

COMO O DIREITO PENAL PODE (OU NÃO) REAGIR AO USO DE INTELIGÊNCIA ARTIFICIAL EM PRÁTICAS ILÍCITAS

HOW CRIMINAL LAW CAN (OR CANNOT) REACT TO THE USE OF ARTIFICIAL INTELLIGENCE IN ILLEGAL PRACTICES

Recebido em 22.09.2025

Aprovado em 18.06.2026

Pedro Henrique Maciel de Araújo¹**Cássio André Borges dos Santos²**

RESUMO

O crescimento da inteligência artificial (IA) tem impactado profundamente os diversos setores da sociedade, incluindo a esfera criminal. A utilização dessa tecnologia para a prática de crimes, como fraudes automatizadas, produção de *deepfakes*, disseminação automatizada de desinformação e ataques cibernéticos, levanta questões importantes sobre a capacidade do Direito Penal contemporâneo de lidar com essas novas formas de ilicitude, trazendo à tona o problema central deste estudo: como o Direito Penal brasileiro pode — ou não — reagir ao uso da IA em crimes diante da ausência de normatização específica e dos princípios de intervenção mínima e proporcionalidade. O trabalho tem por objetivo analisar a adequação e os limites do Direito Penal frente a esses ilícitos, compreendendo os mecanismos que tornam a IA um instrumento delitivo, avaliando a suficiência do ordenamento jurídico nacional em comparação às práticas internacionais, identificando desafios probatórios e investigativos e discutindo alternativas de atualização legislativa e interpretativa. Utiliza-se metodologia qualitativa, de caráter exploratório e descritivo, com abordagem dedutiva, apoiada em pesquisa bibliográfica, análise documental de normas e estudo de exemplos concretos. Conclui-se que o Direito Penal deve equilibrar inovação tecnológica e segurança jurídica, garantindo a proteção dos direitos fundamentais diante do cenário tecnológico no qual se insere.

Palavras-chave: direito penal. inteligência artificial. práticas ilícitas.

¹Graduando em Direito pela Universidade do Estado do Amazonas (UEA). E-mail: pedro.henri.araujo@hotmail.com. ORCID: <https://orcid.org/0009-0000-9982-6416>.

² Doutor em Direito Público pela Universidade de Coimbra e em Direito Constitucional pela Universidade Federal de Minas Gerais (UFMG). Mestre em Direito Constitucional pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Graduado em Direito pela Universidade Federal do Amazonas (UFAM). Professor Adjunto da graduação e pós-graduação da Universidade do Estado do Amazonas (UEA) e Juiz de Direito no Tribunal de Justiça do Amazonas (TJAM). E-mail: cadred@uol.com.br. ORCID: <https://orcid.org/0000-0003-2168-5363>.

ABSTRACT

The growth of artificial intelligence (AI) has profoundly impacted various sectors of society, including the criminal sphere. The use of this technology to commit crimes such as automated fraud, deepfake production, automated dissemination of disinformation, and cyberattacks raises important questions about the ability of contemporary criminal law to address these new forms of illegality, highlighting the central problem of this study: how Brazilian criminal law can—or cannot—respond to the use of AI in crimes in the absence of specific regulations and the principles of minimal intervention and proportionality. This study aims to analyze the adequacy and limits of criminal law in the face of these offenses, understanding the mechanisms that make AI a criminal instrument, assessing the sufficiency of the national legal system in comparison with international practices, identifying evidentiary and investigative challenges, and discussing alternatives for legislative and interpretative updates. A qualitative, exploratory, and descriptive methodology is used, with a deductive approach, supported by bibliographic research, documentary analysis of regulations, and the study of concrete examples.

Keywords: artificial intelligence. criminal law. illicit practice.

1 INTRODUÇÃO

É fato que a inteligência artificial trouxe inovações em todos os aspectos da sociedade, seja facilitando questões cotidianas, seja maximizando o potencial evolutivo tecnológico com sua alta capacidade de analisar dados em níveis inumanos. Por outro lado, essa mesma tecnologia passou a ser utilizada para fins inicialmente não planejados, alterando sua destinação para a ilicitude por meio de criminosos que dela se aproveitam devido às mesmas capacidades e habilidades pelas quais conquistou o mundo há alguns anos.

Dentro desse contexto, é importante mencionar que muitas condutas ilícitas que antes demandavam muito esforço por parte dos indivíduos, agora são delegadas ao computador que, por sinal, melhora exponencialmente a efetividade do resultado ilícito. Por exemplo, se anteriormente um criminoso precisava convencer, por meio de mensagens, uma mãe a transferir dinheiro a seu suposto filho (estelionato), hoje basta fazer com que uma IA reproduza uma voz idêntica da personalidade suposta, não havendo margem de dúvida por parte da vítima, consumando o crime por meio de um único áudio criado artificialmente.

Por isso, os operadores do direito possuem o dever de se adaptar a essa nova realidade e trazer o direito penal como a solução para esses conflitos, através da atualização e transformação das ideias preconcebidas que criaram esse ramo jurídico, de

forma que traga uma maior segurança jurídica e a certeza de que o meio digital não é uma terra sem lei, e de que atos, ainda que anônimos, podem ser combatidos e responsabilizados.

Por fim, a relevância deste estudo reside na necessidade de adaptação do Direito Penal a um ambiente digital cada vez mais complexo e interconectado. Ao refletir sobre os riscos e potencialidades da IA, pretende-se contribuir para o debate acadêmico e social sobre a proteção eficaz de bens jurídicos e o fortalecimento do Estado Democrático de Direito diante das transformações tecnológicas em curso.

2 A INTELIGÊNCIA ARTIFICIAL E O DIREITO PENAL

A Inteligência Artificial (IA) surgiu ainda na primeira metade do século XX, sendo desenvolvida por Warren McCulloch e Walter Pitts, que propunham um modelo de neurônios artificiais. A base de sua pesquisa esteve alicerçada em três pilares, ou seja, no conhecimento da filosofia básica relacionada com a função dos neurônios do cérebro; o estudo formal da lógica proposicional desenvolvida por Russel e Whitehead; e, por fim, a teoria computacional de Turing (Russel; Norvig, 2013).

Desde então, o avanço significativo das tecnologias trouxe impactos gradativos na forma de evolução de cérebro artificial, chegando ao ponto deste se tornar capaz de analisar quantidades inimagináveis de dados, trazendo simplificação e praticidade para o trabalho humano, aumentando ainda mais a velocidade evolutiva, características que, teoricamente, são benéficas à sociedade.

Contudo, chegando ao ponto de estar intrinsecamente presente na sociedade, a IA inevitavelmente se tornaria objeto de discussões perante o Direito, já que este, pelo seu próprio conceito, é um conjunto de normas de conduta social, imposto coercitivamente pelo Estado, para realização de segurança, segundo critérios de justiça (Nader, 2003). E como toda tecnologia, os seus usos são bastante diversificados, de forma que a ciência penal teve de intervir ao se deparar com indivíduos que deturparam as características benéficas da tecnologia e dela se aproveitaram em prol de seus próprios interesses ilícitos, afinal, segundo Carvalho e Giongo (2019, p. 1), “a esfera de atuação do direito

penal não fica imune às alterações sofridas na sociedade e à implementação de novos conflitos oriundos do boom tecnológico”.

Dentro desse cenário, o que antes parecia ser uma dádiva evolutiva, agora se tornou um perigo invisível, capaz de atingir uma grande quantidade de pessoas, ou causar grandes danos, com apenas um clique. Para entender o desafio gerado por essa situação, é necessário primeiro compreender como a IA funciona. Segundo Giuffrida, Lederer e Vermeys (2018, p. 753):

O aprendizado de máquina pode ser resumido como a capacidade de um computador de modificar sua programação para dar conta de novos dados e modificar suas operações de acordo com eles. Ele usa computadores para executar modelos preditivos que aprendem com os dados existentes para prever futuros comportamentos, resultados e tendências. O aprendizado de máquina, portanto, depende de dados. Quanto mais dados puder acessar, melhor poderá aprender.

Logo, diante das vastas possibilidades de o infrator obter informações das vítimas dentro da internet e redes sociais em tempos modernos, o computador consegue a matéria-prima necessária para gerar conteúdos capazes de enganá-las, tudo isso sem que o agente precise se expor de maneira explícita e com o benefício de não gerar vestígios fáceis de identificação e rastreamento. Isso cria um ambiente propício ao surgimento de indivíduos que, a princípio, não praticariam ilícitos, mas, ao equilibrarem a facilidade e anonimidade para cometer delitos, e as dificuldades para identificá-lo por parte das autoridades, escolhem a saída mais fácil e ilícita.

Por outro lado, também podemos dizer que a IA e o Direito Criminal possuem dupla dimensão, uma vez que os próprios operadores do direito podem se utilizar desse mecanismo tecnológico nas investigações a fim de responsabilização dos criminosos, trazendo a sua função precípua de maximizar a eficiência do trabalho humano, através de análises preditivas, processamento de dados, reconstrução virtual de cenas de crimes, entre diversas outras modalidades práticas. É válido destacar também os limites que devem ser observados ao utilizar essas ferramentas de forma que não viole os direitos fundamentais à privacidade, à dignidade humana e ao devido processo legal.

3 PANORAMA JURÍDICO ATUAL

Uma vez estabelecida a necessidade de o Direito Penal combater as práticas ilícitas viabilizadas pelo uso da inteligência artificial, busca-se compreender se o ordenamento jurídico atual possui as diretrizes, os princípios e as normas capazes de colocar em prática a inibição dessa cadeia de crimes tecnológicos.

Do ponto de vista normativo, a legislação brasileira ainda não dispõe de lei específica que discipline a responsabilidade penal no contexto de crimes praticados por meio ou com o auxílio da IA. O Código Penal de 1940, evidentemente, não contemplou tal realidade tecnológica, e as normas mais recentes — como a Lei nº 12.965/2014 (Marco Civil da Internet) e a Lei nº 14.155/2021, que trata de crimes digitais —, embora importantes, não diferem a gravidade dos crimes pelo grau de complexidade na utilização de recursos tecnológicos, sendo limitadas à superficialidade e à generalização de condutas ilícitas que envolvam meios eletrônicos. A exemplo disso, tem-se o crime de fraude eletrônica, previsto no artigo 171, § 2º-A, do Código Penal:

Estelionato

Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:

Fraude eletrônica

§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021)

Pela interpretação do texto legislativo, o crime se consuma com a utilização das informações obtidas, sem especificar a forma pela qual tais dados foram recolhidos, bastando a expressão “induzido a erro”, o que pode gerar uma deturpação da gravidade nas formas de execução do crime, pois uma situação em que um indivíduo fornece seus dados descuidadamente a um desconhecido que entrou em contato oferecendo serviços é completamente diferente, e bem menos grave, de uma situação em que um filho fornece seus dados bancários após a solicitação de seu pai por meio de um áudio criado por inteligência artificial, que se utilizou de vídeos anteriores que o próprio filho publicava em suas redes para criar uma cópia indistinguível.

Este é só um exemplo de como a ausência de normas específicas mais graves e severas para o uso de IA pode representar uma insegurança massiva na sociedade, pois,

dessa forma, o emprego de fraudes e enganações comuns possuirão o mesmo peso que um recurso tecnológico capaz de destruir a linha entre o que é real e o que não é.

Em resposta a esse cenário, atualmente tramita o Projeto de Lei 2338/23, cujo objetivo é a regulamentação do uso de inteligência artificial no Brasil, classificando os sistemas conforme seus níveis de risco e distinguindo a IA comum da IA generativa. O texto prevê avaliação preliminar de risco obrigatória apenas para sistemas generativos e de propósito geral (GPT, por exemplo), a fim de identificar potenciais impactos antes da entrada no mercado. Além disso, proíbe tecnologias de risco excessivo, como armas autônomas, sistemas que disseminem exploração infantil ou que façam previsão de crimes com base em perfis de comportamento (policiamento preditivo). O uso de câmeras de reconhecimento em locais públicos será restrito a situações específicas, mediante autorização judicial. A proposta também disciplina os direitos autorais, permitindo o uso de conteúdos protegidos apenas para fins de pesquisa, educação e jornalismo sem fins comerciais, garantindo remuneração ou veto ao titular quando empregados no desenvolvimento de sistemas comerciais de IA.

Essa iniciativa demonstra a necessidade cada vez mais elevada de pôr rédeas em um ser artificial e sem fronteiras, com a capacidade de atingir qualquer pessoa em qualquer lugar do planeta. Porém, apesar da boa intenção, o texto legislativo se restringe à responsabilidade civil e sanções administrativas, como multa de até 50 milhões de reais, por exemplo, deixando de lado o aspecto penal relevante, permanecendo insuficiente para suprir as nuances da realidade.

No cenário internacional e em outros países, esse tema também é debatido com a devida seriedade, sendo a União Europeia um dos principais expoentes que buscam conscientizar a sociedade global sobre os perigos que permeiam o mundo digital, fazendo isso através da confecção da primeira lei abrangente do mundo que regulamenta a IA (*EU AI Act*³), publicada em junho de 2024, cujos efeitos, em sua maior parte, deverão ser aplicados 24 meses após sua entrada em vigor. De forma geral, esse Ato tem amplo escopo de aplicação, impactando primordialmente fornecedores/desenvolvedores dentro

³ Cf. UNIÃO EUROPEIA. Regulamento (UE) 2024/1689, de 13 de junho de 2024 (Regulamento Inteligência Artificial). Jornal Oficial da União Europeia, L, 2024/1689, 12 jul. 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ%3AL_202401689. Acesso em: 28 ago. 2025.

ou fora da UE que colocam sistemas de IA no mercado ou em serviço (para uso próprio por uma entidade pública ou privada).

Já nos Estados Unidos foram apresentados mais de mil projetos de lei relacionados à inteligência artificial nos primeiros meses de 2025. Apesar da ausência de uma legislação federal específica sobre o tema, em 2023 a administração Biden havia editado uma ordem executiva destinada a promover o uso seguro e responsável da IA no país. Contudo, logo no início de seu mandato, o presidente Donald Trump revogou essa medida e determinou a revisão das normas que pudessem restringir a inovação tecnológica.

Nesse cenário, em maio, o Senado norte-americano promoveu audiências para discutir de que forma a redução de barreiras regulatórias ao longo da cadeia de desenvolvimento da IA poderia impulsionar a inovação e consolidar a liderança dos Estados Unidos no setor⁴.

Diante desse panorama nacional e internacional, é notável ver que, apesar do surgimento cada vez mais frequentes de regulações sobre a IA, o âmbito Penal dessas questões permanece insuficiente às demandas reais. As práticas ilícitas envolvendo inteligências tecnológicas ainda não são enquadradas em tipos penais tradicionais, o que pode não abarcar adequadamente a gravidade e a especificidade de tais condutas. A ausência de normatização específica, para além do âmbito cível e administrativo, fragiliza a eficácia da tutela penal e deixa lacunas interpretativas, que poderão gerar tanto impunidade quanto excessos punitivos.

Portanto, o desafio atual é equilibrar inovação tecnológica e segurança jurídica. O Direito Penal, por sua natureza de *ultima ratio*, deve resistir a respostas precipitadas, mas não pode se manter inerte frente às transformações trazidas pela IA. Os próximos passos apontam para a necessidade de uma atualização legislativa criteriosa, acompanhada de diálogo interdisciplinar entre juristas, técnicos e sociedade, estabelecendo limites claros

⁴ Cf. ESTADOS UNIDOS. Senate Committee on Commerce, Science, and Transportation. **Winning the AI Race: Strengthening U.S. Capabilities in Computing and Innovation**. Washington, D.C., 8 maio 2025. Disponível em: <https://www.commerce.senate.gov/2025/5/winning-the-ai-race-strengthening-u-s-capabilities-in-computing-and-innovation> 2. Acesso em: 28 ago. 2025.

para a utilização da inteligência artificial e a correspondente punição de indivíduos, e não apenas pessoas jurídicas, que dela se utilizam para propósitos ilegais.

4 INTELIGÊNCIA ARTIFICIAL COMO INSTRUMENTO DO CRIME

Adentrando na parte prática da problemática, é perceptível como a deturpação dos recursos disponíveis nas novas tecnologias tem-se espalhado cada vez mais em diferentes camadas das infrações. Nessa dimensão, a tecnologia não atua de forma autônoma como autora de condutas, mas sim como meio pelo qual agentes humanos potencializam ou sofisticam a prática delitiva.

Sob a ótica penal, esse enquadramento mantém o foco na responsabilidade humana. O sujeito ativo do crime continua sendo a pessoa que manipula, controla ou se beneficia da utilização da IA. Assim, os tipos penais já existentes — como estelionato, falsificação de documento, crimes contra a honra, crimes contra sistemas informáticos ou mesmo lavagem de dinheiro — podem ser aplicados a essas condutas, ainda que o *modus operandi* envolva a mediação tecnológica.

Primeiramente, é preciso entender a base pela qual utilização das IAs se torna tão eficaz. No século XX, houve o surgimento do Teste de Turing, cujo objetivo principal era medir a capacidade de uma máquina exibir comportamento inteligente equivalente ao de um ser humano, ou indistinguível deste. O teste foi introduzido pelo matemático Alan Mathison Turing, em seu artigo de 1950 denominado "*Computing Machinery and Intelligence*" (Turing, 1950). O teste inicia-se com as seguintes palavras: "Eu proponho considerar a questão: as máquinas podem pensar?". Já que "pensar" é um termo de difícil de definição, o autor preferiu "trocar a pergunta por outra, a qual está relacionada à anterior, e é expressa em palavras menos ambíguas". Para isso, ele propôs o jogo da imitação, que consiste em uma situação em que um interrogador humano conversa simultaneamente com duas testemunhas, uma humana e uma máquina, apenas por meio da conversação escrita. Ambas as testemunhas tentam convencer o interrogador de que são O humano real. Se o interrogador não conseguir identificar de forma confiável quem é o humano, considera-se então que a máquina passou no teste

O novo questionamento de Turing consiste no seguinte: "Há como imaginar um computador digital que faria bem o 'jogo da imitação?'". Alan Turing acreditava que esta questão poderia ser respondida, sendo que no restante do artigo, o matemático estabelece argumentos contra as principais objeções à proposta inicial de que "máquinas podem pensar". Turing concluiu, por fim, que se um computador fosse capaz de enganar um terço de seus interlocutores, fazendo-os acreditar que ele seria um ser humano, então estaria pensando por si próprio.

De volta à atualidade, os pesquisadores Cameron R. Jones e Benjamin K. Bergen, do Departamento de Ciência da Computação da Universidade Cornell, nos Estados Unidos, decidiram conduzir um novo experimento, com base nos estudos de Turing, tendo como objeto as inteligências artificiais atuais (Jones, Bergen, 2025). Como resultado, o modelo GPT-4.5, da OpenAI, quando instruído a adotar uma persona semelhante à humana, conseguiu enganar 73% dos participantes e se passar por humano, obtendo uma taxa de sucesso muito superior a um terço, como proposto por Turing.

Diante desse cenário, uma vez comprovada a habilidade de se passar por seres humanos, a inteligência artificial ganha novos contornos que podem ser usados e abusados por aproveitadores em diversas situações possíveis.

4.1 Crimes Cibernéticos e Automação Delitiva

Os crimes cibernéticos são aqueles em que a atuação da inteligência artificial mais se destaca, de forma a usar toda sua capacidade e escala para atingir um número significativo de vítimas, diminuindo o trabalho do criminoso e maximizando sua eficiência.

Dentro desse contexto, um dos crimes mais comum é o *phishing*, o qual se baseia em fraudes para enganar as vítimas através do envio de mensagens, geralmente e-mails, roubando a identidade de instituições e empresas legítimas como disfarce. O alvo, então, fornece seus dados, como número de cartão ou informações financeiras, acreditando fielmente no texto produzido artificialmente, que se torna cada vez mais adaptado ao perfil da vítima por ter acesso às suas redes sociais e bancos de dados públicos, tornando-a mais vulnerável a ataques.

Existe também os ataques de *ransomware*, que se baseiam em programas que sequestram dados dos usuários, criptografando-os, e exigindo um resgate em dinheiro para a recuperação de tais informações. Para evitar e se proteger dessa ameaça, os indivíduos se veem cada vez mais obrigados a guardar seus dados com mais sistemas de segurança e *backups* em outros locais.

Todos esses sistemas informatizados e automatizados com aprendizado de máquina conseguem identificar rapidamente as vulnerabilidades da rede e se esquivar dos programas de segurança comuns, criando um ambiente extremamente valioso para o criminoso, uma vez que ele não precisa atuar diretamente nos crimes, reduzindo drasticamente as possibilidades de ser rastreado ou identificado, sendo essa uma das características mais graves e alarmantes quando se trata de crimes utilizando inteligência artificial.

4.2. Crimes Patrimoniais e Financeiros

No campo patrimonial, as fraudes bancárias e financeiras foram aprimoradas a ponto de quase se tornar ficção, principalmente pela difusão de uma ferramenta chamada *deepfakes*, que surgiu pelas possibilidades trazidas pela IA. Geralmente, os criminosos se utilizam das informações disponíveis na rede, como imagem, sons, áudio, para criar uma versão completamente artificial, mas incrivelmente real de uma pessoa conhecida pela vítima, que, ao se deparar com o falso, abaixa sua guarda, tornando-se vulnerável ao delito. A exemplo disso, em 2024, um funcionário financeiro de uma empresa multinacional pagou US\$ 25 milhões a fraudadores que usaram tecnologia *deepfake* para se passar por diretor financeiro da empresa em uma videoconferência, juntamente com diversas outros funcionários que a vítima acreditava serem reais, mas não passavam de criações falsas⁵.

Além disso, é válido destacar também o fato de que os sistemas inteligentes conseguem burlar sistemas de segurança de instituições financeiras e realizar transações

⁵ CHEN, Heather; MAGRAMO, Kethleen. **Funcionário de multinacional paga US\$ 25 mi a golpista que usou "deepfake" para simular reunião**. CNN Brasil, 4 fev. 2024. Disponível em: <https://www.cnnbrasil.com.br/internacional/funcionario-de-multinacional-paga-us-25-mi-a-golpista-que-usou-de-epfake-para-simular-reuniao/>. Acesso em: 23 jul. 2026.

fraudulentas de forma quase indetectável, através da detecção e exploração de vulnerabilidades em segundos, rompendo com a lógica de defesa baseada em tempo de resposta.

Da mesma forma, a criptografia altamente avançada proporcionada pela IA é profundamente explorada no âmbito da lavagem de dinheiro, já que os sistemas podem estruturar operações extremamente complexas, espalhando-as por diversas jurisdições e países pelo mundo, gerando uma dificuldade intrínseca na localização da origem ilícita dos valores. Assim, nota-se a forma pela qual os recursos tecnológicos se tornam capazes de criar uma verdadeira camuflagem financeira, exigindo que o Direito Penal igualmente se renove e se aprimore nesse combate virtual.

4.3. Crimes Contra a Honra e Manipulação de Informação

Outra área em que a IA pode ser extremamente crítica e nociva diz respeito ao campo das honras objetiva e subjetiva na sociedade, que se materializam tanto pelas *deepfakes* quanto pelas *fakenews*. Nesse sentido, descreve Prado (2008, p. 213):

A honra, do ponto de vista objetivo, seria a reputação que o indivíduo desfruta em determinado meio social, a estima que lhe é conferida; subjetivamente, a honra seria o sentimento da própria dignidade ou decoro. A calúnia e a difamação atingiriam a honra no sentido objetivo (reputação, estima social, bom nome); já a injúria ofenderia a honra subjetiva (dignidade, decoro).

Dentro desse contexto, esse tipo de crime pode ser agravado pela potencialidade lesiva inerente ao ambiente virtual, tendo em vista o alcance em número de pessoas e a rapidez com que a informação chega aos destinatários, tudo em questão de segundos. Levando esse fator na ponderação, por exemplo, a prática de racismo pela internet em conjunto com crime contra a honra poderá ter sua pena aumentada, pelo fato de usar meios de comunicação social ou publicação de qualquer natureza, passando a ter pena de reclusão de dois a cinco anos e multa (Pinheiro, 2009).

Porém, novamente a legislação pátria deixa a desejar ante a ausência de especificidade quanto ao uso de IA, pois tais crimes, como o racismo, podem ser evoluídos a níveis jamais registrados com o uso da criatividade criminosa. No artigo “*Deepfake* na perspectiva da semiótica” publicado em 2021, os autores apresentam

possíveis aplicações dessa tecnologia no futuro. “É provável que, no futuro, as *deepfakes* evoluam para pornografia de vingança, cyberbullying, desqualificação de provas em tribunais, sabotagem política, propaganda terrorista, chantagem, manipulação de mercado e notícias falsas (De Souza, Santaella, 2021).

No âmbito da pornografia, pelo menos, o legislador se atentou para esses problemas ao criar um tipo penal que, embora não contemple a profundidade e amplitude da inteligência artificial, é suficiente – por enquanto – para sua repreensão, que se encontra representado pelo termo “montagem” no parágrafo único do artigo 216-B do Código Penal:

Registro não autorizado da intimidade sexual

Art. 216-B. Produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes: (Incluído pela Lei nº 13.772, de 2018)

Pena - detenção, de 6 (seis) meses a 1 (um) ano, e multa.

Parágrafo único. Na mesma pena incorre quem realiza montagem em fotografia, vídeo, áudio ou qualquer outro registro com o fim de incluir pessoa em cena de nudez ou ato sexual ou libidinoso de caráter íntimo. (Incluído pela Lei nº 13.772, de 2018)

Outro ponto relevante para discussão é a seara política, visto que a difusão de vídeos falsificados com falas ou comportamentos atribuídos a candidatos ou autoridades tem potencial para manipular a opinião pública e comprometer a integridade eleitoral.

A proliferação desse conteúdo falso indistinguível do real pode levar a uma erosão generalizada da confiança pública. Este ambiente de incerteza constante sobre a veracidade das informações pode resultar em um ceticismo extremo, onde os cidadãos passam a duvidar até mesmo de fatos e evidências legítimas, comprometendo as bases do discurso democrático e a própria noção de verdade objetiva (Tavares, 2024).

Nessa temática, o Tribunal Superior Eleitoral (TSE) regulamentou o uso da inteligência artificial (IA) na propaganda de partidos, coligações, federações partidárias, candidatas e candidato, alterando a Resolução nº 23.610/2019⁶, que trata de propaganda eleitoral, incluindo diversas novidades que envolvem a inteligência artificial, como a

⁶ Cf. BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.610, de 18 de dezembro de 2019**. Dispõe sobre propaganda eleitoral, utilização e geração do horário gratuito e condutas ilícitas em campanha eleitoral. Brasília, DF, 2019. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019>. Acesso em: 23 jul. 2026.

proibição das *deepfakes*; obrigação de aviso sobre o uso de IA na propaganda eleitoral; restrição do emprego de robôs para intermediar contato com o eleitor (a campanha não pode simular diálogo com candidato ou qualquer outra pessoa); e responsabilização das *big techs* que não retirarem do ar, imediatamente, conteúdos com desinformação, discurso de ódio, ideologia nazista e fascista, além dos antidemocráticos, racistas e homofóbicos.

Como forma de comprovar essa urgência social, a empresa *iProov* realizou um estudo no qual testou 2.000 consumidores do Reino Unido e dos EUA, expondo-os a uma série de conteúdos reais e *deepfakes* gerados por IA, muitas vezes concebidos para se fazerem passar por pessoas. O resultado mostrou que apenas 0,1% dos participantes conseguiram distinguir com exatidão os conteúdos reais dos falsos em todos os estímulos, incluindo imagens e vídeos⁷. Assim, esse número mínimo revela que essa ameaça invisível não apenas afeta indivíduos, mas ameaça diretamente a credibilidade de instituições democráticas.

5 DESAFIOS PROBATÓRIOS E INVESTIGATIVOS

Além da própria dificuldade em detectar os crimes que se utilizam de inteligência artificial, outro ponto relevante que representa um desafio para os operadores do direito é a capacidade em trazer elementos que evidenciem a prática do crime, através de um processo legal e investigativo, sem ferir direitos fundamentais da pessoa humana. Para isso, o Capítulo II, Título VII, do Código de Processo Penal trouxe o procedimento relativo ao exame de corpo de delito, da cadeia de custódia e das perícias em geral, ditando uma forma específica com que os vestígios encontrados sejam analisados e apresentados.

Sobre isso, a garantia da validade legal da prova digital reside, fundamentalmente, na preservação da cadeia de custódia, de forma que a documentação minuciosa de cada etapa – desde a apreensão até a apresentação em juízo – é essencial para assegurar a rastreabilidade e a integridade da prova, afastando qualquer alegação de adulteração ou manipulação (Lima, Júnior, 2021)

⁷ Cf. IPROOV. Estudo iProov revela o ponto cego do Deepfake: apenas 0,1% das pessoas conseguem detectar com precisão as falsificações profundas geradas por IA. Londres: iProov, 12 fev. 2025. Disponível em: <https://www.iproov.com/pt/press/study-reveals-deepfake-blindspot-detect-ai-generated-content>. Acesso em: 23 jul. 2026.

Porém, no que tange especificamente a crimes que utilizam IA, dois fatores sobrepesam a balança quando se trata de provar, quais sejam, a escala e a velocidade. Isso se deve uma vez que a automatização permite a replicação do mesmo ataque a milhares de vítimas de forma instantânea, ampliando o alcance e o dano causado.

Tendo essa problemática em vista, a ciência forense digital (CFD), ramo da Ciência Forense que trata da análise e investigação de conteúdos associados a dispositivos digitais (Casey, 2011), precisou se adaptar e aprender a usar essa tecnologia pensante a favor do processo científico.

A maior parte da história da ciência criminal é marcada pelo uso de procedimentos tradicionais para todos os fatos que ocorriam no mundo físico (entrevista de testemunhas, coleta de impressões digitais, entre outros). Porém, a partir do surgimento das redes sociais no mundo, os dados relativos aos crimes possivelmente foram disponibilizados nessas mídias, assim como as informações decorrentes dele, já que tais dados foram espalhados entre usuários e ambientes virtuais, culminando em um cenário em que a habilidade humana já não dava conta de processar tudo. Nesse contexto, os métodos de IA se apresentam como um meio prático para transpor essas barreiras, analisando, processando e organizando as informações para que o perito seja capaz de utilizar sua experiência da melhor forma (Pollitt, 2010).

No cenário brasileiro, em junho de 2025, o Ministério da Justiça e Segurança Pública publicou a Portaria 961/25⁸, que autoriza o uso de tecnologias da informação, incluindo ferramentas baseadas em inteligência artificial, por servidores dos órgãos de segurança pública, no âmbito de investigações criminais. Isso comprova que a inteligência artificial deve ser combatida com os mesmos recursos que a tornaram o principal instrumento para o cometimento de crimes, trazendo, porém, certas regulações e limitações, conforme a supramencionada Portaria, no sentido de que o uso das soluções tecnológicas para obtenção de dados sigilosos dependerá de autorização judicial e deverá estar vinculado a investigação criminal ou à instrução processual, por exemplo.

⁸ BRASIL. Ministério da Justiça e Segurança Pública. **Portaria MJSP nº 961, de 24 de junho de 2025**. Estabelece diretrizes sobre uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública. **Diário Oficial da União**: seção 1, Brasília, DF, ed. 120, p. 104, 30 jun. 2025. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-mjsp-n-961-de-24-de-junho-de-2025-638661609>. Acesso em: 23 jul. 2026.

Entre suas diversas aplicações, a IA se destaca, por exemplo, na análise de fotografias de cenas de crimes, identificando e classificando de forma automática diversas formas de evidências, como manchas de sangue, cartuchos de armas, reconhecimento facial e impressões digitais, economizando o tempo dos investigadores e fazendo com que nenhuma evidência seja deixada ao acaso, além de acelerar o processo de apreensão do criminoso (De Souza, 2024).

No combate ao terrorismo, a IA representar um ponto central para que as forças policiais identifiquem a origem dos ilícitos. Assim, o computador será capaz de recolher, tratar e apresentar aos responsáveis pela investigação criminal informações relacionadas com ações de terrorismo, desde locais de incitamento, conversão de fiéis (radicalismo), identificação de potenciais autores de futuras atuações terroristas, financiamento de células terroristas, indicação de quem efetuou as publicações na internet, etc. (Ramos, 2023).

Outro cenário em que a IA se mostra bastante útil é na identificação de lavagem de dinheiro, usando o sistema de *machine learning* para pontuar clientes com o objetivo de prever a propensão a perpetrar um crime financeiro, através da análise e mudanças de comportamento, organizando-os em um sistema de maior ou menor risco. Segundo o relatório da *McKinsey & Company*, os bancos podem melhorar a identificação de atividades suspeitas em até 40%, reduzindo significativamente o número de falsos positivos (Doppalapudi, 2022).

Do ponto de vista processual, todos esses dados e constatações reforçam que a evolução tecnológica representa um desafio cada vez mais onipresente na atuação do direito penal na sociedade. A união dos recursos científicos e humanos, agentes nacionais e internacionais, convergem na criação de um sistema que seja capaz de combater quaisquer formas de inovação criminal, trazendo eficiência ao trabalho dos peritos e das autoridades responsáveis pela investigação para que estes possam cumprir seus papéis na aplicação do Direito Penal em todos os seus âmbitos.

CONSIDERAÇÕES FINAIS

A evolução tecnológica é um fenômeno que não pode ser parado e estará cada vez mais presente em nosso cotidiano, alterando e influenciando a vida individual e a vida em sociedade, podendo, inclusive, ditar o curso da história a favor daqueles que souberem usá-la, seja positiva ou negativamente. Esse fato revela dois cenários: a potencialização de práticas ilícitas de forma inédita e a insuficiência de um ordenamento jurídico que, desde seu surgimento, sempre esteve um passo atrás das tecnologias.

A grande questão que se discute não é apenas se o Direito Penal pode reagir – afinal, ou ele responde à IA, mesmo que forçadamente, ou a sociedade entra em colapso diante da dominação virtual desta tecnologia sem limites –, mas como e em que medida trazer essas respostas através da cooperação interdisciplinar com as ciências cibernéticas e tecnológicas, honrando os pilares fundamentais e constitucionais que servem de base para a ordem e justiça que se espera em um Estado Democrático de Direito.

As discussões sobre regulamentação em outros países, como os debates no Senado norte-americano e a aprovação do *AI Act* na União Europeia, reforçam que a questão é global e exige diálogo entre juristas, cientistas da computação, legisladores e sociedade civil. Também ficou evidente que a própria IA pode ser uma aliada no combate ao crime, desde que utilizada dentro dos limites legais e éticos, contribuindo para investigações mais eficientes, análise de grandes volumes de dados e detecção de fraudes.

Assim, a inteligência artificial não deve ser vista apenas como ameaça, mas também como um fenômeno que forçará a modernização do Direito de forma geral, exigindo a ampliação do escopo de análise das áreas jurídicas, inclusive a criminal, para alcançar fronteiras além daquelas físicas. Dessa forma, o Direito Penal conseguirá cumprir o seu papel de proteger a dignidade humana em meio a tantos seres artificiais.

REFERÊNCIAS

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 2.338, de 2023**. Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Brasília, DF: Câmara dos Deputados, 2023. Disponível em:

https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2868197&filena me=PL%202338/2023. Acesso em: 19 ago. 2025.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Diário Oficial da União: seção 1, Rio de Janeiro, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 28 ago. 2025.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Diário Oficial da União: seção 1, Rio de Janeiro, 13 out. 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 28 ago. 2025.

BRASIL. Ministério da Justiça e Segurança Pública. **Portaria MJSP nº 961, de 24 de junho de 2025**. Estabelece diretrizes sobre uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública. Diário Oficial da União: seção 1, Brasília, DF, ed. 120, p. 104, 30 jun. 2025. Disponível em:

<https://www.in.gov.br/en/web/dou/-/portaria-mjsp-n-961-de-24-de-junho-de-2025-638661609>. Acesso em: 28 ago. 2025.

BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.610, de 18 de dezembro de 2019**. Dispõe sobre propaganda eleitoral, utilização e geração do horário gratuito e condutas ilícitas em campanha eleitoral. Diário Oficial da União: seção 1, Brasília, DF, 2019. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-deze mbro-de-2019>. Acesso em: 20 ago. 2025.

CARVALHO, Andersson Vieira; GIONGO, Juliana Leonora Martinelli. Veículos autônomos no Brasil: situações dilemáticas envolvendo programadores e estado de necessidade. In: **CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE**, 2019, Santa Maria. Santa Maria: UFSM, 2019.. Disponível em: <https://www.ufsm.br/app/uploads/sites/563/2019/09/5.12.pdf>. Acesso em: 12 ago. 2025.

CASEY, E. **Digital evidence and computer crime**: Forensic science, computers, and the internet. s.l.: Academic Press, 2011.

CNN Brasil. Funcionário de multinacional paga US\$ 25 mi a golpista que usou “deepfake” para simular reunião. Brasília, 4 fev. 2024. Disponível em: <https://www.cnnbrasil.com.br/internacional/funcionario-de-multinacional-paga-us-25-mi-a-g olpista-que-usou-deepfake-para-simular-reuniao/>. Acesso em: 27 ago. 2025.

ESTADOS UNIDOS. Senate Committee on Commerce, Science, and Transportation. **Winning the AI Race: Strengthening U.S. Capabilities in Computing and Innovation**. Washington, D.C., 8 maio 2025. Disponível em: https://www.commerce.senate.gov/2025/5/winning-the-ai-race-strengthening-u-s-capabiliti es-in-computing-and-innovation_2. Acesso em: 27 ago. 2025.

DE SOUZA, Carlos Eduardo; SANTAELLA, Lucia. Deepfakes na perspectiva da semiótica. TECCOGS: **Revista Digital de Tecnologias Cognitivas**, n. 23, 2021.

DE SOUZA, Lana Corina Laranjeira; RIBEIRO, Letícia Alves; FERREIRA, Rafael Lima Gomes. **Inteligência artificial: o futuro da investigação criminal**. Humanidades (Montes Claros), v. 13, n. Supl. 1, 2024.

DOPPALAPUDI, Prashant Kumar et al. The fight against money laundering: machine learning is a game changer. **McKinsey & Company**, 7 out. 2022.

GIUFFRIDA, Iria; LEDERER, Fredric; VE RMEYS, Nicolas. **A legal perspective on the trials and tribulations of ai**: how artificial intelligence, the internet of things, smart contracts, and other technologies will affect the law. Case Western Reserve Law Review, v. 68, n. 3, p. 747–782, 2018

IPROOV. **Estudo iProov revela o ponto cego do Deepfake: apenas 0,1% das pessoas conseguem detectar com precisão as falsificações profundas geradas por IA**. Londres: iProov, 12 fev. 2025. Disponível em: <https://www.iproov.com/pt/press/study-reveals-deepfake-blindspot-detect-ai-generated-content>. Acesso em: 28 ago. 2025.

JONES, Cameron R.; BERGEN, Benjamin K. **Large language models pass the turing test**. arXiv preprint arXiv:2503.23674, 2025.

LIMA, Renato Brasileiro de; LOPES JR., Aury. **Direito processual penal**. São Paulo: Saraiva Educação, 2021.

NADER, Paulo. **Introdução ao estudo do direito**. 23. ed. rev. e atual. Rio de Janeiro: Forense, 2003.

PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Saraiva, 2009.

POLLITT, M. **A history of digital forensics**. In: International Conference on Digital Forensics (IFIP). s.l.: s.n., 2010. p.3-15.

PRADO, L. R. **Curso de direito penal Brasileiro**: volume II, parte especial. Londrina: Ed. Thoth, 2008.

RAMOS, Armando Dias. A IA e a sua aplicação na investigação criminal: contributo para a identificação de perfis na criminalidade organizada. **Anatomia do Crime**, n. 17, p. 159-168, jan./jun. 2023.

UNIÃO EUROPEIA. Parlamento Europeu; Conselho da União Europeia. **Regulamento (UE) 2024/1689, de 13 de junho de 2024**, que cria regras harmonizadas em matéria de inteligência artificial [...] (Regulamento Inteligência Artificial). Jornal Oficial da União Europeia, L, 2024/1689, 12 jul. 2024. Disponível em:

ISSN nº 2359-0106

Vol. 13, n. 1, 2026.

<https://doi.org/10.20873/ufv.2359-0106.2026.v13n1.p48-66>

https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ%3AL_202401689. Acesso em: 28 ago. 2025.

TAVARES, Cláudio de Mello. Inteligência artificial e deepfakes: desafios jurídicos e tecnológicos para a integridade do processo democrático e as implicações para as eleições municipais de 2024. **Revista Justiça Eleitoral em Debate**, v. 14, n. 1, p. 49-58, 2024.

TURING, A. M. Computing machinery and intelligence. **Mind**, v. LIX, n. 236, p. 433-460, out. 1950. Disponível em: <https://doi.org/10.1093/mind/LIX.236.433>. Acesso em: 23 jul. 2026.