DIREITO PENAL, SOCIEDADE DA INFORMAÇÃO E TECNOLOGIA: A INTELIGÊNCIA ARTIFICIAL NA OBTENÇÃO E VALIDAÇÃO DE PROVAS DIGITAIS

CRIMINAL LAW, INFORMATION SOCIETY AND TECHNOLOGY: ARTIFICIAL INTELLIGENCE IN THE ACQUISITION AND VALIDATION OF DIGITAL EVIDENCE

Edielma Rocha Dutra
Pós-graduada em Direito Processual Penal pela Instituto Damásio de Direito/IBMEC,
Mestre em Direito da Sociedade da Informação nas Faculdades Metropolitanas Unidas e
Oficial de Promotoria no Ministério Público do Estado de São Paulo (MPSP).
edielmadutra@mpsp.mp.br
Cássia Luize Ferreira da Silva
Mestre em Direito da Sociedade da Informação nas Faculdades Metropolitanas Unidas e
Advogada.
cassialuize01@gmail.com
Greice Patrícia Fuller
Pós-Doutora em Direito Ambiental pela Universidade de Navarra/Espanha,
Doutora e Mestre em Direito das Relações Sociais pela Pontifícia Universidade Católica de São Paulo (PUC/SP),
Professora do Programa de Mestrado em Direito da Sociedade da Informação e da Graduação das Faculdades Metropolitanas Unidas (FMU) e
Líder do Projeto de Pesquisa Efetividade jurisdicional estatal certificado pelo CNPq do Programa em Direito da sociedade da informação.
greice.fuller@fmu.br

RESUMO

O presente artigo analisa a intersecção entre o Direito Penal e a Inteligência Artificial (IA) no contexto da Sociedade da Informação. Com o avanço da tecnologia digital, a IA emerge como uma ferramenta valiosa para a obtenção e validação de provas digitais, prometendo aumentar a eficiência do sistema de justiça criminal. No entanto, seu uso também traz desafios éticos e legais, como o viés algorítmico e a proteção dos direitos individuais. A pesquisa aborda diretrizes estabelecidas, como o Regulamento de Inteligência Artificial da União Europeia nº 2024/1689 e a Resolução nº 332/2020 do CNJ e discute a importância da regulamentação e da capacitação dos profissionais do Direito. Para isso, foi adotado o método dedutivo reflexivo-

crítico, que envolveu uma ampla pesquisa bibliográfica, incluindo a análise de artigos acadêmicos, teses, legislação pertinente e a avaliação da jurisprudência relacionada ao tema.

Palavras-chave: Direito Penal - Inteligência Artificial - Sociedade da Informação – Ética - Regulamentação.

ABSTRACT

This article analyzes the intersection between Criminal Law and Artificial Intelligence (AI) within the context of the Information Society. With the advancement of digital technology, AI emerges as a valuable tool for obtaining and validating digital evidence, promising to increase the efficiency of the criminal justice system. However, its use also brings ethical and legal challenges, such as algorithmic bias and the protection of individual rights. The research addresses established guidelines, such as the European Union Artificial Intelligence Regulation No. 2024/1689 and CNJ Resolution No. 332/2020 and discusses the importance of regulation and the training of legal professionals. To achieve this, a reflective-critical deductive method was adopted, involving extensive bibliographic research, including the analysis of academic articles, theses, relevant legislation, and an evaluation of the jurisprudence related to the topic.

Keywords: Criminal Law - Artificial Intelligence - Information Society – Ethics – Regulation.

INTRODUÇÃO

Na contemporaneidade, a Sociedade da Informação transformou radicalmente a forma como os dados são gerados, armazenados e processados. Essa revolução tecnológica não apenas alterou dinâmicas sociais e econômicas, mas também impactou profundamente os sistemas de justiça, em especial o Direito Penal. A crescente digitalização do cotidiano traz à tona novos desafios e oportunidades, uma vez que a tecnologia é cada vez mais utilizada como ferramenta para a investigação e a prova de delitos. Nesse contexto, a Inteligência Artificial (IA) se destaca como um recurso promissor para a coleta e análise de provas digitais, oferecendo soluções que prometem aumentar a eficiência e a precisão nas ações judiciais.

A utilização da IA no Direito Penal é respaldada por diretrizes éticas e legais que buscam assegurar a proteção dos direitos fundamentais e a transparência nos processos judiciais. O Conselho Nacional de Justiça (CNJ), por meio da Resolução nº 332/2020, estabelece parâmetros para o uso responsável da IA no Judiciário, enfatizando a importância da supervisão humana e da explicabilidade dos sistemas. Contudo, a implementação da IA no sistema de justiça não é isenta de controvérsias, justificando a análise do tema sobre obtenção

e validação das provas digitais. Questões como o viés algorítmico, a proteção da privacidade e a responsabilidade em decisões automatizadas levantam preocupações sobre o impacto da tecnologia na equidade e na justiça, desafiando a integridade do sistema penal.

Diante desse cenário, o objetivo deste artigo é explorar as interações entre a IA e o Direito Penal, examinando não apenas as vantagens e inovações que essa tecnologia pode trazer, mas também os riscos e desafios que devem ser enfrentados. Ao analisar como a IA pode ser utilizada na obtenção e validação de provas digitais, bem como as implicações éticas de sua aplicação, busca-se contribuir para o entendimento das tendências atuais e futuras no campo do Direito, promovendo um debate necessário sobre a utilização responsável da tecnologia no sistema de justiça. Assim, é fundamental que profissionais do Direito, legisladores e a sociedade em geral estejam preparados para lidar com as complexidades introduzidas pela IA, assegurando que os avanços tecnológicos sirvam para fortalecer, e não para fragilizar, os princípios fundamentais da justiça.

Pretende-se responder o seguinte problema de pesquisa: quais são os principais desafios éticos e legais associados à utilização da Inteligência Artificial na obtenção e validação de provas digitais no Direito Penal? Este questionamento é crucial, uma vez que a crescente adoção de tecnologias de IA no sistema de justiça levanta preocupações sobre a transparência, a responsabilidade e a proteção dos direitos individuais. À medida que algoritmos e sistemas automatizados se tornam ferramentas cada vez mais presentes em investigações criminais, é fundamental analisar como esses avanços podem afetar a imparcialidade e a legitimidade das decisões judiciais, além de garantir que os princípios fundamentais da justiça sejam respeitados.

Para abordar essa questão, foi utilizado o método dedutivo reflexivo-crítico, que envolveu uma ampla pesquisa bibliográfica, envolvendo a análise analítica de artigos acadêmicos, teses, legislação pertinente, bem como a avaliação de jurisprudência relacionada ao tema.

O artigo foi dividido em três seções, quais sejam: 1) Introdução à inteligência artificial no Direito Penal; 2) Métodos de obtenção e validação de provas digitais; e 3) Implicações e desafios da integração da IA na obtenção e validação de provas digitais.

1. INTRODUÇÃO À INTELIGÊNCIA ARTIFICIAL NO DIREITO PENAL

1.1. Tipos de inteligência artificial e o marco regulatório europeu

A doutrina mais atualizada aponta diversos tipos de Inteligência Artificial (IA), classificadas de acordo com seu nível de sofisticação, capacidade e usos. No entanto, apontam-se como principais as seguintes: Inteligência Artificial Estreita (ANI), Inteligência Geral Artificial (AGI) e Superinteligência Artificial (ASI).

A Inteligência Artificial Estreita (ANI), também conhecida como IA fraca, é projetada para executar tarefas específicas, não sendo capaz de aprender além das suas capacidades programadas. Exemplos: Alexa da Amazon e Siri da Apple, que usam reconhecimento de fala; Netflix e outras plataformas de *streaming*, que usam dados do usuário para fornecer recomendações personalizadas; etc. Também é utilizada em vários setores profissionais (saúde, finanças, fábricas, atendimento ao cliente e segurança). A Inteligência Artificial Super (ASI) opera além do nível de inteligência humana, sendo capaz de superar os seres humanos em potencialmente todos os campos do conhecimento e atividade. No entanto, atualmente é um conceito hipotético, pois nenhum sistema ainda alcançou a ASI. Apesar disso, é um tópico de muita discussão e debate no campo da IA. A Inteligência Artificial Geral (AGI), também conhecida como IA forte, tem como objetivo realizar tarefas intelectuais da mesma forma que um ser humano pode. Assim, visa a aprender e a se adaptar a novas situações, assim como uma pessoa faria, e não se limita a uma tarefa ou área específica, podendo ser aplicada em diversos campos. Por fim, a Inteligência Artificial Super (ASI) opera além do nível de inteligência humana, sendo capaz de superar os seres humanos em potencialmente todos os campos do conhecimento e atividade. No entanto, atualmente é um conceito hipotético, pois nenhum sistema ainda alcançou a ASI. Apesar disso, é um tópico de muita discussão e debate no campo da IA.[1]

Ademais, o Regulamento de Inteligência Artificial da União Europeia (Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024), que cria regras harmonizadas em matéria de inteligência artificial, é o primeiro ato legislativo do mundo em matéria de inteligência artificial. Visa a garantir que os sistemas de IA são seguros, éticos e confiáveis. As regras impõem obrigações aos fornecedores e aos responsáveis pela implantação

[1] UNIVERSITY OF WOLVERHAMPTON. *What are the different types of artificial intelligence?* 2023. Disponível em: https://online.wlv.ac.uk/. Acesso em: 11 out. 2024.

de tecnologias de IA e regulam a autorização de sistemas de inteligência artificial no mercado único da UE.

O Regulamento de IA da UE classifica os sistemas de inteligência artificial em quatro níveis de risco: risco mínimo ou nulo, onde a maioria dos sistemas, como jogos baseados em IA e filtros de *spam*, não são regulamentados; risco limitado, que inclui sistemas como chatbots e geradores de conteúdo, exigindo transparência para informar os usuários sobre a origem gerada por IA; risco elevado, que abrange sistemas usados em diagnósticos médicos, condução autônoma e identificação biométrica, necessitando de testes rigorosos, transparência e supervisão humana para operar no mercado da UE; e risco inaceitável, que proíbe sistemas que ameaçam a segurança ou direitos humanos, como manipulação cognitivo-comportamental e reconhecimento facial em tempo real por autoridades, exceto em casos específicos. Além disso, modelos de IA de finalidade geral, que podem executar diversas tarefas, estão sujeitos a requisitos de transparência se não apresentarem riscos sistêmicos, enquanto aqueles que apresentam tais riscos devem seguir regras mais rigorosas.[2]

Enquanto primeiro ato legislativo do mundo que regula a IA, as regras da UE poderão estabelecer uma referência mundial na regulamentação da IA, tal como aconteceu com o Regulamento Geral sobre a Proteção de Dados (RGPD) para a privacidade dos dados, promovendo uma inteligência artificial ética, segura e fiável em todo o mundo.

1.2. Intersecção da sociedade da informação e a criminalidade

A introdução da Inteligência Artificial (IA) representa um avanço significativo, mas também traz consigo um cenário repleto de incertezas. Essa tecnologia, ainda em sua fase inicial de aplicação na justiça, oferece ferramentas inovadoras para a análise de evidências e a investigação criminal. A capacidade da IA de processar grandes volumes de dados pode potencialmente aumentar a eficiência das investigações, permitindo a identificação de padrões que, de outra forma, poderiam passar despercebidos. No entanto, a natureza emergente dessa tecnologia ressalta a necessidade de cautela, especialmente considerando a escassez de regulamentações que orientem seu uso ético e responsável.

[2] COMISSÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho. Disponível em: https://digital-strategy.ec.europa.eu/. Acesso em: 12 out. 2024.

Além disso, a ausência de diretrizes claras levanta questões importantes sobre a responsabilidade e a supervisão nas decisões influenciadas pela IA. A possibilidade de decisões judiciais serem moldadas por algoritmos, que podem operar com dados enviesados ou incompletos, gera preocupações sobre a equidade e a justiça no tratamento dos indivíduos. O desenvolvimento de normas que garantam a transparência nos processos algorítmicos e a supervisão humana efetiva se tornam, portanto, imprescindíveis.

Diante desses aspectos, é fundamental iniciar a análise da Inteligência Artificial no Direito Penal com uma breve contextualização da sociedade da informação. Essa nova era, caracterizada pela produção e circulação massiva de dados, transforma a maneira como a informação é gerada, compartilhada e utilizada.

A sociedade da informação é um conceito que emergiu nas últimas décadas, caracterizando uma transformação profunda nas dinâmicas sociais, econômicas e culturais, impulsionada pelo avanço das tecnologias digitais. Nesse novo paradigma, a informação se torna o principal recurso econômico, moldando a forma como indivíduos, organizações e governos interagem e tomam decisões. A era da informação é marcada pela ubiquidade da internet, que proporciona acesso instantâneo a vastos volumes de dados e facilita a comunicação em tempo real entre diversas partes, transcendendo fronteiras geográficas e temporais.

Fujita e Barreto Junior[3] afirmam que a era contemporânea atravessa um novo estágio de desenvolvimento econômico, cultural, social e político, que se convencionou chamar de sociedade da informação. Essa mudança provoca uma série de novos desafios e paradoxos para a seara jurídica.

Castells, em sua análise, apresenta a sociedade da informação e destaca o surgimento simultâneo de atividades criminosas nesse ambiente. Ele observa:

> Vários acontecimentos de importância histórica transformaram o cenário social da vida humana. Uma revolução tecnológica concentrada nas tecnologias da informação começou a remodelar a base material da sociedade em ritmo acelerado. Economias por todo o mundo passaram a manter interdependência global, apresentando uma nova forma de relação entre a economia, o Estado e a sociedade em um sistema de geometria variável. [...] Simultaneamente, as atividades criminosas e organizações ao estilo da máfia de todo o mundo também se tornaram globais e informacionais, propiciando os meios para o encorajamento de hiperatividade mental e desejo

[3] FUJITA, Jorge Shiguemitsu; BARRETO JUNIOR, Irineu Francisco. O direito ao esquecimento e a liberdade de informar na sociedade da informação. *Revista de Direitos Fundamentais e Democracia*, v. 25, n. 2, p. 5-27, maio/ago. 2020, p. 7.

> proibido, juntamente com toda e qualquer forma de negócio ilícito procurado por nossas sociedades, de armas sofisticadas à carne humana.[4]

Nesse sentido, Fuller[5] ressalta que, à medida que novas tecnologias se expandem, surgem situações fáticas complexas e dinâmicas que carecem de regulamentação jurídica, especialmente no campo do Direito Penal.

A emergência de novos crimes, com configurações típicas e *modus operandi* específicos, é uma consequência direta da evolução tecnológica acelerada. Crimes digitais, que vão desde fraudes eletrônicas até invasões de sistemas, entre outros, surgem de forma exponencial, refletindo a criatividade e a adaptação dos criminosos a um ambiente em constante mudança.

Em contrapartida, a implementação de ferramentas tecnológicas para a prevenção e repressão dessas atividades ilícitas ocorre de maneira significativamente mais lenta. Essa disparidade não apenas compromete a eficácia das investigações e ações penais, mas também expõe a necessidade urgente de um esforço coordenado para desenvolver e adaptar regulamentações que acompanhem o ritmo das transformações sociais e tecnológicas, garantindo que o sistema de justiça permaneça relevante e eficaz na proteção dos direitos fundamentais e na manutenção da ordem pública.

1.3. A inteligência artificial no sistema de justiça criminal

A integração da tecnologia no Direito Penal não é um fenômeno recente. Desde a introdução das primeiras técnicas de identificação, como a impressão digital no final do século XIX, até o uso de DNA na década de 1980, a tecnologia tem desempenhado um papel crucial na evolução das investigações criminais. Conforme exemplifica Simon Andrew Cole[6], a impressão digital foi introduzida pela primeira vez como método de identificação em 1892 por Juan Vucetich, revolucionando a forma como os criminosos eram identificados e processados.

---

[4] CASTELLS, Manuel. *A sociedade em rede: a era da informação: economia, sociedade e cultura*. v. 1. 6. ed. São Paulo: Paz e Terra, 1999, p. 39-40.

[5] FULLER, Greice Patrícia. Os delitos e as novas tecnologias em face da relação dialógica com os direitos humanos. In: SARLET, Ingo Wolfgang; WALDMAN, Ricardo Libel (org.). *Direitos humanos e fundamentais na era da informação*. Porto Alegre: Fundação Fênix, 2020, p. 217.

[6] COLE, Simon Andrew. *Suspect identities: a history of fingerprinting and criminal identification*. Cambridge: Harvard University Press, 2001, p. 128.

Da mesma forma, a análise de DNA, utilizada em investigações desde a década de 1980, tem se mostrado uma ferramenta poderosa para a identificação de suspeitos e a exoneração de inocentes, como apontam Michael Lynch et al..[7]

Neste contexto, a Inteligência Artificial (IA) representa a próxima grande evolução na aplicação da tecnologia ao Direito Penal. Definida como a capacidade de uma máquina de imitar funções cognitivas humanas, como aprendizado e resolução de problemas, a IA pode analisar grandes volumes de dados, identificar padrões e prever comportamentos, podendo vir a tornar-se uma ferramenta essencial para investigações criminais.

Segundo Stuart Jonathan Russell e Peter Norvig[8], a IA abrange uma variedade de tecnologias, incluindo aprendizado de máquina, processamento de linguagem natural e redes neurais, que podem ser aplicadas em diversas áreas do Direito Penal. Não obstante, a introdução da IA no Direito Penal traz tanto oportunidades quanto desafios. Se, por um lado, a IA pode aumentar a eficiência e a precisão das investigações, por outro, levanta questões éticas e legais significativas, como a privacidade, a transparência e o viés algorítmico.

Pedro Domingos[9] observa que a IA tem a capacidade de processar e analisar dados em uma velocidade que supera a capacidade humana, identificando padrões e conexões que poderiam passar despercebidos em análises tradicionais.

Ferramentas de IA podem analisar dados de diversas fontes, como redes sociais, registros telefônicos, e-mails e transações financeiras, para identificar padrões e conexões relevantes para uma investigação criminal. Viktor Mayer-Schönberger e Kenneth Cukier[10] ressaltam que a habilidade da IA em lidar com *big data* permite que investigadores processem rapidamente informações massivas.

Exemplos práticos incluem ferramentas como IBM Watson e Palantir Gotham, que são utilizadas por agências de segurança para analisar dados e identificar possíveis ameaças ou atividades criminosas, como destacado por Yuval Noah Harari.[11] Essas tecnologias não apenas

---

[7] LYNCH, Michael; COLE, Simon Andrew; McNALLY, Ruth; JORDAN, Kathleen. *Truth machine: the contentious history of DNA fingerprinting*. Chicago: University of Chicago Press, 2008, p. 121.
[8] RUSSELL, Stuart; NORVIG, Peter. *Inteligência artificial: uma abordagem moderna*. 4. ed. São Paulo: LTC, 2022, p. 36.
[9] DOMINGOS, Pedro. *The master algorithm: how the quest for the ultimate learning machine will remake our world*. New York: Basic Books, 2015, p. 78.
[10] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big data: a revolution that will transform how we live, work, and think*. New York: Houghton Mifflin Harcourt, 2013, p. 126.
[11] HARARI, Yuval Noah. *21 lessons for the 21st century*. London: Penguin Random House, 2018, p. 28.

facilitam a coleta de informações, mas também ajudam na priorização de recursos e na tomada de decisões estratégicas em tempo real.

Outras tecnologias de IA que têm sido amplamente adotadas em investigações criminais incluem o reconhecimento facial e de voz. Essas tecnologias permitem a identificação de suspeitos por meio de imagens de câmeras de segurança e gravações de áudio.

Ademais, os algoritmos de reconhecimento facial podem comparar imagens de suspeitos com bancos de dados fotográficos, sendo amplamente utilizados em aeroportos, eventos públicos e investigações de crimes.[12] Quanto ao reconhecimento de voz, Daniel Jurafsky e James Howard Martin[13] afirmam que essas tecnologias podem analisar gravações de áudio para identificar falantes específicos, contribuindo em investigações de crimes como sequestros e extorsões.

Além disso, a IA é utilizada para monitorar e rastrear atividades suspeitas na internet e nas redes sociais. Algoritmos analisam postagens, mensagens e interações online para identificar comportamentos que possam indicar atividades criminosas. Destaque-se que as ferramentas de IA podem identificar ameaças, discursos de ódio e atividades terroristas nas plataformas digitais. Adicionalmente, Eric Wai Ting Ngai e seus coautores explicam que algoritmos de IA podem monitorar transações financeiras para detectar padrões de lavagem de dinheiro e financiamento de atividades ilícitas.[14]

1.4. A inteligência artificial no cenário brasileiro

No Brasil, os Ministérios Públicos também estão se preparando para deixar de utilizar ferramentas analógicas. É o que aponta o último relatório "Levantamento de Iniciativas de IA no Ministério Público", realizado pela Comissão de Planejamento Estratégico (Estratégia Nacional do MP Digital), publicado pelo Conselho Nacional do Ministério Público em 2023.[15]

---

[12] SANTO DIGITAL. Reconhecimento facial: como funciona e benefícios para prevenção a fraudes. 2024. Disponível em: https://santodigital.com.br/.

[13] JURAFSKY, Daniel; MARTIN, James Howard. *Speech and language processing*. 3. ed. Stanford: Stanford University, 2024, p. 333.

[14] NGAI, Eric Wai Ting; HU, Yong; WONG, You-hing; CHEN, Yijun; SUN, Xin. The application of data mining techniques in financial fraud detection: a classification framework and an academic review of literature. *Decision Support Systems*, v. 50, n. 3, p. 559-569, fev. 2011, p. 559-569.

[15] CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO (CNMP). *Levantamento de iniciativas de IA no Ministério Público*. 2023. Disponível em: https://www.cnmp.mp.br/. Acesso em: 25 set. 2024.

Conforme informações apresentadas no relatório “Levantamento de Iniciativas de IA no Ministério Público”, inúmeros sistemas que possuem estrutura de inteligência artificial ou que utilizam inteligência artificial estão em desenvolvimento e alguns já estão em utilização.

- **Ministério Público Federal**

O Ministério Público Federal apresenta alguns sistemas em desenvolvimento. Entre eles, destacamos o sistema TRIA (Triagem em Habeas Corpus) que utiliza Inteligência Artificial (IA) para automatizar a extração de informações das decisões proferidas pelo Superior Tribunal de Justiça (STJ) em Habeas Corpus (HC). A ferramenta compara essas decisões com os pareceres emitidos pelo MPF nos mesmos processos, identificando se a decisão foi favorável ou contrária à manifestação do membro do MPF ou se ocorreu sem a manifestação prévia do órgão. Esse mecanismo facilita a triagem dos HCs nos gabinetes criminais da Procuradoria-Geral da República (PGR), otimizando o trabalho dos procuradores ao dar uma visão clara sobre o alinhamento das decisões judiciais com as posições do MPF.

Com uma base de dados composta por 15 mil decisões/acórdãos do STJ e cerca de 48 mil pareceres do MPF, o TRIA emprega um modelo de aprendizado supervisionado, utilizando o algoritmo Random Forest, e apresenta uma acurácia de 94,80%. Esse nível de precisão indica uma ferramenta robusta, que já está em produção e integra informações diretamente no sistema de tramitação processual do MPF, o Sistema Único, potencializando a eficiência da análise de casos.

O sistema de Resultados de Julgamentos é outra iniciativa do MPF que emprega IA para automatizar a extração de dados das sentenças em ações penais, ajudando servidores dos gabinetes de primeira instância a preencher informações sobre o resultado dos julgamentos no Sistema Único. A ferramenta captura informações detalhadas como réu, resultado do julgamento, fundamentação jurídica, base normativa, pena, multa, data da sentença e juiz responsável. Com uma base de treinamento composta por 3797 sentenças, a tecnologia emprega um modelo de Reconhecimento de Entidade Nomeada (NER) desenvolvido com a biblioteca Spacy e técnicas de Transformers, resultando em uma acurácia de 88,21%. A implementação em produção mostrou variações na precisão dependendo da entidade extraída, com algumas alcançando mais de 90% de precisão, enquanto outras ainda apresentam acurácia inferior a 80%. Esse sistema proporciona um avanço significativo na automação e padronização do registro de informações processuais, facilitando o trabalho dos servidores.

A Triagem de Inquéritos Policiais é outra iniciativa em desenvolvimento pelo MPF que utiliza IA para identificar automaticamente o motivo da entrada de inquéritos policiais, como dilação de prazo ou relatório final, a partir da análise das peças processuais. A ferramenta visa a simplificar a triagem desses inquéritos nos gabinetes criminais, agilizando a gestão dos casos. Com uma base de dados inicial de cerca de 12 mil peças processuais, o sistema aplicará técnicas de Processamento de Linguagem Natural (PLN) para classificar os documentos. A expectativa é de que, ao entrar em produção, a ferramenta se torne um suporte essencial para os servidores, reduzindo o tempo e o esforço necessário para organizar e gerenciar inquéritos, promovendo uma triagem mais eficiente e assertiva.

- **Ministério Público do Distrito Federal e Territórios**

O PEPSI (Sistema de Apoio às Promotorias de Execução Penal), desenvolvido pelo Ministério Público do Distrito Federal e Territórios (MPDFT), é uma ferramenta que integra diversas fontes de dados relevantes para a execução penal, como o PJE (SEEU), BNMP e SIAPEN. Utilizando *Support Vector Machine* (SVM) e *Tesseract*, o sistema organiza informações para auxiliar na tomada de decisão, sugerindo manifestações baseadas em casos similares. Apesar dos desafios relacionados à extração de dados dos processos do PJE e à formação de equipes multidisciplinares, o PEPSI visa a reduzir o tempo necessário para coleta e exame de material, otimizando o fluxo de trabalho das promotorias de execução penal. Com a visualização integrada e sugestões automatizadas, o PEPSI tem potencial para melhorar a eficiência e a qualidade das manifestações processuais, contribuindo para um sistema de justiça mais ágil e eficiente.

- **Ministério Público do Estado da Bahia**

O Fratria é uma ferramenta desenvolvida pelo Ministério Público do Estado da Bahia (MPBA) que aplica técnicas de IA para a automação de tarefas relacionadas a procedimentos extrajudiciais, como inquéritos policiais. Utilizando modelos de linguagem de grande escala (LLM) e outras tecnologias, o sistema sugere decisões aos membros do MPBA, como a proposição de denúncias, arquivamentos ou outras diligências, e até mesmo pré-minuta as peças processuais correspondentes. O sistema enfrenta desafios como a organização e digitalização dos inquéritos, dificuldades de contratação e questões de conformidade com a Lei Geral de Proteção de Dados (LGPD). Mesmo assim, a iniciativa mostra-se promissora para aumentar a

eficiência e a eficácia das promotorias, reduzindo a carga de trabalho manual e permitindo um foco maior na análise crítica dos casos.

- **Ministério Público do Estado de Minas Gerais**

O Áquila é uma iniciativa do Ministério Público do Estado de Minas Gerais (MPMG) que utiliza IA para reconhecimento de pessoas e objetos em imagens e vídeos, auxiliando na investigação e detecção de crimes. A ferramenta aplica técnicas de visão computacional para identificação de pessoas por meio de características faciais e biométricas, como tatuagens, e de objetos de interesse, como veículos e armas. Com base em *datasets* públicos e criados internamente, o Áquila visa a aprimorar as operações de reconhecimento e busca automática em bases de dados visuais, retornando informações relevantes para os investigadores. Esse sistema tem potencial para se tornar uma ferramenta poderosa para o MPMG, ampliando a capacidade de identificação e monitoramento em investigações criminais e contribuindo para uma atuação mais efetiva do Ministério Público na segurança pública.

O desenvolvimento do Áquila já foi concluído, e, com o objetivo e escopo definidos, metas claras foram traçadas para o desenvolvimento do sistema. O principal desafio foi, dentro dos limites e fronteiras estabelecidos, utilizar ferramentas que o tornassem mais robusto, tendo em vista as situações reais nas quais o sistema será utilizado. Como solução para esse problema, o Áquila foi preparado para receber novos dados constantemente e, dessa forma, aprender novas características sempre que possível. Isso permite que o aprendizado do sistema seja atualizado continuamente, garantindo que ele se mantenha eficaz diante de novas circunstâncias e desafios.

Assim, inúmeras são as ferramentas de inteligência artificial que estão em fase de teste e implementação, que podem apresentar resultados positivos significativos no auxílio das investigações criminais.

Além dos Ministérios Públicos, a Secretaria de Segurança Pública de Alagoas está implementando um programa de inteligência artificial para otimizar o policiamento preditivo, visando a reduzir a criminalidade em até 26%. Desenvolvido pela empresa japonesa Singular Perturbations, o sistema utiliza algoritmos avançados para cruzar dados criminais e prever incidentes em áreas específicas, permitindo ações preventivas mais eficazes. A tecnologia será testada por três meses e, se bem-sucedida, aplicada por dois anos. O programa promete

melhorar a gestão de recursos e estratégias de segurança, baseando-se em uma análise detalhada dos padrões criminais e suas variáveis.[16]

Ainda, segundo o Canal de Ciências Criminais[17]:

> a Universidade Federal do Rio Grande do Sul (UFRGS) e a Polícia Federal (PF) também estão adotando esta abordagem tecnológica. Desde janeiro de 2021, ambas trabalham juntas em um projeto que emprega a inteligência artificial para o desenvolvimento de imagens de suspeitos a partir de amostras de DNA.

Em resumo, no Brasil, diversos projetos estão em desenvolvimento e alguns já estão em utilização, evidenciando o potencial da Inteligência Artificial e outras tecnologias na investigação criminal e na condução de processos. Essas inovações prometem aumentar a eficiência e a precisão do sistema de justiça, facilitando a análise de grandes volumes de dados e a identificação de padrões relevantes. No entanto, essa transformação também traz à tona questões éticas e legais que necessitam de uma avaliação cuidadosa. É fundamental que se estabeleçam diretrizes claras e regulamentações adequadas para garantir que a implementação dessas tecnologias respeite os direitos individuais e promova a justiça, evitando riscos como o viés algorítmico e a violação da privacidade.

2. MÉTODOS DE OBTENÇÃO E VALIDAÇÃO DE PROVAS DIGITAIS

2.1. Provas digitais

A era da informação provocou uma mudança profunda tanto na maneira como os crimes são praticados quanto na forma como são investigados. O surgimento das tecnologias de informação e comunicação resultou em um crescimento expressivo no volume e na diversidade de dados digitais. Informações como e-mails, mensagens instantâneas, registros de chamadas, dados de localização, arquivos armazenados em nuvem, *logs* de sistemas, vídeos e imagens digitais tornaram-se peças-chave nas investigações criminais, configurando-se como autênticas provas digitais.

---

[16] ALAGOAS. Governo do Estado. Programa de inteligência artificial da SSP estima reduzir criminalidade em até 26%. 2024. Disponível em: https://alagoas.al.gov.br/. Acesso em: 25 set. 2024.

[17] CANAL CIÊNCIAS CRIMINAIS. Descubra como a inteligência artificial pode auxiliar no combate ao crime no Brasil. 2023. Disponível em: https://www.mpmt.mp.br/. Acesso em: 25 set. 2024.

Lucien explora como a prova digital pode ser definida ou descrita[18]:

> prova digital não é nada mais nada menos que todo e qualquer dado que esteja armazenado ou que seja transmitido via computador e sirva para apoiar ou para rejeitar alguma teoria sobre como um crime específico aconteceu e que contenha elementos críticos desse crime, como intenção ou álibi.

Da mesma forma, Alexandre Morais da Rosa descreve a prova digital[19]:

> Prova Digital (*e-evidence*). A prova digital (espécie da prova eletrônica) é a obtida e/ou produzida em ambiente eletrônico digital, em que os dados (de base, de tráfego e de conteúdo), em geral vulneráveis, intangíveis e frágeis, devem ser extraídos e tratados em observância às normas técnicas, observada a cadeia de custódia digital, sob pena de ineficácia probatória. A tendência contemporânea é a do uso futuro da tecnologia *blockchain*. Definição de "e-evidence". A definição de "e-evidence" orienta-se pela: (a) relevância (meio de prova adequado ao fim que se destina); (b) confiabilidade (equivalência entre o verificado e o representado); e, (c) suficiência (deve congregar os elementos necessários de superação aos testes de verificação).

Ademais, Rosa salienta que a materialidade é essencial em crimes que deixam rastros, conforme estipulado no artigo 158 do Código de Processo Penal. Nos delitos cometidos por meios digitais ou eletrônicos, é necessário seguir normas técnicas que garantam a existência, validade e eficácia das provas. A evidência digital, ou *e-evidence*, requer que os dados sejam obtidos de maneira válida, indo além da simples captura da imagem ou aparência visível. Este é um dos desafios contemporâneos enfrentados no contexto das provas digitais.

Acerca da natureza das provas digitais, Fernandes e Montes[20] destacam que esses arquivos são essencialmente documentos em formato eletrônico. Ao contrário dos documentos físicos, nos quais as informações são inscritas em papel e são, portanto, tangíveis, os documentos eletrônicos são intangíveis. Embora documentos físicos possam ser digitalizados por meio de fotografias ou escaneamentos, seu processo original de produção permanece físico. Em contraste, documentos eletrônicos estão desvinculados de uma única plataforma de armazenamento físico. Esses arquivos digitais podem transitar entre diversos dispositivos,

---

[18] LUCIEN, Rocha. *Acreditação e admissibilidade de evidências digitais de crimes cibernéticos praticados em computação de nuvem*. 2023. Dissertação (Mestrado em Direito) — Universidade de Brasília, Brasília, 2023, p. 39-40.

[19] ROSA, Alexandre Morais da. Limite penal: o "print screen" é insuficiente à materialidade nos crimes digitais. Consultor Jurídico, 17 jun. 2022. Disponível em: https://www.conjur.com.br/. Acesso em: 12 out. 2024.

[20] FERNANDES, André Luís; MONTES, Rodrigo Henrique de Oliveira. Meta-evidência digital: a dualidade na cadeia de custódia envolvendo dispositivos eletrônicos e evidências digitais. *Revista Eletrônica Direito & TI*, Porto Alegre, v. 1, n. 14, dez. 2022, p. 60-61.

como DVDs, pen-drives, HDs ou plataformas de armazenamento remoto (cloud storage), o que significa que o documento digital não está restrito a um meio físico específico.

Diferentes tipos de evidências digitais possuem particularidades próprias que influenciam diretamente os métodos de coleta e preservação dessas informações.

2.2. Cadeia de custódia das provas digitais

É crucial destacar que a coleta de provas digitais, assim como as provas físicas, deve seguir rigorosamente a cadeia de custódia, para que as evidências sejam consideradas legítimas e válidas.

A cadeia de custódia é o conjunto de procedimentos que garantem a preservação, autenticidade e integridade das provas desde o momento de sua coleta até a sua apresentação em juízo. No Brasil, a cadeia de custódia foi normatizada com a promulgação da Lei n.º 13.964 de 2019, conhecida como 'Pacote Anticrime'. Essa lei introduziu modificações significativas no Código de Processo Penal, incluindo a formalização da cadeia de custódia, que, até então, não possuía regulamentação específica.

Com a alteração realizada no Código de Processo Penal, os procedimentos relacionados com a cadeia de custódia passaram a ser previstos a partir do art. 158-A, em que são estabelecidos controles rigorosos que devem ser seguidos sobre a evidência coletada, desde o momento em que ela é obtida até sua apresentação em tribunal. Esse controle inclui a documentação de cada etapa do processo, como quem teve acesso à evidência, quando, e sob que circunstâncias, garantindo que ela permaneça inalterada. A manutenção da integridade da prova é crucial para que ela possa ser considerada válida, uma vez que qualquer adulteração ou contaminação pode torná-la inadmissível.

No caso de provas digitais, esse cuidado torna-se ainda mais complexo, dado o caráter volátil e facilmente modificável dos dados eletrônicos. Acerca da diferença de manuseio para extração de dados de dispositivos digitais, por exemplo, Simão e outros apontam[21]:

> Diferentemente da abordagem de aquisição de dados em ambientes computacionais, em que geralmente os dados podem ser extraídos no estado em que foram encontrados

[21] SIMÃO, A. M. L.; SÍCOLI, F. C.; MELO, L. P.; DEUS, F. E. D.; SOUSA JÚNIOR, R. T. Aquisição de evidências digitais em smartphones Android. 2011, p. 93. DOI: http://dx.doi.org/10.5769/C2011009.

> e ficam preservados a partir do momento da sua apreensão, a extração de dados de telefones celulares e smartphones normalmente exige a execução de alguma intervenção no dispositivo. Além disso, tendo em vista que utilizam memórias embutidas, cujo acesso, sendo direto ao hardware, é delicado e complexo, é preciso instalar aplicativos ou utilizar ferramentas diretamente no dispositivo para que se proceda à aquisição dos dados armazenados e consequentes evidências.

A exigência de assegurar a autenticidade e integridade dos documentos digitais é comparável à proteção demandada para documentos físicos, conforme ressaltado por Fernandes e Montes[22]:

> assim como ocorre com os documentos físicos em papéis, através de assinaturas e certidões que garantem a sua autenticidade e a sua integridade, aos documentos digitais não é diferente. Surge então a necessidade de garantir aos documentos digitais as mesmas garantias de veracidade da prova que existem nos documentos físicos.

Embora o legislador tenha delineado a cadeia de custódia para as provas físicas, deixando uma lacuna no que diz respeito às provas digitais, é essencial que a observância da cadeia de custódia prevaleça também sobre as evidências digitais. A ideia de cadeia de custódia e preservação da prova já existia antes da positivação desse conceito. É imprescindível que a noção de "prova" inclua a manutenção de sua autenticidade, integridade, rastreabilidade e confiabilidade, atributos fundamentais para garantir a validade e a licitude das evidências.

Nesse sentido, o Superior Tribunal de Justiça (STJ) tem reafirmado a importância da preservação da cadeia de custódia, incluindo casos que envolvem provas digitais. No Agravo Regimental no Habeas Corpus nº 828054/RN, sob relatoria do Ministro Joel Ilan Paciornik, julgado em 23 de abril de 2024, o STJ entendeu que a integridade e confiabilidade das fontes de prova são ônus do Estado, e a falta de procedimentos adequados, como a adoção de técnicas de *hash* e softwares auditáveis, configura uma quebra na cadeia de custódia, tornando as provas inadmissíveis. De acordo com o julgado:

> Diante da volatilidade dos dados telemáticos e da maior suscetibilidade a alterações, imprescindível se faz a adoção de mecanismos que assegurem a preservação integral dos vestígios probatórios, de forma que seja possível a constatação de eventuais alterações, intencionais ou não, dos elementos inicialmente coletados, demonstrando-se a higidez do caminho percorrido pelo material. A auditabilidade, a repetibilidade, a reprodutibilidade e a justificabilidade são quatro aspectos essenciais das evidências digitais, os quais buscam ser garantidos pela utilização de metodologias e procedimentos certificados, como, e.g., os recomendados pela ABNT. A observação

[22] FERNANDES, André Luis; MONTES, Rodrigo Henrique de Oliveira. Meta-evidência digital: a dualidade na cadeia de custódia envolvendo dispositivos eletrônicos e evidências digitais. *Revista Eletrônica Direito & TI*, Porto Alegre, v. 1, n. 14, dez. 2022, p. 61.

> do princípio da mesmidade visa a assegurar a confiabilidade da prova, a fim de que seja possível se verificar a correspondência entre aquilo que foi colhido e o que resultou de todo o processo de extração da prova de seu substrato digital. Uma forma de se garantir a mesmidade dos elementos digitais é a utilização da técnica de algoritmo *hash*, a qual deve vir acompanhada da utilização de um software confiável, auditável e amplamente certificado, que possibilite o acesso, a interpretação e a extração dos dados do arquivo digital. [...] Neste caso, não houve a adoção de procedimentos que assegurassem a idoneidade e a integridade dos elementos obtidos pela extração dos dados do celular apreendido. Logo, evidentes o prejuízo causado pela quebra da cadeia de custódia e a imprestabilidade da prova digital. Agravo regimental provido a fim de conceder a ordem de ofício para que sejam declaradas inadmissíveis as provas decorrentes da extração de dados do celular do corréu, bem como as delas decorrentes.[23]

Aury Lopes Jr., ressalta a importância da cadeia de custódia como um elemento essencial para garantir a validade das provas. Em sua obra *Direito Processual Penal*, o autor afirma que a preservação das fontes de prova, por meio da manutenção da cadeia de custódia, requer a realização de uma série de atos, estabelecendo um verdadeiro protocolo de custódia que é delineado pelo art. 158-B e seguintes. Ele continua[24]:

> Todo esse cuidado é necessário e justificado: quer-se impedir a manipulação indevida da prova com o propósito de incriminar (ou isentar) alguém de responsabilidade, com vistas a obter a melhor qualidade da decisão judicial e impedir uma decisão injusta. Mas o fundamento vai além: não se limita a perquirir a boa ou má-fé dos agentes policiais/estatais que manusearam a prova. Não se trata nem de presumir a boa-fé, nem a má-fé, mas sim de objetivamente definir um procedimento que garanta e acredite a prova independente da problemática em torno do elemento subjetivo do agente. A discussão acerca da subjetividade deve dar lugar a critérios objetivos, empiricamente comprováveis, que independam da prova de má-fé ou "bondade e lisura" do agente estatal.

Aury Lopes Jr.[25] também reforça a necessidade de que, no caso de provas digitais, padrões técnicos e procedimentos formais sejam seguidos rigorosamente, como a utilização de ferramentas auditáveis para coleta e análise e a preservação dos metadados, que são fundamentais para comprovar a autenticidade e integridade da evidência.

> Questão recorrente nas interceptações telefônicas está na violação da "mesmidade" e, por via de consequência, do direito da defesa de ter acesso à integralidade da prova na sua originalidade (manifestação do contraditório=direito a informação e paridade de armas), na medida em que a prova é "filtrada" pela autoridade policial ou órgão acusador, que traz para o processo (e submete ao contraditório diferido) apenas o que lhe interessa. Não é "a mesma" prova colhida, mas apenas aquela que interessa ao acusador, subtraindo o acesso da defesa. A manipulação (e aqui se emprega no sentido

[23] BRASIL. Superior Tribunal de Justiça. AgRg no HC 828054/RN. Rel. Min. Joel Ilan Paciornik, Quinta Turma, julgado em 23 abr. 2024. Disponível em: https://processo.stj.jus.br/. Acesso em: 12 out. 2024.
[24] LOPES JR., Aury. *Direito processual penal*. 20. ed. Rio de Janeiro: Saraiva, 2023, p. 195.
[25] LOPES JR., Aury. *Direito processual penal*, p. 196.

> físico do vocábulo, sem juízo de desvalor ou atribuição de má-fé ao "manipulador") é feita durante a custódia e viola exatamente as regras de preservação da idoneidade. Já a "Desconfiança" (decorrência salutar em democracia, onde se desconfia do poder, que precisa ser legitimado sempre) consiste na exigência de que a prova (documentos, DNA, áudios etc.) deva ser "acreditada", submetida a um procedimento que demonstre que tais objetos correspondem ao que a parte alega ser. Como explica PRADO, o tema de provas exige a intervenção de regras de "acreditação", pois nem tudo que ingressa no processo pode ter valor probatório há que ser "acreditado", legitimado, valorado desde sua coleta até a produção em juízo para ter valor probatório. A cadeia de custódia exige o estabelecimento de um procedimento regrado e formalizado, documentando toda a cronologia existencial daquela prova, para permitir a posterior validação em juízo e exercício do controle epistêmico.

Aury Lopes Jr.[26] enfatiza que a quebra da cadeia de custódia não é apenas um desvio técnico, mas uma violação do devido processo penal que pode levar à ilicitude das provas. Ele argumenta que, apesar da ausência de uma definição legal clara sobre as consequências dessa quebra, deve-se considerá-la uma ofensa às garantias fundamentais, refletindo o descumprimento de normas que são essenciais para a validade probatória. Assim, a violação da cadeia de custódia deve resultar na inadmissibilidade da prova, conforme o que prescreve o art. 157 do Código de Processo Penal, ressaltando que, quando já incorporada ao processo, deve ser desentranhada e considerada sem valor probatório.

2.3. Possibilidade de utilização da IA na coleta e validação de provas digitais

No campo dinâmico e inovador da coleta de provas digitais, existem compreensões crescentes de que a Inteligência Artificial (IA) pode ser empregada para automatizar e otimizar a obtenção de evidências de diversas fontes, incluindo dispositivos móveis, redes sociais, e-mails e sistemas de vigilância. Como destaca Eoghan Casey[27], as ferramentas de IA são capazes de automatizar a coleta de grandes volumes de dados, diminuindo o tempo e o esforço necessários para reunir provas digitais. Da mesma forma, os autores Emilio Ferrara, Onur Varol, Clayon Davis, Filippo Menczer e Alessandro Flammini[28] afirmam que algoritmos de IA podem analisar atividades em redes sociais para identificar padrões de comportamento e potenciais evidências de atividades criminosas.

---

[26] LOPES JR., Aury. *Direito processual penal*, p. 197.
[27] CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers, and the internet*. 3. ed. Baltimore: Academic Press, 2011, p. 502.
[28] FERRARA, Emilio; VAROL, Onur; DAVIS, Clayton; MENCZER, Filippo; FLAMMINI, Alessandro. The rise of social bots. *Communications of the ACM*, v. 59, n. 7, p. 96-104, jul. 2016, p. 96-104.

Uma das possíveis aplicações da IA na validação de provas digitais seria a análise da autenticidade de documentos eletrônicos. Algoritmos de aprendizado de máquina podem ser treinados para reconhecer padrões e características específicas de documentos genuínos, como a presença de metadados consistentes, conformidade com padrões de formatação e ausência de anomalias. Esses algoritmos são úteis para detectar falsificações e alterações em documentos digitais, aumentando a confiabilidade das provas apresentadas.

Outra possível aplicação significativa é apontada pelos autores Anderson Rocha, Walter Scheirer, Terrance Boult e Siome Goldenstein[29], que mencionam a análise da integridade de arquivos de mídia, como imagens e vídeos. A IA pode ser utilizada para identificar manipulações e edições em arquivos de mídia, detectando inconsistências nos metadados, padrões de pixels e outros indicadores de alteração. Essas técnicas são particularmente valiosas em casos de pornografia infantil, *deepfakes* e outras formas de manipulação de mídia.

A IA pode atuar em diversas etapas da validação de provas, desde a coleta e análise de dados até a autenticação e verificação de evidências digitais. Eoghan Casey[30] exemplifica que algoritmos de IA podem ser empregados para coletar e analisar grandes volumes de dados, identificando padrões e correlações que podem ser relevantes para um caso penal.

Os benefícios da utilização da IA na validação de provas incluem a melhoria da precisão, a redução do tempo de análise e a minimização de erros humanos. Quanto à precisão, os algoritmos de IA têm a capacidade de analisar grandes volumes de dados com alta acurácia, identificando detalhes que podem passar despercebidos por analistas humanos, conforme aponta Eoghan Casey[31]. No que diz respeito à redução do tempo de análise, Angus McKenzie Marshall[32] observa que a IA pode processar e analisar dados de forma significativamente mais rápida do que os métodos tradicionais, acelerando o processo de investigação e julgamento. Os mesmos autores afirmam que a utilização da IA pode ajudar a minimizar erros humanos na análise de provas, aumentando a confiabilidade das evidências apresentadas.

Para que essas inovações sejam plenamente eficazes e juridicamente válidas, conforme discutido no tópico acima, é essencial que o uso da IA na coleta de provas respeite

---

[29] ROCHA, Anderson; SCHEIRER, Walter; BOULT, Terrance; GOLDENSTEIN, Siome. Vision of the unseen: current trends and challenges in digital image and video forensics. *ACM Computing Surveys*, v. 43, n. 4, p. 1-42, 2011, p. 1-42.
[30] CASEY, Eoghan. *Digital evidence and computer crime*, p. 467.
[31] CASEY, Eoghan. *Digital evidence and computer crime*, p. 467.
[32] MARSHALL, Angus McKenzie. *Digital forensics: digital evidence in criminal investigations*. Hoboken: John Wiley & Sons, 2009, p. 105.

rigorosamente os procedimentos relativos à cadeia de custódia. Essa observância é fundamental para garantir a integridade, legitimidade e autenticidade de qualquer evidência digital coletada. A cadeia de custódia, como bem sabemos, é um mecanismo necessário para assegurar que as provas digitais sejam preservadas de maneira inalterada, de modo que, ao longo de todo o processo, possam ser rastreadas e verificadas.

Assim, embora a IA traga enormes benefícios para a coleta e validação de provas, também há desafios éticos e riscos importantes. A confiabilidade e a transparência dos algoritmos de IA, bem como a necessidade de profissionais tecnicamente qualificados, são fatores de extrema importância. A proteção da integridade, autenticidade e licitude das provas é a espinha dorsal de qualquer processo justo, e a IA, se bem implementada, pode ser uma poderosa aliada nesse objetivo.

3. IMPLICAÇÕES E DESAFIOS DA INTEGRAÇÃO DA IA NA OBTENÇÃO E VALIDAÇÃO DE PROVAS DIGITAIS

Paralelamente aos avanços, emergem inquietações relevantes acerca dos efeitos sociais e éticos da Inteligência Artificial. Em resposta a isso, a legislação europeia[33] ressalta a importância de criar e implementar sistemas de IA em harmonia com os princípios essenciais e os direitos humanos estabelecidos nos acordos e na Declaração de Direitos Fundamentais da União Europeia. Essa questão traz à tona a necessidade de se ponderar sobre a experiência da UE, considerando que o cenário global compartilha desafios cruciais relacionados à necessidade de normatizar o emprego da IA e o interesse em estabelecer fronteiras legais para as permissões e restrições.

Essa recente e significativa normatização sobre a IA, bem como as diretrizes jurídicas que circunscrevem sua utilização legítima na União Europeia, reforça a necessidade de prevenir aplicações nocivas ou discriminatórias. Além disso, é crucial refletir sobre o impacto dessa regulamentação no sistema judiciário. Um exemplo relevante é o artigo 5º do Regulamento, que aborda as práticas de IA proibidas ("Prohibited AI practices"), destacando os limites impostos para garantir a segurança, a ética e a equidade na utilização da tecnologia.

[33] UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024. Disponível em: https://eur-lex.europa.eu/. Acesso em: 12 out. 2024.

A expansão do uso da Inteligência Artificial (IA) no sistema judiciário apresenta o desafio da opacidade algorítmica, que se refere à dificuldade de compreender completamente como os algoritmos tomam decisões. Isso é particularmente problemático no contexto judicial, onde a transparência e a fundamentação lógica são cruciais para a validade das decisões. Isso porque a opacidade algorítmica pode obscurecer os critérios de tomada de decisão, complicando a conciliação do uso de IA com princípios fundamentais como o devido processo legal.

No Brasil, o Supremo Tribunal Federal (STF) já utiliza IA para agrupar processos por temas e verificar se recursos abordam questões já consolidadas em temas de repercussão geral. Futuramente, planeja-se aprofundar o uso de IA na identificação e respeito aos precedentes vinculantes, além de desenvolver sistemas para resumir processos, sempre sob supervisão de um magistrado. A questão central levantada é a preocupação com a falta de clareza nos processos algorítmicos da Inteligência Artificial (IA) ao condensar um caso jurídico em um resumo de cinco páginas para um ministro do Supremo Tribunal. É crucial reconhecer que este compêndio gerado pela IA provavelmente terá um impacto significativo na compreensão do caso pelo juiz e, consequentemente, na formação de sua decisão ao elaborar a sentença.

Considerando que este resumo se torna parte integrante dos procedimentos judiciais, ele deve estar em conformidade com os princípios do devido processo legal. Isso implica na necessidade de transparência quanto aos métodos utilizados pelo magistrado para chegar às suas conclusões sobre os pontos controversos e relevantes para a discussão jurídica em questão. A opacidade do funcionamento da IA na produção destes resumos levanta questões sobre como garantir que o processo decisório judicial permaneça justo, transparente e em conformidade com os princípios legais estabelecidos, especialmente quando uma ferramenta tecnológica assume um papel tão crucial na apresentação das informações aos juízes.

Ademais, a regulamentação da União Europeia aponta outro desafio crucial: o risco de uma excessiva padronização nas decisões judiciais. Em casos criminais, por exemplo, a determinação da sentença ideal deve considerar não apenas a natureza do delito, mas também o histórico do acusado, as possibilidades de reabilitação e outros fatores humanos que um algoritmo pode não captar adequadamente. Além disso, existe o perigo de que, devido ao viés presente nos dados utilizados para treinar a IA, ocorra um reforço dos estigmas sociais contra grupos vulneráveis já marginalizados pelo direito. Nesse cenário, a IA pode intensificar violências simbólicas ao perpetuar estereótipos e preconceitos existentes na sociedade.

Outro ponto é que o Regulamento nº 2024/1689 do Parlamento Europeu evidencia que o uso não regulamentado de sistemas de IA no âmbito judicial pode aumentar o risco de violações dos direitos fundamentais e de discriminação. Sistemas de IA, se não forem

meticulosamente concebidos e supervisionados, têm o potencial de reproduzir e até mesmo amplificar preconceitos já existentes na sociedade.

É importante verificar que as novas normativas quanto à IA devem observar a ética digital. Nesse ínterim, Luciano Floridi[34] esclarece que a ética digital é uma vertente especializada da ética que se dedica ao estudo e avaliação de questões morais no contexto digital, abrangendo três áreas principais: a gestão de dados e informações (desde sua geração até seu uso final), as tecnologias algorítmicas (como IA, sistemas autônomos, aprendizado de máquina e robótica), e as práticas e infraestruturas tecnológicas (incluindo inovação responsável, desenvolvimento de *software*, *hacking*, códigos de ética profissional e padrões técnicos). Explica, também, que seu objetivo central é desenvolver e promover soluções moralmente íntegras para os desafios éticos emergentes no ambiente digital, definindo condutas apropriadas e fomentando valores éticos no contexto tecnológico. Salienta, ademais, que a ética digital desempenha um papel crucial na formação de políticas e regulamentações digitais, servindo como base para avaliar o que é socialmente aceitável ou desejável no domínio digital. Isso orienta a criação de leis, regulamentos e estruturas de governança para o ecossistema tecnológico, buscando um equilíbrio entre inovação e responsabilidade social. Em suma, a ética digital atua como um guia moral essencial para navegar pelos complexos desafios éticos que surgem com o avanço da tecnologia, moldando a forma como a sociedade interage com e regula o mundo digital, e promovendo uma abordagem ética e responsável no desenvolvimento e uso de tecnologias digitais.

Luciano Floridi, ainda, faz um alerta sobre a ética digital:

> Porque no mesmo contexto em que as pessoas reclamam sobre a velocidade da inovação digital e a tarefa impossível de persegui-la com algum marco normativo, também se encontra igual certeza sobre a seriedade do risco representado pela legislação equivocada. Uma legislação ruim poderia matar completamente a inovação digital ou destruir setores e desenvolvimentos tecnológicos inteiros."[35]

Nesse contexto, a utilização de provas digitais demanda que elas atendam, no mínimo, a dois princípios fundamentais: a autenticidade, que assegura que os fatos apresentados

---

[34] FLORIDI, Luciano. *The ethics of artificial intelligence: principles, challenges, and opportunities*. Oxford: Oxford University Press, 2023, p. 81.
[35] FLORIDI, Luciano. *The ethics of artificial intelligence*, p. 78.

correspondem à realidade do evento jurídico ocorrido e foram gerados pelos seus respectivos autores; e a integridade, que garante que a evidência permaneceu inalterada desde sua coleta.[36]

Assim, a utilização da inteligência artificial na coleta e validação de provas digitais levanta questões preocupantes em relação à autenticidade e integridade das evidências. À medida que essas tecnologias se tornam mais integradas aos processos investigativos, é fundamental abordar as complexidades e os desafios que surgem.

A IA, ao automatizar a coleta de dados de diversas fontes, pode gerar informações que não necessariamente correspondem à realidade dos fatos. A manipulação de algoritmos, seja intencional ou acidental, pode comprometer a autenticidade das provas coletadas. Por exemplo, uma falha em um sistema de IA pode levar à inclusão de dados falsos ou à exclusão de informações relevantes, tornando a evidência apresentada uma representação distorcida da realidade.

A integridade das provas digitais é crítica, pois qualquer alteração nos dados pode prejudicar a confiança que o juiz ou as partes têm nas evidências apresentadas. Os sistemas de IA precisam de controles rigorosos para garantir que as evidências não sejam adulteradas durante o processo de coleta e análise. Isso implica a implementação de métodos de rastreabilidade, onde cada passo no manuseio dos dados é documentado e auditável.

Nesse diapasão, surge outro desafio, que é a questão da responsabilidade. Conforme explica Ugo Pagallo[37], é um desafio significativo determinar quem é responsável por erros ou injustiças decorrentes da utilização de IA na validação de provas.

A responsabilidade pode recair sobre os desenvolvedores, os operadores ou os usuários finais dos sistemas de IA. Dessa forma, é necessário considerar o impacto dessas tecnologias nos direitos fundamentais do acusado, como o direito à privacidade, à proteção de dados pessoais, à ampla defesa e ao contraditório. Além disso, é preciso estabelecer responsabilidades civis e penais pelo uso indevido da IA na obtenção e validação de provas digitais, bem como regulamentar de forma específica a utilização dessas tecnologias no âmbito do Direito Penal.

---

[36] LUCIEN, Rocha. *Acreditação e admissibilidade de evidências digitais*, p. 41.

[37] PAGALLO, Ugo. *The laws of robots: crimes, contracts, and torts*. Torino: Springer, 2013, p. 16.

Lucien[38] destaca que, em razão dos atributos necessários às provas digitais (autenticidade e integridade):

> ratifica-se a importância da presença de especialistas que detenham densos conhecimentos nas áreas de Direito Digital e perícia forense digital em casos dessa natureza, com vistas a evitar a contaminação ou a anulação da prova coletada

Nessa ótica, é fundamental que os profissionais envolvidos na validação de provas digitais tenham conhecimentos técnicos e jurídicos adequados para utilizar e interpretar corretamente as ferramentas de IA. Isso inclui compreensão dos algoritmos utilizados, bem como das possíveis falhas e limitações associadas a esses sistemas.

Eoghan Casey[39] acredita que investir em educação e treinamento para juízes, advogados e outros profissionais do Direito é essencial para garantir que eles compreendam as implicações da utilização de IA e possam tomar decisões informadas.

Tem-se, ainda, a problemática apontada por.[40] Para eles, a falta de transparência nos algoritmos de IA podem dificultar a compreensão e a contestação das decisões automatizadas, comprometendo a justiça e a equidade do sistema judicial. Assim, a necessidade de se garantir que a utilização de IA no Direito Penal seja justa e equitativa é um desafio ético significativo.

Veja-se, ademais, que os algoritmos de IA podem perpetuar ou amplificar vieses existentes nos dados de treinamento, levando a decisões injustas. Dessa forma, é essencial que os desenvolvedores de IA implementem medidas para identificar e mitigar esses vieses, como colocam Jeff Larson, Mattu Surya, Lauren Kirchner e Julia Angwin.[41]

Diante de todos esses aspectos, para que a IA seja utilizada de forma responsável na coleta e validação de provas digitais, é imprescindível que haja uma regulamentação clara. É necessário desenvolver *frameworks* legais e éticos que orientem o desenvolvimento, a implementação e o uso dessas tecnologias, garantindo o respeito aos direitos fundamentais e a

---

[38] LUCIEN, Rocha. *Acreditação e admissibilidade de evidências digitais*, p. 41.
[39] CASEY, Eoghan. *Digital evidence and computer crime*, p. 685.
[40] SELBST, Andrew David; BAROCAS, Solon. The intuitive appeal of explainable machines. *Fordham Law Review*, v. 87, n. 3, 2018, p. 5.
[41] LARSON, Jeff; MATTU, Surya; KIRCHNER, Lauren; ANGWIN, Julia. How we analyzed the COMPAS recidivism algorithm. ProPublica, 23 maio 2016, p. 3. Disponível em: https://www.propublica.org/. Acesso em: 29 set. 2024.

promoção da justiça. Iniciativas como a proposta de regulamentação da IA na União Europeia[42] e a Resolução nº 332/2020 do Conselho Nacional de Justiça no Brasil[43] são passos importantes nessa direção, mas ainda há muito trabalho a ser feito.

A ausência de regulamentação adequada, pode impedir a utilização eficaz da inteligência artificial na coleta e validação de provas digitais. A validade dessas evidências requer a observância de procedimentos rigorosos, que se iniciam com a coleta de dados em um ambiente forense controlado. Cada fase do processo, desde a coleta até a análise e o armazenamento, deve ser meticulosamente documentada. A manutenção de registros detalhados que indiquem quem acessou as evidências, em que momento e por qual motivo, é fundamental para assegurar que não ocorra contaminação ou adulteração dos dados. Essa documentação é vital para a integridade do processo, garantindo que as provas digitais sejam consideradas confiáveis e admissíveis em juízo:

> No âmbito digital, a simples coleta de evidências sem utilização de técnica adequada pode eliminar todas as chances do litígio judicial, devido à contaminação do local do crime. Da mesma forma, ocorre com a coleta sem o emprego de manutenção e de registro histórico cronológico das evidências (cadeia de custódia), haja vista a possibilidade de a parte contrária argumentar sobre as evidências terem sofrido adulterações durante seu manuseio.[44]

Em suma, embora a inteligência artificial tenha o potencial de revolucionar a forma como as provas digitais são coletadas e validadas, sua aplicação requer um esforço contínuo de pesquisa, regulamentação, capacitação e colaboração interdisciplinar. Somente assim será possível construir um sistema de justiça criminal mais eficiente, justo e adaptado às demandas do século XXI.

CONCLUSÃO

A intersecção entre o Direito Penal e a Inteligência Artificial no contexto da Sociedade da Informação apresenta um cenário promissor, mas também repleto de desafios. A utilização

---

[42] COMISSÃO EUROPEIA. Proposal for a regulation on artificial intelligence (Artificial Intelligence Act). Bruxelas: European Commission, 2021, p. 1-108. Disponível em: https://eur-lex.europa.eu/. Acesso em: 29 set. 2024.

[43] 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. Disponível em: https://atos.cnj.jus.br/. Acesso em: 29 set. 2024, p. 1-11.

[44] LUCIEN, Rocha. *Acreditação e admissibilidade de evidências digitais*, p. 41.

de IA para a obtenção e validação de provas digitais tem o potencial de revolucionar o sistema de justiça criminal, oferecendo maior eficiência, precisão e celeridade nos processos investigativos e decisórios. A automação na coleta de grandes volumes de dados, a análise de padrões complexos e a verificação de autenticidade de documentos e arquivos são exemplos concretos de como a tecnologia pode auxiliar na busca pela verdade.

Contudo, à medida que a IA se torna uma ferramenta indispensável, surgem questões éticas e legais que não podem ser ignoradas. O viés algorítmico, a falta de transparência, a confiabilidade dos algoritmos e a rastreabilidade das evidências são fatores que precisam ser rigorosamente regulados. A conformidade com princípios essenciais, como autenticidade e integridade das provas, bem como o cumprimento de normas regulamentadoras, são cruciais para garantir que as evidências digitais sejam admissíveis em juízo e que os direitos fundamentais dos envolvidos sejam respeitados.

Portanto, enquanto o futuro aponta para uma crescente adoção da IA no campo jurídico, é imperativo que a regulamentação e a capacitação dos profissionais do Direito acompanhem essa evolução. Somente assim será possível assegurar que os benefícios da tecnologia sejam plenamente aproveitados, sem comprometer a integridade do processo penal e a proteção dos direitos individuais.

REFERÊNCIAS

ALAGOAS (Estado). Programa de inteligência artificial da SSP estima reduzir criminalidade em até 26%. 2024. Disponível em: https://alagoas.al.gov.br/. Acesso em: 25 set. 2024.

BRASIL. Superior Tribunal de Justiça. AgRg no HC 828054/RN. Rel. Min. Joel Ilan Paciornik, Quinta Turma, julgado em 23 abr. 2024. Disponível em: https://processo.stj.jus.br/. Acesso em: 12 out. 2024.

CANAL CIÊNCIAS CRIMINAIS. Descubra como a inteligência artificial pode auxiliar no combate ao crime no Brasil. 2023. Disponível em: https://www.mpmt.mp.br/. Acesso em: 25 set. 2024.

CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers, and the internet*. 3. ed. Baltimore: Academic Press, 2011.

CASTELLS, Manuel. *A sociedade em rede: a era da informação: economia, sociedade e cultura*. v. 1. 6. ed. São Paulo: Paz e Terra, 1999.

COLE, Simon Andrew. *Suspect identities: a history of fingerprinting and criminal identification*. Cambridge: Harvard University Press, 2001.

COMISSÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho. Disponível em: https://digital-strategy.ec.europa.eu/. Acesso em: 12 out. 2024.

COMISSÃO EUROPEIA. Proposal for a regulation on artificial intelligence (Artificial Intelligence Act). Bruxelas: European Commission, 2021. Disponível em: https://eur-lex.europa.eu/. Acesso em: 29 set. 2024.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). Resolução nº 332, de 21 de agosto de 2020. Disponível em: https://atos.cnj.jus.br/. Acesso em: 29 set. 2024.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO (CNMP). *Levantamento de iniciativas de IA no Ministério Público*. 2023. Disponível em: https://www.cnmp.mp.br/. Acesso em: 25 set. 2024.

DOMINGOS, Pedro. *The master algorithm: how the quest for the ultimate learning machine will remake our world*. New York: Basic Books, 2015.

FERNANDES, André Luis; MONTES, Rodrigo Henrique de Oliveira. Meta-evidência digital: a dualidade na cadeia de custódia envolvendo dispositivos eletrônicos e evidências digitais. *Revista Eletrônica Direito & TI*, Porto Alegre, v. 1, n. 14, dez. 2022.

FERRARA, Emilio et al. The rise of social bots. *Communications of the ACM*, v. 59, n. 7, p. 96-104, jul. 2016. Disponível em: https://cacm.acm.org/. Acesso em: 29 set. 2024.

FLORIDI, Luciano. *The ethics of artificial intelligence: principles, challenges, and opportunities*. Oxford: Oxford University Press, 2023.

FUJITA, Jorge Shiguemitsu; BARRETO JUNIOR, Irineu Francisco. O direito ao esquecimento e a liberdade de informar na sociedade da informação. *Revista de Direitos Fundamentais e Democracia*, v. 25, n. 2, p. 5-27, maio/ago. 2020.

FULLER, Greice Patrícia. Os delitos e as novas tecnologias em face da relação dialógica com os direitos humanos. In: SARLET, Ingo Wolfgang; WALDMAN, Ricardo Libel (org.). *Direitos humanos e fundamentais na era da informação*. Porto Alegre: Fundação Fênix, 2020.

HARARI, Yuval Noah. *21 lessons for the 21st century*. London: Penguin Random House, 2018.

JURAFSKY, Daniel; MARTIN, James Howard. *Speech and language processing*. 3. ed. Stanford: Stanford University, 2024. Disponível em: https://web.stanford.edu/. Acesso em: 29 set. 2024.

LARSON, Jeff et al. How we analyzed the COMPAS recidivism algorithm. *ProPublica*, 23 maio 2016. Disponível em: https://www.propublica.org/. Acesso em: 29 set. 2024.

LOPES JR., Aury. *Direito processual penal*. 20. ed. Rio de Janeiro: Saraiva, 2023. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/. Acesso em: 12 out. 2024.

LUCIEN, Rocha. *Acreditação e admissibilidade de evidências digitais de crimes cibernéticos praticados em computação de nuvem*. 2023. Dissertação (Mestrado em Direito) — Universidade de Brasília, Brasília, 2023.

LYNCH, Michael et al. *Truth machine: the contentious history of DNA fingerprinting*. Chicago: University of Chicago Press, 2008.

MARSHALL, Angus McKenzie. *Digital forensics: digital evidence in criminal investigations*. Hoboken: John Wiley & Sons, 2009.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big data: a revolution that will transform how we live, work, and think*. New York: Houghton Mifflin Harcourt, 2013.

NASSIF, Lilian Noronha. Desafios da coleta de dados e evidências digitais. *O Alferes*, Belo Horizonte, v. 29, n. 74, p. 89-107, jan./jun. 2019.

NGAI, Eric Wai Ting et al. The application of data mining techniques in financial fraud detection. *Decision Support Systems*, v. 50, n. 3, p. 559-569, fev. 2011. Disponível em: https://www.sciencedirect.com/. Acesso em: 29 set. 2024.

PAGALLO, Ugo. *The laws of robots: crimes, contracts, and torts*. Torino: Springer, 2013.

ROCHA, Anderson et al. Vision of the unseen: current trends and challenges in digital image and video forensics. *ACM Computing Surveys*, v. 43, n. 4, p. 1-42, 2011. Disponível em: https://dl.acm.org/. Acesso em: 29 set. 2024.

ROSA, Alexandre Morais da. Limite penal: o "print screen" é insuficiente à materialidade nos crimes digitais. *Consultor Jurídico*, 17 jun. 2022. Disponível em: https://www.conjur.com.br/. Acesso em: 12 out. 2024.

RUSSELL, Stuart; NORVIG, Peter. *Inteligência artificial: uma abordagem moderna*. 4. ed. São Paulo: LTC, 2022.

SANTO DIGITAL. Reconhecimento facial: como funciona e benefícios para prevenção a fraudes. 2024. Disponível em: https://santodigital.com.br/.

SELBST, Andrew D.; BAROCAS, Solon. The intuitive appeal of explainable machines. *Fordham Law Review*, v. 87, n. 3, 2018. Disponível em: https://ir.lawnet.fordham.edu/. Acesso em: 29 set. 2024.

SIMÃO, A. M. L. et al. Aquisição de evidências digitais em smartphones Android. 2011. DOI: http://dx.doi.org/10.5769/C2011009.

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024. Disponível em: https://eur-lex.europa.eu/. Acesso em: 12 out. 2024.

UNIVERSITY OF WOLVERHAMPTON. What are the different types of artificial intelligence? 2023. Disponível em: https://online.wlv.ac.uk/. Acesso em: 11 out. 2024.