CRIMES DIGITAIS IMPULSIONADOS POR INTELIGÊNCIA ARTIFICIAL NO BRASIL: DESAFIOS LEGAIS, MEDIDAS PREVENTIVAS E SOLUÇÕES EFICAZES

DIGITAL CRIMES DRIVEN BY ARTIFICIAL INTELLIGENCE IN BRAZIL: LEGAL CHALLENGES, PREVENTIVE MEASURES, AND EFFECTIVE SOLUTIONS

Jorge Jarrouge Calandra[1]

Resumo: O avanço acelerado da inteligência artificial (IA) e sua integração em múltiplas esferas da vida humana trouxeram ganhos expressivos de eficiência, automação e inovação, mas também favoreceram o surgimento de novas modalidades de criminalidade digital. No Brasil, fatores como vulnerabilidade social, ausência de políticas públicas de segurança da informação, desarticulação institucional e lacunas legislativas agravam o cenário de fraudes, golpes e manipulações de dados mediados por algoritmos. Este artigo tem como objetivo analisar, sob a ótica jurídico-penal e civil, os impactos da IA na prática de crimes digitais, identificar as deficiências normativas brasileiras e propor medidas concretas de prevenção, responsabilização e governança digital. A pesquisa é de natureza bibliográfica, documental e qualitativa, baseada em relatórios oficiais, doutrinas especializadas e legislação comparada. Busca-se compreender de que forma a IA altera a autoria e a imputação penal, bem como os reflexos civis da responsabilidade algorítmica. Conclui-se que o enfrentamento da criminalidade cibernética exige não apenas a atualização dos Códigos Penal e Civil, mas também a criação de uma política nacional de soberania digital, com ênfase na educação cibernética, na cooperação interinstitucional e no uso ético da tecnologia. Assim, a modernização legislativa e institucional é essencial para garantir a proteção da dignidade humana e a segurança jurídica na era algorítmica.

Palavras-chave: Crimes digitais; Inteligência artificial; Direito penal; Responsabilidade civil; Governança digital.

Abstract: The accelerated advancement of Artificial Intelligence (AI) and its integration into multiple spheres of human life have generated significant gains in efficiency, automation, and innovation. However, these same technologies have facilitated the emergence of new forms of digital criminality. In Brazil, factors such as social vulnerability, lack of public policies on information security, institutional fragmentation, and legislative gaps exacerbate a scenario of fraud, scams, and data manipulation mediated by algorithms. This article aims to analyze, from a criminal and civil law perspective, the impact of AI on digital crimes, identify the normative deficiencies of the Brazilian legal framework, and propose concrete measures for prevention, accountability, and digital governance. The research adopts a bibliographic, documentary, and qualitative approach, based on official reports, specialized doctrines, and comparative legislation. It seeks to understand how AI modifies authorship and criminal liability, as well as the civil implications of algorithmic responsibility. The study concludes that combating algorithmic criminality requires not only the modernization of the Brazilian Penal and Civil Codes but also the implementation of a National Digital Sovereignty Policy, emphasizing cyber education, interinstitutional cooperation, and the ethical use of technology. Legislative and institutional modernization thus becomes essential to ensure the protection of human dignity and legal certainty in the algorithmic era.

Keywords: Digital crimes; Artificial Intelligence; Criminal Law; Civil liability; Digital

[1] Graduando em Direito pela FMU/SP. Especialista na área de Tecnologia da Informação, em análise de dados, Business Intelligence, programação de sistemas e automações digitais.

Governance.

INTRODUÇÃO

A inteligência artificial consolidou-se como um dos pilares estruturantes da sociedade contemporânea, influenciando desde diagnósticos médicos e sistemas de segurança pública até operações financeiras de alta complexidade. Essa ubiquidade tecnológica amplia a capacidade humana de decisão e otimiza processos, mas também potencializa riscos de violação de direitos fundamentais e amplia o campo de atuação das fraudes digitais.

No contexto brasileiro, a utilização de ferramentas algorítmicas e automações inteligentes vem sendo explorada por agentes criminosos para ampliar a sofisticação e a escala dos delitos virtuais. Segundo a **Serasa Experian (2025)**, o país registrou **6,9 milhões de tentativas de fraude no primeiro semestre de 2025**, o maior volume já observado, com **53,7% das ocorrências direcionadas ao setor bancário e de cartões**, resultando em **uma tentativa a cada 4,2 segundos**.

A defasagem entre o ritmo tecnológico e a capacidade legislativa evidencia a necessidade de atualização normativa. O **Código Penal (1940)** e o **Código Civil (2002)**, embora sólidos, não preveem condutas praticadas por meio de sistemas autônomos ou decisões algorítmicas. Este estudo busca, portanto, analisar a realidade brasileira sob a ótica jurídico-funcional e propor caminhos de harmonização entre Direito e tecnologia.

1 INTELIGÊNCIA ARTIFICIAL E O NOVO RISCO PENAL

A IA caracteriza-se pela capacidade de aprender e agir de modo autônomo com base em grandes volumes de dados. Essa autonomia cria o chamado “domínio do risco” (GRECO, 2024, p. 83), no qual o controle humano sobre o resultado é parcial.

Conforme Peck (2024), o avanço dos sistemas inteligentes exige que o Direito reconheça o agente algorítmico como extensão da ação humana, sobretudo quando há previsibilidade de risco.

Entre os principais crimes digitais impulsionados por IA estão:

Fraudes eletrônicas: uso de deepfakes e clonagem de voz em esquemas de estelionato e engenharia social.

Ataques cibernéticos automatizados: exploração de vulnerabilidades por IA em tempo real.

Manipulação informacional: disseminação de fake news e criação de perfis

automatizados para influência política.

Aliciamento de menores: uso de avatares e deepfakes em contextos de pedofilia digital. Relatório da Canaltech (2025) aponta que o prejuízo médio por vítima superou R$ 6 mil, e 40 % das pessoas afetadas declararam não ter recuperado os valores perdidos.

2 ENQUADRAMENTO NORMATIVO BRASILEIRO

O arcabouço jurídico atual cobre parcialmente a criminalidade digital:

Constituição Federal (1988), arts. 5º (X, XII) e 22 (I), assegura privacidade e competência penal da União.

Código Penal (Decreto-Lei 2.848/1940), arts. 154-A e 171, trata de invasão e fraude, sem prever mediação algorítmica.

Lei 12.737/2012 (Lei Carolina Dieckmann): tipifica crimes informáticos.

Lei 12.965/2014 (Marco Civil da Internet): define princípios de liberdade e responsabilidade.

Lei 13.709/2018 (LGPD): regulamenta tratamento de dados pessoais e decisões automatizadas.

Lei 14.155/2021: agrava penas para fraudes eletrônicas.

Segundo Doneda (2023), a ausência de previsões sobre riscos algorítmicos "fragiliza o princípio da legalidade penal e compromete a efetividade da tutela dos bens jurídicos".

Há, portanto, necessidade de adaptação normativa para que a legislação acompanhe a complexidade das novas condutas digitais. Além disso, a ausência de parâmetros legais claros quanto à responsabilidade por atos praticados com auxílio de sistemas autônomos gera insegurança jurídica e dificuldade de imputação penal, especialmente em casos que envolvem múltiplos agentes tecnológicos. É indispensável que o legislador estabeleça critérios objetivos de atribuição de culpa e de risco tecnológico, alinhando-se às tendências internacionais de responsabilização por danos decorrentes de decisões algorítmicas.

2.1 Perfis falsos, desinformação e deepfakes: novas vias de criminalidade digital

O fenômeno das *fake news* e dos perfis falsos transformou-se em um dos principais desafios à proteção da honra, da imagem e da própria estabilidade democrática no ambiente digital. A criação e disseminação de informações falsas ou manipuladas passaram a integrar o repertório das práticas criminosas contemporâneas, frequentemente

associadas à calúnia, difamação e injúria (Brasil, 1940).

Segundo investigação da Agência Pública (2023), 80 % dos perfis responsáveis por disseminar *fake news* em redes sociais continuam ativos, mesmo após denúncias e ações de moderação, o que evidencia a ineficácia dos mecanismos de contenção e a fragilidade das políticas de moderação de conteúdo (Agência Pública, 2023).

A propagação deliberada de desinformação, impulsionada por algoritmos e ferramentas de inteligência artificial, constitui ameaça direta aos direitos fundamentais, especialmente à honra subjetiva, à reputação e à privacidade. Como observam Ançanello, Casarin e Furnival (2023, p. 3), a desinformação atua como "elemento corrosivo do debate público e do discernimento social", minando a confiança coletiva nas instituições democráticas.

O uso de inteligência artificial para gerar conteúdo manipulado, incluindo deepfakes de cunho político, financeiro ou sexual, tem ampliado a complexidade da responsabilização penal e civil. Relatório do Digital Forensic Research Lab (DFRLab, 2024) documentou que conteúdos falsos gerados por IA foram utilizados para interferir em pleitos eleitorais locais no Brasil, testando os limites da legislação vigente sobre manipulação digital (DFRLab, 2024).

Essas condutas podem configurar ilícitos penais previstos nos arts. 138 a 140 do Código Penal (Brasil, 1940) — referentes à calúnia, difamação e injúria — e, em hipóteses específicas, falsidade ideológica (art. 299 CP) e associação criminosa (art. 288 CP). No campo civil, a responsabilidade objetiva das plataformas digitais por omissão na retirada de conteúdo ofensivo é consolidada pela jurisprudência do Superior Tribunal de Justiça, que reconhece o dever de diligência dos provedores ao serem formalmente notificados (STJ, 2017).

O enfrentamento desse cenário requer a conjugação de medidas normativas e tecnológicas: aprimoramento da legislação penal, fortalecimento dos mecanismos de rastreabilidade de perfis automatizados (*bots*) e incentivo à educação midiática e digital. Apenas uma abordagem integrada poderá reduzir os impactos da desinformação e restaurar a confiança na esfera informacional brasileira.

3 IMPUTAÇÃO PENAL DIGITAL E AUTORIA ALGORÍTMICA

A questão central é identificar a autoria penal em crimes praticados com ou por meio de IA. Conforme Greco (2024, p. 79), "o agente que cria ou mantém um sistema autônomo com potencial ofensivo assume o risco penal da conduta, ainda que não a controle diretamente."

As principais correntes teóricas são:

Autoria mediata tecnológica — responsabiliza o desenvolvedor ou operador que utiliza a IA como instrumento do crime.

Risco algorítmico — prevê imputação quando o agente omite dever de supervisão.

Imputação funcional — responsabiliza pela negligência técnica grave, ainda que sem dolo direto.

Segundo Opice Blum (2024), a efetividade da persecução penal depende de uma cadeia de custódia digital, que assegure autenticidade e integridade das provas algorítmicas.

Propõe-se a inclusão, no Código Penal, de um Título XII-A – Dos Crimes Digitais e Cibernéticos, com dispositivos que:

Definam autoria algorítmica e corresponsabilidade de provedores;

Tipifiquem uso de IA em fraudes, extorsões, manipulações e crimes sexuais virtuais;

Estabeleçam agravantes específicas para negligência tecnológica.

4 MEDIDAS PREVENTIVAS E POLÍTICA CRIMINAL

O enfrentamento da criminalidade digital requer ações preventivas articuladas em três eixos: educação, estrutura institucional e cooperação internacional.

4.1 Educação e cidadania digital

Para a UNESCO (2024), a alfabetização digital é condição indispensável à democracia informacional.

Defende-se a inserção da educação cibernética obrigatória nas escolas públicas e privadas, abordando ética, segurança e privacidade online.

4.2 Estrutura institucional integrada

Propõe-se a criação do Sistema Nacional de Proteção e Integridade Digital (SNPID), unindo:

Polícia Federal, Ministério Público, Banco Central, ANPD (Agência Nacional de Proteção de Dados) e órgãos de inteligência;

Delegacias e varas digitais especializadas;

Laboratórios de perícia em IA;

Ministério Público Digital.

4.3 Cooperação internacional

Recomenda-se adesão plena à Convenção de Budapeste (2001) e cooperação com a CISA (EUA) e a NIS2 Directive (UE) para rastrear cibercrimes transnacionais.

5 RESPONSABILIDADE CIVIL E PROTEÇÃO DE DADOS

O campo civil também exige atualização. A LGPD (art. 20) garante o direito à revisão de decisões automatizadas, mas não define responsabilidades por danos decorrentes de IA.

Segundo Doneda (2023, p. 97), "a responsabilidade civil na era digital deve equilibrar inovação e proteção da personalidade humana".

Sugere-se acrescentar ao Código Civil um Livro Complementar – Das Relações Jurídicas Digitais, com regras sobre:

- Responsabilidade objetiva por falhas de sistemas autônomos;
- Dever de transparência algorítmica;
- Indenização por danos morais e materiais de origem automatizada.

6 SOLUÇÕES LEGISLATIVAS E INSTITUCIONAIS

Para garantir efetividade imediata, propõem-se medidas concretas:

I. Atualização dos Códigos Penal e Civil, com capítulos sobre crimes e relações digitais;

II. Criação de varas e tribunais especializados em tecnologia;

III. Auditoria obrigatória de algoritmos de alto risco, supervisionada pela ANPD;

IV. Autenticação biométrica obrigatória em transações acima de R$ 500;

V. Integração de IA estatal antifraude, com monitoramento de padrões de golpes e deepfakes;

VI. Implementação da Política Nacional de Soberania Digital, voltada à proteção de dados estratégicos e infraestrutura crítica.

Essas ações transformam o combate à criminalidade digital de reativo em preventivo e proativo, fortalecendo a soberania tecnológica do Estado.

CONSIDERAÇÕES FINAIS

A ascensão da inteligência artificial impõe uma reconfiguração profunda do Direito contemporâneo, exigindo que o ordenamento jurídico acompanhe a velocidade das transformações tecnológicas sem renunciar à proteção da dignidade humana. O desafio reside em equilibrar liberdade e responsabilidade, inovação e segurança, de modo que o progresso digital não se converta em vulnerabilidade social.

Como observa Peck (2024, p. 112), "o Direito deve compreender o código antes que o código substitua o Direito". Essa advertência traduz com precisão a urgência de um reposicionamento institucional do Estado, que deve atuar não apenas de forma reativa, mas preventiva e integradora, coordenando esforços entre Poder Público, setor privado, academia e sociedade civil.

A atualização dos Códigos Penal e Civil, incorporando dispositivos voltados à realidade digital, constitui passo indispensável para conferir segurança jurídica às novas relações algorítmicas. Paralelamente, a educação digital estruturada e o investimento em tecnologia pública de monitoramento e rastreabilidade representam instrumentos concretos de efetividade no combate à criminalidade cibernética.

Entretanto, a modernização normativa deve vir acompanhada de infraestrutura tecnológica estatal integrada, capaz de utilizar inteligência artificial para identificar padrões de fraude, desinformação e deepfakes em tempo real. O fortalecimento de laboratórios forenses digitais, a criação de varas especializadas em crimes cibernéticos e a consolidação de uma rede nacional de inteligência antifraude, sob a coordenação do Ministério da Justiça e da Autoridade Nacional de Proteção de Dados (ANPD), são medidas estratégicas para transformar o combate em ação contínua e preventiva.

No campo social, é essencial implementar uma Política Nacional de Educação Cibernética, inserindo temas de segurança digital, cidadania responsável e uso ético da tecnologia nos currículos escolares. Somente uma população consciente dos riscos poderá resistir à manipulação algorítmica e às campanhas de desinformação automatizada.

No âmbito internacional, o Brasil deve adotar postura ativa em fóruns de governança global de IA, buscando harmonizar princípios de soberania digital, interoperabilidade de dados e responsabilidade transnacional. A cooperação com organismos multilaterais e a participação em tratados de segurança cibernética são condições para proteger infraestruturas críticas e dados sensíveis de interesse nacional.

Em síntese, o enfrentamento dos crimes digitais impulsionados por inteligência artificial exige a convergência entre legislação moderna, ética tecnológica e governança digital efetiva. Somente por meio desta integração será possível edificar um sistema

jurídico capaz de compreender, regular e humanizar a inteligência artificial, assegurando que o desenvolvimento tecnológico permaneça a serviço da sociedade — e não o contrário.

REFERÊNCIAS

AGÊNCIA BRASIL. *Brasileiros perderam em média mais de R$ 6 mil em fraudes digitais*. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2025-06/brasileiros-perderam-em-media-mais-de-r-6-mil-em-fraudes.

AGÊNCIA PÚBLICA. *80 % dos perfis em redes sociais responsáveis por espalhar fake news continuam ativos*. São Paulo, 2023. Disponível em: https://apublica.org/2023/08/80-dos-perfis-em-redes-sociais-responsaveis-por-espalhar-fake-news-continuam-ativos.

ANÇANELLO, Juliana Venancio; CASARIN, Helen de Castro Silva; FURNIVAL, Ariadne Chloe. Competência em informação, fake news e desinformação: análise das pesquisas no contexto brasileiro. **Em Questão**, Porto Alegre, v. 29, 2023. Disponível em: https://seer.ufrgs.br/index.php/EmQuestao/article/view/125782.

BRASSCON. **Relatório de Cibersegurança: Panorama e Insights 2025.** Disponível em: https://brasscom.org.br/wp-content/uploads/2025/07/BRI2-2025-008-Relatorio-de-Ciberseguranca-v13-3.pdf.

BRASIL. **Código Penal.** Decreto-Lei n.º 2.848, de 7 de dezembro de 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.

CANALTECH. *Prejuízo médio com golpes digitais aumentou em 2025*. Disponível em: https://canaltech.com.br/seguranca/brasil-esta-no-topo-do-ranking-mundial-de-vitimas-de-fraudes-digitais/.

DIGITAL FORENSIC RESEARCH LAB (DFRLab). Brazil's electoral deepfake law tested as AI-generated content targeted local elections. **Atlantic Council**, Washington, DC, 2024. Disponível em: https://dfrlab.org/2024/11/26/brazil-election-ai-deepfakes/.

DONEDA, Danilo. **Fundamentos da Proteção de Dados Pessoais.** São Paulo: RT, 2023.

GRECO, Rogério. **Direito Penal Aplicado à Era Digital.** Rio de Janeiro: Impetus, 2024.

GSI – GABINETE DE SEGURANÇA INSTITUCIONAL. **Estratégia Nacional de Cibersegurança**. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao-e-cibernetica/estrategia-nacional-de-ciberseguranca-eciber.

OPICE BLUM, Renato. **Crimes Cibernéticos e Provas Digitais.** São Paulo: RT, 2024.

PECK PINHEIRO, Patrícia. **Direito Digital Sistêmico.** São Paulo: Saraiva, 2024.

SERASA EXPERIAN. **Indicador de Tentativas de Fraude 2025.** São Paulo, 2025. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/indicadores/recorde-quase-7-milhoes-de-tentativas-de-fraude-foram-

registradas-no-1-semestre-de-2025-setor-bancario-e-principal-alvo

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **Recurso Especial n.º 1.660.168/RJ.** Rel. Min. Nancy Andrighi. Terceira Turma. DJe 22 ago. 2017. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=83547256&tipo=0&nreg=&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=&formato=PDF&salvar=false.

UNESCO. **Digital Literacy and Human Rights.** Paris, 2024. Disponível em: https://www.unesco.org/en/human-rights.