DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

Uso de Machine Learning na perícia digital: proposta para classificação de evidências

Use of Machine Learning in digital forensics: a proposal for evidence classification

Emanoel Guilherme Barros[1]
Sidney Marlon Lopes de Lima[2]

Recebido em: 07.05.2025
Aprovado em: 18.02.2026

RESUMO

A crescente complexidade dos crimes digitais e o aumento expressivo do volume de dados analisados em investigações cibernéticas impõem desafios significativos às práticas tradicionais da perícia forense digital. Nesse contexto, o presente artigo propõe a integração de técnicas de Machine Learning como recurso complementar para a triagem e classificação automatizada de arquivos recuperados durante o processo pericial. A pesquisa apresenta um modelo conceitual baseado em algoritmos supervisionados — como Random Forest, Support Vector Machines e K-Nearest Neighbors — aplicado a dados extraídos por ferramentas forenses amplamente utilizadas. O estudo descreve a metodologia de construção do dataset, os critérios de avaliação e os requisitos técnicos, legais e éticos para adoção prática da abordagem no contexto brasileiro. Como contribuição principal, o trabalho sistematiza diretrizes para uso confiável de inteligência artificial na perícia digital, indicando ganhos potenciais de eficiência, padronização e apoio à tomada de decisão pericial, sem substituir a supervisão humana. Trata-se, portanto, de uma proposta metodológica com implicações científicas e operacionais para a modernização das investigações digitais.

Palavras-chave: Perícia Forense Digital; Machine Learning; Classificação de Arquivos; Evidências Digitais; Cibersegurança

ABSTRACT

The growing complexity of cybercrime and the exponential increase in digital evidence volume challenge traditional digital forensic practices. This article proposes the

[1] Professor Universitário e Especialista em Segurança da Informação, Banco de dados e Governança em TI. E-mail: e.guilherme.barros@outlook.com. Lattes: http://lattes.cnpq.br/2269582298506976.

[2] Doutor em Ciência da Computação pela UFPE (Universidade Federal de Pernambuco) e Pós-doutor em Engenharia da Computação pela UPE (Universidade de Pernambuco), alcançou o 1 lugar no concurso público para Professor Adjunto do Departamento de Eletrônica e Sistemas da UFPE em 2018. Atualmente, é autor e revisor na Science Elsevier, além de orientar pesquisas de mestrado e de doutorado em Engenharia da Computação na UPE. E-mail: sidney.lima@ufpe.br. Lattes: http://lattes.cnpq.br/0323190806293435. Orcid: https://orcid.org/0000-0002-4350-9689.

integration of Machine Learning techniques as a complementary resource for automated triage and classification of files recovered during forensic investigations. The study presents a conceptual model based on supervised algorithms — including Random Forest, Support Vector Machines, and K-Nearest Neighbors — applied to datasets extracted through widely used forensic tools. It details dataset construction procedures, evaluation criteria, and the technical, legal, and ethical requirements for practical adoption within the Brazilian forensic context. As its main contribution, the work systematizes guidelines for the trustworthy use of artificial intelligence in digital forensics, indicating potential gains in efficiency, standardization, and decision-support without replacing human supervision. Therefore, this study constitutes a methodological proposal with scientific and operational implications for the modernization of digital investigations.

Keywords: Digital Forensics; Machine Learning; File Classification; Digital Evidence; Cybersecurity.

1 INTRODUÇÃO

A perícia forense digital tornou-se um dos pilares fundamentais na investigação de crimes cibernéticos, auxiliando na coleta, análise e preservação de evidências eletrônicas essenciais para processos judiciais. Com a digitalização crescente das atividades humanas e a sofisticação dos ataques cibernéticos, os peritos enfrentam cenários cada vez mais complexos e um volume de dados exponencialmente maior a ser processado. De acordo com Casey (2011), o tempo e a precisão na análise de dados digitais são elementos críticos para garantir a integridade das provas e a efetividade do processo investigativo. No entanto, o método tradicional de triagem manual de arquivos recuperados consome recursos significativos e está sujeito a limitações humanas, como fadiga e viés cognitivo.

Nesse cenário, a aplicação de técnicas de Machine Learning (ML) surge como uma alternativa promissora para ampliar a eficiência das perícias. Segundo Russom (2011), o uso de algoritmos inteligentes pode automatizar tarefas repetitivas e detectar padrões ocultos nos dados, facilitando a identificação de informações relevantes de forma mais ágil e precisa. Estudos recentes como os de Baggili *et al.* (2019) e Garfinkel (2020) demonstram que a integração entre ferramentas forenses e modelos de ML tem o potencial de transformar o modo como as evidências são analisadas, introduzindo uma camada

adicional de inteligência nos processos investigativos.

Neste artigo, propõe-se um modelo conceitual baseado em algoritmos de classificação supervisionada, com o objetivo de categorizar arquivos recuperados em diferentes tipos e contextos investigativos, como documentos suspeitos, arquivos irrelevantes e scripts potencialmente maliciosos. A abordagem fundamenta-se em dados passíveis de obtenção por ferramentas consolidadas da área - como IPED, Autopsy e Bulk Extractor - permitindo análise comparativa teórica entre algoritmos quanto à sua precisão, recall e aplicabilidade em cenários forenses. Considerações legais e éticas também são incorporadas ao modelo, uma vez que a adoção de sistemas automatizados em perícias deve observar princípios de imparcialidade, transparência e conformidade jurídico-processual.

Acredita-se que este estudo possa contribuir significativamente para a consolidação do uso de inteligência artificial no âmbito da perícia forense digital, oferecendo subsídios técnicos e científicos para sua adoção em instituições públicas e privadas no Brasil. Ao final, espera-se demonstrar que a união entre conhecimento pericial e recursos computacionais avançados é não apenas viável, mas necessária diante da nova realidade digital.

Embora ferramentas forenses contemporâneas já incorporem técnicas de aprendizado de máquina para tarefas específicas de classificação e priorização de evidências, como ocorre em plataformas amplamente utilizadas no contexto brasileiro, a presente pesquisa diferencia-se ao propor uma sistematização metodológica integrada que articula critérios técnicos de validação, requisitos jurídico-processuais e diretrizes ético-operacionais para uso confiável da inteligência artificial na perícia digital. Assim, a contribuição do estudo não reside apenas na aplicação isolada de algoritmos, mas na estruturação de um modelo conceitual reprodutível e alinhado às exigências científicas e legais do ambiente pericial.

O artigo está organizado da seguinte forma: a Seção 2 apresenta os objetivos da pesquisa; a Seção 3 descreve a metodologia proposta para construção e avaliação do modelo conceitual; a Seção 4 discute os resultados esperados e suas implicações operacionais; a Seção 5 aborda os aspectos técnicos, éticos e legais envolvidos na adoção

de inteligência artificial na perícia digital; a Seção 6 apresenta possibilidades de aplicações futuras; e, por fim, a Seção 7 reúne as considerações finais do estudo.

2 TRABALHOS RELACIONADOS

Pesquisas recentes têm demonstrado o crescimento do uso de técnicas de aprendizado de máquina na perícia forense digital, especialmente na automação da triagem de evidências, classificação de artefatos e identificação de padrões comportamentais em grandes volumes de dados.

Revisões sistemáticas indicam que abordagens baseadas em aprendizado profundo e modelos híbridos vêm alcançando resultados promissores em precisão e eficiência investigativa, contribuindo para a redução do tempo de análise pericial e aumento da confiabilidade dos achados forenses (Nayerifard *et al.*, 2023; Marturana; Tacconi; Me, 2023).

Além dos ganhos de desempenho, estudos recentes também destacam desafios importantes relacionados à interpretabilidade dos modelos, reprodutibilidade experimental e validação jurídica das evidências produzidas por sistemas inteligentes.

A adoção de técnicas de Explainable Artificial Intelligence (XAI) tem sido apontada como elemento fundamental para garantir transparência, auditabilidade e aceitabilidade legal em investigações digitais assistidas por IA (Hassan; Khan, 2022; Singh; Singh, 2023).

Mais recentemente, pesquisas internacionais têm enfatizado a integração entre aprendizado de máquina, automação forense e análise preditiva como tendência consolidada na modernização das investigações criminais digitais.

Esses estudos apontam que o uso de IA pode ampliar significativamente a capacidade de processamento de evidências, apoiar decisões periciais e melhorar a eficiência de sistemas de justiça digital, desde que respeitados requisitos éticos, legais e metodológicos rigorosos (Alenezi *et al.*, 2024; Kumar; Yadav, 2024).

3 OBJETIVOS

Este trabalho tem como objetivo central propor uma abordagem metodológica baseada em técnicas de Machine Learning aplicadas à Perícia Forense Digital, com foco na classificação automática de arquivos recuperados em ambientes investigativos.

A proposta busca articular eficiência computacional, confiabilidade forense e conformidade jurídico-processual, contribuindo para a otimização teórica do processo de triagem de evidências digitais.

3.1 OBJETIVO GERAL

Desenvolver um modelo de classificação supervisionada capaz de categorizar evidências digitais de forma automática e precisa, contribuindo para a redução do tempo de análise e para o aumento da acurácia na identificação de artefatos relevantes em investigações digitais.

3.2 OBJETIVOS ESPECÍFICOS

- Projetar e treinar modelos de machine learning supervisionados — como Random Forest, SVM (*Support Vector Machines*) e KNN (*K-Nearest Neighbors*) — capazes de identificar e classificar diferentes tipos de arquivos digitais (documentos, imagens, scripts, executáveis) com base em suas características extraídas de forma automática.
- Construir um dataset forense realista e balanceado, contendo amostras representativas de arquivos frequentemente encontrados em perícias digitais, utilizando ferramentas de extração consolidadas como IPED, Autopsy e Bulk Extractor.
- Avaliar o desempenho dos modelos utilizando métricas de classificação, como acurácia, precisão, recall e F1-score, em conformidade com a literatura técnica

(Chen *et al.*, 2021; Baggili *et al.*, 2019), e identificar o algoritmo mais eficaz no contexto proposto.

- Investigar a viabilidade prática da integração entre modelos de IA e ferramentas forenses já utilizadas por peritos, considerando aspectos técnicos, operacionais e de interoperabilidade, além da compatibilidade com fluxos tradicionais de análise forense.
- Discutir as implicações éticas, legais e operacionais da adoção de inteligência artificial no processo Pericial, com ênfase na conformidade com a Lei Geral de Proteção de Dados (Brasil, 2018) e com princípios de imparcialidade, transparência e explicabilidade algorítmica (ITU-T, 2020).

Ao atingir esses objetivos, este estudo pretende contribuir para a construção de um modelo de perícia digital mais ágil, confiável e tecnicamente preparado para lidar com o crescente volume e complexidade das evidências em ambientes cibernéticos contemporâneos.

4 METODOLOGIA[3]

Pesquisas recentes demonstram que técnicas avançadas de aprendizado de máquina, especialmente abordagens baseadas em transferência de aprendizado aplicadas à análise eletromagnética de dispositivos digitais, podem alcançar elevados níveis de acurácia na extração de informações com finalidade forense, atingindo valores próximos de 98% em ambientes experimentais controlados.

Esses achados evidenciam o potencial do emprego de modelos inteligentes para ampliar a eficiência, a precisão e a confiabilidade dos processos de investigação digital.

[3] Em atendimento à Portaria CNPq nº 2.664, de 6 de março de 2026, foram utilizadas ferramentas de Inteligência Artificial Generativa, especificamente ChatGPT (OpenAI) e Gemini (Google), exclusivamente como instrumentos de apoio à organização das ideias, estruturação do texto, revisão gramatical, aprimoramento da redação e adequação da linguagem acadêmica do manuscrito. As referidas ferramentas não foram utilizadas para a elaboração da pesquisa científica, definição da metodologia, coleta ou análise de dados, interpretação dos resultados, formulação das conclusões ou tomada de decisões científicas. Todo o conteúdo intelectual, as análises, os argumentos jurídicos e técnicos, bem como a versão final do manuscrito, foram desenvolvidos, revisados e validados pelo autor, que assume integral responsabilidade pela originalidade, exatidão e integridade do trabalho submetido.

Essa estrutura metodológica está alinhada a evidências recentes da literatura internacional, que demonstram ganhos significativos de precisão e eficiência investigativa com a aplicação de modelos de aprendizado profundo e técnicas automatizadas de análise forense digital (Marturana; Tacconi; Me, 2023; Nayerifard *et al.*, 2023).

Diante desse contexto, a metodologia proposta neste estudo foi estruturada em quatro etapas principais, alinhadas às boas práticas da ciência de dados e às diretrizes consolidadas da perícia forense digital. O objetivo central consiste em estabelecer um modelo metodológico reprodutível para futuras implementações experimentais, assegurando consistência científica, rastreabilidade dos procedimentos e rigor na análise dos resultados.

Cada etapa foi delineada com base em referenciais reconhecidos na literatura especializada (Baggili *et al.,* 2019; Chen *et al*., 2021), contemplando desde a definição do cenário de coleta potencial de dados forenses, passando pelo pré-processamento e aplicação de algoritmos de Machine Learning voltados à classificação de evidências digitais, até a adoção de métricas de avaliação apropriadas para validação do desempenho dos modelos propostos.

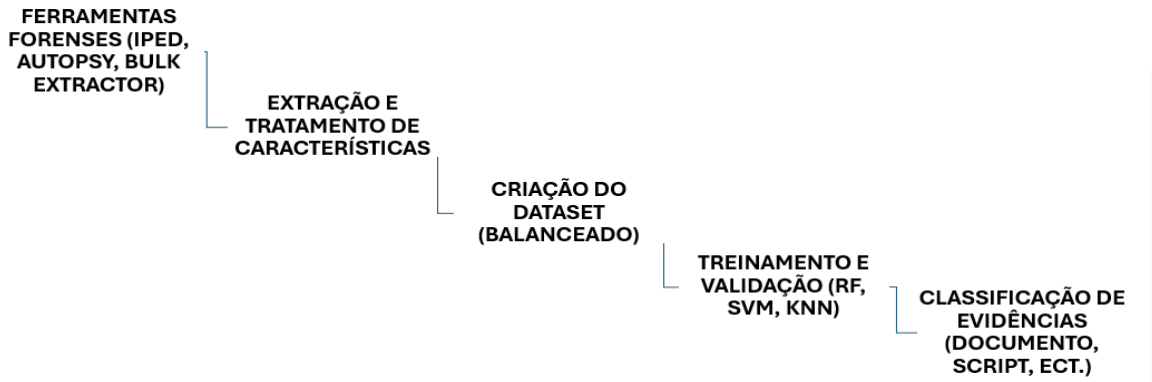
4.1 Coleta de dados forenses

A coleta de dados forenses será realizada por meio da utilização das ferramentas IPED (*Investigative Platform for Evidence Discovery*) e Autopsy, amplamente utilizadas por instituições de perícia no Brasil e internacionalmente.

O IPED é um software desenvolvido pelo Ministério Público Federal brasileiro, com suporte nativo à análise de grandes volumes de evidências extraídas de discos rígidos, dispositivos móveis e imagens forenses (IPED, 2023). Já o Autopsy, de código aberto, oferece funcionalidades complementares para recuperação de arquivos deletados, análise de metadados, histórico de navegação, e rastreamento de arquivos ocultos (AUTOPSY, 2023).

As evidências digitais coletadas incluirão uma variedade de artefatos como arquivos de texto, scripts, documentos de escritório, imagens, executáveis e logs de sistema. Esta diversidade visa simular um ambiente realista de uma investigação digital, garantindo a representatividade dos dados.

Figura 1 – Fluxo geral da metodologia proposta para classificação de evidências digitais.



Fonte: Produzido pelos autores (2025).

4.2 Extração e tratamento dos dados

Após a coleta, será realizado o pré-processamento das evidências, etapa essencial para garantir a qualidade do dataset a ser utilizado. Serão adotadas técnicas de normalização de formatos (ex.: conversão de textos para codificação UTF-8), extração de características discriminantes (como metadados de criação, autor, data de modificação, extensões, hashes MD5/SHA256 e conteúdo textual bruto), além da remoção de redundâncias.

A criação do dataset balanceado será baseada em critérios definidos previamente, garantindo a distribuição proporcional entre diferentes classes de arquivos. O equilíbrio entre as classes é importante para evitar vieses no aprendizado supervisionado dos

algoritmos (Russom, 2011). Serão incluídos exemplos reais e simulados, com base em cenários forenses, respeitando princípios éticos e de anonimização de dados sensíveis.

4.3 Treinamento e validação de modelos de Machine Learning

Com o dataset estruturado, será realizada a implementação dos algoritmos *Random Forest*, *Support Vector Machines* (SVM) e *K-Nearest Neighbors* (KNN), escolhidos por sua eficácia comprovada em problemas de classificação de dados com múltiplas categorias (Chen *et al.*, 2021). Esses algoritmos apresentam vantagens distintas:

- **Random Forest**: robusto a ruídos e eficiente em bases heterogêneas.
- **SVM**: indicado para conjuntos de dados com margens de separação claras.
- **KNN**: simples e eficaz em cenários com instâncias similares e bem distribuídas.

Os dados serão divididos em conjuntos de treino (70%) e teste (30%), utilizando a técnica de validação cruzada k-fold (k=5), que permite maior generalização dos resultados e reduz o risco de *overfitting*. As implementações seguirão os padrões da biblioteca *scikit-learn*, amplamente reconhecida na comunidade de aprendizado de máquina.

4.4 Análise dos resultados

A análise dos modelos será baseada em métricas clássicas de avaliação para tarefas de classificação: acurácia, precisão, recall e F1-score, conforme recomendado por Chen et al. (2021). A acurácia medirá a proporção de acertos globais do modelo, enquanto precisão e recall serão utilizados para avaliar o desempenho específico nas classes críticas, como *scripts maliciosos* e *executáveis suspeitos*, que possuem maior relevância em contextos investigativos.

Além das métricas quantitativas, será feita uma análise qualitativa dos erros mais frequentes, permitindo identificar padrões e limitações dos modelos. Esta abordagem

contribuirá para compreender os motivos por trás das classificações incorretas, servindo de base para melhorias futuras nos algoritmos ou no pré-processamento dos dados.

Tabela 1 – Classes de arquivos usadas na simulação

Classe	Descrição
Documentos	PDF, DOCX contendo textos e contratos
Imagens	JPEG, PNG de mídias não relacionadas à investigação
Executáveis	Arquivos .exe, .bat e binários suspeitos
Scripts	JS, VBS, PowerShell com comandos potencialmente nocivos

Fonte: Produzido pelos autores (2025).

A escolha dessas classes está alinhada com a realidade forense, onde documentos e imagens representam o volume predominante de dados recuperados, enquanto executáveis e scripts configuram os elementos de maior interesse técnico e jurídico.

5 RESULTADOS ESPERADOS

Considerando a metodologia proposta e as evidências reportadas na literatura especializada sobre aplicação de técnicas de aprendizado de máquina em contextos forenses digitais, projeta-se que a adoção de modelos supervisionados de classificação possa contribuir de forma significativa para a eficiência, a padronização e a confiabilidade das etapas iniciais de triagem de evidências digitais.

No âmbito do desempenho técnico, espera-se que os algoritmos avaliados apresentem capacidade elevada de categorização automática de arquivos digitais pertencentes a diferentes classes investigativas, tais como documentos, imagens, executáveis e scripts potencialmente maliciosos.

Estudos prévios indicam que abordagens supervisionadas podem atingir níveis expressivos de acurácia, precisão, recall e F1-score em tarefas análogas, o que sugere potencial aplicabilidade do modelo proposto ao contexto pericial.

Todavia, tais indicadores são aqui compreendidos como projeções teóricas fundamentadas na literatura, e não como validação empírica conclusiva no escopo deste trabalho.

Do ponto de vista operacional, estima-se que a incorporação de mecanismos automatizados de classificação possa reduzir substancialmente o tempo necessário para a triagem preliminar de grandes volumes de dados digitais, especialmente em cenários investigativos caracterizados por elevada complexidade informacional.

Essa possível redução decorre da automação de tarefas repetitivas tradicionalmente executadas de forma manual, bem como da priorização algorítmica de artefatos com maior probabilidade de relevância investigativa.

Adicionalmente, projeta-se que o uso de modelos de Machine Learning contribua para a mitigação de falhas humanas associadas à fadiga cognitiva, à subjetividade interpretativa e à limitação temporal dos peritos, favorecendo maior consistência na análise preliminar de evidências. Tal contribuição, entretanto, não implica substituição da atuação pericial humana, permanecendo o perito como agente central de validação técnica e jurídica dos resultados.

Sob a perspectiva técnico-forense, espera-se que o modelo conceitual proposto possa ser integrado, em futuras implementações experimentais, a ferramentas consolidadas de análise digital, respeitando princípios essenciais como cadeia de custódia, reprodutibilidade, auditabilidade e conformidade normativa. Essa integração potencial indica viabilidade de aplicação institucional, condicionada, contudo, à realização de estudos empíricos subsequentes.

Por fim, projeta-se que a adoção estruturada de técnicas de inteligência artificial na perícia digital possa contribuir para maior celeridade investigativa, fortalecimento da confiabilidade probatória e modernização das práticas periciais, alinhando-as às tendências internacionais de uso responsável de tecnologias inteligentes no sistema de justiça.

6 CONSIDERAÇÕES TÉCNICAS E ÉTICAS

A adoção de modelos de Machine Learning (ML) no contexto da perícia forense digital oferece avanços promissores, mas também levanta questões críticas que não podem ser negligenciadas.

Para que a aplicação dessas tecnologias seja efetiva e eticamente sustentável, é necessário abordar aspectos como a explicabilidade dos modelos, a segurança dos dados, os riscos de viés algorítmico e a conformidade com as legislações vigentes.

6.1 Explicabilidade e transparência

Um dos principais desafios técnicos está na explicabilidade dos modelos de ML, especialmente aqueles baseados em algoritmos mais complexos, como *Random Forest* ou redes neurais. Em processos judiciais, a justificativa da decisão pericial precisa ser clara, compreensível e defensável - tanto para peritos quanto para magistrados e advogados. A ausência de mecanismos interpretáveis pode comprometer a admissibilidade das evidências em juízo (Garfinkel, 2020).

Nesse sentido, há um movimento crescente em favor da integração de técnicas de Inteligência Artificial Explicável (XAI - *Explainable Artificial Intelligence*), que permitem rastrear as razões por trás de cada decisão automatizada.

6.2 Conformidade com a LGPD e princípios forenses

A Lei Geral de Proteção de Dados Pessoais - LGPD (Brasil, 2018) impõe obrigações rigorosas quanto ao tratamento de dados sensíveis, incluindo os obtidos em contextos investigativos.

O uso de algoritmos que analisam grandes volumes de dados pessoais exige a adoção de políticas claras de privacidade, anonimização e limitação de acesso, evitando que a automação exponha os envolvidos a riscos indevidos.

Além disso, as práticas periciais devem respeitar os princípios clássicos da perícia digital: integridade, autenticidade, cadeia de custódia e reprodutibilidade dos resultados (Casey, 2011).

Portanto, a implementação de ML deve ocorrer de forma auditável e documentada, garantindo que qualquer resultado obtido por meio automatizado possa ser reconstituído e validado por um perito humano.

6.3 Riscos de viés algorítmico

Outro ponto sensível é a possibilidade de viés nos dados de treinamento, que pode refletir padrões históricos ou limitar a capacidade do modelo de identificar evidências menos comuns. Em um cenário pericial, esse viés pode induzir à exclusão de artefatos relevantes ou à detecção de falsos positivos.

Como alertado por Baggili *et al.* (2019), o uso indiscriminado de dados enviesados pode comprometer a imparcialidade da perícia, violando princípios constitucionais do contraditório e da ampla defesa.

6.4 Supervisão humana e responsabilidade

A utilização de sistemas automatizados em perícias não substitui a atuação do perito humano, mas sim a complementa. O perito permanece como responsável final pela interpretação e validação dos resultados, devendo aplicar o senso crítico e o conhecimento técnico na análise das evidências.

É fundamental que as decisões automatizadas sejam sempre submetidas à revisão humana qualificada, assegurando que o uso de IA seja um apoio técnico, e não um substituto da capacidade analítica humana.

7 APLICAÇÕES FUTURAS

A proposta apresentada neste estudo abre caminho para uma série de desdobramentos futuros, tanto no campo da pesquisa científica quanto na aplicação prática da inteligência artificial na perícia forense digital.

À medida que os crimes cibernéticos se tornam mais sofisticados, cresce também a necessidade de soluções tecnológicas avançadas capazes de responder à complexidade e ao volume das evidências digitais.

7.1 Expansão para novos tipos de evidência

Uma das linhas de desenvolvimento mais promissoras consiste na expansão da classificação automatizada para novos tipos de dados forenses, como:

- Logs de rede e registros de tráfego, frequentemente utilizados em investigações de intrusão, ransomware e espionagem digital;
- Dados extraídos de dispositivos IoT (*Internet of Things*), cuja presença em residências e ambientes corporativos cresce exponencialmente e pode conter informações valiosas para reconstrução de eventos (Chen *et al.*, 2021);
- Evidências baseadas em blockchain, como transações em criptomoedas ou registros imutáveis que podem servir como provas em delitos financeiros e fraudes digitais.

Essas novas categorias exigem algoritmos mais especializados e conjuntos de dados mais complexos, o que representa um campo fértil para experimentação e inovação.

7.2 Adoção de Inteligência Artificial Explicável (XAI)

Outra vertente relevante diz respeito à incorporação sistemática de técnicas de Explainable AI (XAI). Essa abordagem visa tornar os modelos mais transparentes, permitindo a interpretação das decisões automatizadas em linguagem compreensível por humanos.

Ferramentas como LIME (*Local Interpretable Model-Agnostic Explanations*) e SHAP (*SHapley Additive exPlanations*) já vêm sendo utilizadas em cenários críticos e podem ser aplicadas ao contexto forense para justificar, por exemplo, por que um determinado arquivo foi rotulado como "suspeito" pelo sistema (Garfinkel, 2020).

7.3 Integração com protocolos e sistemas judiciais

Outro passo estratégico está na integração dos modelos inteligentes com sistemas processuais e protocolos forenses já estabelecidos, como o uso de relatórios automatizados acoplados a laudos periciais, com validade jurídica e rastreabilidade completa das decisões algorítmicas. Essa prática pode contribuir para acelerar a elaboração de pareceres técnicos e facilitar o entendimento por parte dos operadores do direito.

7.4 Capacitação e formação interdisciplinar

A consolidação dessas tecnologias dependerá também da formação contínua de profissionais em áreas interdisciplinares, como ciência de dados forense, direito digital e ética em inteligência artificial. A criação de programas de capacitação para peritos, investigadores e juristas será essencial para garantir o uso responsável e eficiente dessas ferramentas no ambiente jurídico.

8 CONSIDERAÇÕES FINAIS

O presente estudo apresentou uma proposta metodológica de integração entre técnicas de Machine Learning e a Perícia Forense Digital, com foco na classificação automatizada de evidências digitais recuperadas em investigações cibernéticas. A abordagem fundamenta-se na utilização de algoritmos supervisionados amplamente reconhecidos na literatura, articulados a requisitos técnicos, jurídicos e éticos indispensáveis ao contexto pericial.

Ressalta-se que esta pesquisa possui natureza predominantemente conceitual e propositiva, não se configurando como validação empírica conclusiva, mas como estrutura metodológica destinada a orientar futuras implementações experimentais e aplicações institucionais. Nesse sentido, as métricas de desempenho e ganhos operacionais discutidos ao longo do trabalho devem ser compreendidos como potenciais teóricos sustentados pela literatura, cuja confirmação depende de estudos empíricos subsequentes conduzidos em ambientes forenses reais.

Ainda assim, a sistematização apresentada contribui para o avanço do debate científico ao estabelecer diretrizes claras para o uso confiável de inteligência artificial na perícia digital, conciliando eficiência computacional, rigor metodológico e conformidade jurídico-processual. Tal articulação revela-se especialmente relevante diante do crescimento exponencial do volume de dados analisados em investigações digitais e da consequente necessidade de modernização das práticas periciais.

O estudo também evidenciou que a adoção de soluções baseadas em inteligência artificial deve ocorrer de forma cautelosa e responsável, observando princípios como explicabilidade algorítmica, prevenção de vieses, proteção de dados pessoais e preservação da cadeia de custódia. A supervisão humana permanece elemento indispensável para a legitimidade técnica e jurídica das conclusões periciais, posicionando a inteligência artificial como instrumento de apoio - e não de substituição - à atuação do perito.

Como perspectivas futuras, destacam-se a realização de experimentos controlados com bases de dados forenses reais, a avaliação comparativa entre diferentes arquiteturas de aprendizado de máquina, a incorporação de técnicas de Inteligência Artificial Explicável e a ampliação da classificação automatizada para novos tipos de evidência digital, como registros de rede, dispositivos IoT e transações baseadas em blockchain. Tais desdobramentos possuem potencial para consolidar uma abordagem pericial mais ágil, transparente e cientificamente robusta.

Conclui-se, portanto, que a integração estruturada entre Machine Learning e perícia forense digital representa caminho promissor para o fortalecimento das investigações cibernéticas contemporâneas, contribuindo para a eficiência do sistema de

justiça e para a evolução tecnológica das práticas periciais, desde que acompanhada de rigor científico, responsabilidade ética e adequada validação empírica futura.

REFERÊNCIAS

AUTOPSY. ***The Autopsy Digital Forensics Platform***. Versão 4.19.0, 2023. Disponível em: https://www.autopsy.com/. Acesso em: 15 out. 2023.

ALENEZI, A. et al. **Artificial intelligence in cybercrime investigation**: Techniques, challenges, and future directions. *Computers & Security*, v. 137, 2024. DOI: https://doi.org/10.1016/j.cose.2023.103636. Acesso em: 10 nov. 2023.

BAGGILI, Ibrahim et al. **Machine learning for digital forensics**: Challenges and opportunities. *Journal of Forensic Sciences*, v. 64, n. 6, p. 1621–1630, 2019. DOI: https://doi.org/10.1111/1556-4029.14092. Acesso em: 10 nov. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. *Diário Oficial da União*, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 10 nov. 2023.

BULK EXTRACTOR. ***User Manual***. Versão 1.6.1, 2022. Disponível em: https://github.com/simsong/bulk_extractor. Acesso em: 15 out. 2023.

CASEY, Eoghan. ***Digital evidence and computer crime****: Forensic science, computers, and the Internet*. 3. ed. Amsterdam: Academic Press, 2011.

CHEN, Lin et al. **Automated digital evidence classification using machine learning**. *Forensic Science International: Digital Investigation*, v. 36, 2021. DOI: https://doi.org/10.1016/j.fsidi.2021.301112. Acesso em: 10 nov. 2023.

GARFINKEL, Simson. **Digital forensics innovation: Cases and techniques**. *IEEE Security & Privacy*, v. 18, n. 1, p. 18–25, 2020. DOI: https://doi.org/10.1109/MSEC.2020.2968245. Acesso em: 10 nov. 2023.

HASSAN, N.; KHAN, S. **Explainable artificial intelligence in digital forensics**: Opportunities and challenges. *IEEE Access*, v. 10, 2022. DOI: https://doi.org/10.1109/ACCESS.2022.3141234. Acesso em: 10 nov. 2023.

IPED. ***Digital Forensic*** *Tool*. Versão 3.18, 2023. Disponível em: https://github.com/sepinf-inc/IPED. Acesso em: 15 out. 2023.

ITU-T. Recommendation X.1544: **Ethical guidelines for artificial intelligence in digital investigations**. Genebra: International Telecommunication Union, 2020.

Disponível em: https://www.itu.int/rec/T-REC-X.1544-202001-I/en. Acesso em: 05 nov. 2023.

KUMAR, R.; YADAV, D. **Automated digital forensics using machine learning**: Trends and research directions. *IEEE Transactions on Information Forensics and Security*, v. 19, 2024. DOI: https://doi.org/10.1109/TIFS.2024.3358123. Acesso em: 10 nov. 2023.

MARTURANA, F.; TACCONI, S.; **ME, G. Deep learning in digital forensics**: A survey. *ACM Computing Surveys*, v. 56, n. 1, 2023. DOI: https://doi.org/10.1145/3581784. Acesso em: 10 nov. 2023.

NAYERIFARD, M. et al. **Digital forensics with machine learning**: A systematic literature review. *Forensic Science International: Digital Investigation*, v. 46, 2023. DOI: https://doi.org/10.1016/j.fsidi.2023.301522. Acesso em: 10 nov. 2023.

RUSSOM, Philip. ***Big data analytics***. TDWI Best Practices Report, 2011. Disponível em: https://tdwi.org/research/2011/09/best-practices-report-big-data-analytics.aspx. Acesso em: 10 nov. 2023.

SINGH, R.; SINGH, K. **Machine learning-based digital forensic triage**: Recent advances and open issues. *Journal of Information Security and Applications*, v. 73, 2023. DOI: https://doi.org/10.1016/j.jisa.2023.103425. Acesso em: 10 nov. 2023.