Revista Multidisciplinar do Nordeste Mineiro, v.18, 2025
ISSN 2178-6925
DOI: 10.61164/x5fcqh87

DESAFIOS NA IDENTIFICAÇÃO CRIMINAL EM MEIOS ELETRÔNICOS: O PAPEL DA INTELIGÊNCIA ARTIFICIAL NA INVESTIGAÇÃO E PREVENÇÃO DE CRIMES DIGITAIS

CHALLENGES IN CRIMINAL IDENTIFICATION IN ELECTRONIC MEDIA: THE ROLE OF ARTIFICIAL INTELLIGENCE IN THE INVESTIGATION AND PREVENTION OF DIGITAL CRIMES

Hárnefer Wagmacker dos Santos
Graduando em Direito, Faculdade de Ensino Superior de Linhares, Brasil
E-mail: harneferpessoal@gmail.com

Alexandre Jacob
Mestre, Faculdade de Ensino Superior de Linhares, Brasil
E-mail: alexandre.jacob10@gmail.com

Recebido: 15/09/2025 – Aceito: 20/09/2025

Resumo:

O presente artigo tem como objetivo analisar os principais desafios na identificação de criminosos em meios eletrônicos e explorar o potencial da inteligência artificial como ferramenta auxiliar na investigação e prevenção de crimes digitais. Em um contexto marcado pelo uso crescente de tecnologias como VPN, criptografia e *deepfakes* por parte de infratores, os métodos tradicionais de investigação se mostram insuficientes. A pesquisa, de natureza qualitativa e bibliográfica, analisa as aplicações da IA na análise de dados, identificação de padrões e reconhecimento de comportamentos suspeitos, bem como discute os limites éticos, legais e técnicos dessa abordagem. Ao final, propõe diretrizes para a implementação segura e eficaz da IA no âmbito da segurança pública, visando o respeito aos direitos fundamentais.

Palavras-chave: Direito processual penal. Política criminal. Tecnologias no processo. Inteligência artificial. Limites.

Abstract:

This article aims to analyze the main challenges in identifying criminals in electronic environments and to explore the potential of artificial intelligence as a tool for assisting in the investigation and

ISSN 2178-6925
DOI: 10.61164/x5fcqh87

prevention of digital crimes. In a context marked by the increasing use of technologies such as VPN, encryption, and deepfakes by offenders, traditional investigative methods are proving insufficient. This qualitative and bibliographic research examines AI applications in data analysis, pattern recognition, and detection of suspicious behavior, while also addressing the ethical, legal, and technical limits of this approach. Finally, it proposes guidelines for the safe and effective implementation of AI in the field of public security, with respect to fundamental rights.

***Keywords**: Criminal procedural law. Criminal policy. Technologies in the process. Artificial intelligence. Limits.*

1. Introdução

A evolução das tecnologias de informação e comunicação, aliada à expansão do acesso à internet, tem transformado profundamente os modos de interação social, de consumo e, também, de prática delitiva. Crimes que antes demandavam presença física ou contato direto com a vítima migraram para o meio digital, assumindo novas formas e exigindo novas abordagens por parte dos órgãos de segurança e investigação (Castells, 2003).

De acordo com dados de pesquisas, houve um aumento expressivo nos registros de crimes cibernéticos nos últimos cinco anos, impulsionado pelo uso de ferramentas tecnológicas como redes privadas virtuais (VPN), criptografia de ponta a ponta e programas de anonimização de navegação (Brant; Costa, 2022). Tais recursos dificultam sobremaneira a rastreabilidade das ações delituosas e, consequentemente, a identificação dos autores.

Nesse contexto, a inteligência artificial (IA) desponta como potencial aliada na investigação criminal, especialmente por sua capacidade de lidar com grandes volumes de dados, identificar padrões e realizar análises preditivas (Russell; Norvig, 2021). Ferramentas baseadas em IA já vêm sendo utilizadas em diversos países na detecção de fraudes, no monitoramento de redes sociais e no reconhecimento facial, com variados graus de sucesso.

No entanto, o uso de IA em atividades de segurança pública e investigação criminal não está isento de desafios e controvérsias. Questões como viés algorítmico, respeito à privacidade, responsabilidade por decisões automatizadas e limites legais para a vigilância têm ocupado um espaço central no debate acadêmico e institucional (Cath *et al*., 2018; Monteiro; Doneda, 2021).

ISSN 2178-6925
DOI: 10.61164/x5fcqh87

Diante desse cenário, a presente pesquisa busca responder à seguinte questão: quais são os principais desafios enfrentados na identificação de criminosos em meios eletrônicos e de que forma a inteligência artificial pode contribuir, de maneira ética e legal, para a investigação e prevenção de crimes digitais? Para tanto, parte-se da análise das estratégias empregadas por infratores digitais, da discussão sobre as possibilidades e limitações das ferramentas de IA e da investigação dos impactos jurídicos e éticos de sua utilização no âmbito investigativo.

Assim, o estudo se justifica pela necessidade de se compreender as transformações nas dinâmicas criminais e os riscos e oportunidades advindos da incorporação de tecnologias inteligentes no campo da persecução penal. Mais do que uma ferramenta, a inteligência artificial representa uma nova racionalidade de controle social, cujo uso exige critérios normativos claros e salvaguardas compatíveis com os direitos fundamentais assegurados pela Constituição da República de 1988.

2. A Evolução dos Crimes Digitais e Conceito e os Desafios da Identificação

Com o avanço das tecnologias da informação e comunicação, a sociedade passou a experimentar profundas transformações em suas relações sociais, econômicas e políticas. Paralelamente, o ambiente digital tornou-se terreno fértil para o surgimento e a proliferação de novas formas de criminalidade. Os chamados crimes digitais ou cibernéticos não apenas replicam práticas delituosas já conhecidas, mas também introduzem modalidades inéditas, como o acesso não autorizado a sistemas informatizados, o vazamento de dados sensíveis e a criação de conteúdos falsos por meio de *deepfakes* (Levy, 2019).

De acordo com pesquisas, mais de 50 milhões de brasileiros foram vítimas de crimes digitais em um único ano, resultando em prejuízos econômicos e sociais significativos (Melo, 2025). A crescente sofisticação dos criminosos digitais, aliada à facilidade de acesso a ferramentas de anonimização, representa um enorme desafio para as forças de segurança pública e os órgãos de persecução penal.

ISSN 2178-6925
DOI: 10.61164/x5fcqh87

Mecanismos como redes privadas virtuais (VPN), navegadores que ocultam o endereço IP, sistemas de criptografia de ponta a ponta e redes descentralizadas como a dark web dificultam a rastreabilidade das condutas criminosas, tornando a identificação dos autores uma tarefa complexa (Rezende, 2020). A utilização de identidades falsas, perfis falsificados e até a prática de *spoofing*, manipulação de dados que simulam origem confiável, agravam ainda mais esse cenário de incerteza e impunidade.

Além disso, a emergência de tecnologias baseadas em inteligência artificial, como os *deepfakes*, compromete a veracidade das provas digitais. A manipulação audiovisual tem sido utilizada tanto para fins de difamação quanto para ludibriar investigações e gerar falsas pistas, o que compromete a integridade dos processos penais e desafia os mecanismos de verificação de autenticidade (Ferraz; Oliveira, 2023).

A doutrina jurídica nacional reconhece que a criminalidade digital impõe a necessidade de redefinir os parâmetros tradicionais da investigação criminal. Como destaca Danilo Doneda (2020), a descentralização da ação criminosa e a sua materialização em ambientes não físicos demandam o uso de novas tecnologias, bem como a construção de uma política pública de segurança informacional integrada, com investimentos em capacitação técnica e tecnológica.

Dessa forma, evidencia-se que o combate aos crimes digitais exige não apenas a atualização normativa, mas, sobretudo, a incorporação de ferramentas tecnológicas inteligentes, capazes de atuar de forma eficiente frente a um cenário de constante mutação. A seguir, serão exploradas as potencialidades da inteligência artificial como instrumento de apoio à investigação criminal.

3. Aplicações da Inteligência Artificial na Investigação Criminal

A inteligência artificial tem ganhado crescente destaque como ferramenta de apoio às atividades investigativas em contextos digitais. Sua capacidade de processar grandes volumes de dados, identificar padrões complexos e realizar análises em tempo real apresenta vantagens significativas em relação aos

ISSN 2178-6925
DOI: 10.61164/x5fcqh87

métodos tradicionais de investigação, sobretudo frente à velocidade e à escala dos crimes cibernéticos contemporâneos (Russell; Norvig, 2021).

Entre as principais aplicações da IA na seara criminal, destaca-se o uso de algoritmos de aprendizado de máquina para o reconhecimento de padrões comportamentais suspeitos em redes sociais, fóruns e plataformas de comunicação digital. Sistemas como o CrimeRadar, desenvolvido no Brasil, utilizam IA para mapear incidências criminais com base em dados históricos, permitindo a previsão de ocorrências em determinadas regiões e horários (Silva, 2020).

Ferramentas de reconhecimento facial também têm sido amplamente utilizadas por agências de segurança pública para identificar suspeitos em tempo real, especialmente em locais públicos monitorados por câmeras. Embora essas tecnologias tenham elevado o índice de identificação de foragidos, seu uso tem gerado preocupações quanto à precisão e ao viés algorítmico, especialmente em relação à população negra e periférica (Martin; Whitten-Woodring, 2022).

Outra aplicação relevante é a análise automatizada de registros eletrônicos, como e-mails, logs de acesso, metadados e transações financeiras. Sistemas de IA são capazes de cruzar milhares de informações e detectar anomalias que poderiam passar despercebidas em uma análise humana, contribuindo para o desmantelamento de esquemas de fraude, lavagem de dinheiro e tráfico de dados (Brant; Costa, 2022).

Apesar das promessas, é preciso reconhecer que a IA não é isenta de falhas. Além das limitações técnicas, como taxas de falsos positivos e a opacidade dos algoritmos, existem riscos significativos de abuso quando tais tecnologias são utilizadas sem a devida regulamentação, transparência e supervisão (Cath *et al*., 2018).

Assim, o uso da inteligência artificial no processo investigativo requer não apenas investimento em infraestrutura tecnológica, mas também uma abordagem ética e jurídica que garanta sua compatibilidade com os princípios do Estado Democrático de Direito.

Revista Multidisciplinar do Nordeste Mineiro, v.18, 2025
ISSN 2178-6925
DOI: 10.61164/x5fcqh87

4. Limites Éticos e Jurídicos do Uso da Inteligência Artificial na Investigação Criminal

O uso da inteligência artificial no processo investigativo levanta profundas questões éticas e jurídicas que precisam ser enfrentadas com seriedade pelo legislador, pelo Judiciário e pelos operadores do Direito. A principal preocupação está em garantir que os instrumentos de IA empregados na segurança pública não violem direitos fundamentais assegurados pela Constituição da República, como a dignidade da pessoa humana, a privacidade, a presunção de inocência e o devido processo legal (Brasil, 1988).

Do ponto de vista ético, a principal controvérsia gira em torno da autonomia das decisões algorítmicas. Em diversos sistemas baseados em IA, como os de reconhecimento facial, a tomada de decisão é automatizada e pouco transparente, o que dificulta a identificação de erros, vieses e discriminações. Estudos demonstram que algoritmos treinados com dados enviesados tendem a reproduzir desigualdades estruturais, afetando desproporcionalmente populações vulneráveis (Eubanks, 2018).

Além disso, o princípio da prestação de contas (*accountability*) ainda é pouco desenvolvido em sistemas de IA utilizados por órgãos públicos. Como sustenta Reuben Binns (2018), a ausência de clareza sobre quem responde por uma decisão automatizada compromete o controle institucional e dificulta a reparação de danos em caso de erros, como prisões indevidas ou acusações infundadas.

No plano jurídico, a Lei Geral de Proteção de Dados Pessoais (LGPD) impõe limites importantes à coleta, tratamento e compartilhamento de dados, inclusive em contextos de segurança pública. O artigo 20 da LGPD garante ao cidadão o direito de revisão de decisões tomadas com base exclusivamente em tratamento automatizado, o que pode incluir sistemas de IA (Brasil, 2018). No entanto, ainda há lacunas sobre como esse direito deve ser exercido no contexto das investigações criminais.

A ausência de uma legislação específica que regulamente o uso da IA no processo penal gera insegurança jurídica e dificulta a criação de protocolos

ISSN 2178-6925
DOI: 10.61164/x5fcqh87

padronizados. Como apontam Monteiro e Doneda (2021), é essencial que o ordenamento jurídico brasileiro avance na construção de princípios próprios para a regulação da IA, com destaque para a transparência algorítmica, a supervisão humana, o direito à explicação e a não discriminação.

Por fim, é necessário considerar o princípio da proporcionalidade na aplicação dessas tecnologias. O uso de sistemas invasivos, como vigilância em massa ou rastreamento indiscriminado, pode configurar abuso de poder estatal, especialmente se não houver controle judicial ou critérios objetivos de necessidade e adequação (Zuboff, 2021).

A utilização ética e juridicamente aceitável da IA na investigação criminal exige, portanto, um arcabouço normativo robusto, bem como a articulação entre o desenvolvimento tecnológico e os princípios democráticos que regem o Estado de Direito.

5. O Posicionamento dos Tribunais

A aplicação de ferramentas tecnológicas na identificação de criminosos em ambientes digitais ainda é incipiente no Brasil, mas já tem gerado debates judiciais e administrativos relevantes. Embora a legislação nacional ainda careça de normativas específicas sobre o uso da inteligência artificial na persecução penal, decisões judiciais começam a delinear os contornos jurídicos desse novo paradigma investigativo.

Um dos primeiros casos envolvendo reconhecimento facial com tecnologia de IA no Brasil ocorreu durante o carnaval de 2019, em Salvador-BA. O sistema identificou e permitiu a prisão de um foragido da justiça, gerando elogios por sua eficácia. No entanto, também foi alvo de críticas por falta de transparência no processo e ausência de regulamentação legal específica (Rocha; Ferraz, 2021).

Outro exemplo de uso institucional de IA se encontra no Ministério Público do Rio de Janeiro, que implementou o sistema "MP em Mapas" para identificação de áreas com maior concentração de criminalidade. Embora não atue diretamente na identificação individual de criminosos, a ferramenta tem servido como base para ações estratégicas e distribuição de recursos (Mattos, 2022).

ISSN 2178-6925
DOI: 10.61164/x5fcqh87

O Brasil ainda não possui legislação específica que regule o uso de inteligência artificial em investigações criminais. A Lei Geral de Proteção de Dados estabelece princípios para o tratamento de dados pessoais, incluindo o direito à revisão de decisões automatizadas (Art. 20), mas carece de dispositivos específicos para o uso investigativo e repressivo de IA (Doneda; Monteiro, 2020).

Por sua vez, o Supremo Tribunal Federal (STF) tem reafirmado em diversas ocasiões a centralidade dos direitos fundamentais como limite à atuação estatal, inclusive no uso de tecnologias digitais. No julgamento da ADI nº. 6.387-DF, por exemplo, o STF suspendeu o compartilhamento irrestrito de dados entre órgãos públicos e privados, reforçando a necessidade de proteção à privacidade dos cidadãos (STF, 2020).

A análise dos casos evidencia a urgência de um marco normativo que regule o uso de tecnologias de IA pela segurança pública, de forma a garantir critérios de transparência, controle humano, proporcionalidade e revisão de decisões automatizadas. A ausência de parâmetros claros contribui para o risco de arbitrariedades, violações de direitos e perda de confiança social nos instrumentos tecnológicos empregados pelo Estado (Cath *et al*., 2018).

6. Propostas Para Implementação Ética da Inteligência Artificial

Diante dos avanços tecnológicos e da crescente adoção de ferramentas de inteligência artificial em investigações criminais, torna-se imperativo estabelecer diretrizes normativas, técnicas e éticas que assegurem a legalidade e a legitimidade de seu uso. Tais diretrizes devem equilibrar o interesse público na efetiva prevenção e repressão de crimes com a proteção dos direitos e garantias fundamentais assegurados pela ordem constitucional brasileira.

A regulação da IA no contexto investigativo deve partir de princípios já consolidados na doutrina jurídica e em documentos internacionais. É necessário que os órgãos públicos responsáveis pela investigação criminal adotem práticas de governança algorítmica, como a elaboração de pareceres técnicos prévios ao uso de IA, a realização de auditorias independentes e a publicação de relatórios de impacto sobre direitos fundamentais. Além disso, devem ser criados comitês

ISSN 2178-6925
DOI: 10.61164/x5fcqh87

éticos interdisciplinares para avaliação contínua do uso de tais tecnologias (Monteiro; Doneda, 2021).

A utilização de IA em processos investigativos deve estar sujeita ao controle do Poder Judiciário, especialmente quando envolver medidas invasivas, como vigilância, quebra de sigilo ou restrição de direitos. É essencial garantir a ampla defesa e o contraditório quanto a provas obtidas por meio automatizado, assegurando ao acusado o direito de questionar a validade dos algoritmos e sua aplicação ao caso concreto (Bioni, 2020).

A formação de profissionais do Direito, da segurança pública e da tecnologia deve ser prioridade, de modo a assegurar a adequada compreensão dos limites e potencialidades da IA. Programas de capacitação técnica e ética são indispensáveis para promover o uso responsável dessas ferramentas no ambiente institucional (Brant; Costa, 2022).

Considerando o caráter transnacional dos crimes digitais, recomenda-se a adoção de tratados e acordos internacionais que harmonizem padrões legais e técnicos sobre o uso da IA na segurança pública. Simultaneamente, o Congresso Nacional deve avançar em projetos de lei que regulamentem de forma específica a aplicação de IA no sistema de justiça criminal, conforme já vem sendo proposto em países da União Europeia e da América do Norte (Monteiro; Doneda, 2021).

A adoção dessas diretrizes visa não apenas aprimorar a eficácia da atuação estatal frente aos desafios do cibercrime, mas também consolidar uma cultura jurídica que valorize a proteção de direitos fundamentais diante da incorporação de tecnologias emergentes.

7. Conclusão

A presente pesquisa teve como objetivo central analisar os principais desafios enfrentados na identificação de criminosos em meios eletrônicos, bem como investigar o potencial da inteligência artificial como ferramenta auxiliar nas investigações e na prevenção de crimes digitais. O estudo demonstrou que o ambiente virtual impõe obstáculos substanciais às estratégias tradicionais de persecução penal, exigindo a incorporação de tecnologias inteligentes capazes

ISSN 2178-6925
DOI: 10.61164/x5fcqh87

de lidar com a complexidade e a dinamicidade da criminalidade digital contemporânea.

Foi possível observar que criminosos utilizam mecanismos sofisticados de anonimização, como VPN, criptografia de ponta a ponta, redes descentralizadas e técnicas de falsificação digital, o que dificulta a atribuição de autoria e compromete a eficácia das investigações. Nesse cenário, a IA se mostra uma aliada promissora, oferecendo soluções para análise de grandes volumes de dados, reconhecimento de padrões comportamentais, rastreamento de transações suspeitas e identificação automatizada de indivíduos.

Entretanto, também ficou evidente que o uso da inteligência artificial na segurança pública levanta sérias preocupações éticas e jurídicas, especialmente no tocante ao respeito à privacidade, à não discriminação, à transparência algorítmica e ao controle judicial das decisões automatizadas. A ausência de uma regulamentação específica no Brasil agrava esse cenário, tornando urgente a construção de um marco legal que discipline o uso da IA de forma equilibrada e compatível com os valores democráticos.

Foram propostas diretrizes que contemplam princípios como a legalidade, a supervisão humana, a governança algorítmica, o controle judicial e a capacitação institucional, com vistas a garantir uma aplicação ética, segura e eficiente da IA no âmbito da investigação criminal. A adoção dessas diretrizes poderá contribuir para a consolidação de uma cultura jurídica que valorize simultaneamente a eficácia investigativa e a proteção dos direitos fundamentais.

Conclui-se, portanto, que a inteligência artificial representa uma oportunidade singular para modernizar as práticas investigativas frente aos desafios impostos pelos crimes digitais, desde que seu uso seja pautado por critérios normativos claros, responsabilidade institucional e compromisso com os princípios do Estado Democrático de Direito.

8. Referências

BINNS, Reuben. *Algorithmic accountability and public reason.* ***Philosophy & Technology***, v. 31, n. 4, 2018.

ISSN 2178-6925
DOI: 10.61164/x5fcqh87

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2020.

BRANT, Rafael; COSTA, Leandro. Inteligência artificial na segurança pública: promessas e desafios. **Revista Brasileira de Segurança Pública**, v. 16, n. 2, 2022.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília-DF: Senado, 1988. Disponível em: https://tinyurl.com/29ucwd3a. Acesso em: 11 jun. 2025.

BRASIL. **Lei nº. 13.709 de 14 de agosto de 2018**. Lei geral de proteção de dados pessoais. Brasília-DF: Senado, 2018. Disponível em: https://tinyurl.com/mtcea948. Acesso em: 11 jun. 2025.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

CATH, Corinne; WACHTER, Sandra; MITTELSTADT, Brent; TADDEO, Mariarosaria; FLORIDI, Luciano. *Artificial intelligence and the 'good society': the US, EU, and UK approach.* ***Science and Engineering Ethics***, v. 24, 2018.

DONEDA, Danilo. **Direito, privacidade e tecnologias digitais**. São Paulo: Thomson Reuters Brasil, 2020.

DONEDA, Danilo; MONTEIRO, Ronaldo Lemos. Privacidade, proteção de dados e novas tecnologias. *In*: DONEDA, D.; MENDES, L. C. (Org.). **Direito e internet**. São Paulo: Revista dos Tribunais, 2020.

EUBANKS, Virginia. ***Automating inequality****: how high-tech tools profile, police, and punish the poor*. New York: St. Martin's Press, 2018.

FERRAZ, Carolina; OLIVEIRA, Gabriel M. Deepfakes e os desafios probatórios no processo penal. **Revista Brasileira de Direito Processual Penal**, v. 9, n. 1, 2023.

LEVY, Steven. **Hackers**: *heroes of the computer revolution*. New York: O'Reilly Media, 2019.

MARTIN, Nina; WHITTEN-WOODRING, Jenifer. *Algorithmic BIAS in criminal justice: ethical implications and accountability.* ***Journal of Ethics and Technology***, v. 18, n. 3, 2022.

MATTOS, Luciano. **Relatório de atividades**: 1º quadrimestre 2022. Rio de Janeiro: MPRJ, 2022.

ISSN 2178-6925
DOI: 10.61164/x5fcqh87

MELO, Luiza. Golpes virtuais aumentam e não fazem distinção de idade. **Senado Notícias**, 11 abr. 2025. Disponível em: https://tinyurl.com/mrafy4fc. Acesso em: 10 ago. 2025.

MONTEIRO, Felipe; DONEDA, Danilo. Inteligência artificial e o direito: fundamentos para uma regulação no Brasil. **Revista Brasileira de Direito Digital**, v. 3, n. 1, 2021.

REZENDE, Fernando A. Criptografia, anonimato e investigação digital: dilemas da era da informação. **Revista de Direito Digital e Cibernético**, v. 2, n. 3, 2020.

ROCHA, Matheus; FERRAZ, Carolina. Reconhecimento facial e os riscos à privacidade: uma análise do caso Salvador. **Revista de Direito, Tecnologia e Sociedade**, v. 7, n. 1, 2021.

RUSSELL, Stuart; NORVIG, Peter. **Inteligência artificial**. 3. ed. São Paulo: Pearson, 2021.

SILVA, Aroldo Nicácio. **Sistemas móveis como suporte à atividade da polícia militar do Paraná**. 2020, 62 fl. Monografia (Especialização em Desenvolvimento para Dispositivos Móveis e Internet das Coisas) – Universidade Tecnológica Federal do Paraná, Curitiba, 2020.

STF. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº. 6.387-DF**. Tribunal Pleno. Relatora: Ministra Rosa Weber. Brasília-DF: DJe, 12 nov. 2020.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2021.