

**XIV ENCONTRO INTERNACIONAL
DO CONPEDI BARCELOS -
PORTUGAL**

**GOVERNO DIGITAL, DIREITO E NOVAS
TECNOLOGIAS**

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Profa. Dra. Samyra Haydêe Dal Farra Napolini - FMU - São Paulo

Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Relações Internacionais para o Continente Americano:

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do Sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

Relações Internacionais para os demais Continentes:

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

Educação Jurídica

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR

Prof. Dr. Rubens Beçak - USP - SP

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - MS

Eventos:

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Comissão Especial

Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG

Prof. Dr. Rogério Borba - UNIFACVEST - SC

G326

Governo digital, direito e novas tecnologias [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Ana Catarina Almeida Loureiro; Danielle Jacon Ayres Pinto; José Renato Gaziero Cella. – Barcelos, CONPEDI, 2025.

Inclui bibliografia

ISBN: 978-65-5274-207-0

Modo de acesso: www.conpedi.org.br em publicações

Tema: Direito 3D Law

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Internacionais. 2. Governo digital. 3. Direito e novas tecnologias. XIV Encontro Internacional do CONPEDI (3; 2025; Barcelos, Portugal).

CDU: 34



XIV ENCONTRO INTERNACIONAL DO CONPEDI BARCELOS - PORTUGAL

GOVERNO DIGITAL, DIREITO E NOVAS TECNOLOGIAS

Apresentação

No XIV Encontro Internacional do CONPEDI, realizado nos dias 10, 11 e 12 de setembro de 2025, o Grupo de Trabalho - GT “Governo Digital, Direito e Novas Tecnologias”, que teve lugar na tarde de 12 de setembro de 2025, destacou-se no evento não apenas pela qualidade dos trabalhos apresentados, mas pelos autores dos artigos, que são professores pesquisadores acompanhados de seus alunos pós-graduandos. Foram apresentados artigos objeto de um intenso debate presidido pelos coordenadores e acompanhado pela participação instigante do público presente no Instituto Politécnico do Cávado e do Ave - IPCA, em Barcelos, Portugal.

Esse fato demonstra a inquietude que os temas debatidos despertam na seara jurídica. Cientes desse fato, os programas de pós-graduação em direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao direito. Para apresentar e discutir os trabalhos produzidos sob essa perspectiva.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema “Governo Digital, Direito e Novas Tecnologias”. Trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em direito, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores

Prof. Dr. José Renato Gaziero Cella

**INTELIGÊNCIA ARTIFICIAL E SEUS IMPACTOS NA PROTEÇÃO DE DADOS E
NO DIREITO PENAL: ESTUDO DA LEGISLAÇÃO BRASILEIRA À LUZ DO
DIREITO COMPARADO**

**ARTIFICIAL INTELLIGENCE AND ITS IMPACTS ON DATA PROTECTION AND
CRIMINAL LAW: A STUDY OF BRAZILIAN LEGISLATION IN LIGHT OF
COMPARATIVE LAW**

**Renata Apolinário de Castro Lima
Gil César de Carvalho Lemos Morato
Roberto Apolinário de Castro**

Resumo

O artigo analisa a interseção entre a inteligência artificial (IA), a proteção de dados pessoais e o Direito Penal, com foco no ordenamento jurídico brasileiro e em comparações internacionais. Inicialmente, apresenta-se a evolução da IA e os desafios éticos e jurídicos envolvidos, destacando-se a necessidade de equilíbrio entre inovação tecnológica e proteção dos direitos fundamentais. Em seguida, examina-se o regime jurídico brasileiro de proteção de dados, com ênfase na Constituição da República de 1988 e Lei Geral de Proteção de Dados (LGPD), à luz do uso intensivo de dados pela IA traçando paralelos com o Regulamento Geral sobre a Proteção de Dados (GDPR), da União Europeia. No campo penal, discute-se a utilização de sistemas de IA na segurança pública, no processo penal e na investigação criminal, considerando benefícios e riscos relacionados à privacidade, à não discriminação, ao devido processo legal e às garantias fundamentais. Analisa-se também o cenário normativo brasileiro, com destaque para propostas legislativas voltadas à regulamentação da IA, bem como, experiências estrangeiras. A metodologia adotada é descritiva e crítica, combinando análise normativa, doutrinária e empírica. Conclui-se com sugestões de aprimoramento normativo para que o desenvolvimento da IA ocorra em conformidade com os princípios da dignidade humana, da liberdade e da proteção de dados.

Palavras-chave: Inteligência artificial, Proteção de dados, Direito penal, Privacidade, Legislação brasileira

article discusses the use of AI systems in public security, criminal procedure, and criminal investigations, considering benefits and risks related to privacy, non-discrimination, due process, and fundamental guarantees. It also analyzes the Brazilian regulatory landscape, highlighting legislative proposals aimed at AI regulation, as well as foreign experiences. The methodology adopted is descriptive and critical, combining normative, doctrinal, and empirical analysis. The article concludes with suggestions for regulatory improvements to ensure that AI development aligns with the principles of human dignity, freedom, and data protection.

Keywords/Palabras-claves/Mots-clés: Artificial intelligence, Data protection, Criminal law, Privacy, Brazilian legislation

1 INTRODUÇÃO

A evolução acelerada da Inteligência Artificial (IA), entendida como ramo da computação que simula a capacidade humana de aprender, decidir e solucionar problemas, por meio de algoritmos avançados, tem provocado profundas transformações sociais.

Essas mudanças, impõem novos desafios à ordem jurídica, especialmente, nas áreas da proteção de dados pessoais e do Direito Penal, diante do uso massivo de informações e automação de decisões, antes exclusivamente humanas.

No Brasil e no mundo, intensificam-se os debates sobre como regulamentar a IA de forma a “promover a inovação tecnológica, sem comprometer direitos fundamentais dos indivíduos” (Bird, 2020).

No campo da proteção de dados e privacidade, a crescente capacidade da IA de coletar, cruzar e analisar grandes volumes de informações pessoais, impõe desafios significativos ao arcabouço jurídico vigente, notadamente, quanto à proteção dos direitos fundamentais e à autodeterminação informativa.

Frequentemente, dados pessoais tensionam os marcos legais existentes. No Brasil, a Constituição da República de 1988 consagra, de forma implícita, os direitos à intimidade, vida privada e sigilo das comunicações (BRASIL, 1988), enquanto a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) estabelece um regime abrangente de proteção, inspirado em normas internacionais como o GDPR da União Europeia (UNIÃO EUROPEIA, 2016).

Contudo, a aplicação desses diplomas legais, frente à IA suscita questões complexas, como a responsabilização, transparência algorítmica e efetividade dos direitos dos titulares, envolvendo temas como “transparência de algoritmos, possibilidade de discriminação algorítmica e o controle do titular sobre seus dados em sistemas automatizados” (Diakopoulos, 2016; Dieter, 2016, p. 38-41).

No Direito Penal, o uso de IA por órgãos de segurança pública e Judiciário apresenta uma dualidade: “de um lado, ferramentas de IA prometem aperfeiçoar a eficiência da investigação criminal, a análise de evidências e a uniformização de decisões; de outro, alertam juristas e acadêmicos para riscos significativos à preservação de garantias processuais e de direitos fundamentais” (Piló; Brasil, 2024, p. 272-299).

Tecnologias como reconhecimento facial em massa, policiamento preditivo e algoritmos judiciais podem gerar “violações à privacidade, discriminação de grupos minoritários e enfraquecimento do controle humano sobre atos estatais com potencial de restrição da liberdade individual” (Angwin, 2016, p. 14).

Esse cenário suscita importantes questionamentos sobre os limites jurídicos do uso da IA, bem como sobre a necessidade de criação de normas específicas que assegurem que a busca por eficiência não se sobreponha à justiça e à dignidade humana.

Diante disso, este artigo tem por objetivo analisar criticamente o estado atual da legislação brasileira aplicável à IA, com ênfase na proteção de dados e no Direito Penal, contrastando-o com experiências normativas estrangeiras.

Serão examinados os principais marcos normativos-legais, constitucionais e infralegais, com o intuito de identificar lacunas, riscos e possibilidades de aprimoramento. O estudo articula doutrina clássica, como Beccaria (2000) e Foucault (1987), com contribuições contemporâneas sobre a relação entre IA e Direito.

Espera-se, com isso, identificar avanços, deficiências e caminhos de aprimoramento normativo. O trabalho organiza-se em capítulos: o 2 trata dos aspectos gerais da IA e seus desafios regulatórios; o 3 analisa a proteção de dados pessoais no contexto da IA, no Brasil e no exterior; o 4 discute os impactos da IA no Direito Penal, com enfoque nos riscos e respostas jurídicas; e o 5 apresenta as considerações finais e propostas.

2 DESAFIOS REGULATÓRIOS DA INTELIGÊNCIA ARTIFICIAL: PROTEÇÃO DE DADOS E DIREITO PENAL

A rápida evolução da Inteligência Artificial insere em evidência a dificuldade das estruturas jurídicas em se adaptarem ao ritmo da inovação tecnológica. Desde a formulação do projeto pioneiro de pesquisa em IA, na década de 1950, os avanços nesse campo confrontam os modelos normativos tradicionais, sobretudo, no que diz respeito à responsabilização, à proteção de dados pessoais e aos limites éticos da atuação automatizada.

A crescente assimetria entre o avanço tecnológico e a regulação jurídica tem se intensificado, impondo aos juristas, legisladores e operadores do Direito, a necessidade de uma reflexão contínua sobre a suficiência e atualidade dos marcos legais, diante das transformações promovidas pela Inteligência Artificial à nova realidade imposta pela era algorítmica. Na conferência de Dartmouth, em 1956 (Nerdia, 1956), até os modernos sistemas de aprendizado de máquina e IA generativa, o avanço tecnológico, em regra, precede a elaboração de normas jurídicas específicas, gerando lacunas regulatórias que desafiam a eficácia do ordenamento jurídico.

Como ressaltado por Kevin Ashley, “a ética é um componente crucial no desenvolvimento e na implementação da IA no Direito” (Ashley, 2017, p. 35, tradução nossa),

destacando-se a necessidade de que valores fundamentais orientem a implementação de algoritmos nas práticas jurídicas, sob risco de abalar a legitimidade das decisões automatizadas no âmbito jurídico. Assim, a comunidade internacional tem empreendido esforços, no sentido de formular princípios e diretrizes orientadoras para o desenvolvimento e uso ético da Inteligência Artificial e gerir seu uso responsável, de modo a coibir práticas abusivas e salvaguardar os direitos fundamentais.

Entidades internacionais e fóruns multilaterais, vêm assumindo protagonismo na definição de diretrizes ético-jurídicas para o uso da Inteligência Artificial.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE), por exemplo, em 2019, editou uma Recomendação sobre a Inteligência Artificial, na qual estabelece princípios fundamentais como transparência, responsabilidade, robustez técnica e respeito aos Direitos Humanos, orientando o desenvolvimento e a aplicação ética dessa tecnologia.

No mesmo sentido, a UNESCO aprovou, em 2021, a primeira diretriz global sobre ética da inteligência artificial, com foco na proteção dos Direitos Humanos e uso responsável da tecnologia, ressaltando que a inteligência artificial deve sempre “promover os direitos humanos e a dignidade”, nunca o contrário (UNESCO, 2021, p. 5).

Na União Europeia, além do GDPR voltado à proteção de dados, está em trâmite avançada um Regulamento Europeu de IA, conhecido como *Artificial Intelligence Act*, que dispõe um modelo de regulação baseado no risco: Os sistemas de Inteligência Artificial são classificados com base em seu potencial de risco, considerando o grau de impacto que podem gerar aos direitos fundamentais, à segurança ou à ordem pública (baixo, alto risco ou inaceitáveis), sendo proibidos, por exemplo, aqueles dirigidos a *scoring* social ou identificação biométrica em tempo real, com a finalidade de seguridade pública, dada a sua incompatibilidade com os direitos fundamentais (UNIÃO EUROPEIA, 2021).

Essas iniciativas representam uma convergência no reconhecimento de que a IA deve se orientar, por meio de valores como transparência, não-discriminação, segurança, prestação de contas (*accountability*) e controle humano, a fim de evitar um “descontrole algorítmico” que venha a ameaçar liberdades individuais (Diakopoulos, 2016, p. 28-37).

No Brasil, o debate regulatório também ganhou força nos últimos anos. Após a entrada em vigor da LGPD em 2020, marco legal voltado principalmente ao tratamento de dados pessoais, o legislador brasileiro passou a analisar uma legislação específica sobre a IA.

Uma Comissão de Juristas foi instituída no Senado Federal, em 2021, para elaborar um anteprojeto, resultando na apresentação do Projeto de Lei (PL) nº 21/2020, buscando estabelecer princípios, deveres e direitos para o uso da IA no Brasil.

Em 2024, esse PL foi amplamente debatido no Congresso, com participação de acadêmicos, entidades da sociedade civil e órgãos, como a Autoridade Nacional de Proteção de Dados (ANPD).

Dentre os consensos estabelecidos, sobressai a necessidade de compatibilizar a nova lei de IA com os preceitos da LGPD, evitando assim sobreposições ou contradições, por exemplo, garantindo que os dispositivos de proteção de dados já consagrados, sejam observados pelos sistemas de IA, sem criar obrigações conflitantes.

Também se discutem no projeto, instrumentos de controle algorítmico, como avaliação de impacto de IA, e a proposta prevê a rotulagem de sistemas de alto risco, com o objetivo de aplicar requisitos específicos de transparência e segurança, dever de transparência sobre uso de IA, motivados em propostas estrangeiras e adaptados ao contexto nacional (ANPD, 2023).

Embora até o momento da redação deste artigo, o marco legal brasileiro de IA ainda não tivesse sido definitivamente aprovado, sua tramitação demonstra uma tendência de incorporar ao ordenamento doméstico as melhores práticas internacionais, mas com atenção às especificidades locais, como a realidade econômica, social e cultural brasileira (Cortiz, 2023).

Finalmente, ressalta-se que a resposta do Poder Judiciário brasileiro à crescente difusão da inteligência artificial tem se manifestado por meio de iniciativas institucionais voltadas à regulamentação, à transparência e ao uso ético dessas tecnologias, o que já começa no campo infralegal, com a edição da Resolução 332/2020 do Conselho Nacional de Justiça, que estabelece normas e princípios para o uso de Inteligência Artificial no âmbito do Poder Judiciário (BRASIL, 2020).

Essa resolução, recentemente atualizada em 2025 para abranger novas tecnologias, como a IA generativa, orienta os tribunais a realizarem avaliação prévia de impactos dos sistemas de IA utilizados, bem como, a verificarem os critérios de transparência, explicabilidade, supervisão humana e respeito às garantias processuais em quaisquer ferramentas adotadas (BRASIL, 2020).

Em outras palavras, o CNJ sinaliza que a IA deverá ser tratada como mecanismo auxiliar, e não substitutiva da atuação humana, ou seja, decisões judiciais não poderão ser direcionadas exclusivamente a algoritmos, devendo o magistrado compreender os fatores considerados e manter a responsabilidade final sobre o julgamento.

Tais parâmetros ecoam princípios internacionais, como os enunciados pela Comissão Europeia para a Eficiência da Justiça (CONSELHO DA EUROPA, 2018), reforçando a importância de imparcialidade e controle humano na aplicação de IA no âmbito da justiça.

Essa convergência normativa evidencia que, apesar das diferenças culturais e jurídicas, evidenciam-se preocupações universais na regulação da IA, especialmente, no que restringe à proteção de direitos fundamentais.

3 DESAFIOS DA PROTEÇÃO DE DADOS PESSOAIS FRENTE À INTELIGÊNCIA ARTIFICIAL: PERSPECTIVAS BRASILEIRAS E GLOBAIS

A proteção de dados pessoais se destaca, na sociedade da informação, como garantia essencial à privacidade e à autodeterminação informativa. No Brasil, embora a Constituição de 1988 não mencione expressamente a “privacidade” como direito autônomo, consagra em seu art. 5º, incisos X e XII, a inviolabilidade da intimidade, vida privada, honra, imagem e sigilo de comunicações, assegurando reparação por dano decorrente de sua violação (BRASIL, 1988).

Complementarmente, o inciso LXXII institui o habeas data, assegurando acesso e retificação de dados pessoais, pioneiro no controle informacional.

Tais garantias formam, “um arcabouço robusto de tutela da privacidade no ordenamento brasileiro” (Frazão, 2019).

Com a intensificação do tratamento automatizado de dados, o Brasil promulgou a Lei nº 13.709/2018 – LGPD, que entrou em vigor em 2020, estabelecendo regras gerais e princípios para o uso de dados pessoais em qualquer setor (BRASIL, 2018). Inspirada no GDPR europeu (UNIÃO EUROPEIA, 2016), a LGPD define “dado pessoal” e “dado pessoal sensível”, e consagra princípios como finalidade, necessidade, transparência, prevenção e responsabilização (art. 6º).

Inclui, ainda, como fundamento, o respeito à privacidade (art. 2º, I) e confere ao titular direitos como o acesso facilitado (art. 9º) e a revisão de decisões automatizadas (art. 20).

Esse último dispositivo é crucial no contexto da IA, pois impede que indivíduos sejam submetidos a decisões unicamente automatizadas sem possibilidade de revisão humana. Aplicações como algoritmos de score de crédito ou sistemas de triagem curricular automatizados devem garantir ao titular a ciência e contestação da decisão, conforme previsão análoga do art. 22 do GDPR (UNIÃO EUROPEIA, 2016).

Contudo, a doutrina aponta lacunas: não há clareza sobre como deve ocorrer essa revisão humana ou qual grau de explicação algorítmica é exigido (Wachter; Mittelstadt; Floridi, 2017, p. 76–99).

No Brasil, a ANPD vem tratando o tema. Em 2022, realizou consulta pública sobre decisões automatizadas, visando orientar práticas de transparência e governança em IA (ANPD,

2022). Ainda sem regulamentação específica, espera-se que diretrizes futuras definam o que caracteriza uma decisão automatizada de “caráter significativo” e como garantir compreensão ao titular.

Um dos principais desafios da LGPD frente à IA reside na fluidez entre dados pessoais e não pessoais. Como observa Lucas Borges, da ANPD, muitos sistemas de IA de alto impacto operam sobre grandes massas de dados, sendo tênue a distinção entre o que é ou não pessoal (Carvalho, 2023).

Mesmo dados anonimizados podem gerar impactos individualizados, especialmente com técnicas como o *data enrichment*, que cruzam bancos de dados e inferem novos atributos comportamentais dos titulares. Se realizados sem consentimento ou transparência, esses tratamentos podem violar os princípios da necessidade e finalidade (Noletto; Domingues, 2023).

A conformidade da IA com a LGPD demanda estruturas de governança robustas, como avaliação de impacto (DPIA), *privacy by design* e auditorias independentes para identificação de vieses (Bioni, 2020, p. 86). Nesse ponto, o Brasil se alinha à vertente regulatória europeia inaugurada pelo GDPR, adotada também por países que enfrentam desafios semelhantes na harmonização entre inovação tecnológica e direitos fundamentais.

Além do GDPR, a União Europeia dispõe da Diretiva 2016/680/UE, aplicável a autoridades policiais e judiciárias, com foco na limitação do uso de dados e no controle institucional para garantir a segurança pública com respeito aos direitos individuais (UNIÃO EUROPEIA, 2016, p. 89).

Nos Estados Unidos, a ausência de uma lei federal geral de proteção de dados confere maior liberdade ao setor privado, como evidencia o caso da Clearview AI, que criou um banco com bilhões de imagens públicas usadas por órgãos de segurança. Enquanto autoridades europeias declararam a prática ilícita sob o GDPR, nos EUA apenas legislações locais impuseram restrições à tecnologia.

Esse contraste evidencia que regimes legais sólidos, como o brasileiro, são cruciais para prevenir abusos e fomentar inovação com responsabilidade. A omissão regulatória, por sua vez, tende a gerar situações de descontrole e correções reativas.

Importa destacar que proteção de dados não se opõe à inovação. Ao contrário, constitui elemento essencial para o desenvolvimento tecnológico sustentável e confiável. A Exposição de Motivos da LGPD afirma que a lei busca equilibrar o direito fundamental à proteção de dados com o fomento à inovação (BRASIL, 2018).

Da mesma forma, o Senado Federal, no debate do marco legal da IA, tem defendido que a regulação deve proteger as pessoas “mas não ser restritiva a ponto de impedir o

desenvolvimento econômico e tecnológico do país” (SENADO FEDERAL, 2023). Essa visão reforça que a proteção de dados deve caminhar junto à inovação, garantindo direitos e impulsionando soluções tecnológicas responsáveis.

4 INTELIGÊNCIA ARTIFICIAL NO DIREITO PENAL: DESAFIOS, APLICAÇÕES E SOLUÇÕES JURÍDICAS

A incorporação de tecnologias baseadas em Inteligência Artificial, no âmbito do Direito Penal, abrangendo a segurança pública, investigação policial, processo penal e execução penal, tem se desenvolvido progressivamente, porém constante, em diversos países.

No Brasil, já se vislumbram iniciativas como o uso de câmeras inteligentes de vigilância, aptas a reconhecer foragidos por meio do reconhecimento facial em locais públicos, *softwares* de análise preditiva de manchas criminais (*crime mapping*), utilizados por secretarias de segurança pública, assim como sistemas automatizados de triagem de processos penais.

Essas aplicações evidenciam como a IA pode aprimorar a eficiência operacional e a capacidade analítica das autoridades: Um sistema de visão computacional, é capaz de escanear milhares de rostos, simultaneamente e em tempo real, identificando suspeitos, com mandado de prisão; algoritmos podem detectar padrões em bancos de boletins de ocorrência, contribuindo para alocação mais estratégica do policiamento ostensivo.

Modelos de linguagem natural, são capazes de auxiliar na identificação de precedentes relevantes em grandes volumes de processos criminais. Em um país, com altos índices de criminalidade, e um Judiciário abarrotado por processos, é assimilável que essas tecnologias, sejam vistas com interesse pelos gestores públicos, pois sinalizam maior eficiência e racionalização de recursos na gestão pública.

No entanto, a literatura crítica, aliada à experiência internacional, tem chamado atenção para os diversos riscos e impactos negativos decorrentes do uso indiscriminado da IA na esfera penal. Uma das questões mais debatidas se trata da discriminação algorítmica. Sistemas de IA, são treinados com base em dados pretéritos.

Se as bases de dados utilizadas refletem preconceitos ou desigualdades estruturais da sociedade, ainda que de forma inconsciente, há risco significativo de que os algoritmos venham a reproduzir, ou até intensificar tais vieses.

Nos Estados Unidos, um estudo paradigmático de Angwin (2016) revelou que um *software* de avaliação de risco criminal (COMPAS), empregado na análise de concessão de liberdade condicional e fiança, o sistema evidenciava viés racial. Embora a raça não fosse

expressamente considerada como variável, o algoritmo tendia a *scores* de risco mais elevados a réus negros do que a réus brancos com antecedentes semelhantes, resultando em tratamento desigual.

O episódio revelou a complexidade envolvida em escrutinar e ajustar sistemas opacos de tomada de decisão automatizada algorítmica, suscitando debates jurídicos sobre a violação do princípio da igualdade e a garantia de um julgamento imparcial e equitativo.

Cenário semelhante poderia se verificar no Brasil, caso ferramentas de pontuação de riscos ou de reconhecimento facial viessem a ser implementadas sem os devidos cuidados. Estudos já indicam que tecnologias de reconhecimento facial, possuem taxas de erro significativamente maiores para pessoas negras e mulheres, por fragilidade na diversidade dos dados de treinamento (Silva, 2020, p. 66-67).

De tal modo, identificações equivocadas poderiam recair de forma desproporcional sobre grupos minoritários, resultando em abordagens policiais indevidas e, em casos mais graves, prisões injustificadas, o que viola direitos e garantias fundamentais, como a presunção de inocência e a não discriminação (BRASIL, 1988).

Diante disso, alguns estados brasileiros e diversos países estrangeiros, passaram a impor restrições. Na Europa, por exemplo, intensificaram-se os debates sobre *AI Act* incluindo o banimento do reconhecimento facial em espaços públicos ou impondo-lhe limitações rigorosas. Nos EUA, cidades como São Francisco (Van Sant, Shannon; Gonzales, 2019) e Boston (Jarmanning, 2020), baniram o uso governamental de reconhecimento facial, considerando seus efeitos potencialmente invasivos e excludentes. A transparência e o direito ao contraditório figuram como preocupações centrais.

No processo penal, é garantia fundamental que ambas as partes tenham pleno acesso às provas e aos mecanismos que subsidiam as decisões judiciais, assegurando a possibilidade de impugnação e fiscalização dos instrumentos utilizados, o que é essencial à preservação do contraditório e da ampla defesa previstos na Constituição da República de 1988 (BRASIL, 1988).

Caso um magistrado ou comissão utilize um sistema de inteligência artificial para avaliar, por exemplo, a probabilidade de reincidência de um réu ao decidir sobre a substituição da pena ou a progressão de regime, é imperativo que tal algoritmo seja dotado de transparência e esteja sujeito ao escrutínio das partes envolvidas no processo.

Do contrário, tais decisões poderiam decorrer de lógicas internas, não acessíveis nem compreensíveis, comprometendo a legitimidade do processo, até para o próprio julgador, o que colocaria em risco a legitimidade do ato jurisdicional.

O CNJ, ao editar a Resolução 332/2020, enfatizou que a utilização de IA pelos órgãos judiciários deve preservar a publicidade dos atos processuais e a explicitação dos fundamentos das decisões (BRASIL, 2020).

Isso implica, por exemplo, que se um sistema sugerir determinada sentença, o magistrado deve fundamentar em sua decisão os elementos concretos fáticos e jurídicos, que embasem o resultado, não podendo escudar-se na alegação de que foi o computador quem indicou. Mais que isso, eventuais algoritmos usados precisam ser auditáveis.

Parte expressiva da doutrina sustenta a necessidade de *algorithmic accountability*, ou seja, que “desenvolvedores e operadores de IA possam ser compelidos a fornecer informações técnicas suficientes para verificar se o sistema opera dentro dos limites da lei” (Pasquale, 2015, p. 84).

No cenário brasileiro, essa discussão é preliminar, mas adquire crescente importância frente a iniciativas como a do Projeto Victor, do STF (SUPREMO TRIBUNAL FEDERAL, 2021), no qual se utiliza da IA para efetivar a análise de repercussão geral em recursos extraordinários, ou os projetos de tribunais estaduais para automação de classificações de processos.

Propõe-se, no âmbito acadêmico, a inclusão de normas específicas na legislação processual, com vistas a demandas que impeçam decisões judiciais exclusivamente automatizadas e garantam o acesso do perito indicado pelas partes ao algoritmo em casos contenciosos, algo anteriormente discutido, por exemplo, na França, onde se analisa o direito ao acesso ao código-fonte de algoritmos públicos.

No âmbito das investigações e da atuação policial, o uso da inteligência artificial suscita importantes questionamentos quanto à legalidade, de meios de obtenção de prova e privacidade. A Constituição da República de 1988, prevê no art. 5º, LVI, que “são inadmissíveis, no processo, as provas obtidas por meios ilícitos” (BRASIL, 1988).

Caso a polícia faça uso de um programa de coleta automatizada de dados, como técnicas de *scraping* em redes sociais sem autorização judicial e dele extrair indícios, há risco de essa prova ser considerada ilícita, análoga a uma diligência ilícita.

Um caso hipotético: Se um algoritmo for utilizado para analisar comunicações em massa e, a partir da identificação de padrões, gerar suspeitas sobre determinado indivíduo, sem que exista autorização judicial prévia para a interceptação dessas comunicações, tal conduta poderá violar diretamente o sigilo de dados e comunicações, em afronta aos direitos fundamentais à privacidade e à intimidade previstos na Constituição da República de 1988.

Portanto, a IA não isenta as autoridades do cumprimento dos procedimentos legais tradicionais, como obtenção de ordens judiciais para quebras de sigilo. Além disso, a *profiling* preventivo de indivíduos, predizer quem tem propensão a cometer crimes, entra em colisão com os princípios estruturantes do Direito Penal de responsabilização por atos efetivamente praticados e não com base em características subjetivas ou punições por meras intenções, o que remete a advertências clássicas presentes em distopias literárias.

A propósito, parte da doutrina tem invocado o princípio da presunção de inocência, como fundamento para criticar sistemas algorítmicos de antecipação penal, de *predictive policing* que podem rotular “cidadãos ou bairros inteiros como perigosos com base em dados históricos, frequentemente perpetuando a seletividade penal” (Lopes; Araújo, 2021, p. 123-145).

Diante desses desafios, quais caminhos têm sido trilhados no plano normativo? No Brasil, além da normativa geral de proteção de dados já discutida, que delimita limites importantes, por exemplo, proibição de uso de dados pessoais sensíveis sem base legal adequada, o que incide em sistemas de IA que coletam essas informações, vislumbra-se movimentação legislativa e jurisprudencial.

Em 2022, tramitou perante o Congresso um projeto visando regulamentar o uso de reconhecimento facial por órgãos de segurança, estabelecendo critérios de necessidade, proporcionalidade e supervisão humana obrigatória, em consonância com as diretrizes internacionais de Direitos Humanos. Embora tal projeto não tenha sido convertido em lei até o momento, ele reflete a percepção de se evitar um cenário de “*big brother*” estatal violador de privacidade (BRASIL, 2022).

Por sua vez, o Supremo Tribunal Federal deve julgar em breve medidas que contestam a legitimidade jurídico-constitucional da vigilância em larga escala, frente às garantias fundamentais, por exemplo, debate-se se o uso de câmeras inteligentes em estádios de futebol, feriria o direito de imagem e privacidade dos torcedores inocentes, que têm seus rostos escaneados sem consentimento. É possível que o STF, estabeleça diretrizes constitucionais, exigindo lei específica e parâmetros rigorosos para uso dessas tecnologias.

No plano internacional, é digno de nota o movimento da União Europeia, para disciplinar a aplicação da IA no sistema de Justiça Criminal, no contexto de sua proposta regulatória em trâmite: Algoritmos utilizados para contribuir com decisões judiciais, serão classificados como alto risco, necessitando conformidade com requisitos rigorosos de transparência, gerenciamento de risco e documentação (UNIÃO EUROPEIA, 2021).

Ademais, caso sejam empregados sistemas de inteligência artificial voltados à avaliação de risco de indivíduos, no contexto penal, ela provavelmente estará sujeita a obrigações de auditoria independente e possíveis sanções em caso de vieses indevidos, em sintonia com a visão de *zero tolerance* para evidências de tratamento desigual gerado por sistemas automatizados naquele continente.

Nos Estados Unidos, ainda que a regulação seja mais fragmentada, o Poder Judiciário tem começado a se debruçar sobre essas questões: Em Wisconsin, a Suprema Corte Estadual decidiu em 2016, que magistrados, podem usar *software* de risco (como o COMPAS) como ferramenta auxiliar na sentença, mas não como base exclusiva, e o réu deverá ter acessibilidade aos resultados. Essa decisão, ainda que insuficiente, representou ao menos uma limitação ao poder decisório cego da máquina (Wisconsin, 2016).

Sob a perspectiva dogmática, também se debate a possibilidade de atribuição de responsabilidade penal no contexto da inteligência artificial.

No âmbito civil-consumerista, discute-se sobre a responsabilidade do desenvolvedor, do operador ou, inclusive, se cogita a personalização jurídica da inteligência artificial, por meio da criação de uma personalidade eletrônica que permita sua responsabilização autônoma, proposta esta que, contudo, tem sido amplamente criticada pela maioria da doutrina especializada (Roque, 2023) .

No Direito Penal, a atribuição de responsabilidade direta a sistemas de inteligência artificial é inadmissível, pois a culpabilidade exige consciência e vontade, características exclusivamente humanas. Porém, pode-se responsabilizar penalmente pessoas por resultados originários da IA. Essas situações-limite denotam a necessidade de atualização interpretativa e possivelmente legislativa.

A maioria dos ordenamentos, incluindo o brasileiro, tem interpretado à luz da analogia normativa, se aplica a teoria tradicional da ação por meio de outrem, nos crimes dolosos, ou do nexo de causalidade culposos.

No âmbito do direito comparado, ainda não se verificam tipificações penais específicas voltadas a condutas envolvendo inteligência artificial. No Brasil, poderiam ser aplicados tipos penais já existentes, como lesão corporal ou homicídio culposos, em combinação com normas relativas à responsabilidade pela produção, especialmente nos casos que envolvam defeitos de produto, conforme previsto no Código de Defesa do Consumidor (BRASIL, 1990), em tese.

De todo modo, trata-se de um universo jurídico que deverá ser aprofundado à medida que surgirem casos concretos. Em síntese, a introdução da inteligência artificial no universo do Direito Penal proporciona benefícios indiscutíveis em termos de eficiência, mas

simultaneamente representa risco de retrocessos em garantias fundamentais se não for acompanhada de estrutura jurídica apropriada.

Piló e Brasil (2024), suscitam que, “justamente por lidar com bens jurídicos sensíveis: liberdade, vida, integridade, o uso de máquinas inteligentes no processo penal deve ser limitado e criteriosamente controlado, e não expandido sem reservas”.

Esses doutrinadores concluíram, após análise geral, pela necessidade de frear o entusiasmo orientado tecnologicamente e colocar “praticamente em todos os aspectos, limites à utilização de máquinas com IA no Direito Penal” (Piló; Brasil, 2024, p. 269-271), a fim de preservar a dignidade da pessoa humana e coibir limitações ilegítimas de garantias.

Tal posicionamento revela um prudente alinhamento com o princípio da precaução tecnológica proposto por (Jonas, 2006, p. 184) “a ideia de que, diante da possibilidade de impactos gravíssimos de novas tecnologias, deve-se exigir responsabilidade e cautela de seus criadores e usuários”. Afinal, no âmbito do processo penal, erros ou abusos podem acarretar consequências irreversíveis para a vida dos indivíduos.

Dessa forma, torna-se imperativo que o legislador, o Poder Judiciário e a comunidade acadêmica, permaneçam vigilantes na elaboração de parâmetros normativos claros e eficazes para a regulação da inteligência artificial, com vistas a garantir que ela atue como aliada da justiça, e não como ameaça.

5 CONCLUSÃO

A interseção entre inteligência artificial, proteção de dados pessoais e direito penal configura uma fronteira emergente e dinâmica no campo jurídico, na qual inovações tecnológicas demandam releituras de normas clássicas e, muitas vezes, a criação de novos *frameworks* jurídicos.

A análise desenvolvida ao longo deste artigo, evidencia que o Brasil já avançou importantes rumos a uma regulação equilibrada da matéria, mas ainda enfrenta desafios significativos.

No âmbito da proteção de dados e da privacidade, o ordenamento jurídico brasileiro conta atualmente com uma base normativa robusta, fundamentada na Constituição da República de 1988 e materializada pela Lei Geral de Proteção de Dados (LGPD), apta a prover instrumentos eficazes para enfrentar diversos desafios impostos pela inteligência artificial.

Princípios como transparência, finalidade e não discriminação, bem como, direitos assegurados ao titular, constituem alicerces para garantir que o tratamento massivo de dados

por sistemas inteligentes não se afaste dos valores fundamentais da sociedade, como a privacidade, igualdade e autonomia individual.

Não obstante, será fundamental monitorar a concretização prática dessas garantias: a ANPD - Autoridade Nacional de Proteção de Dados, os Ministérios Públicos e o Poder Judiciário apresentam papel fundamental na interpretação e aplicação da LGPD a casos concretos de uso de IA, definindo padrões jurisprudenciais.

A elaboração de normas complementares, seja pela Autoridade Nacional de Proteção de Dados (ANPD), por meio de regulamentações sobre decisões automatizadas, avaliações de impacto e outras medidas, seja pelo Poder Legislativo, mediante a criação de leis específicas para o tratamento de dados no âmbito da segurança pública, é indispensável para a segurança da proteção dos direitos fundamentais, o que poderá suprir lacunas e clarificar pontos obscuros, assegurando maior segurança jurídica, tanto aos titulares de dados, quanto aos agentes que desenvolvem e utilizam IA.

No tocante ao Direito Penal, vislumbra-se que a adoção da IA deve ser conduzida com vigilância reforçada. Os benefícios prometidos, embora reais, não podem ofuscar a exigência de que o devido processo legal e os direitos fundamentais do investigado ou réu sejam rigorosamente respeitados.

É alentador que instituições como o Conselho Nacional de Justiça (CNJ), já tenham se manifestado, estabelecendo diretrizes éticas para o uso da Inteligência Artificial no âmbito do Poder Judiciário, e que o debate legislativo esteja atento a temas sensíveis, tais como o reconhecimento facial e a polícia preditiva.

Recomenda-se, por exemplo, o desenvolvimento de protocolos públicos de auditoria algorítmica para todas as ferramentas de inteligência artificial utilizadas na persecução penal, envolvendo especialistas independentes e mecanismos de controle externo, tais como defensorias públicas, Ordem dos Advogados do Brasil (OAB) e instituições acadêmicas.

Tal medida visa testar e corrigir eventuais vieses antes da adoção oficial dos sistemas. Ademais, sugere-se a capacitação técnica dos operadores do direito, incluindo delegados, promotores, magistrados, advogados e demais profissionais da área jurídica, para que possam compreender plenamente as potencialidades e limitações dessas tecnologias.

No plano jurisprudencial, cabe aos Tribunais Superiores, em momento oportuno, estabelecer entendimentos orientadores, por exemplo, definindo se o uso de determinado algoritmo de vigilância configura violação a direitos fundamentais, ou estabelecendo critérios para a admissibilidade de provas provenientes de algoritmos.

Essa construção jurisprudencial será substancialmente facilitada, se fundamentada em estudos empíricos e interdisciplinares, o que reforça a importância do diálogo entre o Direito e áreas como Ciência da Computação, Estatística e Sociologia, para a adequada avaliação dos impactos da inteligência artificial.

A comparação internacional oferece lições valiosas. Observa-se que a União Europeia se destaca como referência na conciliação entre inovação tecnológica e proteção dos direitos fundamentais, seja por meio da aplicação rigorosa do Regulamento Geral sobre a Proteção de Dados (GDPR), seja pela arquitetura regulatória setorial atualmente em elaboração, como o *AI Act*.

Países como o Brasil, podem se inspirar nessa experiência, adaptando-a às especificidades locais, ao mesmo tempo em que contribuem com perspectivas próprias, especialmente, ao incorporar preocupações relativas às desigualdades sociais e disparidades regionais que caracterizam a realidade brasileira e que podem ser potencialmente agravadas ou mitigadas pela regulação da inteligência artificial.

Por sua vez, a experiência norte-americana ilustra os riscos associados a uma abordagem *laissez-faire*: a ausência de um marco regulatório geral, favoreceu avanços tecnológicos acelerados, porém não sem o custo de incidentes notórios relacionados à violação de privacidade e a decisões judiciais equivocadas fundamentadas em algoritmos opacos, problemas estes que vêm sendo enfrentados apenas posteriormente.

O desafio consiste em buscar um equilíbrio virtuoso entre esses modelos, evitando tanto a paralisia regulatória quanto a permissividade irresponsável, para assegurar uma regulação eficaz e justa.

Conclui-se, portanto, que o ordenamento jurídico brasileiro se encontra em constante evolução diante dos desafios impostos pela inteligência artificial, exigindo atualizações e ajustes permanentes.

A proteção de dados pessoais deve continuar ocupando posição central nesse debate, funcionando como verdadeiro fio condutor na formulação de quaisquer normas relacionadas à IA, vez que grande parte dos riscos advém do uso intensivo de informações individuais.

No âmbito penal, impõe-se a utilização prudente e subsidiária da Inteligência Artificial, que jamais deve substituir a racionalidade humana e os princípios do Direito Penal liberal, estabelecidos desde o Iluminismo.

Como alertou Cesare Beccaria no século XVIII, é preferível prevenir os crimes do que puni-los arbitrariamente, entretanto, tal prevenção não pode se legitimar por meio de práticas que sacrifiquem a liberdade sem justa causa.

Parafraseando esse pensamento, em um contexto contemporâneo, poder-se-ia afirmar que prevenir o crime com o auxílio da IA é desejável, desde que se evite a criminalização do inocente e a violação da dignidade humana, sob a justificativa de uma suposta eficiência.

Em síntese, o percurso a ser seguido é o do aperfeiçoamento normativo responsável, pautado no conhecimento técnico-científico e nos valores democráticos. A inteligência Artificial, deve estar a serviço do ser humano e da sociedade, nunca o inverso.

Compete ao Direito, amparado pela doutrina clássica e contemporânea, bem como, pelos exemplos internacionais, delinear os contornos dessa relação, assegurando que a revolução trazida pela Inteligência Artificial seja acompanhada por uma correspondente evolução nas garantias jurídicas. Somente assim será possível usufruir plenamente dos benefícios da IA, em segurança e desenvolvimento, sempre sob a égide do Estado de Direito e do irrestrito respeito aos direitos humanos.

REFERÊNCIAS

ANGWIN, Julia. Machine Bias: *Avaliação de Risco e Discriminação Algorítmica*. Revista de Ética Legal, v. 23, n. 3, 2016.

ANPD (Autoridade Nacional de Proteção de Dados). *Análise Preliminar do PL 2338/2023 – Regulamentação de IA e Convergência com a LGPD*. Brasília: ANPD, 2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-analise-preliminar-do-projeto-de-lei-no-2338-2023-que-dispoe-sobre-o-uso-da-inteligencia-artificial>. Acesso em: 20 abr. 2025.

ANPD (Autoridade Nacional de Proteção de Dados). *Tomada de Subsídios sobre Inteligência Artificial e Revisão de Decisões Automatizadas*. Brasília: ANPD, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/aceso-a-informacao/participacao-social>. Acesso em: 28 abr. 2025.

ASHLEY, Kevin D. *Inteligência Artificial e Análise Jurídica: Novas Ferramentas para a Prática Jurídica na Era Digital*. Cambridge: Cambridge University Press, 2017.

BECCARIA, Cesare. *Dos Delitos e das Penas*. 2. ed. São Paulo: Martines, 2000.

BIONI, Bruno. *Proteção de Dados Pessoais: A Função e os Limites do Consentimento*. Rio de Janeiro: Forense, 2020.

BIRD, Eleanor. *A ética da inteligência artificial: Questões e iniciativas*. Bruxelas: Serviço de Pesquisa do Parlamento Europeu, 2020. Disponível em: https://efaidnbmnnnibpcajpcglclefindmkaj/https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU%282020%29634452_EN.pdf. Acesso em: 22 abr. 2025.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 3.069, de 22 de dezembro de 2022. *Dispõe sobre o uso de tecnologia de reconhecimento facial automatizado no âmbito das forças de segurança pública e dá outras providências*. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2345261>. Acesso em: 30 maio 2025.

BRASIL. *Código de Defesa do Consumidor*. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 12 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/18078.htm. Acesso em: 30 maio 2025.

BRASIL. CONSELHO NACIONAL DE JUSTIÇA. *Resolução nº 332, de 21 de agosto de 2020*. Dispõe sobre a utilização de inteligência artificial no Poder Judiciário e o respeito aos direitos fundamentais. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3429>. Acesso em: 30 maio. 2025.

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: 28 abr. 2025.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 30 maio. 2025.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 24 abr. 2025.

BRASIL. SENADO FEDERAL. *Projeto de Lei nº 2338/2023*. Regulamenta o uso da Inteligência Artificial no Brasil. Brasília, 2023. (Em tramitação). Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 30 maio. 2025.

CARVALHO, Lucas Borges de. *Equilíbrio entre inovação e direitos na regulação da IA. Debate Público CTIA – Senado Federal*, 19 out. 2023. (Participação como gerente de projetos da ANPD). Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/comissao-temporaria-de-ia-debate-os-efeitos-da-inteligencia-artificial-nos-direitos-fundamentais-do-titular-de-dados-pessoais>. Acesso em: 30 maio. 2025.

CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA (CADE). *Organização para a Cooperação e Desenvolvimento Econômico – OCDE*. Brasília: CADE. Disponível em: <https://www.gov.br/cade/pt-br/centrais-de-conteudo/internacional/cooperacao-multilateral/organizacao-para-a-cooperacao-e-desenvolvimento-economico-ocde-1>. Acesso em: 30 maio 2025.

CONSELHO DA EUROPA. Comissão Europeia para a Eficiência da Justiça (CEPEJ). *Carta Ética Europeia sobre o Uso da Inteligência Artificial nos Sistemas Judiciais e seu Ambiente*. Estrasburgo, 2018. Disponível em: <https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0>. Acesso em: 30 maio 2025.

CONSULTOR JURÍDICO. *OCDE atualiza 1ª norma intergovernamental sobre IA do mundo*. 12 maio 2024. Disponível em: <https://www.conjur.com.br/2024-mai-12/ocde-atualiza-1a-norma-intergovernamental-sobre-ia-do-mundo/>. Acesso em: 30 maio 2025.

CORTIZ, Diogo. *Brasil no G20: 7 pontos sobre IA para diminuir dependência dos ricos*. UOL, 7 dez. 2023. Disponível em: <https://www.uol.com.br/tilt/colunas/diogo-cortiz/2023/12/07/brasil-no-g20-7-pontos-sobre-ia-para-diminuir-dependencia-dos-ricos.htm>. Acesso em: 30 maio 2025.

DIAKOPOULOS, Nicholas. *Transparência e Responsabilidade na Inteligência Artificial no Direito Penal*. Revista de Tecnologia Jurídica, v. 12, n. 1, 2016.

DIETER, Robert. *Discriminação Algorítmica no Sistema de Justiça Criminal: Lições do Caso COMPAS*. Revista de Ética e Tecnologia, v. 8, n. 4, p. 112-128, 2016.

FOUCAULT, Michel. *Vigiar e Punir*. Petrópolis: Vozes, 1987.

FRAZÃO, Ana. *Quais devem ser os parâmetros éticos e jurídicos para a utilização da inteligência artificial?* Brasília, 2019. Disponível em: https://efaidnbmninnibpcajpcglclefindmkaj/https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/170750/2020_frazao_ana_parametros_eticos.pdf?sequence=1. Acesso em: 30 maio 2025.

JARMANNING, Ally. *Boston Lawmakers Vote To Ban Use Of Facial Recognition Technology By The City*. NPR, 24 jun. 2020. Disponível em: <https://www.npr.org/sections/live-updates-protests-for-racial-justice/2020/06/24/883107627/boston-lawmakers-vote-to-ban-use-of-facial-recognition-technology-by-the-city>. Acesso em: 30 maio 2025.

JONAS, Hans. *O Princípio Responsabilidade: Ensaio de uma Ética para a Civilização Tecnológica*. Rio de Janeiro: PUC-Rio. Contraponto, 2006.

LOPES, Maria A.; ARAÚJO, Felipe. *Inteligência artificial preditiva e a presunção de inocência*. Revista Brasileira de Ciências Criminais, v. 30, n. 141, 2021.

NERDIA, 1956: *Conferência de Dartmouth*. Disponível em: <https://nerdia.com.br/1956-conferencia-de-dartmouth/>. Acesso em: 30 maio 2025.

NOLETO, Aline; DOMINGUES, Patrícia. *Marco Legal da IA e LGPD: novos desafios na privacidade e enriquecimento de dados*. Consultor Jurídico (Conjur), 6 dez. 2023. Disponível em: <https://www.conjur.com.br/2023-dez-06/marco-legal-da-ia-e-lgpd-novos-desafios-na-privacidade-e-enriquecimento-de-dados/>. Acesso em: 20 abr. 2025.

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

PILÓ, Xenofontes C.; BRASIL, Deilton R. *A Utilização da Inteligência Artificial no Direito Penal e seus Reflexos nas Garantias e Direitos Fundamentais*. Revista EJEJ, Belo Horizonte, v. 1, n. 1, 2024.

ROQUE, Bruna Tamy Yamamoto. *A responsabilidade civil da inteligência artificial*. 2023. Trabalho de Conclusão de Curso. Bacharelado em Direito. Universidade Federal de Santa Catarina. Centro de Ciências Jurídicas, Florianópolis, 2023. Disponível em: <https://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.ufsc.br/bitstream/handle/123456789/253839/A%20Responsabilidade%20Civil%20da%20Intelig%c3%aancia%20Artificial%20.docx.pdf?sequence=1&isAllowed=y>. Acesso em: 30 maio 2025.

SENADO FEDERAL. *Regulação da inteligência artificial exige cuidado com dados pessoais, aponta debate*. Agência Senado, 19 out. 2023. Disponível em: https://www12.senado.leg.br/noticias/materias/2023/10/19/regulacao-da-inteligencia-artificial-exige-cuidado-com-dados-pessoais-aponta-debate?utm_source=chatgpt.com. Acesso em: 20 abr. 2025.

SILVA, Bárbara Jennifer Paz de Abreu da Silva. *Inteligência artificial e suas implicações ético-jurídicas*. Dissertação (Mestrado em Direito e Gestão) - Faculdade de Direito da Universidade Nova de Lisboa, 2020. Disponível em: https://efaidnbmnnnibpcajpcglclefindmkaj/https://run.unl.pt/bitstream/10362/104098/1/Silva_2020.pdf. Acesso em: 20 abr. 2025.

SUPREMO TRIBUNAL FEDERAL (Brasil). *Projeto Victor avança em pesquisa e desenvolvimento para automação de processos*. Brasília. DF: STF, 17 nov. 2021. Disponível em: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=471331&ori=1>. Acesso em: 30 maio 2025.

UNESCO. *Recomendação sobre a Ética da Inteligência Artificial*. Paris: UNESCO, 2022. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000381137_por. Acesso em: 24 abr. 2025.

UNIÃO EUROPEIA. Parlamento Europeu; Conselho da União Europeia. *Diretiva (UE) 2016/680, de 27 de abril de 2016: relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho*. Jornal Oficial da União Europeia, L 119, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016L0680>. Acesso em: 30 maio 2025.

UNIÃO EUROPEIA. *Proposta de Regulamento do Parlamento Europeu e do Conselho estabelecendo regras harmonizadas em matéria de inteligência artificial (Artificial Intelligence Act)*, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Acesso em: 26 abr. 2025.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016*. Regulamento Geral de Proteção de Dados (GDPR). *Jornal Oficial da União Europeia*, 2021.

VAN SANT, Shannon; GONZALES, Richard. *San Francisco Approves Ban On Government's Use Of Facial Recognition Technology*. NPR, 14 maio 2019. Disponível em: <https://www.npr.org/2019/05/14/723193785/san-francisco-considers-ban-on-governments-use-of-facial-recognition-technology>. Acesso em: 30 maio 2025.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*. *International Data Privacy Law*, v. 7, n. 2, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469. Acesso em: 30 maio 2025.

WISCONSIN. Supreme Court. *State v. Loomis*. 2016. Disponível em: <https://law.justia.com/cases/wisconsin/supreme-court/2016/2015ap000157-cr.html>. Acesso em: 30 maio 2025.