologias baseadas em inteligência artificial e algoritmos automatizados de decisão.

Inclusive, essa compreensão foi recentemente reforçada pelo Superior Tribunal de Justiça (STJ), ao julgar o Recurso Especial n.º 2.135.783/DF. Na decisão, a Corte reconheceu a incidência do artigo 20 da LGPD em uma relação contratual de natureza privada, entre um motorista de aplicativo e a empresa Uber. O tribunal entendeu que, ainda que a plataforma digital possua a prerrogativa de realizar a suspensão imediata do perfil de motoristas por meio de uma decisão automatizada, não exime a empresa do dever de informar de maneira

9 Lei Geral de Proteção de Dados Pessoais (LGPD) , Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

clara e acessível os motivos que ensejaram a medida, tampouco impede que o titular dos dados exerça seu direito de defesa e pleiteie a revisão da decisão por um agente humano.

Aprofundando o tema, Floridi et al. (2018) dispõe que o princípio da explicabilidade se estrutura em duas dimensões complementares: Intelligibility (inteligibilidade) – ou seja, a capacidade de entender como o sistema funciona; Accountability (responsabilização ou prestação de contas) – ou seja, a capacidade de atribuir responsabilidade ética, legal ou institucional, tanto que essa abordagem acolhida por normativas como a Resolução CNJ nº 332/2020, que exige explicações auditáveis em sistemas de IA no Judiciário. Herzog (2022), por sua vez, ressalta a necessidade de adequação contextual da explicação, a fim de que seja efetiva e não meramente formal.

Um dos principais entraves à explicabilidade é a limitação imposta pela proteção a segredos comerciais, prevista no art. 20, §1º, da LGPD. Mesmo na Administração Pública, essa restrição pode subsistir, sobretudo quando há contratação de soluções tecnológicas desenvolvidas por agentes privados. Soma-se a isso a alta complexidade técnica de modelos como o deep learning, que dificulta a produção de explicações claras e acessíveis. Por isso, a explicabilidade, no setor público, deve ser entendida como extensão do dever de motivação previsto na Lei nº 9.784/1999, exigindo uma nova concepção: a motivação algorítmica, apta a revelar os critérios técnicos e jurídicos que sustentam a decisão automatizada (PINHEIRO, 2023).

3.2. ACCOUNTABILITY ALGORÍTMICA NA ADMINISTRAÇÃO PÚBLICA

A accountability algorítmica refere-se à obrigação de prestar contas, justificar decisões e responder por efeitos derivados do uso de sistemas de Inteligência Artificial (IA), sobretudo quando aplicados por entes estatais. Sua presença é essencial para assegurar que a delegação de decisões a agentes automatizados não implique um

"vácuo" de responsabilidade pública, contrariando os princípios da legalidade e da moralidade administrativa (art. 37 da CF/88).

No contexto brasileiro, encontra respaldo na LGPD, que, ao regulamentar o tratamento automatizado de dados, confere prerrogativas à Autoridade Nacional de Proteção de Dados (ANPD) para auditorias e fiscalização (art. 20, §2º). Além disso, a Resolução CNJ nº 332/2020 estabelece que os sistemas de Inteligência Artificial utilizados no Poder Judiciário devem ser obrigatoriamente passíveis de auditoria humana, consolidando um padrão normativo de controle institucional robusto, centrado na prestação de contas, rastreabilidade decisória e responsabilização pessoal e institucional, arts. 25 e 26 da resolução. O Projeto de Lei nº 2.338/2023, ao prever a Análise de Impacto Algorítmico (AIA) para sistemas de alto risco, avança na construção de uma governança proativa, baseada na prevenção e não apenas na reação a falhas.

Contudo, persistem desafios substanciais: a complexidade técnica de sistemas baseados em *machine learning*, a indefinição quanto à responsabilidade entre desenvolvedor, gestor público e operador do sistema, e a limitada capacitação das instituições fiscalizadoras para auditar algoritmos sofisticados. Conforme destaca Burrell (2016), muitos modelos operam como "caixas-pretas", o que dificulta a atribuição clara de culpa ou dolo.

Nesse cenário, torna-se indispensável incorporar a accountability desde o design dos sistemas — por meio das abordagens de *accountability by design* —, assegurando transparência procedimental e registros de uso. A ausência dessa estrutura pode comprometer direitos fundamentais, gerar decisões discriminatórias e minar a confiança pública na Administração Digital. O controle social e a supervisão pelos órgãos de fiscalização devem ser reforçados com recursos técnicos, humanos e normativos adequados, sob pena de os sistemas algorítmicos se tornarem imunes ao escrutínio democrático.

3.3. CASOS CONCRETOS E DESAFIOS PRÁTICOS

A adoção de sistemas de Inteligência Artificial por órgãos governamentais não é um fenômeno recente, mas sua consolidação em funções decisórias tem levantado desafios significativos quanto à transparência, à proteção de direitos fundamentais e à accountability algorítmica.

Um exemplo notório é o do sistema SyRI (Systeem Risico Indicatie), desenvolvido nos Países Baixos. Veale e Zuiderveen Borgesius (2021) explicam que se tratava de uma ferramenta automatizada de vigilância social destinada à identificação de potenciais fraudes em programas de benefícios públicos, mediante o cruzamento de dados pessoais provenientes de diversas bases governamentais. Em 2020, o Tribunal de Haia determinou sua suspensão imediata, ao concluir que o sistema violava direitos humanos fundamentais — notadamente o direito à privacidade — conforme assegurado pela Convenção Europeia dos Direitos Humanos. A ausência de critérios transparentes e a assimetria informacional entre o Estado e os cidadãos foram considerados incompatíveis com os princípios democráticos e de devido processo.

No Brasil, destaca-se o caso do sistema Victor, implementado pelo Supremo Tribunal Federal (STF) com a finalidade de auxiliar na triagem de processos com repercussão geral. Embora represente um avanço na gestão judiciária e na racionalização do acervo processual, o sistema ainda carece de clareza metodológica quanto aos critérios de priorização e classificação dos processos, o que tem gerado preocupações quanto à sua conformidade com os princípios constitucionais do contraditório, da ampla defesa e da motivação das decisões.

No âmbito do Conselho Nacional de Justiça (CNJ), a Resolução nº 332/2020 estabelece diretrizes para o uso ético e transparente da IA no Judiciário, exigindo, por exemplo, que as decisões automatizadas sejam auditáveis e supervisionadas por magistrados. Essa normativa reflete uma preocupação legítima com a manutenção da motivação

das decisões judiciais, mesmo diante da automação de etapas procedimentais.

Tais experiências demonstram que, embora os sistemas de IA possam contribuir para maior eficiência e celeridade, sua utilização deve ser acompanhada de mecanismos que assegurem a compreensão dos critérios adotados e a possibilidade de revisão adequada. O desafio, portanto, consiste em equilibrar inovação tecnológica e garantia de direitos, com foco na legitimidade e confiabilidade das decisões judiciais.

4. CONCLUSÕES

A adoção de sistemas de Inteligência Artificial pela Administração Pública brasileira demanda o fortalecimento de garantias jurídicas voltadas à transparência e ao controle democrático. Neste cenário, a explicabilidade e a accountability algorítmica configuram-se como pilares fundamentais para assegurar a legitimidade das decisões automatizadas, especialmente diante de potenciais riscos à publicidade, à motivação e aos direitos fundamentais dos cidadãos.

Embora o ordenamento jurídico nacional, notadamente a Constituição Federal e a Lei Geral de Proteção de Dados Pessoais, já contenha dispositivos aplicáveis à matéria, persistem lacunas normativas, dificuldades técnicas e limitações institucionais que comprometem sua efetividade. Os casos analisados evidenciam a urgência de aprimorar os mecanismos de controle, desde o desenho dos sistemas até sua supervisão contínua.

Dessa forma, torna-se imprescindível que o futuro marco legal da inteligência artificial no Brasil incorpore exigências de explicabilidade por design, auditorias independentes e protocolos de responsabilização claros, de modo a assegurar uma transformação digital compatível com os princípios do Estado Democrático de Direito.

REFERÊNCIAS

ESTADOS UNIDOS. Executive Office of the President. **Blueprint for an AI Bill of Rights: making automated systems work for the American people**. Washington, D.C.: The White House, 2022. Disponível em: https://www.whitehouse.gov/ostp/ai-bill-of-rights/. Acesso em: 09 maio 2025.

BURRELL, Jenna. **How the machine 'thinks': Understanding opacity in machine learning algorithms**. *Big Data & Society*, v. 3, n. 1, p. 1–12, 2016.

UNIÃO EUROPEIA. Comissão Europeia. **Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Artificial Intelligence Act**). Bruxelas, 21 abr. 2021. COM(2021) 206 final. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52021PC0206. Acesso em: 09 maio 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Diário Oficial da União, Brasília, DF, 5 out. 1988.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Lei Geral de Proteção de Dados Pessoais – LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. **Projeto de Lei nº 2.338, de 2023**. Estabelece normas gerais sobre o desenvolvimento, a implementação e o uso responsável de sistemas de inteligência artificial no Brasil. Senado Federal. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/158889. Acesso em: 09 maio 2025.

BRASIL. **Resolução nº 332, de 21 de agosto de 2020**. Dispõe sobre a ética, a transparência e a governança no uso de Inteligência Artificial no Poder Judiciário. *Conselho Nacional de Justiça*, 2020.

BRASIL. Superior Tribunal de Justiça. 3ª Turma. **Recurso Especial n. 2.135.783 – DF**. Relatora: Ministra Nancy Andrighi. Julgado em: 18 jun. 2024. Informativo de Jurisprudência n. 817. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Informativos-de-Jurisprudencia.aspx, Acesso em: 31 maio 2025.

FLORIDI, Luciano et al. **AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations**. *Minds and Machines,* v. 28, p. 689–707, 2018.

KAUFMAN, Dora. Inteligência artificial e os desafios éticos: a restrita aplicabilidade dos princípios gerais para nortear o ecossistema de IA. *PAULUS – Revista de Comunicação da FAPCOM,* São Paulo, v. 5, n. 9, p. 73–84, jan./jul. 2021. DOI: https://doi.org/10.31657/rcp.v5i9.453.

HERZOG, Anya. **Designing for Algorithmic Explainability: Legal Standards and Design Considerations**. *Law and Ethics of Human Rights,* v. 16, n. 2, p. 271–297, 2022.

PINHEIRO, Luiz Fernando. **A motivação algorítmica no processo administrativo: desafios e perspectivas à luz da Lei 9.784/99 e da LGPD**. *Revista Brasileira de Direito Público*, v. 19, n. 76, p. 45–68, 2023.

SUPREMO TRIBUNAL FEDERAL (STF). **Sistema Victor: inteligência artificial a serviço do STF**. Brasília: STF, 2024. Disponível em: https://www.stf.jus.br. Acesso em: 09 maio 2025.

VEALE, Michael; BRACKEEN, Frederik Zuiderveen. *Fairness and the European Union's Artificial Intelligence Act*. Maastricht Journal of European and Comparative Law, [S.l.], v. 28, n. 5, p.

627–640, 2021. Disponível em: https://journals.sagepub.com/doi/full/10.1177/13882627211031257. Acesso em: 31 maio 2025.

IMPORTÂNCIA DO PROGRAMA DE *COMPLIANCE* NAS PLATAFORMAS DIGITAIS DE APOSTAS DE QUOTA FIXA (*BETS*) NO BRASIL: PREVENÇÃO À LAVAGEM DE DINHEIRO, PROTEÇÃO DE DADOS E RESPONSABILIDADE SOCIAL

Roberta Carolaine Lira Lopes

Advogada especialista em Direito Civil pela PUC/MG, Profissional de Compliance Certificada pela LEC Certification Board (LCB) e acadêmica em Especialização em Direito, Compliance e Mecanismos Anticorrupção pela Universidade do Estado do Amazonas - UEA /AM.

Ana Karoline Farias Barros

Advogada, Profissional de Compliance Certificada pela LEC Certification Board (LCB) e acadêmica em Especialização em Direito, Compliance e Mecanismos Anticorrupção e MBA em ESG e Sustentabilidade, ambas pela Universidade do Estado do Amazonas - UEA /AM.

Carlos Augusto da Silva

Graduado em Ciências Sociais (UFAM/1997), especialização em Pedagogia e Gestão empresarial (UFAM/2025), mestrado em Ciências do Ambiente e Sustentabilidade na Amazônia (UFAM/2010), doutorado em Sociedade e Cultura na Amazônia (UFAM/2016). Servidor aposentado pela Ufam, atualmente professor colaborador das Universidades Federal do Amazonas e Universidade do Estado do Amazonas, lecionando disciplinas em graduação, pós-graduação e orientando mestrando e doutorando, na linha de pesquisa Dinâmicas Socioambientais, no campo da a Arqueologia da Amazônia.

Palavras-chaves: *Compliance*. Apostas Digitais. Governança Regulatória. Proteção de Dados. Responsabilidade Social.

1 OBJETIVOS

Este trabalho tem como objetivo analisar criticamente a relevância dos programas de compliance no contexto das plataformas digitais de apostas de quota fixa no Brasil. Diante do crescimento acelerado desse mercado e da intensificação do uso de tecnologias que promovem jogos de forma personalizada e contínua, busca-se compreender como o compliance pode atuar como mecanismo de prevenção à lavagem de dinheiro, proteção de dados pessoais dos usuários e mitigação dos impactos sociais relacionados ao vício em jogos. Pretende-se ainda examinar as recentes medidas regulatórias adotadas pelo Estado brasileiro, especialmente por meio da Secretaria de Prêmios e Apostas, e suas implicações para a governança, integridade e responsabilidade das operadoras digitais. Além disso, o estudo visa fomentar reflexões acadêmicas e institucionais sobre a necessidade de construção de políticas públicas e estruturas jurídicas eficazes, capazes de equilibrar inovação tecnológica, liberdade econômica e justiça social no ambiente digital das apostas.

2 METODOLOGIA

A metodologia adotada nesta pesquisa é qualitativa, de natureza exploratória e descritiva, baseada em uma revisão bibliográfica e documental. Foram analisadas normas jurídicas nacionais, além de documentos institucionais, artigos acadêmicos e relatórios técnicos de organizações internacionais como o GAFI/FATF. A seleção das fontes priorizou dados atualizados e diretamente relacionados ao funcionamento dos sites de apostas, à proteção de dados, à prevenção à lavagem de dinheiro e à promoção de jogo responsável. Também foram considerados debates recentes no Congresso Nacional e na mídia especializada, como os desdobramentos da CPI das Apostas Esportivas, para contextualizar os desafios regulatórios e éticos enfrentados por esse setor. A análise foi conduzida com foco nas

interseções entre direito digital, governança regulatória e compliance corporativo, buscando identificar tendências, riscos e perspectivas para o fortalecimento de um ambiente digital mais íntegro, seguro e socialmente responsável.

3 DESENVOLVIMENTO DA PESQUISA

O crescimento exponencial das plataformas digitais de apostas de quota fixa (*bets*) no Brasil tem remodelado o cenário jurídico, econômico e social do setor de entretenimento e jogos (AMERICO, 2024). Facilitadas pelo acesso móvel e pela digitalização de serviços, essas plataformas operam em um ambiente altamente dinâmico e transnacional, o que amplia os riscos regulatórios e evidencia a urgência da implementação de programas de compliance robustos. A digitalização desse mercado não só democratizou o acesso ao jogo como também expôs os usuários a vulnerabilidades financeiras, tecnológicas e sociais que exigem atenção normativa qualificada.

A base normativa que fundamenta a atuação dessas plataformas é composta principalmente pelas Leis nº 13.756/2018 e nº 14.790/2023, que legalizaram e regulamentaram as apostas de quota fixa, conferindo ao Ministério da Fazenda, por meio da Secretaria de Prêmios e Apostas (SPA-MF), o papel de órgão regulador. Diversas portarias publicadas em 2024 estruturam um modelo de compliance regulatório que orienta as empresas quanto à prevenção à lavagem de dinheiro, ao financiamento do terrorismo, à segurança da informação e à integridade do ambiente digital (BRASIL, 2024a). Essas normas se aplicam diretamente à operação das plataformas, exigindo desde a identificação digital de usuários (KYC) até o envio eletrônico de comunicações obrigatórias ao COAF (BRASIL, 2024a).

Os sites de apostas têm características específicas que aumentam a complexidade regulatória. Por serem acessados remotamente, operarem 24 horas por dia e utilizarem algoritmos para promover jogos e ofertas personalizadas, eles criam um ambiente propício à

circulação de grandes volumes de dinheiro e dados sensíveis. Isso os torna especialmente vulneráveis à lavagem de dinheiro, dado que o ambiente dos jogos de azar permite a dissimulação de valores por meio de ganhos fictícios (BOTTINI, 2024), prática combatida por meio da aplicação de políticas de compliance baseadas em monitoramento algorítmico, análise comportamental e inteligência artificial. Práticas como o fracionamento de apostas, transferências suspeitas entre contas e padrões de movimentação atípicos são alguns dos indicadores que essas plataformas devem detectar em tempo real (GAFI/FATF, 2024).

A proteção de dados pessoais dos usuários dessas plataformas é igualmente crucial, sendo regulada pela Lei Geral de Proteção de Dados (LGPD). As apostas digitais demandam o fornecimento de dados bancários, documentos de identidade, geolocalização e até perfis comportamentais, que devem ser tratados em conformidade com os princípios de finalidade, necessidade, transparência e segurança. Plataformas que negligenciam essas práticas podem sofrer sanções da Autoridade Nacional de Proteção de Dados (ANPD), além de danos reputacionais e perda de confiança por parte dos usuários. Dessa forma, a cibersegurança e a governança de dados tornam-se pilares indispensáveis nos programas de compliance dessas empresas. (BRASIL, 2018).

Outro ponto relevante é a responsabilidade social no ambiente digital. As plataformas não apenas facilitam o acesso ao jogo, mas também podem impulsionar práticas de consumo problemático, especialmente entre jovens e grupos vulneráveis. A lógica de funcionamento dessas plataformas, baseada em notificações constantes, gamificação e recompensas imediatas, pode induzir ao vício em jogos, o que torna imprescindível a adoção de ferramentas digitais de jogo responsável, como autoexclusão, limites de tempo, bloqueios voluntários e sistemas automatizados de alerta sobre comportamentos compulsivos (AMERICO, 2024). Nesse aspecto, o compliance também assume função pedagógica e preventiva, promovendo práticas de cuidado com os usuários.

Ainda, o papel dessas plataformas no ecossistema digital exige que sejam vistas como agentes reguláveis (AMERICO, 2024). A ausência de fiscalização rigorosa e de políticas públicas voltadas para o uso consciente dessas ferramentas pode transformar um ambiente de entretenimento em um espaço de risco social elevado.

A consolidação de uma regulação eficaz depende do reconhecimento de que os sites de apostas não são apenas veículos tecnológicos, mas estruturas complexas com potencial de impacto sistêmico. Sua regulamentação exige articulação entre direito digital, proteção de dados, combate à criminalidade financeira e promoção da inclusão digital com responsabilidade. A maturidade institucional nesse campo requer o fortalecimento de órgãos reguladores, a incorporação de boas práticas internacionais e o desenvolvimento contínuo de mecanismos de compliance digital. Com isso, será possível compatibilizar inovação tecnológica com integridade institucional e justiça social.

4 CONCLUSÃO

O avanço das plataformas digitais de apostas de quota fixa no Brasil trouxe acessibilidade e crescimento econômico, mas também revelou fragilidades estruturais que exigem respostas normativas urgentes. Nesse contexto, os programas de compliance emergem como instrumentos centrais para a integridade do setor, atuando na prevenção à lavagem de dinheiro, proteção de dados pessoais e mitigação de impactos sociais relacionados ao vício em jogos.

A criação da Secretaria de Prêmios e Apostas e a publicação de portarias específicas marcaram avanços significativos na regulação do setor. No entanto, permanecem desafios como a resistência à implementação de estruturas robustas de integridade, a ausência de políticas públicas voltadas à proteção de grupos vulneráveis e o uso limitado de tecnologias de monitoramento ético.

Conclui-se que o compliance deve ser compreendido não apenas como obrigação legal, mas como estratégia de governança capaz de alinhar inovação digital com responsabilidade institucional. O fortalecimento desse ecossistema exige cooperação entre Estado, setor privado e sociedade civil para assegurar um ambiente regulado, seguro e socialmente justo.

REFERÊNCIAS

AMERICO, Lucas Batista. *Proteção de dados pessoais em apostas de quota fixa no Brasil: o caso BET365*. 2024. 87 f. Monografia (Graduação em Direito) – Escola de Direito, Turismo e Museologia, Universidade Federal de Ouro Preto, Ouro Preto, 2024. Disponível em: https://www.monografias.ufop.br/handle/35400000/7139. Acesso em: 1 jun. 2025.

BOTTINI, Pierpaolo Cruz. Os riscos de lavagem de dinheiro no setor de jogos de azar. Disponível em: https://direito.usp.br/noticia/06a24156015f-os-jogos-de-azar-e-a-lavagem-de-dinheiro. Acesso em: 01 jun.2025.

BRASIL. Senado Federal. Comissão Parlamentar de Inquérito das Apostas Esportivas. Página oficial. Disponível em: https://legis.senado.leg.br/atividade/comissoes/comissao/2703. Acesso em: 1 jun. 2025.

BRASIL. Lei nº 9.613, de 3 de março de 1998. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9613.htm. Acesso em 01 jun.2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 01 jun.2025.

BRASIL. Ministério da Fazenda. Secretaria de Prêmios e Apostas. Portaria SPA/MF nº 1.143, de 11 de julho de 2024. Dispõe sobre os procedimentos de prevenção à lavagem de dinheiro e financiamento ao terrorismo no mercado de apostas de quota fixa. *Diário Oficial da União*, Brasília, DF, 11 jul. 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-spa/mf-n-1.143-de-11-de-julho-de-2024-571718850. Acesso em: 01 jun.2025.

GAFI/FATF. *Recommendations for Combating Money Laundering and the Financing of Terrorism and Proliferation*. Disponível em: https://www.fatf-gafi.org. Acesso em 15 dez.2024.

OPACIDADE VERSUS EXPLICABILIDADE: DESAFIOS PARA A UTILIZAÇÃO DA IA NA ADMINISTRAÇÃO PÚBLICA

Alcian Pereira de Souza

Professor Adjunto da UEA. Doutor em Ciências pela FEA/USP, Mestre em Direito pela UEA. Pesquisador Líder do Grupo de Pesquisa CNPQ "Direito, Tecnologia e Inovação". Coordenador Geral do Núcleo de Direito, Tecnologia & Inovação- LAWin/UEA e atualmente é Diretor da Escola de Direito da UEA (ED/UEA).

Rodrigo de Almeida Grangeão

Graduando do 7º período do curso de direito da Universidade do Estado do Amazonas

PALAVRAS-CHAVE: Administração Pública - explicabilidade - eficiência - transparência.

1. OBJETIVOS

No contexto de intensas mudanças tecnológicas e de uma sociedade globalizada, os sistemas de inteligência artificial transformaram o modo de execução de diversos serviços, com o fim de atingir os melhores resultados com o menor gasto de recursos. Nesse viés, este estudo possui como objetivo central, a investigação dos principais aspectos do uso da inteligência artificial no serviço público, bem como os principais desafios para a sua implementação, em face dos princípios constitucionais. Como consequência, buscou-se compreender os conceitos de explicabilidade e opacidade desses sistemas, e suas aplicações em consonância aos princípios da publicidade e transparência.

2. METODOLOGIA

Com o fim de alcançar o objetivo esperado por esta pesquisa, foi feita a análise de livros e artigos científicos produzidos com ênfase nos aspectos da explicabilidade e do uso da inteligência artificial na Administração Pública. Além disso, utilizaram-se dados estatísticos fornecidos pela UNESCO e de outras pesquisas relacionadas com a temática pesquisada e seus desdobramentos. A metodologia utilizada foi a bibliográfica descritiva, com a finalidade de explorar o tema por meio de uma percepção qualitativa do problema.

3. DESENVOLVIMENTO DA PESQUISA

3.1 INTELIGÊNCIA ARTIFICIAL E EXPLICABILIDADE

Em um contexto mundial de constantes mudanças tecnológicas, a inteligência artificial surgiu como uma ferramenta capaz de otimizar as atividades humanas, proporcionando uma maior eficiência, principalmente no que tange à execução de atividades repetitivas e burocráticas.

Nesse sentido, a inteligência artificial na visão de Figueiredo e Cabral constitui um instrumento complexo, que possui como função central o armazenamento e processamento de informações a fim de atuar na resolução de problemas e tomadas de decisões, com método e velocidade próprios. (2020, p. 85-86).

No entanto, o cerne reside em como compatibilizar o uso dessas novas tecnologias com a função pública e a busca pela eficiência administrativa, visando, além disso, a finalidade pública e o bem-estar coletivo. Nesse viés, a explicabilidade dos sistemas de inteligência artificial tem sido colocada em discussão, em face dos princípios que regem o ordenamento jurídico brasileiro, como a publicidade e o dever de prestar contas.

Alves e Andrade definem o conceito de explicabilidade das IA's:

> "Um sistema inteligente dotado de inteligência artificial explicável (XAI) é aquele que possui interpretabilidade ou explicabilidade, quer dizer, capacidade para explicar suas predições, por meio de estratégias textuais ou visuais que forneçam compreensão qualitativa sobre seu processo de predição (Ribeiro et al., 2018, p. 2). O sistema de IA explicável está habilitado a fornecer explicações sobre sua operação, tornando seu comportamento mais inteligível para os humanos (Gunning et al., 2019). Significa dizer que um sistema XAI deve estar apto a explicar, de maneira apropriada a um ser humano, a lógica interna de sua predição: o que foi feito, o que está fazendo agora e o que acontecerá a seguir" (2022, p. 8)

Nesta esteira, o foco central da explicabilidade das IA's reside em explicar os processos algorítmicos adotados, os resultados e a sua influência nas decisões. Para isso, é necessário que o sistema forneça informações para compreensão do processo de entrada (input) e saída (output) dos dados (Pádua; Lorenzetto, 2024, p. 357).

O conceito de explicabilidade da I.A. se diferencia substancialmente da interpretabilidade destes sistemas, principalmente quanto ao público-alvo a que se destina compreender as informações. Enquanto a interpretabilidade refere-se ao nível de compreensão que os especialistas em computação possuem dos processos e dados fornecidos, a explicabilidade, em contrapartida, diz respeito àquelas informações que podem ser compreendidas para todos, de modo acessível (Pádua; Lorenzetto, 2024, p. 357-358).

3.2 TRANSPARÊNCIA COMO DIRETRIZ PARA A FUNÇÃO PÚBLICA

De fato, a transparência na Gestão Pública configura não mais uma diretriz ou valor a ser seguido, mas sim uma obrigação do administrador público, em face do princípio da indisponibilidade

do interesse público. O princípio da publicidade é um princípio constitucional explícito, previsto no artigo 37, caput, da Constituição Federal, que constitui um requisito de eficácia para os atos administrativos estatais. (Brasil, 1988).

Nesse sentido, Gutman e Thompson (1996) defendem que o princípio da publicidade além de constituir um dever dos gestores públicos, também caracteriza-se como um instrumento de participação política dos cidadãos:

> "Além disso, a publicidade não apenas constrange as autoridades públicas a fazerem o que deles é esperado por todos, mas é também valiosa "por ser uma amiga da accountability", bem como por encorajar "os cidadãos a deliberar sobre políticas públicas" e por possibilitar "que autoridades aprendam sobre a e da opinião pública" (1996, p. 97).

A associação da eficiência, a publicidade e o dever de prestar contas reflete uma tendência atual do governo, que por meio desses instrumentos, oportuniza a participação da sociedade como agentes de controle da atividade administrativa. Consoante a isto, cumpre citar, por exemplo, o Decreto nº 9.203/2017 que define a transparência, a prestação de contas, e a integridade como princípios que regem a governança pública na Administração Pública Federal (Brasil, 2017).

Na era tecnológica, portanto, é inviável desassociar a atividade administrativa eficiente da utilização dos novos mecanismos de automação de tarefas, sendo incluídos neste meio os sistemas de Inteligência Artificial. Esta situação pode ser demonstrada, portanto, na adoção das IAs pelo Poder Judiciário, conforme exemplificado pelos dados do Painel de Projetos de Inteligência Artificial no ano de 2023, coletados pelo Conselho Nacional de Justiça, que expõem que cerca de 62 tribunais no país possuem projetos de IA's em andamento ou em vias de implementação, com predominância dos tribunais da justiça estadual (CNJ, 2023).

3.3 A OPACIDADE ALGORÍTMICA COMO UM DESAFIO PARA A UTILIZAÇÃO DAS IA'S NO SETOR PÚBLICO

Adotados tais critérios, os sistemas de inteligência artificial devem fornecer informações legítimas e aptas a serem compreendidas, diante da imposição do princípio da publicidade e da transparência. Contudo, as IA's possuem uma característica inerente à sua natureza, denominada opacidade, que pode configurar um óbice à explicabilidade algorítmica.

Consoante a isso, Morais e Mafra definem a opacidade da seguinte maneira:

> "A opacidade (ou blackbox) consiste, então, nessa impossibilidade de se conhecer objetivamente os caminhos pelos quais as informações de entrada se transformaram nas informações de saída. E isso se dá em dois níveis: um de acesso, no sentido de transparência do sistema de IA, referente à estrutura mesma do sistema ou, de maneira simples, sobre o "como funciona"(?) e um de explicabilidade, ou seja, a possibilidade de ser capaz de compreender o "como se chegou ao resultado"(?). Mais simplesmente ainda: o "como decide?" e o "como decidiu?"" (2023, p. 525-526)

Os especialistas definem essa característica como uma verdadeira "caixa preta", pela qual não é possível identificar os caminhos utilizados pela IA para atingir os resultados, apenas é possível compreender os aspectos de entrada (input) e saída (output). Visto isso, quando se tratar de decisões estatais que impactam na qualidade de vida, no patrimônio e na liberdade das pessoas, o cuidado deve ser redobrado, segundo o documento Recomendações sobre a Ética da Inteligência Artificial, elaborado pela UNESCO, o qual aborda, na *Policy Area 1* (Avaliação de aspectos éticos), que devem ser adotados requisitos claros para transparência e auditabilidade desses sistemas,

principalmente quando utilizados nas tomadas de decisões estatais, de forma a abordar também os seus comportamentos e aspectos essenciais (UNESCO, 2021).

De forma complementar, Alves e Andrade defendem que a medida correta a ser adotada para combater a opacidade algorítmica seria o desenvolvimento das IA's, para a inclusão de propriedades explicativas, ou seja, inserir propriedades nesses sistemas que possibilitem explicitar as razões e as causas para a tomada de decisões, o que os autores categorizam como IA explicativa (2022, p.360-361).

4. CONCLUSÃO

O uso das novas tecnologias como os sistemas de inteligência artificial no setor público constitui um instrumento para a busca dos melhores resultados com a menor utilização de recursos públicos, reflexo do corolário do princípio da eficiência administrativa. A adoção desses novos mecanismos deve respeitar as regras e princípios estabelecidos no ordenamento jurídico pátrio, como o princípio da publicidade, no entanto, a característica da opacidade das IA's vai de encontro com tais premissas, eis que oculta a motivação, causas e o caminho causal utilizado para a tomada de decisão nesses sistemas.

Em face disso, tem surgido diversas discussões no âmbito acadêmico quanto à utilização desses mecanismos na atividade estatal, principalmente na tomada de decisões que afetem a vida, o patrimônio e os direitos fundamentais dos cidadãos. Assim, como medida remediadora, devem ser realizadas auditorias constantes, revisões humanas e a implementação de mecanismos explicativos nas IA's que permitam uma maior explicabilidade de suas ações.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, M. A. S.; ANDRADE, O. M. 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.** Revista de Direito Público, v. 18, n. 100, 2022. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5973. Acesso em: 28 maio. 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 29 maio. 2025.

BRASIL. Decreto nº 9.203/2017 - Dispõe sobre a política de governança da administração pública federal, direito autárquica e fundacional. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/d9203.html. Acesso em 29 maio. 2025.

CONSELHO NACIONAL DE JUSTIÇA. **Painel de Projetos de IA no Poder Judiciário - 2023.** Brasília: CNJ, 2023. Disponível em: https://paineisanalytics.cnj.jus.br/single/?appid=43bd4f8a-3c8f-49e7-931f-52b789b933c4&sheet=e4072450-982c-48ff-9e2d-361658b99233&theme=horizon&lang=pt-BR&opt=ctxmenu,currsel&select=Ramo%20da%20Justi%C3%A7a,&select=Tribunal,&select=Seu%20Tribunal/%20Conselho%20possui%20Projeto%20de%20IA?. Acesso em 29 maio. 2025.

FIGUEIREDO, Carla Regina Bortolaz de; CABRAL, Flávio Garcia. **Inteligência artificial: machine learning na Administração Pública: Artificial intelligence: machine learning in public administration**. International Journal of Digital Law, Belo Horizonte, v.1, n. 1, p. 79–96, 2020. Disponível em: https://journal.nuped.com.br/index.php/revista/article/view/figueiredov1n1. Acesso em: 28 maio. 2025.

GUTMANN, A.; THOMPSON, D. **Democracy and disagreement. Cambridge: Harvard University Press**, 1996.

MORAIS, José Luis Bolzan de; MAFRA, Lígia Kunzendorff. **Inteligência artificial em decisões judiciais: opacidade versus garantias processuais.** Novos Estudos Jurídicos, Itajaí (SC), v. 28, n. 3, p. 516-535, 2023. DOI: 10.14210/nej.v28n3.p516-535

PÁDUA, Sergio Rodrigo de; LORENZETTO, Bruno Meneses . **O direito fundamental à explicabilidade da inteligência artificial utilizada em decisões estatais**. REVISTA DA AGU, *[S. l.]*, v. 23, n. 02, 2024. Disponível em: https://revistaagu.agu.gov.br/index.php/AGU/article/view/3480. Acesso em: 28 maio. 2025.

UNESCO. **Recommendation on the Ethics of Artificial Intelligence**. 24 nov. 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000380455. Acesso em: 28 maio. 2025.

DISCRIMINAÇÃO ALGORÍTMICA E SEUS IMPACTOS NA SOCIEDADE CAPITALISTA CONTEMPORÂNEA

João Victor de Almeida Grangeão

Graduando do 10º período do curso de Economia da Universidade Federal do Amazonas.

Kelly Borges de Almeida Rocha

Mestra em Serviço Social e Sustentabilidade na Amazônia pela UFAM. Assistente Social do Instituto de Desenvolvimento Agropecuário e Florestal Sustentável do Estado do Amazonas (IDAM).

Rodrigo de Almeida Grangeão

Graduando do 7º período do curso de Direito da Universidade do Estado do Amazonas.

PALAVRAS-CHAVE: Discriminação Algorítmica - Inteligência Artificial - Capitalismo - Sociedade .

1. OBJETIVOS

O presente resumo se destina a análise do fenômenos da discriminação algorítmica a partir do contexto da relações socio-econômicas na sociedade capitalista contemporânea, bem como os principais impactos gerados por essa problemática, como a coisificação das relações e o agravamento de desigualdades sociais. Outrossim, objetivou-se abordar os principais conceitos relacionados ao funcionamento das IA's (Inteligência Artificial), e as diretrizes para sua utilização ética.

2. METODOLOGIA

Com o fim de alcançar o objetivo esperado por esta pesquisa, foi feita análise de livros e artigos científicos produzidos com ênfase nos aspectos da discriminação algorítmica e seus impactos na sociedade capitalista. Além disso, utilizaram-se dados estatísticos fornecidos pela UNESCO e de outras pesquisas relacionadas com a temática abordada e seus desdobramentos. A metodologia utilizada foi a bibliográfica descritiva, com a finalidade de explorar o tema por meio de uma percepção qualitativa do problema.

3. DESENVOLVIMENTO DA PESQUISA

3.1 ASPECTOS FUNDAMENTAIS DA DISCRIMINAÇÃO ALGORÍTMICA

Na sociedade contemporânea, a utilização dos sistemas de inteligência artificial para a otimização de atividades cotidianas tornou-se uma realidade, em razão da sua celeridade e eficiência. Esses mecanismos são compostos por micro unidades denominadas algoritmos, aplicados em diversos softwares e programas computacionais que se utilizam do aprendizado de máquina (machine learning) a fim de treiná-los para a execução de tarefas específicas (Cozman; Neri, 2021, p. 22-25).

Nesse contexto, a tomada de decisões é feita através de um processo complexo que envolve a execução dos dados de entrada (input) para a obtenção dos dados de saída (output) (Leal; Paulo, 2023, p.168-169). No entanto, os produtos deste processamento podem ter efeitos negativos, como é o caso da discriminação algorítmica baseada em vieses algorítmicos.

Diante disso, Leal e Paulo conceituam discriminação algorítmica da seguinte forma:

> O termo discriminação algorítmica se refere às discriminações promovida pelos algoritmos ao

> discriminar pessoas com base em características e padrões predeterminados, o que conduz naturalmente a resultados injustos e desiguais. Tais discriminações estão, geralmente, relacionadas com a amostragem de dados coletada e armazenada na base de dados utilizada pelo algoritmo em questão (2023, p.169)

Tal fenômeno ocorre, pois os algoritmos são programados com base em dados diretamente influenciados por fatores econômicos, sociais e culturais, vieses e equívocos humanos, oriundos de sistemas compostos por escolhas tipicamente humanas, e portanto, dotados de falibilidade (Duarte; Negócio, 2022, p.220).

Um exemplo de sistema em que foi possível observar a prática de discriminação algorítimica em suas decisões, é o COMPAS, IA norte-americana responsável por auxiliar a tomada de decisões no sistema penitenciário do país por meio do fornecimento de dados para subsidiar a concessão de liberdade provisória, a definição de valores e fiança, e até mesmo, fornecer embasamentos para a sentença criminal. Todavia, após a realização de estudos por ONG's locais, observou-se que o sistema estava propenso a classificar os acusados negros com maior grau de periculosidade que os acusados brancos, mesmo com as situações fáticas semelhantes (Angwin, *et al,* 2016).

Esse problema decorre do fato de que a inteligência artificial é "alimentada"via dados influenciados pelas atividades humanas, e em razão disso, de forma conectada, esses sistemas absorvem os vieses e preconceitos e replicando-os em seus resultados e tomadas de decisões. Consoante a isto, os novos marcos regulatórios relacionados à inteligência artificial têm adotado maneiras de combater a discriminação algorítmica e evitar a repetição dos erros anteriormente cometidos.

Como reflexo dessas novas políticas, cita-se o documento Recomendação sobre a Ética da Inteligência Artificial, elaborado pela UNESCO no ano de 2021, o qual prevê como alguns dos seus princípios-base a não discriminação, supervisão e determinação

humana, transparência, explicabilidade e responsabilidade, de forma a direcionar a utilização ética dos mecanismos de IA. (UNESCO, 2021)

3.2 DISCRIMINAÇÃO ALGORÍTMICA E SEUS IMPACTOS SOCIOECONÔMICOS

Em uma sociedade cada dia mais informatizada e "conectada" é comum utilizar plataformas digitais em atividades rotineiras ou para processos mais complexos como triagem de benefícios sociais, seleção de emprego, dentre outros. Todavia, essas transformações tecnológicas afetam, de modo específico, os direitos sociais, já que a discriminação algorítmica pode marginalizar indivíduos ou grupos sociais, principalmente, quanto à invisibilidade ou tratamento discriminatório em sistemas automatizados. Assim, a consolidação da denominada Sociedade da Informação impõe, de forma crescente, a necessidade de conectividade para o pleno exercício da cidadania.

Contudo, é imperioso considerar a realidade do Brasil que traz em sua história marcas de desigualdades, conforme Ianni:

> "os prenúncios do Brasil Moderno esbarravam em pesadas heranças de escravismo, autoritarismo, coronelismo, clientelismo. As linhas de castas, demarcando relações sociais e de trabalho, modos de ser e pensar, subsistiam por dentro e por fora das linhas de classes em formação. O povo, enquanto coletividade de cidadãos, continuava a ser uma ficção política (1989, p. 30).

Portanto, acrescenta-se, ainda, neste contexto, que milhares de brasileiros permanecem à margem da chamada rede mundial de computadores, seja pela ausência de dispositivos como smartphones ou computadores, pela falta de habilidades técnicas para operar essas ferramentas ou pelo receio em relação ao ambiente digital, são os chamados excluídos digitais, o que resulta, progressivamente, na

restrição de direitos humanos e fundamentais, diante da migração de uma diversidade de serviços e funções sociais para plataformas digitais (Gomes, 2023).

Sublinha-se que os computadores não compreendem palavras que denotam uma avaliação subjetiva, sendo que a problemática se refere às especificações fornecidas a ele. Desta maneira, reforça-se a desigualdade de classe, raça e gênero, bem como, dificulta o acesso a direitos e desumaniza o atendimento, desfocando dos sujeitos e coisificando suas particularidades e carecimentos.

Logo, a sociabilidade capitalista gera a subordinação da sociabilidade humana a coisas, e isto pode ser, também, visualizado na esfera do *on-line,* por meio do processo da "dataficação" transformação da vida humana em dados (Feliciano, et al., 2022). Importa ressaltar que a lógica de produção capitalista busca, incessantemente, por novas formas de ampliação da mais-valia e como consequência o aumento da exploração do trabalhador.

Feliciano et al., (p. 316, 2022), embasado pelo conceito de Shoshana Zuboff, destaca que o capitalismo de vigilância é "[...] um novo poder econômico, fincado na rastreabilidade de informações e de dados que circulam na internet, capturáveis para a análise e a monetização pelas empresas". Neste processo a tendência é fetichizar essas informações e coisificar as relações sociais.

A crescente adoção de tecnologias baseadas em inteligência artificial e algoritmos tem levantado sérias preocupações sobre a reprodução e o agravamento de desigualdades sociais. A chamada discriminação algorítmica ocorre quando sistemas automatizados tomam decisões enviesadas, refletindo ou amplificando preconceitos existentes na sociedade. Diante desse cenário, os governos desempenham um papel fundamental na prevenção desse tipo de discriminação, podendo atuar por meio de medidas regulatórias, institucionais, técnicas e educativas.

Outro aspecto essencial é a formulação de políticas públicas que assegurem a diversidade e representatividade nos dados utilizados para treinar algoritmos. Dados tendenciosos, que não refletem realidades

sociais desiguais, podem levar a decisões injustas, segregativas e desconexas. Por isso, o governo deve exigir testes de viés e equidade antes da implementação de sistemas automatizados em larga escala, acrescenta-se, ainda, quanto a importância da transparência e fiscalização desses dados.

Portanto, combater a discriminação algorítmica exige uma postura ativa, coordenada e multidimensional por parte do Estado, que deve garantir que o uso de tecnologias emergentes não aprofunde desigualdades, mas sim promova direitos, inclusão e equidade.

4. CONCLUSÃO

A utilização da inteligência artificial nas relações humanas e na realização das atividades cotidianas constitui um reflexo da sociedade informatizada e da busca pela eficiência, aspectos típicos do sistema capitalista e sua abordagem produtiva. Consoante a isso, os sistemas de IA, por serem alimentados por dados essencialmente humanos, são influenciados por fatores sociais, culturais, políticos e econômicos, e podem gerar a replicação de vieses discriminatórios em suas tomadas de decisões.

Este fenômeno pode causar diversas consequências negativas no âmbito social, como a tomada de decisões excludentes, a coisificação das relações humanas, a exclusão digital e o agravamento das desigualdades sociais, razão pela qual se exige uma atuação mais ativa do Estado quanto à formulação de políticas públicas que assegurem a representatividade nos dados utilizados para o treinamento de algoritmos.

REFERÊNCIAS BIBLIOGRÁFICAS

ANGWIN, Julia; LARSON, Jeff; SURYA, Mattu; KIRCHNER, Lauren. **Machine Bias**. Pro Publica, 23 de maio de 2016. Disponível em: https://www.propublica.org/ article/machine-bias-risk-assessments-in-criminal-sentencing. Acesso em 30 maio. 2025.

COZMAN, Fabio G.; NERI, Hugo. **O que, afinal, é Inteligência Artificial? In:** COZMAN, Fábio G.; PLONSKI, Guilherme Ary; NERI, Hugo. Inteligência Artificial: Avanços e Tendências. São Paulo: Instituto de Estudos Avançados, p. 19-27, 2021

DUARTE, Alan.; NEGÓCIO, Ramos de Vasconcelos. **Todos São Iguais Perante o Algoritmo? Uma Resposta Cultural do Direito à Discriminação Algorítmica**. Revista de Direito Público, *[S. l.]*, v. 18, n. 100, 2022. DOI: 10.11117/rdp.v18i100.5869. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5869. Acesso em: 30 maio. 2025.

FELICIANO, Guilherme Guimarães. NASPOLINI, Samyra Haydêe Dal Farra. FOGAROLLI FILHO, Paulo Roberto. SOUZA, Devanildo de Amorim. **O capitalismo de vigilância e seus efeitos**: discriminação algorítmica e reificação humana. *Revista de Direito Brasileira*, Florianópolis, v. 33, n. 12, p. 309-332, set./dez. 2022.

GOMES, Camila Paula de Barros. **Exclusão digital como forma de violação dos direitos humanos**. 2023.

IANNI, Octavio. **A questão social**. Revista Ciência & Trópico, v. 17, 1989. Disponível em: <https://fundaj.emnuvens.com.br/CIC/article/view/436>. Acesso em: 27 maio. 2025.

LEAL, Mônia Clarissa Hennig.; PAULO, Lucas Moreschi. **Algorítmos discriminatórios e jurisdição constitucional: os riscos jurídicos e sociais do impacto dos vieses nas plataformas de inteligência artificial**

de amplo acesso. Revista de Direitos e Garantias Fundamentais, *[S. l.]*, v. 24, n. 3, p. 165–187, 2023. DOI: 10.18759/rdgf.v24i3.2311. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/2311. Acesso em 30 maio. 2025.

UNESCO. **Recommendation on the Ethics of Artificial Intelligence**. 24 nov. 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000380455. Acesso em: 30 maio. 2025.

GESTÃO DE PROJETOS NA ADEQUAÇÃO À LGPD NA ADMINISTRAÇÃO PÚBLICA: UMA REFLEXÃO SOBRE DESAFIOS, METODOLOGIAS E CONSTRUÇÃO PRÁTICA DE CONHECIMENTO

Tayna Lanay Carvalho Veloso de Almeida, Pós- Graduanda UEA
Bernardo Silva de Seixas, Doutor em Direito Constitucional – FADISP

Palavras-chave: LGPD; Gestão de Projetos; Administração Pública; Data Protection Management System; Governança de Dados.

1 OBJETIVO

Este trabalho tem como objetivo refletir, a partir de uma perspectiva prática, sobre os desafios da gestão de projetos de adequação à Lei Geral de Proteção de Dados (LGPD) no setor público. A proposta é discutir como esse campo, ainda em processo de consolidação, se estrutura na intersecção entre metodologias tradicionais de gestão de projetos, práticas ágeis, *frameworks* de risco e modelos de governança como o *Data Protection Management System* (DPMS), desenvolvido inicialmente para setores como hotelaria, comércio e serviços. A reflexão busca compreender de que forma esses referenciais podem, ou não, serem aplicados no contexto da administração pública, considerando suas especificidades éticas, operacionais e jurídicas.

2 METODOLOGIA

A pesquisa adota abordagem qualitativa e fenomenológica, fundamentada na prática vivenciada pela autora enquanto gestora de projetos de adequação à LGPD em órgãos públicos do Estado do Amazonas. Complementa-se com revisão bibliográfica especializada, abordando referenciais de gestão de projetos (PMBOK Guide), metodologias ágeis (Scrum), frameworks de gestão de risco (NIST

Privacy Framework, ISO/IEC 27001 e 27701) e a própria LGPD. Trata-se de um estudo reflexivo, que articula teoria, prática e crítica institucional.

3 DESENVOLVIMENTO

A adequação à Lei Geral de Proteção de Dados (LGPD) na administração pública impõe desafios que transcendem o mero cumprimento formal da legislação. Trata-se de edificar uma governança de dados alinhada aos princípios constitucionais da administração pública — legalidade, impessoalidade, moralidade, publicidade e eficiência — conforme previsto no artigo 37, caput, da Constituição Federal de 1988. Essa realidade levanta questionamentos essenciais: como estruturar projetos de proteção de dados em instituições públicas que não foram concebidas, historicamente, sob uma lógica de governança da informação? E quais instrumentos são necessários para compatibilizar as obrigações decorrentes da proteção de dados com o funcionamento tradicional da administração burocrática?

Nesse cenário, é importante reconhecer que a gestão de projetos voltados à LGPD ainda se configura como um campo em construção. Não há, até o momento, uma metodologia própria consolidada ou formalmente reconhecida no meio acadêmico. O que se observa, na prática, é uma engenharia de adaptação: a incorporação criativa de metodologias desenvolvidas em outros contextos — especialmente industriais, comerciais, de serviços e, notadamente, da hotelaria, setor no qual se consolidou o chamado Data Protection Management System (DPMS), modelo tradicionalmente voltado ao setor privado. O DPMS oferece um arcabouço estruturado de governança da proteção de dados, ideal para ambientes corporativos, mas sua transposição direta para a realidade do setor público encontra limites evidentes. A lógica de mercado, centrada na competitividade e no cliente, não encontra correspondência direta no contexto da administração pública, cuja razão de existir está vinculada ao interesse coletivo e

ao dever constitucional de prestar serviços públicos com qualidade e equidade. Assim, aplicar frameworks como o DPMS de forma indistinta requer não apenas sensibilidade, mas também discernimento técnico e político, a fim de reinterpretar premissas e adaptá-las à lógica institucional pública.

A gestão de projetos em proteção de dados encontra no PMBOK Guide uma referência metodológica robusta. Elementos como o registro e a estratégia das partes interessadas, o desenvolvimento do plano de gerenciamento, a coleta de requisitos e a definição do escopo revelam-se centrais no desenho e na execução de projetos de LGPD no setor público. Aqui, o mapeamento das partes interessadas ultrapassa os muros institucionais, incorporando a própria sociedade como stakeholder, em virtude dos princípios da transparência e da responsabilidade pública, especialmente diante da sensibilidade de alguns dados que apenas os entes públicos detêm. O plano de gerenciamento do escopo, por sua vez, precisa abarcar mais do que entregáveis técnicos: ele deve refletir um processo de transformação institucional que perpassa desde a revisão normativa até uma profunda mudança cultural no modo como os dados são tratados. Isso exige dos agentes públicos um conhecimento aprofundado sobre as normas de proteção de dados, indo além da mera adequação formal.

Ferramentas como a matriz de rastreabilidade de requisitos, a documentação de processos, os planos de comunicação e os planos de risco assumem, nesse contexto, um papel estratégico. Deixam de ser apenas registros burocráticos para se tornarem instrumentos vivos de governança, transparência e accountability, fortalecendo o compromisso institucional com a privacidade e a segurança da informação. Para garantir a efetividade desses instrumentos, é indispensável integrar frameworks como o NIST Privacy Framework, o NIST SP 800-53, e as normas ISO/IEC 27001 e ISO/IEC 27701, que funcionam como alicerces invisíveis da estrutura organizacional, garantindo que a proteção de dados não se restrinja ao plano documental, mas represente um compromisso concreto com a segurança e a gestão de riscos.

O desafio, no entanto, não se limita às ferramentas. A própria natureza da administração pública impõe complexidades específicas. Burocracia, resistência à mudança, escassez de recursos humanos especializados e, frequentemente, uma baixa maturidade digital constituem um cenário onde a aplicação de metodologias requer, mais do que rigor técnico, uma escuta institucional refinada, capaz de captar resistências, mobilizar engajamento e construir aderência entre os diversos setores envolvidos. Essa complexidade torna evidente que projetos de LGPD não pertencem a uma única disciplina. Sua implementação exige a articulação de saberes jurídicos, tecnológicos, gerenciais e comunicacionais. O gestor de projetos atua como um tradutor entre mundos distintos — da linguagem normativa à técnica, das demandas dos servidores aos objetivos das consultorias, dos dados pessoais às narrativas institucionais.

Além disso, a gestão desses projetos demanda uma abordagem flexível e iterativa. Na prática, o planejamento raramente segue uma lógica linear. Inspirados em abordagens ágeis como o Scrum, os ciclos de revisão e ajuste tornam-se a regra, uma vez que cada entrega revela novas necessidades e oportunidades de melhoria. Nesse sentido, o cronograma deixa de ser uma estrutura rígida para se tornar uma ferramenta de organização e aprendizado coletivo, que se molda à medida que o projeto avança.

Neste contexto, a comunicação ganha status de tecnologia de governança. Não se trata apenas de informar, mas de construir compreensão compartilhada, alinhar expectativas, fomentar adesão institucional e, sobretudo, legitimar os processos de transformação. Projetos de adequação à LGPD somente prosperam quando são compreendidos por quem os executa e acolhidos por quem deles depende.

A experiência na região amazônica reforça e aprofunda esses desafios. As distâncias geográficas, as desigualdades digitais, a precarização estrutural e a ausência histórica de uma cultura de proteção de dados tornam a implementação da LGPD não apenas uma tarefa técnica, mas também um exercício de resistência. Adequar-se à

LGPD nesses territórios é afirmar, na prática, o direito fundamental à privacidade, reconhecendo-o como pilar de cidadania e de dignidade humana, mesmo — e especialmente — nos contextos mais adversos.

4 CONSIDERAÇÕES FINAIS

A gestão de projetos aplicada à LGPD na administração pública não é simplesmente a aplicação de metodologias. Ela é uma construção prática, ética e reflexiva, feita na confluência entre marcos regulatórios, frameworks técnicos e a complexidade social e institucional dos órgãos públicos.

Mais do que entregar documentos, o projeto entrega uma transformação: uma cultura que compreende os dados pessoais não como ativos institucionais, mas como expressões da dignidade, da cidadania e dos direitos fundamentais.

Portanto, gerir projetos de LGPD é, antes de tudo, um compromisso com a construção de uma administração pública mais ética, eficiente, transparente e alinhada às exigências democráticas do nosso tempo.

REFERÊNCIAS

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

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27001:2013**. Information technology — Security techniques — Information security management systems — Requirements. Genebra: ISO, 2013.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27701:2019**. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. Genebra: ISO, 2019.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management.** Gaithersburg, MD: NIST, 2020.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Special Publication 800-53 Rev. 5. **Security and Privacy Controls for Information Systems and Organizations.** Gaithersburg, MD: NIST, 2020.

PROJECT MANAGEMENT INSTITUTE (PMI). **A Guide to the Project Management Body of Knowledge (PMBOK® Guide).** 7. ed. Pennsylvania: PMI, 2021.

MEMÓRIA E DESENVOLVIMENTO: A TRAJETÓRIA DO PATRIMÔNIO CULTURAL BRASILEIRO, OS DESAFIOS E A INTELIGÊNCIA ARTIFICIAL

Thiago Snaider Nunes da Cruz[10]

PALAVRAS-CHAVE: Patrimônio cultural brasileiro. Bens culturais. Inteligência artificial.

1. OBJETIVOS

O presente estudo tem como objetivo geral abordar o patrimônio cultural brasileiro a mediante a utilização da inteligência artificial como meio de promoção. Para tanto, os objetivos específicos são a identificação e conceituação das dimensões do patrimônio cultural brasileiro; a sintetização da institucionalização e trajetória da proteção do patrimônio cultural brasileiro; para, ao fim, apresentar a inteligência artificial como meio de disseminação dos bens culturais.

2. METODOLOGIA

O caminho metodológico escolhido para a abordagem das questões apresentadas no presente artigo possui como alicerce o procedimento bibliográfico e documental, utilizando do arcabouço doutrinário e normativo acerca do tema, isto mediante uma abordagem qualitativa, com amparo no método dedutivo.

10 Mestrando no Programa de Pós-Graduação em Direito Ambiental (PPGDA) da Universidade do Estado do Amazonas (UEA). Lattes: http://lattes.cnpq.br/9012860961538404. E-mail: tsndc.mda24@uea.edu.br.

3. DESENVOLVIMENTO

3.1 PATRIMÔNIO CULTURAL NO BRASIL

O patrimônio cultural brasileiro é constituído por bens de natureza material e imaterial. Entretanto, durante a primeira metade do século XX, o patrimônio cultural no Brasil, conhecido apenas como patrimônio histórico, foi pautado pelas concepções de monumentalidade e excepcionalidade. Estas estruturas físicas e tangíveis constituem-se na dimensão material do patrimônio (Cunha Filho; Magalhães, 2024, p. 33). O resguardo dos bens culturais exclusivamente sob o aspecto material foi a regra nas Constituições Brasileiras anteriores à Constituição Federal de 1988. Contudo, a partir da década de 1970, tornou-se crescente o anseio pela proteção de outras manifestações culturais não relacionadas exclusivamente à dimensão física, a exemplo das "lendas, mitos, ritos, saberes e técnicas", conhecidos atualmente por compor a dimensão imaterial do patrimônio cultural (Fonseca, 2001, p. 69).

A dimensão imaterial do patrimônio cultural consiste nas práticas intangíveis. O art. 216 da Constituição Federal de 1988, de forma inédita, apregoa maneiras de manifestação e define como se constitui o patrimônio cultural material e imaterial brasileiro, não mais conhecido como patrimônio histórico, mediante uma lista não exaustiva de bens que, para assim serem considerados, devem ser portadores de referência. As dimensões material e imaterial do patrimônio cultural brasileiro, apesar de apresentadas de modo individualizado, são, em verdade, complementos e encontram-se presentes de forma uníssona nos bens culturais

Além disso, a identificação e seleção do patrimônio cultural depende da constatação de valores, memórias e significados. Para tanto, como menciona o art. 216 da Constituição Federal de 1988, há a necessidade de serem identificadas referências culturais à identidade, à ação, à memória dos diferentes grupos formadores da sociedade brasileira, que os caracteriza e individualiza. Segundo Maria Cecilia

Londres Fonseca (2001, p. 113), tratar de referências culturais significa "dirigir o olhar para representações que configuram uma identidade da região para seus habitantes, e que remetem à paisagem, às edificações e objetos, aos fazeres e saberes, às crenças, hábitos, etc".

Assim, o patrimônio cultural emana da própria sociedade, cujos indivíduos são intérpretes no processo de levantamento das referências culturais, dotando a um bem material ou imaterial o caráter de bem cultural, possibilitando, junto ao Poder Público, a adoção de medidas necessárias à proteção e promoção do bem, assegurando o protagonismo da população, primordial interessada na defesa de seus bens identitários.

3.2 INSTITUCIONALIZAÇÃO E TRAJETÓRIA DA PROTEÇÃO DO PATRIMÔNIO CULTURAL

Os alicerces do patrimônio cultural no Brasil são estabelecidos a partir da década de 1930, durante o Estado Novo. Dentre as diversas reformas realizadas por Getúlio Vargas, buscou-se a instituição de uma identidade nacional, invocando o apoio popular mediante a criação de símbolos relacionados à pátria, vinculados a uma concepção de cultura única e nacional, desaguando na ideia de nação brasileira (Fonseca, 2017, p. 88).

Com a criação do Serviço do Patrimônio Histórico e Artístico Nacional (SPHAN) através da Lei n.º 378, de 13 de janeiro de 1937, valorou-se a proteção de monumentos relacionados à tradição, impondo-se uma narrativa civilizatória hierarquizada do passado sobre o presente (Gonçalves, 2002, p. 117), narrativa esta escolhida e fomentada pelo próprio Estado.

Logo após a criação do SPHAN, o Decreto-Lei n.º 25, de 30 de novembro de 1937, que organiza a proteção do patrimônio histórico e artístico nacional, oficializou a salvaguarda dos bens dotados de excepcional valor arqueológico, etnográfico, bibliográfico ou artístico através do tombamento, cuja seleção dependia exclusivamente de

critérios adotados pela autoridade de agentes do SPHAN, mediante caráter discricionário e uma interpretação voltada à concepção de nação (Fonseca, 2017, p. 114).

Essa forma de conceber o patrimônio cultural permeou as décadas seguintes, findando teoricamente com a Constituição Federal de 1988, que reconheceu a diversidade cultural, encartando no §1º, do art. 216, diversos instrumentos para a salvaguarda e promoção do patrimônio cultural, listando, além de outras formas de acautelamento, inventários, registros, vigilância, tombamento, desapropriação, ou mesmo registro, oriundo do Decreto n.º 3.551, de 04 de agosto de 2000.

Assim como são realizados avanços na definição do patrimônio cultural brasileiro, há a constante necessidade de atualizar a maneira como os bens culturais são apresentados e comunicados à sociedade. A partir do ano de 2004, o Instituto do Patrimônio Histórico e Artístico Nacional (IPHAN) iniciou Projeto Sistemas de Informações, projeto visando acompanhar as mudanças tecnológicas, modernizar e computadorizar seu banco de dados.

Como aponta Abrantes (2014, p. 155) a informação em "diferentes formatos e distintos suportes, em vários arquivos nas unidades institucionais" dificulta sobremaneira a organização e a logística de um sistema integrado de informações sobre bens culturais, além da inerente necessidade de atingir e comunicar de forma completa e inteligível à população que por vezes não possui o devido letramento digital.

A Rede de Arquivos, repositório de documentos digitalizados do IPHAN que está em desenvolvimento desde 2013, e o Acervo Digital de Bens Culturais Registrados, são os principais meios de acesso às informações referentes ao patrimônio cultural brasileiro, entretanto, ainda não dispõem de sistema de pesquisa através de inteligência artificial capaz de refinar de refinar e processar os dados de maneira intuitiva e personalizada.

3.3 IA E PATRIMÔNIO CULTURAL

O ser humano possui como um de seus principais instrumentos para convivência em sociedade a informação. A informação possibilita e instiga a procura por novos saberes, possibilitando a formação de opiniões e concepções, que poderão ser aprofundadas e desenvolvidas, criando outras informações e conhecimentos (Machado, 2018, p. 25-26). Nesse contexto, a presença das tecnologias de inteligência artificial (IA) tem se tornado rotineira nas práticas sociais, impactando a forma como são obtidas e processadas as informações.

No Brasil, o Projeto de Lei n.º 2.338/2023, que atualmente se encontra em trâmite legislativo, busca as lacunas conceituais e principiológicas da utilização da inteligência artificial. Contudo, enquanto não é finalizado o processo legislativo, figura como linha guia a Estratégia Brasileira de Inteligência Artificial (EBIA).

Na EBIA constam como principais eixos a possibilidade de "promover o bem-estar social, o crescimento econômico e cultural, e de promover a inclusão por meio de suas aplicações", mediante a instituição de programas que assegurem a utilização da IA dessa forma (MCTI, 2021, p. 15). Logo, apesar das diversas obscuridades acerca do uso da IA, é possível conceber a sua utilização em prol da cultura, aplicando-se, também ao patrimônio cultural.

Nesse sentido, uma parceria entre a International Business Machines Corporation (IBM) e a Universidade de São Paulo, iniciada em 2023, "está utilizando tecnologias de Inteligência Artificial (IA) para fortalecer e revitalizar as línguas indígenas brasileiras" (Geiger, 2024). Para tanto, são utilizadas técnicas de processamento de linguagem natural (PLN), possibilitando o acesso de novas geração ao patrimônio cultural de comunidades indígenas (Geiger, 2024).

A associação de tecnologias de inteligência artificial com as ciências de voltadas à preservação cultural pode ser utilizada para fomentar e valorizar o patrimônio cultural (Oliveira, 2024, p. 32). Para tanto, é essencial a promoção de programas que possam sustentar o

desenvolvimento tecnológico nesta área, exigindo do Poder Público uma abordagem ativa e inovadora.

Assim, é indiscutível o esforço logístico do IPHAN ao catalogar e alimentar a Rede de Arquivos, entretanto, em um mundo globalizado onde os avanços tecnológicos são constantes, há a necessidade de serem desenvolvidos meios para não apenas disponibilizar bens culturais, mas que possam facilitar seu acesso e compreensão, utilizando-se, por exemplo do auxílio da inteligência artificial.

4. CONCLUSÕES

No presente estudo, foi abordado o patrimônio cultural brasileiro, sua trajetória e sua conexão com a inteligência artificial como possível meio facilitador do acesso e promoção dos bens culturais. Contudo, apesar dos esforços logísticos do IPHAN, não basta que a informação sobre os bens culturais seja catalogada, deve, assim como os próprios bens culturais, ser apresentada de forma acessível à comunidade, com o intuito de que esta possa absorvê-los e dar-lhes novos significados, ante a própria mutabilidade do patrimônio cultural brasileiro.

Assim, concluo que um dos caminhos é a inserção da inteligência artificial fomentada pelas informações e documentos do próprio IPHAN, como meio oficial de confiável de disseminação e promoção dos bens culturais, sendo este um caminho para futuras pesquisas e estudos do patrimônio cultural brasileiro.

REFERÊNCIAS

ABRANTES, Andreza Rigo. **Tecnologias Digitais como instrumentos de preservação do patrimônio urbano edificado**. 2014. Dissertação (Mestrado Profissional) – Instituto do Patrimônio Histórico e Artístico Nacional. Rio de Janeiro, 2014.

BRASIL. **Constituição (1988).** Constituição da República Federativa do Brasil. Diário Oficial [da] República Federativa do Brasil. Brasília, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 maio de 2025.

CUNHA FILHO, Francisco Humberto; MAGALHÃES, Allan Carlos Moreira. **É disso que o povo gosta:** o patrimônio cultural no cotidiano da comunidade. São Paulo: Dialética, 2024.

FONSECA, Maria Cecília Londres. **O patrimônio em processo:** trajetória da política federal de preservação no Brasil. 4.ed. Rio de Janeiro: Editora UFRJ, 2017.

FONSECA, Maria Cecília Londres. **Referências culturais: bases para novas políticas de patrimônio**. Boletim de Políticas Setoriais, nº 02. Brasília: IPEA, 2001.

GEIGER, Marina. **Preservação das línguas indígenas: Iniciativa da IBM e USP impulsiona o uso de IA para fortalecer culturas nativas**. Disponível em: <https://brasil.newsroom.ibm.com/preservacao-das-linguas-indigenas>. Acesso em: 14 maio de 2025.

GONÇALVES, José Reginaldo Santos. Monumentalidade e cotidiano: os patrimônios culturais como gênero de discurso. In: OLIVEIRA, Lucia Lippi de. (Org.). **Cidade:** história e desafios. Rio de Janeiro: Editora FGV, 2002.

MACHADO, Paulo Affonso Leme. **Direito à informação e meio ambiente**. São Paulo: Malheiros, 2018.

MCTI. **Estratégia Brasileira de Inteligência Artificial – EBIA**. Brasília: Ministério da Ciência, Tecnologia e Inovação, 2021.

OLIVEIRA, Vagner Inacio de. **Aprendizado de Máquina e Patrimônio Cultural:** Extração Automática de Metadados de Acervos Digitais de Museus Brasileiros na Plataforma Tainacan. 2024. Dissertação (Mestrado – Engenharia Elétrica) – Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas. Campinas, 2024.

PODER CONSTITUINTE DERIVADO REFORMADOR E NOVAS TECNOLOGIAS: MEIO AMBIENTE DIGITAL.

Vitor Luiz Maia da Silva Xavier

Mestrando em Direito Ambiental do Programa de Pós-Graduação em Direito Ambiental da Universidade do Estado do Amazonas – PPGDA/UEA. vitor.luiz2107@gmail.com.

Lincy Ester da Silva Parente

Pós-graduada (Especialista) em Direito Civil pela PUC/MG. lincy@ow.adv.br;

PALAVRAS-CHAVE: Constituição de 1988; Meio ambiente digital; Salvaguardas Constitucionais; Poder constituinte derivado; Inovações Tecnológicas.

1. OBJETIVOS:

O presente trabalho tem por objetivo analisar de que modo a Constituição Federal de 1988, por meio da atuação do poder constituinte derivado reformador, tem buscado se adaptar às transformações tecnológicas impostas pela sociedade da informação. A partir do reconhecimento do meio ambiente digital como uma nova dimensão do meio ambiente cultural, o estudo visa identificar as principais salvaguardas constitucionais que já garantem a proteção desse espaço e examinar como emendas constitucionais e propostas legislativas têm contribuído para assegurar direitos fundamentais nesse novo cenário digital.

2. METODOLOGIA:

A pesquisa desenvolvida é de natureza qualitativa, voltada à compreensão interpretativa da realidade jurídico-constitucional.

Adota-se o método dedutivo, partindo de premissas gerais sobre o poder constituinte e o conceito de meio ambiente para, então, examinar como a Constituição de 1988 se ajusta às novas demandas do meio ambiente digital. Quanto aos meios, a investigação é bibliográfica e documental, com análise de doutrina, legislação, jurisprudência e propostas de emenda constitucional.

3. DESENVOLVIMENTO DA PESQUISA:

3.1. MEIO AMBIENTE DIGITAL E A CONSTITUIÇÃO FEDERAL

Constituir, de acordo com o dicionário, significa "dar início a; organizar ou estabelecer". Nesse sentido, a Constituição de um Estado é o documento que dá origem e organiza sua estrutura, ela reúne todos os elementos essenciais ao Estado, como a organização dos poderes, os direitos e garantias fundamentais, dentre outros. Esse marco inicial, o nascimento de um Constituição, ocorre por meio do exercício do Poder Constituinte Originário.

Desse modo, o Poder Constituinte, de acordo com Santos (2022, p.143) "Consiste no Poder-Jurídico-Político de elaborar, criar e instituir a Constituição de um determinado Estado, bem como alterar, reformar e complementar essa Constituição." Ou seja, por meio desse Poder se inaugura bem como altera uma Constituição. Com relação a alteração, se faz por meio do Poder constituinte derivado reformador, através das emendas constitucionais.

Posto isso, o conceito de meio ambiente, conforme disposto na Lei nº 6.938/81 e no art. 225 da CF/88, é uno e indivisível, podendo ser abordado sob diferentes aspectos: natural, artificial, do trabalho e cultural. O meio ambiente digital surge como uma faceta contemporânea do meio ambiente cultural, reconhecido inclusive pelo Supremo Tribunal Federal (ADPF 857/2024).

Esse espaço virtual abriga relações humanas mediadas por tecnologias digitais, exigindo proteção jurídica similar à de ambientes físicos. Fiorillo (2025) destaca que o meio ambiente digital deve ser

cuidado com base nos princípios do direito ambiental. A crescente dependência tecnológica da sociedade impõe ao ordenamento jurídico o dever de acompanhar tais transformações.

3.2. SALVAGUARDAS CONSTITUCIONAIS APLICÁVEIS

A Constituição Federal de 1988 oferece um conjunto expressivo de salvaguardas que, embora elaboradas antes da ascensão da era digital, são plenamente aplicáveis à proteção do meio ambiente digital. A cidadania, prevista no art. 1º, inciso II, como um dos fundamentos da República, ganha novas dimensões no contexto da sociedade da informação, dando origem ao conceito de cidadania digital. Esta abrange o direito de acesso à internet, à informação e à proteção dos dados pessoais, fundamentais para a plena inclusão do indivíduo na vida social e política contemporânea.

O artigo 5º da Constituição é especialmente relevante nesse contexto, por abrigar garantias essenciais que se projetam sobre o ambiente digital. A liberdade de pensamento e de expressão, a inviolabilidade da vida privada, da honra e da imagem, bem como o direito de resposta, o acesso à informação e a proteção de dados pessoais, esta última recentemente reforçada pela Emenda Constitucional nº 115/2022, são todos dispositivos que sustentam uma base normativa para a atuação ética e segura no ciberespaço.

Além disso, os direitos culturais, expressos nos artigos 215 e 216, ampliam o reconhecimento do meio ambiente digital como parte integrante do patrimônio cultural, assegurando a todos o direito de acesso às fontes da cultura nacional e à preservação das formas de expressão popular. O capítulo dedicado à Comunicação Social, que abrange os artigos 220 a 224, complementa esse sistema de garantias ao assegurar a liberdade de manifestação do pensamento, da informação e da criação artística e científica, sem censura ou licença. Por fim, o artigo 225, que trata do direito ao meio ambiente ecologicamente equilibrado, deve ser interpretado de forma a incluir

a dimensão digital como espaço de vida e de relações humanas, exigindo, portanto, proteção jurídica condizente com sua relevância na contemporaneidade.

3.3. O PAPEL DO PODER CONSTITUINTE DERIVADO REFORMADOR

Diante das mudanças constantes provocadas pela transformação digital, o poder constituinte derivado reformador assume papel central na atualização da ordem constitucional. Desde sua promulgação, a Constituição de 1988 vem sendo modificada por diversas emendas, com o objetivo de incorporar novos direitos e ajustar o texto às exigências sociais, políticas e tecnológicas do país. A atuação desse poder tem sido crucial para garantir a longevidade da Constituição sem comprometer seus valores fundamentais.

A Emenda Constitucional nº 115, de 2022, representa um marco nesse processo, ao incluir a proteção de dados pessoais no rol dos direitos e garantias fundamentais. Essa medida reflete o esforço institucional de responder às demandas por segurança e privacidade na era digital. De modo complementar, surgem propostas como a PEC nº 47/2021, que busca inserir na Constituição o direito à inclusão digital, reconhecendo que o acesso à internet se tornou condição essencial para o exercício pleno da cidadania. A justificativa da proposta enfatiza que a internet é um meio de acesso à educação, saúde, trabalho e à informação, sendo, portanto, elemento estruturante da vida social contemporânea.

Mais recentemente, a PEC nº 29/2023 propôs incluir dispositivos constitucionais voltados à integridade mental e à transparência algorítmica, reconhecendo os impactos da inteligência artificial na vida cotidiana. A proposta reflete a preocupação com o uso ético e responsável das tecnologias emergentes, especialmente aquelas baseadas em algoritmos e sistemas autônomos. Tais iniciativas legislativas revelam o esforço do poder constituinte derivado em alinhar o texto constitucional com a realidade de uma sociedade

hiperconectada e dependente de soluções tecnológicas complexas, sem deixar de lado a proteção aos direitos fundamentais.

CONCLUSÃO.

A evolução tecnológica desafia constantemente o texto constitucional. O reconhecimento do meio ambiente digital como espaço que exige proteção jurídica é uma conquista interpretativa, mas também normativa, que se concretiza por meio do poder constituinte derivado reformador.

A Constituição de 1988 já contempla salvaguardas relevantes, mas a necessidade de atualização permanece, como demonstrado pelas recentes emendas e propostas legislativas. O desafio atual é assegurar que a proteção dos direitos fundamentais se estenda de forma plena ao ciberespaço, garantindo inclusão, segurança, ética e sustentabilidade digital.

REFERÊNCIAS .

Brasil. **Constituição da República Federativa do Brasil**. Brasília, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 01/06/2025.

Brasil. Senado Federal. **Proposta de Emenda à Constituição nº 29, de 2023.** Dispõe sobre a transparência algorítmica e a integridade mental no desenvolvimento científico e tecnológico. Brasília, DF: Senado Federal, 2023. Disponível em: https://legis.senado.leg.br/sdleggetter/documento?dm=9386704&ts=1733680966467&disposition=inline Acesso em: 01/06/2025.

Brasil. Senado Federal. **Proposta de Emenda à Constituição nº 47, de 2021**. Dispõe sobre a inclusão digital e o direito ao acesso à internet. Brasília, DF: Senado Federal, 2021. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9055515&ts=1719863399098&disposition=inline . Acesso em: 01/06/2025.

Brasil. Lei nº 6.938, de 31 de agosto de 1981. **Dispõe sobre a Política Nacional do Meio Ambiente, seus fins e mecanismos de formulação e aplicação, e dá outras providências**. 1981. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l6938.htm . Acesso em: 01/06/2025.

Brasil**.** Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental n. 857**. Relator: André Mendonça. Julgado em 01/06/2025.

Dicionário Online. **Constiuição**. Disponível em: https://www.dicionarioonline.com.br. Acesso em: 01/06/2025.

Fiorillo, Celso Antonio Pacheco. **Curso de Direito Ambiental Brasileiro**. São Paulo, Saraiva jur,2025.

Santos, Eduardo dos. **Manual de Direito Constitucional**. São paulo: editora juspodivim,2022.

REDEFININDO A PRIVACIDADE NA SOCIEDADE ALGORÍTMICA: IA, PROTEÇÃO DE DADOS E DIREITOS FUNDAMENTAIS NO BRASIL

Albefredo Melo de Souza Júnior

Advogado. Professor efetivo da Escola de Direito da Universidade Estadual do Amazonas (ED/UEA). Membro do Núcleo de Direito, Tecnologia e Inovação (LAWin/UEA). Mestre em Direito (Unilasalle/RS).

Yara Queiroz Freitas

Graduanda do 9° período do curso de Direito pela Universidade Estadual do Amazonas.

Palavras-chave: Privacidade, Lei Geral de Proteção de Dados (LGPD), Inteligência Artificial, Algoritmos, Direitos Fundamentais.

1. OBJETIVOS

Este artigo analisa como os algoritmos de Inteligência Artificial (IA) desafiam os direitos fundamentais no contexto da privacidade e da proteção de dados pessoais no Brasil. A partir de uma revisão das principais inovações tecnológicas — especialmente nas redes sociais e outros sistemas automatizados —, propomos uma redefinição do conceito de privacidade na era digital. A pesquisa examina os desafios legais, éticos e sociais do tratamento massivo de dados, com ênfase na legislação brasileira (Constituição Federal, LGPD, Marco Civil da Internet), e reflete sobre medidas necessárias para assegurar esses direitos em uma sociedade cada vez mais orientada por algoritmos. O trabalho visa, assim, contribuir para o debate acadêmico e jurídico sobre os caminhos de fortalecimento das garantias individuais diante dos avanços tecnológicos.

2. METODOLOGIA

A metodologia empregada consistiu em pesquisa bibliográfica e documental de natureza qualitativa. Foram consultados artigos científicos, livros de doutrina jurídica especializada em direito digital, proteção de dados e IA, legislação brasileira pertinente (Constituição Federal de 1988, Lei nº 13.709/2018 - LGPD, Lei nº 12.965/2014 - Marco Civil da Internet, Código Civil), jurisprudência selecionada dos tribunais superiores (STF e STJ), além de documentos e guias orientadores publicados pela Autoridade Nacional de Proteção de Dados (ANPD). Essa abordagem permitiu uma análise aprofundada das implicações jurídicas, éticas e sociais do uso de algoritmos de IA no contexto da proteção da privacidade e dos dados pessoais no Brasil.

3. DESENVOLVIMENTO

A acelerada expansão das tecnologias digitais, com destaque para a Inteligência Artificial (IA) e seus algoritmos, está transformando profundamente as dinâmicas sociais e a maneira como os dados pessoais são coletados, processados e utilizados. Embora essa transformação digital traga benefícios como serviços otimizados e experiências personalizadas, ela também cria desafios complexos para a privacidade e a proteção dos direitos fundamentais, exigindo uma análise jurídica cuidadosa e atualizada.

3.1. A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL E A AUTODETERMINAÇÃO INFORMATIVA

A Constituição Federal de 1988 (Art. 5º, X) e o Código Civil (Art. 21) protegem a intimidade, a vida privada, a honra e a imagem. No entanto, a ideia tradicional de privacidade como o simples "direito de ser deixado em paz" tornou-se insuficiente na sociedade da informação. Reconhecendo isso, a Emenda Constitucional nº 115/2022

elevou a proteção de dados pessoais à categoria de direito fundamental (Art. 5º, LXXIX, CF/88), reforçando sua importância e a necessidade de tutela pelo Estado.

Diante desse cenário, ganha destaque o conceito de autodeterminação informativa: o direito de cada pessoa controlar suas próprias informações, decidindo quem pode acessá-las, para quê e como. Esse poder de controle é a base da Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018), refletido em seus fundamentos (Art. 2º) e princípios (Art. 6º), como o respeito à privacidade e à própria autodeterminação informativa. A LGPD concretiza esse direito ao garantir aos titulares um conjunto de ferramentas para exercer esse controle (Art. 18), como o acesso aos seus dados, a correção, a exclusão, a oposição a certos tratamentos, a informação sobre com quem os dados são compartilhados e, fundamentalmente, a possibilidade de retirar o consentimento previamente dado (Art. 8º, §5º). Cumpre destacar que o Habeas Data (Art. 5º, LXXII, CF/88) já é um instrumento constitucional que garante o acesso e a retificação de informações pessoais.

Todavia, a coleta massiva e automatizada de dados (comportamento online, localização, interações, biometria) por algoritmos de IA frequentemente ocorre com base em consentimentos vagos ou pouco claros. Isso viola o princípio da transparência exigido pela LGPD (Art. 6º, VI) e enfraquece a capacidade do indivíduo de controlar suas informações. Esse modelo alimenta o chamado 'capitalismo de vigilância', termo cunhado por Shoshana Zuboff (2019). Trata-se de um fenômeno que transforma dados pessoais em ativos econômicos, utilizados para prever comportamentos, moldar decisões dos usuários e direcionar publicidade. Esse processo, frequentemente em desconformidade com os direitos dos titulares, contribui para a dissolução da linha entre o público e o privado nas interações digitais. Além disso, a exposição constante nas plataformas pode comprometer a autonomia e afetar a dignidade das pessoas.

3.2. ALGORITMOS DE IA, NOVAS AMEAÇAS E A RESPONSABILIDADE DIGITAL

Os algoritmos que operam em redes sociais e sistemas de recomendação, frequentemente otimizados para maximizar o engajamento, podem inadvertidamente criar 'bolhas informacionais' e 'câmaras de eco'. Essa dinâmica limita a exposição dos usuários a perspectivas diversas e reforça vieses preexistentes, contribuindo para a polarização do debate público e expondo as pessoas a desinformação e conteúdos de baixa qualidade, o que afeta diretamente a formação de opinião.

Ademais, um risco inerente e grave associado à Inteligência Artificial é o viés algorítmico. Quando algoritmos são treinados com dados históricos que refletem preconceitos sociais, eles podem não apenas reproduzir, mas até intensificar discriminações baseadas em critérios como raça ou gênero em diversas aplicações, desde reconhecimento facial até análise de crédito. A Lei Geral de Proteção de Dados (LGPD) proíbe expressamente o tratamento de dados para fins discriminatórios (Art. 6º, IX), impondo um dever de cuidado aos responsáveis pelo tratamento. Todavia, a dificuldade em compreender como o algoritmo toma suas decisões - o chamado problema da 'caixa-preta' - representa um obstáculo significativo para identificar e corrigir esses vieses.

Os deepfakes representam um desafio crescente, esses são capazes de gerar vídeos e áudios falsos extremamente realistas, minando a confiança na informação e nas instituições. A disseminação maliciosa desses conteúdos pode causar danos reputacionais severos, manipular a opinião pública, especialmente em períodos eleitorais, e até incitar violência. Embora o Brasil ainda não possua uma tipificação penal específica para 'deepfakes', tais condutas podem ser enquadradas em crimes já existentes (como os contra a honra, falsidade ideológica ou estelionato), a depender do caso concreto. O debate legislativo sobre o tema está em curso, como demonstra o PL 2630/2020 (PL das Fake News), que visa abordar a desinformação

de forma mais ampla (Ressalta-se que este projeto de lei ainda está em tramitação no Congresso Nacional, sujeito a alterações em seu texto e conteúdo). A responsabilidade civil pelos danos causados é igualmente crucial, envolvendo a identificação dos criadores e a eventual responsabilização das plataformas digitais, conforme as regras do Marco Civil da Internet.

A própria velocidade algorítmica das redes sociais também potencializa fenômenos como a **'cultura do cancelamento'**. Julgamentos públicos sumários, muitas vezes baseados em informações parciais ou falsas, podem levar à destruição de reputações e ao ostracismo social. Juridicamente, essa questão reside na complexa tensão entre a liberdade de expressão, garantida pela Constituição e pelo Marco Civil, e a proteção aos direitos da personalidade (honra, imagem), assegurada pela Constituição e pelo Código Civil. O Supremo Tribunal Federal (STF), no julgamento do Tema 786, estabeleceu que o 'direito ao esquecimento' (entendido como o poder de impedir a divulgação de fatos verídicos do passado) não se aplica de forma irrestrita no Brasil, mas ressalvou a possibilidade de análise de abusos na liberdade de expressão. A responsabilidade das plataformas por conteúdos gerados por terceiros segue, em regra, o disposto no Art. 19 do Marco Civil, que exige ordem judicial para remoção (salvo exceções), sendo a LGPD também aplicável devido ao tratamento de dados pessoais envolvido."

3.3. DESAFIOS DA REGULAÇÃO, ACCOUNTABILITY ALGORÍTMICA E O PAPEL DA ANPD

Apesar da LGPD e da proteção de dados como direito fundamental, regular a IA e proteger dados eficazmente ainda apresenta desafios. A tecnologia avança rapidamente, e a complexidade dos algoritmos dificulta a fiscalização.

Um conceito chave é a **accountability algorítmica**, ou seja, a responsabilização por decisões algorítmicas. A LGPD exige que os agentes de tratamento demonstrem ter adotado medidas para

cumprir a lei (princípio da responsabilização, Art. 6º, X). Para a IA, isso significa ter mecanismos para entender, auditar e responder por decisões automatizadas, especialmente as de grande impacto. A "opacidade" de muitos sistemas (a dificuldade em explicar a decisão) é um obstáculo. A LGPD garante ao titular o direito de pedir a revisão de decisões automatizadas que afetem seus interesses (Art. 20), mas a utilidade desse direito depende da capacidade de fornecer explicações claras (explicabilidade).

A Autoridade Nacional de Proteção de Dados (ANPD) tem um papel central. Ela deve zelar pela proteção de dados, criar normas, fiscalizar e aplicar sanções (Art. 55-J, LGPD). A ANPD busca trazer segurança jurídica publicando guias (sobre agentes de tratamento, segurança, etc.) e resoluções (como a que trata de pequenas empresas - Res. CD/ANPD nº 2/2022). Sua atuação na fiscalização do uso de IA e na orientação sobre temas como avaliação de impacto à proteção de dados será essencial.

Outros desafios persistem, como identificar responsáveis em cadeias complexas de tratamento ou combater a disseminação internacional de deepfakes. A moderação de conteúdo online permanece como um ponto de tensão entre proteger direitos e garantir a liberdade de expressão (o STF debate a constitucionalidade do Art. 19 do Marco Civil). Ademais, discute-se a necessidade de uma lei específica para IA no Brasil (como o PL 21/2020), que busca definir princípios e regras para o desenvolvimento e uso da tecnologia, muitas vezes com base na análise de riscos. A título de comparação, na União Europeia, a proposta do AI Act estabelece parâmetros rigorosos de avaliação de risco e exigências de transparência para sistemas de IA, servindo como referência relevante para o debate regulatório brasileiro.

4. CONCLUSÃO

A sociedade digital, cada vez mais dependente de algoritmos e IA, enfrenta o desafio de proteger a privacidade e os dados pessoais, agora direitos fundamentais no Brasil. A natureza fluida da privacidade na era digital exige não só repensar o conceito à luz da autodeterminação informativa, mas também adaptar e aplicar as leis existentes para lidar com as novas vulnerabilidades tecnológicas.

Embora a LGPD seja um avanço crucial, sua aplicação prática diante da complexidade dos algoritmos ainda encontra obstáculos. A proteção efetiva dos direitos fundamentais requer o combate aos vieses algorítmicos, respostas jurídicas às ameaças de deepfakes e desinformação, e uma análise crítica das dinâmicas de poder nas plataformas digitais. Garantir transparência (na medida do possível), mecanismos eficazes de responsabilização (accountability) e reparação de danos, além de promover a educação digital, são passos indispensáveis para um ambiente digital mais justo e seguro.

A complexidade do tema exige a colaboração de diferentes setores da sociedade. Isso inclui o governo — como o Legislativo, o Judiciário e a Autoridade Nacional de Proteção de Dados (ANPD) —, o setor privado, representado por desenvolvedores, plataformas e empresas, além da sociedade civil. Somente através do diálogo e da construção de soluções jurídicas, técnicas e éticas será possível garantir que a tecnologia, especialmente a IA, sirva à dignidade humana e aos direitos fundamentais. O desafio contemporâneo não é impedir o avanço tecnológico, mas assegurar que ele se desenvolva em consonância com os valores fundamentais da dignidade humana, da privacidade e da democracia.

REFERÊNCIAS BIBLIOGRÁFICAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado*. Versão 2.0. Brasília: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 1 jun. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Resolução CD/ANPD nº 2, de 27 de janeiro de 2022*. Dispõe sobre a aplicação da Lei nº 13.709/2018 para agentes de tratamento de pequeno porte. *Diário Oficial da União*, Brasília, DF, 28 jan. 2022. Seção 1, p. 43.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 3. ed. Rio de Janeiro: Forense, 2021.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 1 jun. 2025.

BRASIL. *Lei nº 10.406, de 10 de janeiro de 2002*. Institui o Código Civil. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 1 jun. 2025.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 1 jun. 2025.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República.

Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 1 jun. 2025.

BRASIL. Supremo Tribunal Federal. *Recurso extraordinário (RE) 1.010.606/RJ*. Relator: Min. Dias Toffoli. Julgado em: 11 fev. 2021. Repercussão Geral – Tema 786.

BRASIL. Supremo Tribunal Federal. *Ações diretas de inconstitucionalidade (ADI) 6387, 6388, 6389, 6390 e 6393*. Medida Provisória nº 954/2020. Compartilhamento de dados de usuários de telefonia com o IBGE. Relatora: Min. Rosa Weber. Julgado em: 7 maio 2020. Medida cautelar.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de internet*. 2. ed. São Paulo: Juarez de Oliveira, 2008.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD: Lei Geral de Proteção de Dados Pessoais comentada*. 4. ed. São Paulo: Thomson Reuters Brasil, 2022.

MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang (coords.). *Tratado de proteção de dados pessoais*. 2. ed. Rio de Janeiro: Forense, 2022.

SOUZA, Carlos Affonso Pereira de. *Direito e internet: a regulamentação das redes*. Curitiba: Juruá, 2016.

TEIXEIRA, Tarcízio; LEMOS, Ronaldo (coords.). *Marco Civil da Internet*. São Paulo: Atlas, 2014.

USO INDEVIDO DE IMAGENS EM PLATAFORMAS DIGITAIS: UMA ANÁLISE DO CONTROLE SOBRE A PRÓPRIA IMAGEM À LUZ DAS NOVAS TECNOLOGIAS DE COMUNICAÇÃO

MISUSE OF IMAGES ON DIGITAL PLATFORMS: A LEGAL ANALYSIS OF THE RIGHT TO IMAGE AUTONOMY IN THE CONTEXT OF EMERGING COMMUNICATION TECHNOLOGIES

Maria Clara Santana Barros de Oliveira[1]
Yasmim Ferreira Derzi2
Franklin Carioca Cruz3

RESUMO

O presente trabalho visa discutir os desafios jurídicos e sociais decorrentes do uso indevido de imagens em plataformas digitais, especialmente diante do avanço acelerado das tecnologias de comunicação. A pesquisa analisa os mecanismos de proteção do direito à imagem no ambiente virtual, destacando os entraves à tutela da privacidade, da honra e da dignidade da pessoa humana. Considerando o aumento exponencial de casos envolvendo exposição não autorizada, compartilhamento indevido e uso comercial sem consentimento, busca-se compreender de que maneira o ordenamento jurídico brasileiro responde a essas demandas e quais os limites do controle sobre a própria imagem no ambiente digital.

Palavras-chave: Direito à imagem; privacidade; personalidade; inovação; legislação.

Keywords: Right to image; privacy; personality; innovation; legislation.

1. OBJETIVOS

1.1. Objetivo Geral: Analisar os desafios jurídicos e sociais relacionados ao uso indevido de imagens em plataformas digitais, à luz do ordenamento jurídico brasileiro, com ênfase na proteção dos direitos da personalidade, especialmente o direito à imagem, à privacidade, à honra e à dignidade da pessoa humana, consagrados no artigo 5º da Constituição Federal.

1.2. Objetivos Específicos:

1.2.1. Investigar os fundamentos legais que amparam o direito à imagem no Brasil e sua aplicação no contexto digital contemporâneo.

1.2.2. Identificar os principais tipos de violações envolvendo o uso não autorizado de imagens nas plataformas digitais, como exposição indevida, vazamentos e uso comercial sem consentimento.

1.2.3. Avaliar os limites e as possibilidades de controle sobre a própria imagem no ambiente digital diante da rápida evolução tecnológica e da difusão de ferramentas como deepfakes.

1.2.4. Promover uma reflexão sobre a eficácia das normas jurídicas vigentes e apontar possíveis lacunas legislativas ou interpretativas que dificultam a proteção efetiva do direito à imagem na esfera virtual.

2. METODOLOGIA

Foi utilizado uma abordagem qualitativa com objetivo descritivo com o método dedutivo para o desenvolvimento do trabalho, baseado em uma revisão bibliográfica e documental, que incluiu o estudo de artigos científicos, livros doutrinários especializados e materiais acadêmicos que abordam o direito à imagem e o uso indevido no contexto das plataformas digitais.

Além da análise teórica, foi realizada uma pesquisa jurisprudencial detalhada, focando em casos específicos que foram

objeto de julgamento de mérito no Brasil, tanto em Tribunais Estaduais quanto no Superior Tribunal de Justiça (STJ). Esses casos envolvem a divulgação não autorizada de imagens pessoais, vazamento de fotos íntimas, uso indevido de imagens em campanhas publicitárias e manipulações digitais, como deepfakes, que afetaram diretamente a honra, a privacidade e a dignidade das vítimas.

3. DESENVOLVIMENTO DA PESQUISA

O direito à imagem, como expressão dos direitos da personalidade, possui respaldo jurídico na Constituição Federal de 1988, que em seu artigo 5º, incisos V e X, assegura a indenização por dano material e moral decorrente de sua violação, e garante a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas. No âmbito infraconstitucional, o Código Civil (arts. 11 a 21) trata da proteção da personalidade, dispondo que o exercício desses direitos é intransmissível, irrenunciável e limitado pelo interesse social e pelos direitos de terceiros. A Lei Geral de Proteção de Dados (Lei nº 13.709/2018), por sua vez, ampliou o arcabouço protetivo ao considerar a imagem um dado pessoal sensível, exigindo consentimento expresso e finalidade legítima para seu tratamento. Isso significa que, mesmo quando uma imagem é divulgada inicialmente de forma voluntária, seu uso posterior, principalmente com fins comerciais ou sensacionalistas, exige nova autorização — sob pena de configurar ato ilícito. Tal interpretação já encontra eco na jurisprudência, como nos casos de uso indevido de imagens íntimas ou privadas em contextos diversos do originalmente consentido, em que o Superior Tribunal de Justiça tem reconhecido a existência de dano moral e fixado indenizações com base no método bifásico de arbitramento.

As novas tecnologias digitais, especialmente as que envolvem inteligência artificial e manipulação de conteúdo visual — como os *deepfakes* —, têm aprofundado os dilemas jurídicos relacionados ao controle sobre a própria imagem. Trata-se de uma problemática

ainda não enfrentada de forma sistemática pela legislação brasileira, gerando uma lacuna normativa em relação à responsabilização de criadores e divulgadores desse tipo de conteúdo. Danilo Doneda (2006) já advertia sobre a fragilidade da legislação frente à velocidade das inovações tecnológicas e defendia a criação de um regime jurídico próprio para dados sensíveis, com maior proteção processual e civil. Ingo Sarlet (2012), por sua vez, enfatiza que a dignidade da pessoa humana — enquanto fundamento da República — deve guiar a interpretação jurídica sempre que a exposição da imagem comprometer a identidade moral do indivíduo. A jurisprudência, embora ainda incipiente no que tange aos *deepfakes*, têm sinalizado um esforço hermenêutico para adaptar os dispositivos civis existentes às novas realidades, reconhecendo a responsabilidade objetiva em determinadas hipóteses, sobretudo quando há relação de consumo ou envolvimento de plataformas digitais com fins lucrativos.

Seguindo uma análise mais objetiva da pesquisa, torna-se indispensável apresentar os casos mais recorrentes envolvendo o uso indevido da imagem no ambiente digital. No atual cenário das tecnologias de informação, é frequente o compartilhamento de imagens entre pessoas que mantêm relações afetivas ou vínculos de confiança. No entanto, observa-se um crescimento exponencial de casos em que essas imagens são divulgadas sem autorização, prática que, apesar de cada vez mais comum, ainda é subestimada por grande parte da população, que tende a negligenciar os seus efeitos jurídicos e sociais.

Diante dessa realidade, o Superior Tribunal de Justiça (STJ) tem consolidado entendimento no sentido de que a divulgação de imagens ou conteúdos íntimos fora do contexto da relação afetiva configura ato ilícito, ensejando o dever de indenizar. As decisões reconhecem que a violação da privacidade, da honra e da dignidade da vítima, especialmente quando perpetrada por pessoa com quem mantinha relação de confiança, é passível de reparação civil, com a fixação de valores compensatórios proporcionais à extensão dos danos sofridos. Esse posicionamento foi reforçado, por exemplo, em decisão

proferida pelo STJ no ano de 2017, que analisou caso de divulgação não autorizada de conteúdo íntimo.

RECURSO ESPECIAL. ART. 535 DO CPC/1973. NÃO VIOLAÇÃO. DANO MORAL. VALOR DA INDENIZAÇÃO. EXCEPCIONALIDADE. INTERVENÇÃO DO STJ. DIREITO À INTIMIDADE, PRIVACIDADE, HONRA E IMAGEM. VALOR DA INDENIZAÇÃO. CRITÉRIOS DE ARBITRAMENTO EQUITATIVO. MÉTODO BIFÁSICO. VALOR BÁSICO E CIRCUNSTÂNCIAS ESPECÍFICAS DO CASO. CONDUTA QUE CONFIGURA SEXTING E CIBERBULLYING.[..] **4. Devem ser considerados como pertencentes à vida privada da pessoa não só os fatos da vida íntima, como todos aqueles em que não haja o interesse da sociedade de que faz parte. 5. A revelação de fatos da vida íntima da pessoa, consubstanciada na divulgação, pela internet, de fotografias no momento em que praticava atos de cunho sexual, em local reservado e não acessível ao público em geral, assim como nos juízos de valor e na difamação que se seguiram às publicações, são capazes de causar à vítima transtornos imensuráveis, injustificáveis, a merecer reprimenda adequada.[...]** 12. Recurso especial parcialmente provido. (REsp n. 1.445.240/SP, relator Ministro Luis Felipe Salomão, Quarta Turma, julgado em 10/10/2017, DJe de 22/11/2017.

Além dos casos derivados de relações interpessoais, há situações envolvendo o uso indevido da imagem com finalidade econômica. Trata-se de práticas em que terceiros, sem qualquer autorização, se apropriam de imagens publicadas na internet, seja por particulares ou por veículos de comunicação, visando obter lucro, ampliar audiência ou gerar engajamento nas redes sociais. Esse tipo de conduta, além de violar direitos da personalidade, acarreta prejuízos significativos à vítima, que muitas vezes sequer consentiu com a divulgação original.

Exemplo emblemático dessa modalidade de violação é o caso julgado, no qual uma mulher grávida, vítima de um acidente que a deixou tetraplégica, foi exposta publicamente. Durante o parto, ocorrido em ambiente hospitalar, a equipe médica realizou filmagens não autorizadas, que posteriormente foram divulgadas em redes

sociais e em páginas de veículos de comunicação de ampla circulação, sem o consentimento da paciente.

CIVIL. AGRAVO INTERNO NO AGRAVO EM RECURSO ESPECIAL. DECISÃO DA PRESIDÊNCIA. RECONSIDERAÇÃO. USO INDEVIDO DE IMAGEM. PUBLICAÇÃO NÃO AUTORIZADA. DANOS MORAIS. CABIMENTO. QUANTUM INDENIZATÓRIO ADEQUADO. AGRAVO INTERNO PROVIDO PARA CONHECER DO AGRAVO EM RECURSO ESPECIAL. RECURSO ESPECIAL DESPROVIDO.[...] 2. "A jurisprudência deste Tribunal se firmou no sentido de que a publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais gera o dever de indenização por danos morais, embora não haja conotação ofensiva ou vexatória" (AgInt no AREsp 1.790.362/PB, Relator Ministro RAUL ARAÚJO, Quarta Turma, julgado em 23/8/2021, DJe de 24/9/2021). [...] (AgInt no AREsp n. 1.983.027/SP, relator Ministro Raul Araújo, Quarta Turma, julgado em 17/3/2025, DJEN de 25/3/2025.)

Tal conduta resultou em grave afronta à sua privacidade, dignidade e integridade, demonstrando de forma clara a urgência da tutela efetiva dos direitos da personalidade no contexto digital.

4. CONSIDERAÇÕES FINAIS

Diante do cenário complexo e dinâmico proporcionado pelas plataformas digitais, evidencia-se que o uso indevido de imagens representa um dos principais desafios à proteção dos direitos da personalidade na contemporaneidade. A pesquisa demonstrou que, embora o orde ordenamento jurídico brasileiro disponha de fundamentos normativos sólidos — como os previstos na Constituição Federal, no Código Civil e na Lei Geral de Proteção de Dados —, há entraves significativos quanto à sua efetividade diante das novas tecnologias, sobretudo aquelas que permitem a rápida disseminação e manipulação de conteúdo visual.

A análise jurisprudencial reforça a percepção de que o Poder Judiciário tem buscado acompanhar essas transformações,

reconhecendo a gravidade de violações relacionadas à imagem pessoal, à privacidade e à dignidade humana. Contudo, também revela a existência de lacunas interpretativas e normativas, especialmente no enfrentamento de práticas mais sofisticadas como os deepfakes e o uso comercial indevido de imagens sem consentimento expresso.

Portanto, é essencial que as plataformas digitais adotem uma postura mais ativa na proteção do direito à imagem, implementando protocolos obrigatórios de remoção rápida de conteúdos ilícitos, como já ocorre em iniciativas da *SaferNet* com o Ministério Público. Também é necessário fortalecer as Defensorias Públicas e órgãos de proteção ao consumidor, garantindo atendimento célere às vítimas, especialmente em casos de vazamento de imagens íntimas. A inclusão da educação digital crítica nas escolas e a capacitação contínua de operadores do Direito em temas tecnológicos são medidas fundamentais para enfrentar, de forma eficaz e humanizada, as violações de direitos no ambiente virtual. Essas ações articuladas representam um caminho concreto para a construção de uma tutela jurídica mais eficiente frente aos desafios da era digital.

REFERÊNCIAS

AMARAL, Anderson. A ação de indenização por exposição à imagem em redes sociais e a violação dos direitos fundamentais. *JusBrasil*, 2016. Disponível em: https://www.jusbrasil.com.br/artigos/a-acao-de-indenizacao-por-exposicao-a-imagem-em-redes-sociais-e-a-violacao-dos-direitos-fundamentais/381890368. Acesso em: 24 maio 2025.

BRASIL. Superior Tribunal de Justiça. *AgRg no AREsp 1.790.362/PB*. Relator: Ministro Raul Araújo. Quarta Turma. Julgado em 22 set. 2020. Publicado em 28 set. 2020. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?b=ACOR&livre=AREsp+1.790.362%2FPB&O=JT. Acesso em: 24 maio 2025.

BRASIL. Superior Tribunal de Justiça. *AInt no AREsp 2.461.673/SP*. Relator: Ministro Marco Aurélio Bellizze. Terceira Turma. Julgado em 12 dez. 2022. Publicado em 15 dez. 2022. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?2461673. Acesso em: 23 maio 2025.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

JURISPRUDÊNCIAS DO STJ. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?b=ACOR&livre=uso+indevido+de+imagem&O=JT. Acesso em: 24 maio 2025.

MARGALHO, Rafael Andrade de. Redes sociais digitais e direitos da personalidade. *Revista do Judiciário Brasileiro – ReJuB*, Edição Especial Direito Digital, Brasília, p. 641-666, jul./dez. 2023. Disponível em: https://revistadaenfam.emnuvens.com.br/renfam/article/view/238/96. Acesso em: 24 maio 2025.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*. Porto Alegre: Livraria do Advogado, 2012. Disponível em: https://www.

mprj.mp.br/documents/20184/172905/a_eficacia_dos_direitos_fundamentais_2012.pdf. Acesso em: 24 maio 2025.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS (TJDFT). Direito de imagem. *Direito Fácil – Edição semanal.* Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/direito-de-imagem. Acesso em: 24 maio 2025.