

VIESES ALGORÍTMICOS E DISCRIMINAÇÃO NO SISTEMA PENAL: DESAFIOS DA REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL NO BRASIL

Gabriella Marques de Souza¹

Augusto Martins de Jesus²

RESUMO: O presente artigo analisa as implicações jurídicas e éticas da ausência de regulamentação penal específica da inteligência artificial no Brasil, diante da crescente utilização de sistemas automatizados no âmbito da justiça criminal. A pesquisa examina riscos como a discriminação algorítmica, a opacidade dos sistemas e a dificuldade de responsabilização por danos decorrentes de decisões automatizadas. Por meio de revisão bibliográfica, análise de casos concretos e estudo comparativo dos modelos regulatórios adotados pela União Europeia, Estados Unidos e China, o trabalho identifica diretrizes para a construção de um marco regulatório brasileiro voltado à proteção dos direitos fundamentais. A regulação ética da inteligência artificial é indispensável para assegurar a dignidade da pessoa humana, a igualdade, o devido processo legal e a segurança jurídica, sem comprometer o desenvolvimento tecnológico responsável.

Palavras-chave: Inteligência Artificial. Direito Penal. Responsabilidade Penal. Regulação Ética. Discriminação Algorítmica. Direitos Fundamentais.

INTRODUÇÃO

A inteligência artificial (IA) consolidou-se, nas últimas décadas, como uma das tecnologias mais disruptivas³ da contemporaneidade, impactando os modos de produção, comunicação, tomada de decisões e organização social. Seu emprego em áreas como indústria, saúde, educação, segurança pública e sistema de justiça ampliou a eficiência de processos e suscitou novas e complexas questões éticas, jurídicas e políticas. No âmbito jurídico-penal, esse fenômeno assume contornos ainda mais sensíveis, uma vez que envolve diretamente a liberdade individual, a dignidade da pessoa humana, a igualdade material e as garantias do devido processo legal.

¹ Graduanda em Direito pela Fundação Educacional de Fernandópolis. E-mail: gabi.m__@outlook.com.br

² Professor da Fundação Educacional de Fernandópolis (FEF), onde atua como orientador acadêmico. Mestre em Jornalismo pela Universidade Estadual de Ponta Grossa. Bacharel em Jornalismo pela Universidade do Estado de Minas Gerais, em Direito pelo Centro Universitário de Votuporanga (Unifev) e em Publicidade e Propaganda pela Cruzeiro do Sul Virtual (Universidade de Franca – Unifran). Especialista em Lei Geral de Proteção de Dados e em Direito Público (Faculdade Legale). E-mail: augustodejesus@fef.edu.br

³ O termo “disruptiva” é utilizado para designar inovações capazes de provocar rupturas significativas em modelos, práticas e estruturas previamente consolidadas, substituindo padrões tradicionais por novas formas de organização, produção ou funcionamento. No contexto tecnológico, uma inovação disruptiva aprimora processos existentes e transforma profundamente setores inteiros da sociedade, alterando relações econômicas, sociais e jurídicas.

A utilização de sistemas algorítmicos para fins de vigilância, reconhecimento facial, análise preditiva de crimes e apoio à tomada de decisões judiciais revela o avanço tecnológico como instrumento potencial de eficiência estatal, mas, simultaneamente, revela riscos concretos de discriminação, opacidade decisória e dificuldade de responsabilização. Casos amplamente divulgados de prisões injustas baseadas em reconhecimento facial, tanto no Brasil quanto no exterior, mostram o impacto real dessas tecnologias sobre vidas humanas e expõem as fragilidades de sua aplicação sem controle normativo rigoroso. Nesse cenário, a inteligência artificial deixa de ser apenas uma ferramenta tecnológica e passa a assumir o papel de agente estruturante de práticas institucionais, com capacidade de produzir efeitos jurídicos relevantes.

O objeto de estudo do presente artigo consiste, precisamente, na análise das implicações da ausência de regulamentação penal específica da inteligência artificial no contexto brasileiro, com especial atenção aos riscos éticos, às violações de direitos fundamentais e aos desafios relativos à responsabilização por danos decorrentes de decisões automatizadas. Parte-se da compreensão de que o atual ordenamento jurídico nacional, embora disponha de instrumentos como a Constituição Federal, o Código Penal, a Lei Geral de Proteção de Dados e a Resolução CNJ nº 332/2020, ainda carece de um marco normativo próprio, sistemático e específico para a governança da inteligência artificial.

A justificativa da pesquisa reside na constatação de que o uso crescente da inteligência artificial no sistema de justiça penal ocorre em um ambiente de fragilidade regulatória, o que potencializa riscos de perpetuação de desigualdades estruturais, sobretudo quando considerados os vieses raciais, sociais e econômicos incorporados aos algoritmos. A relevância social do estudo está na defesa da proteção de direitos fundamentais diante da expansão das tecnologias de vigilância e automação decisória. Já sua relevância jurídica manifesta-se na necessidade de oferecer subsídios teóricos e normativos para a construção de um modelo regulatório compatível com os princípios constitucionais brasileiros. No plano acadêmico, o trabalho se justifica pela lacuna existente na produção científica nacional, especialmente em língua portuguesa, sobre regulação penal da inteligência artificial, racismo algorítmico e governança ética de sistemas automatizados.

A problemática central da pesquisa emerge da seguinte indagação: de que maneira a ausência de um marco regulatório penal específico para a inteligência artificial compromete a tutela dos direitos fundamentais e a efetividade da responsabilidade jurídica no Brasil? A partir dessa questão, o estudo investiga como a opacidade algorítmica, a discriminação automatizada e a dificuldade de imputação de responsabilidade agravam fragilidades já

existentes no sistema penal.

O objetivo geral do artigo é analisar criticamente as consequências jurídicas e éticas da falta de regulamentação da inteligência artificial no campo penal brasileiro, à luz da Constituição Federal, da legislação infraconstitucional e das experiências regulatórias internacionais. Como objetivos específicos, busca-se: examinar os riscos da aplicação da IA no sistema penal, com destaque para a discriminação algorítmica e a violação de garantias processuais; analisar modelos regulatórios adotados por outras jurisdições, como União Europeia, Estados Unidos e China; avaliar as implicações dessas experiências para a realidade brasileira; e propor diretrizes normativas para um marco regulatório ético e juridicamente adequado.

No que se refere à metodologia, a pesquisa adota abordagem qualitativa, de natureza teórico-dogmática, com emprego de revisão bibliográfica, análise documental, estudo de casos concretos e método comparativo. A escolha dessa metodologia justifica-se pela necessidade de compreender o fenômeno de forma interdisciplinar, articulando fundamentos do Direito Penal, do Direito Constitucional, da proteção de dados e da ética da tecnologia. A análise comparada dos modelos internacionais permite identificar boas práticas e limites regulatórios, oferecendo parâmetros para a construção de soluções adequadas ao contexto brasileiro.

A estrutura do artigo foi organizada de modo a permitir uma progressão lógica do raciocínio. Inicialmente, discute-se a inteligência artificial e a lacuna regulatória existente no Brasil, revelando seus impactos no sistema de justiça criminal. Em seguida, desenvolve-se um estudo comparativo das abordagens internacionais adotadas pela União Europeia, Estados Unidos e China, destacando seus fundamentos, objetivos e técnicas regulatórias. Posteriormente, são apresentadas propostas normativas para o controle ético e penal da inteligência artificial no Brasil, abordando classificação por níveis de risco, responsabilização penal, proteção de dados sensíveis, supervisão humana, transparência, criação de autoridade reguladora e capacitação do sistema de justiça. Por fim, as considerações finais sintetizam os principais resultados e apontam perspectivas futuras para o tema.

Dessa forma, a presente pesquisa busca contribuir para o debate contemporâneo sobre a regulação da inteligência artificial no Brasil, especialmente no âmbito penal, reconhecendo a complexidade do tema e a necessidade de um equilíbrio permanente entre inovação tecnológica, proteção de direitos fundamentais e justiça social.

1. INTELIGÊNCIA ARTIFICIAL E A LACUNA REGULAMENTAR: DESAFIOS PARA A JUSTIÇA E A RESPONSABILIDADE PENAL

No cenário contemporâneo, a Inteligência Artificial (IA) vem tomando espaço do debate público, com uma ampla gama de aplicações que permeiam desde áreas tradicionais, como a indústria, o comércio e a agricultura, até setores mais complexos, como a Saúde e o Direito⁴. Sob essa perspectiva, os professores Haenlein e Kaplan (2019, s.p) em sua obra “*A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence*” definem a inteligência artificial como “a capacidade de um sistema interpretar dados externos corretamente, aprender a partir desses dados e usar esses aprendizados para alcançar objetivos e realizar tarefas específicas por meio de adaptação flexível”. Essa definição destaca três elementos fundamentais: (1) a interpretação precisa de informações, (2) o aprendizado contínuo e (3) a aplicação adaptativa, que tornam os sistemas de IA ferramentas poderosas em diversas áreas, incluindo o Direito Penal.

Na seara penal, a inteligência artificial vem sendo aplicada em alguns campos, tendo como exemplos os sistemas de controle, checagens, verificações de correção, predição de cenários, recomendações de estratégias para a defesa ou acusação, incrementos em automação de processamento de documentos, reconhecimento facial etc. (PEIXOTO, 2020). Apesar disso, existem alguns riscos que devem ser levados em consideração, tais como, a discriminação algorítmica e a violação dos direitos humanos.

Cabe ressaltar que a aplicação da inteligência artificial carrega consigo um duplo impacto: ao mesmo tempo que ela é um avanço tecnológico, com características inovadoras e revolucionárias para o âmbito jurídico, é preciso ter cautela com as questões éticas, sociais e legais. No âmbito investigativo, a IA vem se demonstrando capaz de analisar rapidamente grande volume de dados, sendo um recurso valioso para o Poder Público. A título de exemplo, tem-se o reconhecimento facial, utilizado na identificação de suspeitos em câmeras de segurança (CAMPELO, 2023).

Um caso emblemático envolvendo o uso de inteligência artificial no auxílio de investigações, ocorreu em janeiro de 2020 com um homem negro estadunidense. Robert Williams foi algemado na frente de suas filhas e esposa, acusado de roubar uma loja de luxo. A prisão ocorreu com a ajuda de um software de reconhecimento facial que comparando as fotos de seus documentos pessoais com as câmeras de segurança soltou o mandado de

⁴ A utilização do termo “Direito” com inicial maiúscula justifica-se por sua compreensão enquanto ciência social aplicada e sistema normativo em constante construção, que não se apresenta como uma ciência exata ou fechada, mas como um campo dinâmico, histórico e interpretativo, permanentemente influenciado por transformações sociais, políticas, econômicas e tecnológicas. Nesse sentido, a grafia em maiúscula reflete seu status de área do conhecimento dotada de autonomia científica e relevância institucional.

prisão. Mesmo as fotos sendo divergentes, os policiais tardaram a duvidar do sistema operacional de IA (SILVA, 2022).

Citando caso análogo mais próximo, um homem negro brasileiro foi preso injustamente em frente a sua família em uma festa em Salvador-BA, após ter seu rosto reconhecido pelo software de reconhecimento facial. De acordo com o Portal G1, ainda não se sabe como que o rosto do homem foi parar no banco de dados do reconhecimento facial, visto que ele nunca tivera cometido nenhum crime. Cabe ressaltar, que além do constrangimento da prisão equivocada, o injustiçado perdeu, também, o emprego, saindo prejudicado diante dessa situação (ALENCAR, 2023).

Esses casos revelam um dos riscos citados acima: a discriminação algorítmica, mais especificadamente, o racismo algorítmico. Sobre esse tema, o especialista Tarcízio Silva (2022, p. 37) em seu livro “Racismo algorítmico: inteligência artificial e discriminação nas redes digitais” expõe: “se a tecnologia é erroneamente enquadrada e percebida como neutra, a tal equívoco se soma a negação do racismo como fundante de relações e hierarquias sociais em países como o Brasil.”. Portanto, por meio dessa consideração, pode-se concluir que a tecnologia não é neutra, e tratar ela dessa forma seria um equívoco, especialmente porque tecnologias, como a inteligência artificial, não existem de forma isolada da sociedade. Além disso, essa falsa percepção de neutralidade pode perpetuar o preconceito e as desigualdades sociais, como o racismo estrutural⁵, potencializado por sistemas automatizados. Segundo essa linha de raciocínio, chega-se à conclusão de que as falhas estruturais do sistema penal tornam a adoção de inteligência artificial um risco considerável sem uma regulamentação adequada, pois tais sistemas podem reproduzir e ampliar desigualdades existentes.

A falta de transparência dos algoritmos, muitas vezes tratados como caixas-pretas, dificulta a auditoria e pode comprometer a equidade no tratamento dos réus, especialmente em um sistema que historicamente discrimina por raça, classe e local de residência (LIMA, 2024). Além disso, a utilização de sistemas automatizados para decisões judiciais ou previsões de reincidência tende a reduzir o papel crítico dos operadores do Direito, tratando casos humanos de forma mecanizada e descontextualizada (VIEIRA, 2022).

A ausência de um marco regulatório claro agrava o cenário, dificultando a

⁵ O termo “racismo estrutural”, conforme estudado por Djamila Ribeiro, refere-se a um sistema de opressões que não se manifesta apenas em atitudes individuais, mas está incorporado às estruturas políticas, econômicas, jurídicas e sociais, moldando de forma histórica e contínua as relações de poder e desigualdade. Trata-se de um fenômeno que organiza a própria dinâmica da sociedade, produzindo privilégios e desvantagens de modo sistemático, ainda que sem intenções explícitas dos agentes individuais. Nesse sentido, o racismo estrutural opera de forma difusa, naturalizada e institucionalizada, influenciando inclusive o funcionamento de tecnologias e algoritmos.

responsabilização em casos de erros ou decisões enviesadas, enquanto ferramentas de vigilância como reconhecimento facial colocam em risco direitos fundamentais, como privacidade e liberdade individual. Portanto, é necessário o debate para implementar regulamentações que assegurem a transparência, a ética e a responsabilidade no uso da IA, evitando que se transforme em um instrumento de perpetuação de desigualdades.

Conforme os estudos de Steffen (2023), a IA, quando não regulamentada, pode reproduzir discriminações e comprometer garantias processuais, especialmente no contexto penal, onde a transparência e a imparcialidade são vitais para a Justiça. Além disso, Peixoto (2020) destaca que a adoção dessas tecnologias exige uma abordagem crítica, com o Estado assumindo a responsabilidade de regular o uso e os operadores do Direito desempenhando um papel ativo na supervisão e na aplicação dos princípios constitucionais, como o devido processo legal e a igualdade de tratamento. Para isso, recomenda-se que o Estado estabeleça diretrizes claras e capacite juízes, promotores e advogados para avaliar criticamente decisões baseadas em inteligência artificial, garantindo que não sejam apenas validadas mecanicamente. Assim, a regulamentação ética da tecnologia deve ser uma prioridade coletiva, unindo esforços institucionais e profissionais em prol de um sistema jurídico justo e inclusivo. Os estudos mostram, portanto, que o direcionamento da pesquisa se faz na análise das implicações jurídicas da ausência de regulamentação da inteligência artificial no Direito Penal, com foco nas consequências da não regulamentação para a justiça e equidade, propondo recomendações para um marco regulatório ético e eficaz.

Essa lacuna regulatória também compromete a responsabilidade por erros e abusos. A dificuldade em auditar algoritmos utilizados para predições ou decisões judiciais impede que operadores do Direito e vítimas de decisões enviesadas questionem adequadamente esses sistemas. Isso contraria princípios constitucionais como a ampla defesa e a publicidade dos atos judiciais.

A justificativa, como já relatada na Introdução deste estudo, está vinculada ao cenário atual de expansão da utilização de inteligência artificial em diversas esferas sociais, incluindo o sistema de justiça penal. A ausência de uma legislação adaptada para lidar com os desafios éticos e jurídicos impostos pela IA compromete direitos fundamentais, como a igualdade, a privacidade e o devido processo legal, além de possibilitar a reprodução de preconceitos históricos por meio de algoritmos enviesados (STEFFEN, 2023; PEIXOTO, 2020). O uso de tecnologias como reconhecimento facial e sistemas preditivos tem gerado desafios importantes e polêmicos para a justiça penal, destacando, em suma a necessidade de uma regulamentação.

A integração dessas ferramentas com os princípios constitucionais e os direitos

humanos exige uma abordagem cuidadosa, pois para o desenvolvimento de uma regulamentação eficaz no Brasil, é necessário examinar como outros países têm tratado essa questão. A comparação entre os marcos regulatórios adotados em diferentes contextos internacionais oferece elementos para identificar modelos que podem ser aplicados no país. Na seção seguinte, analisa-se os marcos regulatórios de outros países e as implicações para a regulamentação no Brasil.

2. ESTUDO COMPARATIVO DE ABORDAGENS GLOBAIS E IMPLICAÇÕES PARA A REGULAMENTAÇÃO NO BRASIL

A regulamentação da inteligência artificial no Brasil ainda se encontra em estágio embrionário, carecendo de um marco normativo consolidado. A inexistência de diretrizes específicas para o uso dessas tecnologias compromete a clara delimitação das responsabilidades jurídicas, bem como a definição de critérios objetivos para sua aplicação nos diversos setores da sociedade. Esse quadro torna-se ainda mais complexo diante da limitada produção científica que analisa, de maneira sistematizada, as experiências regulatórias adotadas por outros países.

A análise dos modelos normativos implementados em diferentes ordenamentos jurídicos mostra-se essencial para a construção de uma legislação capaz de contemplar os riscos e impactos decorrentes da inteligência artificial. Contudo, a incipiência da produção acadêmica sobre o tema dificulta a identificação de padrões, tendências e boas práticas. A escassez de estudos comparativos sobre regulações estrangeiras, nesse sentido, compromete a avaliação precisa das vantagens e limitações das distintas abordagens regulatórias.

2.1 União Europeia

Segundo Veale e Borgesius (2021), o modelo europeu de regulação da inteligência artificial representa uma mudança de paradigma ao adotar uma abordagem baseada em riscos, na qual determinadas aplicações são diretamente proibidas por serem incompatíveis com direitos fundamentais, enquanto outras passam a ser rigidamente controladas por requisitos de transparência, segurança e supervisão humana.

Para Floridi et al. (2018), a proposta europeia parte da premissa de que a inteligência artificial deve ser juridicamente moldada de modo a promover a inovação sem abdicar da proteção da dignidade da pessoa humana, da igualdade e da autonomia individual.

A União Europeia (UE) estabeleceu um marco regulatório para a IA com o objetivo de garantir o desenvolvimento e a utilização segura dessa tecnologia. Em abril de 2021, a

Comissão Europeia propôs o *Artificial Intelligence Act*, que classifica os sistemas de IA com base nos riscos que representam. Essa abordagem define quatro categorias: (1) risco inaceitável, (2) alto risco, (3) risco limitado e (4) risco mínimo. Sistemas de IA considerados de risco inaceitável, como manipulação comportamental de grupos vulneráveis ou identificação biométrica em tempo real em espaços públicos, são proibidos, com exceções limitadas para aplicações de segurança.

Sistemas de alto risco, que afetam a segurança ou direitos fundamentais, são submetidos a requisitos rigorosos. Esses incluem avaliações pré-mercado e monitoramento contínuo durante o ciclo de vida do sistema. Áreas como infraestruturas críticas, educação, emprego e aplicação da lei estão sujeitas a essas regras. A legislação também estabelece requisitos de transparência para sistemas generativos, como o ChatGPT, exigindo a divulgação de conteúdo gerado por IA e a prevenção de produção de material ilegal.

A UE busca equilibrar a inovação com a proteção de direitos, permitindo que *startups* testem sistemas de IA em ambientes controlados. A implementação do regulamento será gradual, cuja proibição entrou em vigor em fevereiro de 2025. Regras para sistemas de alto risco terão um período de adaptação de 36 meses após a entrada em vigor da lei. Essa regulamentação reflete a preocupação da União Europeia em garantir que a IA seja desenvolvida de forma segura, transparente e alinhada com valores éticos. O *Artificial Intelligence Act* serve como referência global para a criação de frameworks regulatórios que promovam a inovação responsável e a proteção de direitos fundamentais.

2.2 Estados Unidos

De acordo com Calo (2017), o modelo estadunidense de regulação da inteligência artificial é caracterizado por uma governança fragmentada, marcada por diretrizes administrativas e iniciativas setoriais, sem a construção de um sistema normativo unificado e vinculante.

Citron e Pasquale (2014) alertam que, nos Estados Unidos, a ausência de um marco legal robusto permite que sistemas algorítmicos operem como caixas-pretas, produzindo discriminações e violações de direitos sem que haja mecanismos eficazes de responsabilização. O ex-presidente dos Estados Unidos, Joe Biden, assinou uma ordem executiva em agosto de 2023 para regulamentar o desenvolvimento e o uso da inteligência artificial. A medida visa mitigar riscos associados a preconceitos, violações de direitos civis e impactos na economia e na saúde pública (CITRON; PASQUALE, 2014). A ordem exige que desenvolvedores de sistemas de IA compartilhem com o governo os resultados de testes de

segurança antes de disponibilizá-los ao público. Além disso, orienta agências federais a estabelecer padrões para testes e avaliação de riscos.

Essa iniciativa representa um avanço em relação aos compromissos voluntários assumidos por empresas como OpenAI, Google e Meta, que haviam se comprometido a implementar marcas d'água em conteúdos gerados por IA. A ordem também determina que o Departamento de Comércio desenvolva diretrizes para autenticação de conteúdo e uso de marcas d'água, com o objetivo de identificar materiais produzidos por IA e garantir a confiabilidade das comunicações governamentais. Além disso, o líder da maioria no Senado Americano, Chuck Schumer, afirmou que espera concluir a legislação sobre IA nos próximos meses.⁶ Essas ações refletem um esforço coordenado para estabelecer um marco regulatório que equilibre inovação e segurança no setor de inteligência artificial.

2.2 China

A China, por sua vez, tem adotado uma postura mais intervencionista, por meio de leis como o Regulamento de Gestão de Algoritmos, que exige transparência e responsabilidade no uso de sistemas de IA. A regulamentação da inteligência artificial no país evoluiu ao longo dos anos por meio de uma estrutura normativa que busca equilibrar desenvolvimento tecnológico e controle estatal. Essa regulação pode ser dividida em três fases distintas, com impacto na governança dos sistemas de IA e na responsabilidade dos provedores.

Segundo Rogier Creemers (2022), o modelo chinês de regulação da inteligência artificial “prioriza a integração da governança algorítmica à segurança nacional e ao controle estatal da informação, diferentemente do enfoque ocidental centrado nos direitos individuais”.

Na primeira fase, entre 2017 e 2020, a China formulou diretrizes estratégicas sem imposição de regras obrigatórias. O Plano de Desenvolvimento de IA de Próxima Geração estabeleceu diretrizes gerais para fomentar a indústria e promover a pesquisa. Nesse período, a governança da IA permaneceu baseada em autorregulação, permitindo maior flexibilidade para o setor privado. Entre 2020 e 2022, houve uma transição para um modelo de padronização, com a introdução de normas técnicas e princípios regulatórios. Foram estabelecidas diretrizes para a padronização da IA, sem imposição de conformidade obrigatória. No mesmo período, leis como a Lei de Proteção de Informações Pessoais e a Lei de Segurança de Dados foram promulgadas, criando requisitos para o tratamento de dados em

⁶ Ressalta-se que as informações relativas ao andamento da legislação sobre inteligência artificial nos Estados Unidos correspondem ao contexto existente no momento da elaboração do presente trabalho. Eventuais atualizações posteriores, especialmente no âmbito do Senado norte-americano, não foram objeto de acompanhamento sistemático por esta pesquisa, em razão do recorte metodológico adotado.

sistemas de IA.

A partir de 2022, a regulamentação passou a impor obrigações diretas. Foram implementadas normas específicas para IA generativa, síntese profunda e algoritmos de recomendação. A supervisão governamental foi fortalecida, exigindo rastreabilidade, moderação de conteúdo e avaliação de segurança. Governos locais têm desenvolvido regulamentações adicionais para o setor. O modelo regulatório chinês busca consolidar a governança da IA em três eixos principais: (1) moderação de conteúdo, (2) proteção de dados e (3) governança algorítmica. Uma futura Lei Geral de IA pode unificar esses elementos, ampliando a segurança jurídica e definindo responsabilidades para empresas e desenvolvedores. Esse modelo se diferencia de regulações ocidentais, priorizando controle estatal e integração da IA à segurança cibernética.

2.4 Implicações para o Brasil

No Brasil, a regulamentação da inteligência artificial exige análise constitucional e penal, considerando direitos fundamentais e responsabilização jurídica. O art. 5º, X, da Constituição Federal de 1988 protege a intimidade e a vida privada, enquanto o inciso LVI assegura a presunção de inocência, princípios afetados por sistemas de identificação biométrica ou predição criminal (BRASIL, 1988). No âmbito penal, o art. 13 do Código Penal estabelece o nexo causal como requisito para imputação de responsabilidade, o que se complexifica em decisões automatizadas com resultados lesivos (BRASIL, 1947).

O debate sobre a regulamentação da inteligência artificial ainda se encontra em fase preliminar. Projetos de lei⁷ tramitam no Congresso Nacional, mas não há um marco regulatório consolidado. As propostas discutem princípios éticos, transparência e responsabilidade, mas não definem um modelo de governança específico. A ausência de uma estrutura normativa dificulta a segurança jurídica e a adoção de parâmetros para o uso da inteligência artificial em diferentes setores.

O comparativo entre as regulações internacionais e o cenário brasileiro demonstra a necessidade de avanços na definição de normas específicas. A experiência de outros países sugere que modelos regulatórios devem considerar fatores como transparência,

⁷ Entre os projetos legislativos mais conhecidos e frequentemente associados, ainda que de forma imprecisa, ao debate regulatório das tecnologias digitais, destaca-se o Projeto de Lei nº 2.630/2020, popularmente denominado “Projeto de Lei das Fake News”, cujo objetivo principal é estabelecer normas para a responsabilização e a transparência de plataformas digitais e serviços de mensageria. Embora não trate especificamente da inteligência artificial de forma sistemática, o referido projeto influenciou o debate público sobre regulação tecnológica no Brasil. Durante sua tramitação, houve forte reação de grandes empresas de tecnologia (Big Techs), como Google e Meta, que sustentaram, em campanhas públicas, que a proposta representaria risco à liberdade de expressão e configuraria espécie de censura, o que intensificou a polarização em torno do tema.

monitoramento contínuo e adaptação setorial. A formulação de um arcabouço normativo no Brasil pode se beneficiar da análise dessas abordagens, buscando um equilíbrio entre inovação e segurança jurídica.

Dessa maneira, os desafios relacionados à inteligência artificial no âmbito processual penal têm sido analisados pelos tribunais, que buscam compatibilizar a aplicação dessa tecnologia com a observância dos direitos fundamentais. O exame das decisões judiciais recentes permite avaliar como o Judiciário tem enfrentado essas questões e quais parâmetros têm sido adotados. A construção de um quadro regulatório se torna, portanto, essencial para disciplinar a responsabilidade penal, estabelecer diretrizes éticas e assegurar a proteção dos direitos humanos.

Para discutir essa perspectiva, a próxima seção analisa como os tribunais estão julgando esses casos e apresenta recomendações para a formulação de um marco normativo eficaz.

3. PROPOSTAS NORMATIVAS PARA O CONTROLE ÉTICO E PENAL DA INTELIGÊNCIA ARTIFICIAL

A ausência de um marco normativo consolidado sobre inteligência artificial no Brasil impõe a necessidade, como já pontuado, da construção de uma proposta regulatória que una segurança jurídica, proteção de direitos fundamentais e promoção da inovação. A experiência internacional, especialmente da União Europeia com o *Artificial Intelligence Act*, fornece subsídios valiosos para o desenvolvimento de um modelo brasileiro. Assim, propõe-se um conjunto de diretrizes estruturadas com base na Constituição Federal de 1988, no Código Penal, na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), e na Resolução CNJ nº 332/2020.

3.1 Classificação dos sistemas de IA por níveis de risco

A regulação da inteligência artificial no Brasil demanda, conforme sustentam diversos especialistas, a adoção de um modelo classificatório orientado por níveis de risco, nos moldes do *Artificial Intelligence Act* da União Europeia. Nesse sistema, aplicações consideradas de risco inaceitável devem ser expressamente vedadas, como a identificação biométrica em tempo real em espaços públicos sem autorização judicial, em respeito aos direitos à intimidade, à vida privada, à honra e à imagem, assegurados pelo art. 5º, X, da Constituição Federal. Também se insere nesse rol a predição criminal baseada em critérios discriminatórios, em consonância com o art. 5º, XLII, da CF/88, que tutela a igualdade e tipifica o racismo como crime, bem como a manipulação comportamental de grupos

vulneráveis, vedada à luz do art. 5º, III. Tais limitações buscam prevenir violações a direitos fundamentais e às garantias processuais, especialmente ao devido processo legal, previsto no art. 5º, LIV, da Constituição, segundo o qual “ninguém será privado da liberdade ou de seus bens sem o devido processo legal”.

Floridi (2021) sustenta que a regulação da inteligência artificial deve ser estruturada a partir de uma classificação escalonada de riscos, na qual sistemas capazes de afetar direitos fundamentais estejam sujeitos a controles preventivos mais rigorosos.

Os sistemas de alto risco, aplicados à justiça penal, segurança pública, previdência, saúde e crédito, exigem salvaguardas específicas. Devem ser submetidos a certificação prévia, testes de segurança, conforme o art. 6º, LGPD e avaliações de impacto ético e jurídico. A supervisão humana contínua é essencial para garantir conformidade com princípios como a individualização da pena, prevista no art. 5º, XLVI, CF/88 e a proteção de dados sensíveis, inserida no art. 11, LGPD.

Para sistemas de risco limitado ou mínimo, como ferramentas de produtividade ou análise de dados não críticos, recomenda-se regras de transparência, nos termos do art. 6º, VIII, LGPD, explicabilidade algorítmica e rastreabilidade. Essa abordagem equilibra inovação e proteção de direitos, assegurando que o desenvolvimento tecnológico respeite os limites constitucionais, conforme o art. 5º, XXVII e XXIX, CF/88. A adoção de um modelo escalonado permitiria ao Brasil alinhar-se a padrões internacionais, mitigando riscos sem inviabilizar avanços tecnológicos.

3.2 Responsabilização penal no uso de sistemas de Inteligência Artificial

A regulação da inteligência artificial exige a definição objetiva dos sujeitos responsáveis por danos decorrentes de sistemas autônomos. O art. 13 do Código Penal deve ser adaptado para incluir desenvolvedores, fornecedores, operadores, gestores e entes públicos que utilizem essas tecnologias. Essa ampliação considera a cadeia de desenvolvimento e aplicação dos sistemas, onde a autonomia algorítmica não elimina a responsabilidade.

Propõe-se a criação de tipos penais específicos para condutas como racismo algorítmico (art. 5º, XLII, CF/88) e uso indevido de reconhecimento facial (art. 5º, X, CF/88). As novas tipificações devem observar o princípio da legalidade estrita (art. 5º, XXXIX, CF/88) e da anterioridade penal (art. 1º do CP). Vale destacar que a Resolução CNJ nº 332/2020 e a LGPD (Lei nº 13.709/2018) oferecem parâmetros para governança algorítmica e transparência.

Além disso, a responsabilização deve considerar o nível de risco do sistema,

conforme classificação adotada pela União Europeia. Sistemas de alto risco exigem mecanismos de auditoria e supervisão humana contínua. A ausência de regulação específica pode gerar uma imputação subsidiária de responsáveis e insegurança jurídica em casos de danos difusos. A proposta busca equilibrar inovação tecnológica e proteção de bens jurídicos penalmente relevantes.

3.3 Avaliação de impacto ético, jurídico e social

Mantelero (2018) afirma que a avaliação de impacto algorítmico constitui instrumento indispensável para identificar riscos discriminatórios, violações de privacidade e impactos desproporcionais sobre grupos vulneráveis antes da implementação de sistemas automatizados.

Os sistemas de inteligência artificial classificados como de alto risco devem ser submetidos a avaliações de impacto obrigatórias antes de sua implementação. Conforme o modelo regulatório europeu, essas avaliações devem ser públicas, permitindo o escrutínio por órgãos de controle e sociedade civil. A transparência do processo assegura a conformidade com o princípio da publicidade administrativa, com fulcro no art. 37, §3º, CF/88.

Acrescenta-se que as avaliações devem ser conduzidas por equipes interdisciplinares, compostas por especialistas em direito, ciência da computação e ciências sociais. O art. 6º da LGPD estabelece parâmetros para análise de riscos no tratamento de dados pessoais, que podem ser estendidos para sistemas de IA. A metodologia deve identificar potenciais vieses discriminatórios, violações a direitos fundamentais e impactos desproporcionais em grupos vulneráveis. Ressalta-se, ainda, que os relatórios de avaliação devem conter medidas concretas de mitigação de riscos, incluindo ajustes técnicos e salvaguardas processuais. O art. 20 da LGPD prevê a revisão humana de decisões automatizadas, mecanismo que pode ser incorporado como requisito para sistemas de alto risco. Caso os riscos identificados sejam irredutíveis, as avaliações devem recomendar a suspensão ou descontinuação do uso da tecnologia.

Nesse mesmo raciocínio, a periodicidade das avaliações deve ser estabelecida em regulamento, considerando a evolução tecnológica e a dinâmica dos sistemas de IA. O art. 48 da LGPD prevê a atualização regular de relatórios de impacto, modelo que pode ser adaptado para fins de regulação algorítmica. A publicização dos resultados permite o controle social e judicial, em conformidade com o art. 5º, XXXIII da CF/88.

A obrigatoriedade das avaliações cria, portanto um marco de segurança jurídica para desenvolvedores e operadores de sistemas de IA. O art. 927 do Código Civil, que trata de responsabilidade objetiva, fundamenta a exigência de medidas preventivas para atividades

de risco (BRASIL, 2002) Além disso, a sistematização do processo avaliativo contribui para a formação de jurisprudência especializada em danos algorítmicos.

3.4 Supervisão humana e garantia do contraditório

O uso de sistemas de inteligência artificial em decisões que afetem direitos fundamentais exige salvaguardas processuais específicas. Com efeito, o art. 5º, LV, da CF/88 estabelece o contraditório e ampla defesa como requisitos essenciais para atos judiciais ou administrativos. As decisões automatizadas no processo penal devem ser submetidas obrigatoriamente à revisão por autoridade humana competente, conforme prevê o art. 20, §1º da LGPD.

Por outro lado, a justificativa técnica das decisões algorítmicas deve ser apresentada em linguagem acessível aos sujeitos processuais. Nesse sentido, o art. 93, IX da Constituição determina que todas as decisões judiciais sejam fundamentadas, princípio que se estende às decisões apoiadas por IA. Sistemas de alto risco devem incluir mecanismos de explicação que permitam compreender os critérios e variáveis consideradas.

Dessa maneira, o direito de contestação deve ser assegurado por meio de recursos administrativos e judiciais específicos, isso porque, o art. 5º, LIV da CF/88 garante o devido processo legal, que inclui a possibilidade de impugnação de decisões automatizadas. Na mesma linha, a Resolução CNJ nº 332/2020 estabelece parâmetros para o uso de tecnologias no Poder Judiciário, exigindo transparência nos sistemas decisórios.

Segundo Pasquale (2015), nenhum sistema automatizado pode substituir legitimamente a decisão humana quando estão em jogo direitos fundamentais, sob pena de erosão do contraditório e da própria ideia de justiça. A supervisão humana deve ocorrer em todas as fases processuais relevantes, incluindo instrução, decisão e execução penal. Cumpre destacar que o art. 156 do Código de Processo Penal prevê o dever de fundamentação de atos processuais, que não pode ser substituído por automatismos. Consequentemente, sistemas de apoio à decisão judicial devem preservar a discricionariedade do magistrado, conforme o art. 131 do Código de Processo Penal.

Por fim, a regulamentação deve especificar os parâmetros técnicos mínimos para auditoria de sistemas decisórios. Neste aspecto, o art. 6º, VIII da LGPD estabelece a transparência como princípio para tratamento de dados, aplicável igualmente a sistemas de IA. A explicabilidade dos algoritmos é, portanto, condição necessária para o exercício efetivo do direito de defesa.

3.5 Transparência e dever de informação

O marco regulatório brasileiro, para especialistas, deve estabelecer obrigações de transparência para operadores de sistemas de IA, conforme os parâmetros da Resolução CNJ nº 332/2020 e da LGPD (Lei nº 13.709/2018). O art. 6º, VIII da LGPD prevê o princípio da transparência como requisito para tratamento de dados, aplicável ao desenvolvimento e uso de tecnologias algorítmicas. Nesse contexto, os operadores devem divulgar de forma clara e acessível o emprego de IA em decisões públicas e judiciais, conforme determina o art. 9º da Resolução CNJ nº 332/2020. Mais especificadamente, as informações disponibilizadas devem abranger a finalidade, o funcionamento e os efeitos práticos dos sistemas de IA, uma vez que, o art. 20 da LGPD, assegura ao titular o direito a explicações sobre decisões automatizadas que afetem seus interesses. Além disso, a comunicação deve ser realizada em linguagem compreensível, observando-se o princípio da publicidade (art. 37, §3º da CF/88) e o direito à informação (art. 5º, XXXIII da CF/88).

No plano da proteção dos cidadãos, o marco regulatório deve assegurar mecanismos que garantam a informação adequada sobre seus direitos, incluindo a obrigatoriedade de revisão humana das decisões automatizadas. Nessa direção, o art. 20, §1º, da Lei Geral de Proteção de Dados (LGPD) consagra o direito à intervenção humana nos processos decisórios baseados exclusivamente no tratamento automatizado de dados pessoais. Em complemento, a Resolução nº 332/2020 do Conselho Nacional de Justiça reforça essa garantia ao assegurar a preservação da discricionariedade judicial nos sistemas de apoio à decisão. Como consequência, a adoção de práticas de transparência ativa fortalece o controle social e jurisdicional sobre o emprego de tecnologias no âmbito público.

3.6 Proteção rigorosa aos dados pessoais sensíveis

O regime jurídico da inteligência artificial deve reforçar as salvaguardas relativas ao tratamento de dados pessoais, especialmente nos âmbitos penal e da segurança pública. O art. 7º, I, da Lei Geral de Proteção de Dados (LGPD) estabelece a exigência de consentimento livre, informado e inequívoco para o tratamento de dados, princípio que deve ser observado de forma estrita nas aplicações de IA. Ademais, a finalidade legítima do processamento deve estar expressamente vinculada a objetivos determinados, explícitos e proporcionais, nos termos do art. 6º, II, da LGPD, sendo vedada a utilização para finalidades secundárias não autorizadas.

No que se refere aos dados sensíveis, o seu tratamento por sistemas automatizados deve submeter-se a restrições específicas, conforme dispõe o art. 11 da LGPD. Informações

relativas à raça, etnia, religião, orientação sexual e antecedentes criminais demandam proteção reforçada nos sistemas de perfilamento e em algoritmos preditivos. Nessa perspectiva, o art. 5º, XLII, da Constituição Federal veda práticas discriminatórias, proibição que se estende às aplicações baseadas em inteligência artificial.

Por outro lado, a legislação deve prever sanções penais e administrativas específicas para o uso inadequado de dados por sistemas automatizados. O art. 43 da LGPD dispõe sobre a responsabilização por danos decorrentes de violações à proteção de dados, hipótese que pode ser ampliada para casos envolvendo o uso de inteligência artificial. Além disso, a tipificação de condutas como a manipulação indevida de dados sensíveis deve observar o princípio da legalidade estrita, conforme o art. 5º, XXXIX, da Constituição Federal. Ressalta-se, ainda, que a Resolução CNJ nº 332/2020 estabelece parâmetros complementares para a proteção de dados no âmbito do Poder Judiciário.

3.7 Criação de uma autoridade nacional de inteligência artificial (ANIA)

Segundo Bioni (2021), modelos regulatórios eficazes no campo tecnológico exigem a criação de autoridades independentes com poderes normativos, fiscalizatórios e sancionatórios. Propõe-se que o ordenamento jurídico brasileiro institua uma autarquia federal independente, dotada de competências específicas para a fiscalização dos sistemas de inteligência artificial, a exemplo da Autoridade Nacional de Proteção de Dados (ANPD). Nesse contexto, o art. 37, XIX, da Constituição Federal autoriza a criação de entidades especializadas para a regulação de atividades tecnológicas. Caberia a essa autarquia a edição de normas técnicas relativas ao desenvolvimento, à implementação e à operação de sistemas de IA, em consonância com os parâmetros da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e da futura legislação setorial.

No que se refere às atribuições do órgão, destaca-se a certificação obrigatória dos sistemas classificados como de alto risco. O art. 55 da LGPD prevê a atuação da ANPD como autoridade certificadora dos processos de tratamento de dados, modelo que pode ser aplicado à regulação algorítmica. Ademais, a entidade disporia de poder sancionatório, nos termos do art. 52 da LGPD, com competência para a aplicação de multas e medidas corretivas.

No campo da inovação regulada, a autarquia seria responsável pela autorização de ambientes regulatórios experimentais destinados à realização de testes controlados. Ressalte-se que o art. 4º, III, da LGPD consagra o estímulo à inovação como princípio, compatível com mecanismos de experimentação supervisionada. A fiscalização do cumprimento das normas técnicas observaria os parâmetros do art. 37, §6º, da Constituição Federal, que dispõe sobre os

princípios da administração pública. Por fim, a estrutura organizacional do órgão deve assegurar independência funcional e técnica, em conformidade com o art. 37, *caput*, da CF/88.

3.8 Inclusão de princípios constitucionais e direitos humanos

O ordenamento jurídico brasileiro deve assegurar que a regulamentação da inteligência artificial incorpore expressamente os princípios constitucionais fundamentais. Com efeito, o art. 1º, III da CF/88 estabelece a dignidade da pessoa humana como fundamento da República, princípio que limita o desenvolvimento e aplicação de tecnologias algorítmicas. Ademais, art. 5º, *caput*, garante a igualdade e vedação a discriminações, diretriz essencial para prevenção de vieses em sistemas preditivos e de perfilamento.

Nesse contexto, o princípio da presunção de inocência, inserido no art. 5º, LVII da CF/88, e do devido processo legal, conforme o art. 5º, LIV, devem orientar o uso de IA no sistema penal. Além disso, a Resolução CNJ nº 332/2020 determina que tecnologias no judiciário preservem garantias processuais constitucionais. Assim, sistemas de apoio à decisão judicial não podem substituir a análise humana de elementos subjetivos do caso concreto.

Do mesmo modo, a utilização de IA em políticas públicas deve observar o princípio da proporcionalidade, com observância no art. 5º, II da CF/88. Por sua vez, o art. 3º, IV proíbe práticas discriminatórias, vedação que se estende a algoritmos com potencial excludente. O marco regulatório precisa, portanto, estabelecer salvaguardas contra usos expansivos de vigilância estatal sobre grupos vulneráveis. Complementarmente, a LGPD (Lei nº 13.709/2018) oferece parâmetros para proteção de dados que complementam essas garantias constitucionais.

3.9 Capacitação técnica e interdisciplinariedade no sistema de justiça

Para garantir a efetividade desse marco, o sistema de justiça brasileiro demanda formação especializada para atuar em casos envolvendo inteligência artificial. Nesse sentido, o art. 93, I da CF/88 estabelece a capacitação profissional⁸ como requisito para o exercício da magistratura, princípio extensível a todos os operadores do direito. Nessa perspectiva,

⁸ A expressão “capacidade profissional” deve ser compreendida, no atual contexto do sistema de justiça, de forma ampliada, não se limitando ao domínio técnico-jurídico tradicional, mas englobando também competências digitais e tecnológicas. Essa interpretação ganha reforço normativo com a edição da Resolução CNJ nº 654/2025, que passou a prever, como critério de avaliação para o vitaliciamento de magistrados, a “responsabilidade digital e o uso adequado de ferramentas tecnológicas, incluindo a inteligência artificial”. Tal diretriz atualiza o conteúdo do art. 93, I, da Constituição Federal, evidenciando que a aptidão para o exercício da magistratura, na contemporaneidade, pressupõe formação contínua, letramento digital e capacidade crítica para o uso responsável de sistemas automatizados.

programas de formação continuada devem abordar os limites técnicos e jurídicos da IA, conforme prevê a Resolução CNJ nº 332/2020 em seu artigo 5º.

Segundo Tartuce (2022), a transformação digital do Judiciário impõe a necessidade de formação técnica permanente dos operadores do direito, sob pena de submissão acrítica às tecnologias. Além disso, os tribunais devem estruturar núcleos especializados em perícia e auditoria de sistemas algorítmicos. Conforme o art. 156 do CPP, há previsão legal para a realização de exames técnicos, o que fundamenta a criação de equipes interdisciplinares. Tais núcleos devem contar com especialistas em ciência da computação, estatística e direitos fundamentais, conforme modelo adotado pelo Conselho Nacional de Justiça.

A jurisprudência deve desenvolver parâmetros para análise de casos envolvendo tecnologias automatizadas. O art. 5º, XXXV da CF/88 garante o acesso ao judiciário para revisão de atos lesivos decorrentes de sistemas de IA. Nesse aspecto as decisões judiciais precisam considerar os princípios da proporcionalidade (art. 5º, II) e da motivação (art. 93, IX) ao avaliarem resultados de processos automatizados. A experiência comparada, por sua vez, demonstra a necessidade de critérios uniformes para avaliação de provas técnicas.

3.10 Flexibilidade normativa e cooperação internacional

Para além da estruturação interna, o marco regulatório brasileiro deve prever mecanismos de atualização periódica, a fim de acompanhar a evolução tecnológica. A esse respeito, o art. 8º da LINDB prevê a adaptação do ordenamento jurídico às novas realidades sociais. Com base nesse fundamento, sistemas de revisão normativa periódica podem ser estruturados à semelhança do modelo europeu de avaliação quinquenal do *Artificial Intelligence Act*.

No plano externo, a cooperação internacional deve ser institucionalizada por meio de acordos com organismos como a OCDE e a Unesco. Segundo o art. 4º, IX da CF/88, a cooperação entre os povos constitui um princípio das relações internacionais brasileiras. Nessa linha, o compartilhamento de boas práticas pode seguir os parâmetros estabelecidos nas Diretrizes Éticas para IA da União Europeia e nos princípios da OCDE sobre inteligência artificial.

Por fim, a regulamentação deve prever adaptações setoriais considerando as especificidades tecnológicas e institucionais brasileiras. Nos termos do art. 174 da CF/88 compete ao Estado o dever de promover o desenvolvimento científico e tecnológico nacional. A Resolução CNJ nº 332/2020 oferece modelo para regulação específica no Poder Judiciário, o qual pode ser replicado em outros setores da administração pública. A

harmonização com padrões internacionais, contudo, deve observar os princípios constitucionais estabelecidos no art. 5º da CF/88.

CONSIDERAÇÕES FINAIS

A presente pesquisa teve como propósito central analisar os impactos jurídicos e éticos da ausência de regulamentação penal específica da inteligência artificial no Brasil, diante do avanço acelerado dessas tecnologias no âmbito da justiça criminal. Ao longo do trabalho, foi possível verificar que a utilização de sistemas automatizados, especialmente em atividades de vigilância, reconhecimento facial e apoio à decisão judicial, tem produzido efeitos significativos sobre direitos fundamentais, sem que exista, até o momento, um arcabouço normativo suficientemente estruturado para disciplinar tais práticas.

Os resultados obtidos demonstram que a aplicação da inteligência artificial no campo penal, quando desprovida de controles normativos rigorosos, amplia riscos de discriminação algorítmica, opacidade decisória e fragilização das garantias processuais. Os casos analisados de prisões indevidas baseadas em reconhecimento facial evidenciam que a tecnologia, longe de ser neutra, reproduz desigualdades estruturais já existentes na sociedade, especialmente relacionadas a raça, classe social e território. Assim, constatou-se que a inteligência artificial, quando incorporada a sistemas historicamente seletivos como o penal, pode potencializar mecanismos de exclusão e injustiça.

A análise comparativa das experiências internacionais revelou que diferentes países têm adotado estratégias diversas para a regulação da inteligência artificial. A União Europeia optou por um modelo preventivo e baseado na classificação de riscos, com forte ênfase na proteção de direitos fundamentais. Os Estados Unidos adotam um sistema mais fragmentado, com diretrizes administrativas e ordens executivas, enquanto a China desenvolveu um modelo fortemente intervencionista, centrado no controle estatal e na governança algorítmica. Essas experiências demonstram que não existe um modelo único de regulação, mas que todos reconhecem a necessidade de estabelecer limites jurídicos claros para o uso da inteligência artificial.

No contexto brasileiro, verificou-se que, embora existam instrumentos relevantes como a Constituição Federal, a Lei Geral de Proteção de Dados e a Resolução CNJ nº 332/2020, ainda persiste uma lacuna significativa quanto à regulação penal da inteligência artificial. Os projetos de lei em tramitação no Congresso Nacional representam avanços importantes, mas ainda carecem de consolidação e sistematização. Essa ausência de um marco

regulatório específico compromete a segurança jurídica e a efetividade da responsabilização por danos decorrentes de decisões automatizadas.

As propostas normativas apresentadas no artigo demonstraram-se compatíveis com os princípios constitucionais e com as melhores práticas internacionais. A classificação dos sistemas de IA por níveis de risco, a criação de tipos penais específicos, a exigência de avaliações de impacto ético e jurídico, a supervisão humana obrigatória, a transparência algorítmica, a proteção rigorosa de dados sensíveis e a instituição de uma autoridade nacional de inteligência artificial configuram um conjunto de diretrizes capazes de estruturar um modelo regulatório coerente, equilibrando inovação e tutela de direitos fundamentais.

Os objetivos propostos na introdução foram alcançados. Conseguiu-se identificar os principais riscos da inteligência artificial no sistema penal, analisar criticamente as experiências internacionais e apresentar diretrizes normativas para o contexto brasileiro. No entanto, a pesquisa também revelou lacunas importantes, sobretudo no que se refere à escassez de literatura especializada em língua portuguesa sobre o tema, o que evidencia a necessidade de ampliação dos estudos nacionais sobre inteligência artificial, direito penal e governança algorítmica.

A complexidade da temática restou amplamente demonstrada. A inteligência artificial não se apresenta apenas como uma ferramenta tecnológica, mas como um fenômeno multifacetado, que atravessa dimensões jurídicas, éticas, sociais, políticas e econômicas. Sua regulação exige abordagem interdisciplinar e atualização normativa contínua, considerando a velocidade das transformações tecnológicas. Não se trata, portanto, de um objeto de estudo que se esgota nesta pesquisa. Ao contrário, trata-se de um campo em permanente construção, aberto a múltiplas perspectivas teóricas e práticas.

Ficou evidenciado que a pesquisa não se encerra em si mesma. O avanço da inteligência artificial impõe novos desafios que exigirão constante revisão das normas, capacitação contínua dos operadores do direito e fortalecimento das instituições de controle. A governança da IA deverá ser construída como um processo dinâmico, capaz de acompanhar a evolução tecnológica sem renunciar à centralidade da dignidade da pessoa humana.

A regulamentação ética e penal da inteligência artificial no Brasil é, portanto, necessária e urgente. A ausência de controle normativo adequado pode transformar a tecnologia em instrumento de perpetuação de desigualdades, violação de direitos fundamentais e fragilização da justiça. Ao mesmo tempo, uma regulação bem estruturada permite que a inovação tecnológica seja incorporada de modo responsável, democrático e compatível com os valores constitucionais. O desafio posto ao Direito, portanto, é construir

um modelo regulatório que não apenas acompanhe o progresso tecnológico, mas que também seja capaz de humanizá-lo.

REFERÊNCIAS BIBLIOGRÁFICAS

ALENCAR, Itana. Com mais de mil prisões na BA, sistema de reconhecimento facial é criticado por racismo algorítmico; inocente ficou preso por 26 dias. **G1 Bahia**, Salvador, 01 set. 2023. Disponível em: <https://g1.globo.com>. Acesso em: 02 dez. 2024.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. São Paulo: Thomson Reuters Brasil, 2021.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988. Disponível em: <https://www.planalto.gov.br>. Acesso em: 01 maio 2025.

BRASIL. Decreto-Lei nº 2.848, de 07 de dezembro de 1940. **Institui o Código Penal**. Diário Oficial da União: Brasília, DF, 31 dez. 1940.

BRASIL. Decreto-Lei nº 3.689, de 03 de outubro de 1941. **Código de Processo Penal**. Diário Oficial da União: Brasília, DF, 13 out. 1941.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Código Civil**. Diário Oficial da União: Brasília, DF, 11 jan. 2002.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União: Brasília, DF, 15 ago. 2018.

BRASIL. Decreto-Lei nº 4.657, de 04 de setembro de 1942. **Lei de Introdução às Normas do Direito Brasileiro (LINDB)**. Diário Oficial da União: Brasília, DF, 09 set. 1942.

BRASIL. Conselho Nacional de Justiça. **Resolução nº 332, de 21 de agosto de 2020**. Dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário. Brasília, 2020.

CALO, Ryan. **Artificial intelligence policy: a primer and roadmap**. University of California Davis Law Review, v. 51, 2017.

CAMPELO, João. Uso de reconhecimento facial no Brasil e seus impactos jurídicos. **Revista Brasileira de Segurança Pública**, 2023.

CITRON, Danielle; PASQUALE, Frank. The scored society: due process for automated predictions. Washington Law Review, v. 89, 2014.

CREEMERS, Rogier. **China's algorithmic governance**. Oxford Handbook of Digital Regulation, 2022.

FLORIDI, Luciano et al. **AI4People – An ethical framework for a good AI society**. Minds and Machines, v. 28, 2018.

HAENLEIN, Michael; KAPLAN, Andreas. **A brief history of artificial intelligence**. California Management Review, 2019.

LIMA, David Silva. Os impactos da inteligência artificial na eficácia e equidade do Direito Penal. Revista FT, 2024. Disponível em: <https://revistaft.com.br>. Acesso em: 02 dez. 2024.

MANTELERO, Alessandro. **AI and data protection: challenges and risks**. Computer Law & Security Review, v. 34, 2018.

PASQUALE, Frank. **The black box society**. Cambridge: Harvard University Press, 2015.

PEIXOTO, Wagner. **Inteligência artificial aplicada ao Direito Penal**. Revista Brasileira de Direito Penal, 2020.

SILVA, Tarcízio. **Racismo algorítmico: inteligência artificial e discriminação nas redes digitais**. São Paulo: Sesc, 2022.

STEFFEN, Felipe. **Inteligência artificial, processo penal e garantias fundamentais**. Revista de Direito Penal Contemporâneo, 2023.

TARTUCE, Fernanda. **Justiça digital e formação dos operadores do direito**. São Paulo: Thomson Reuters, 2022.

UNIÃO EUROPEIA. Parlamento Europeu. **Lei da UE sobre IA: primeira regulamentação de inteligência artificial**. 12 jun. 2023. Disponível em: <https://www.europarl.europa.eu>. Acesso em: 22 mar. 2025.

VEALE, Michael; BORGESIU, Frederik Zuiderveen. **Demystifying the draft EU Artificial Intelligence Act**. Computer Law Review International, 2021.

VIEIRA, Ana Luiza Feitosa. **A utilização da inteligência artificial no direito penal e seus impactos na prática jurídica**. Rio de Janeiro: PUC-Rio, 2024. Disponível em: <https://www.maxwell.vrac.puc-rio.br>. Acesso em: 01 abr. 2025.