O IMPACTO DAS NOVAS TECNOLOGIAS NA INVESTIGAÇÃO CRIMINAL: DESAFIOS E LIMITES

Geslaine Frimaio[1], Mark Pereira dos Anjos[2], Octávio Miranda Junqueira[3], Wanderson Gomes de Oliveira[4]

RESUMO

As tecnologias digitais, além de facilitarem a ação de criminosos, também geram novas formas de obtenção de provas. Diante disso, este trabalho busca analisar os principais aspectos jurídicos e técnicos relacionados ao uso de provas digitais, dando ênfase à importância da cadeia de custódia e aos impactos sobre direitos como a privacidade e a proteção de dados. A pesquisa é de caráter qualitativo e foi desenvolvida a partir da revisão de literatura e da análise da legislação atual. Verifica-se que, para que as provas digitais sejam consideradas válidas e confiáveis, é essencial que sua coleta e preservação sigam procedimentos bem definidos e que acompanhem as mudanças tecnológicas. Além disso, a crescente utilização de inteligência artificial nas investigações levanta dúvidas sobre a transparência e a confiabilidade dos métodos usados. Por isso, entende-se que é necessário buscar um equilíbrio entre a eficiência investigativa e a proteção dos direitos fundamentais, tendo em vista que as provas digitais representam um avanço importante no processo penal, mas exige atenção técnica e jurídica para que não se violem garantias básicas do acusado.

Palavras-chave: Provas digitais, investigação criminal, cadeia de custódia, perícia informática; preservação de evidências

THE IMPACT OF NEW TECHNOLOGIES ON CRIMINAL INVESTIGATION: CHALLENGES AND BOUNDARIES

ABSTRACT

Digital technologies, in addition to facilitating criminal activity, also generate new ways of obtaining evidence. In view of this, this paper seeks to analyze the main legal and technical aspects related to the use of digital evidence, emphasizing the importance of the chain of custody and the impacts on rights such as privacy and data protection. The research is qualitative in nature and was developed based on a literature review and an analysis of current legislation. It appears that, for digital evidence to be considered valid and reliable, it is essential that its collection and preservation follow well-defined procedures and keep up with technological changes. In addition, the increasing use of artificial intelligence in investigations raises questions about the transparency and reliability of the methods used. Therefore, it is understood that it is necessary to seek a balance between investigative efficiency and the protection of fundamental rights, given that digital evidence represents an important advance in criminal proceedings, but requires technical and legal attention to ensure that the basic guarantees of the accused are not violated.

Keywords: Digital evidence; criminal investigation; custofy chain; computer expertise; evidence preservation.

1. INTRODUÇÃO

Nos últimos anos, o avanço das tecnologias digitais passou a influenciar diretamente a forma como os crimes são praticados e, ao mesmo tempo, como são investigados. Essa transformação afetou não só a dinâmica das infrações penais, mas também os procedimentos adotados pelas autoridades durante as investigações. Diante da presença cada vez mais comum de evidências digitais, surgiu a necessidade de repensar os métodos tradicionais de coleta e análise de provas, bem como de ajustar o ordenamento jurídico para lidar com esses novos desafios de forma adequada.

Ao mesmo tempo em que as tecnologias digitais acabam facilitando a prática de certos crimes, elas também produzem um volume significativo de informações que podem servir como prova. Dados extraídos de dispositivos eletrônicos, registros de transações virtuais e conversas em ambientes digitais passaram a ser considerados formas relevantes de prova material. Quando submetidas à devida análise pericial, essas evidências podem ajudar a estabelecer uma relação entre o autor e o fato criminoso, contribuindo para a identificação dos envolvidos e oferecendo suporte concreto às investigações e à fase processual.

Com a inclusão crescente de elementos digitais nas provas - anteriormente predominantemente físicas - surgiu a necessidade de uma nova abordagem para o tratamento dessas evidências, exigindo a adaptação de técnicas para atuação em ambientes digitais. Diante desse cenário, ferramentas como a inteligência artificial, combinadas a vastos bancos de dados, têm revolucionado as metodologias investigativas, aumentando a eficiência na identificação de autoria e materialidade delitiva. Dispositivos como celulares, computadores e plataformas de redes sociais constituem, hoje, um acervo probatório essencial para o deslinde das investigações criminais **(**Fontenele Lemos; Homsi Cavalcante; Gonçalves Mota, 2021**).**

Essa nova realidade se reflete em investigações de grande repercussão nacional e internacional, nas quais o uso de evidências digitais se tornou crucial para a condução dos processos. Um exemplo emblemático é a Operação Lava Jato, Operação Lava Jato, iniciada em 2014, é considerada uma das maiores e mais complexas apurações de crimes de corrupção e lavagem de dinheiro na história do país (MPF, [s.d.]**).** No entanto, em 2019, assumiu novos contornos quando o *The Intercept Brasil* divulgou reportagens que revelaram diálogos entre membros da força-tarefa, registrados no aplicativo Telegram. A quebra de sigilo e a

consequente divulgação dessas mensagens trouxeram à luz possíveis irregularidades nos procedimentos adotados (Gabardo et al. 2021).

A crescente dependência de provas digitais não se restringe a casos de grande repercussão, mas também se reflete na rotina das perícias criminais realizadas no país. O impacto desse cenário pode ser observado nos números da Seção de Computação Forense da Polícia Científica do Paraná**,** que, em janeiro de 2024**,** periciou 584 itens em um único mês**,** excedendo a média mensal de 327 peças analisadas ao longo de 2023 (Paraná, 2024). Entre os dispositivos submetidos à perícia, destacam-se celulares, notebooks e tablets**,** todos essenciais para a instrução de inquéritos policiais e a elucidação de crimes.

Entretanto, novos desafios legais têm surgido com a sofisticação dos meios tecnológicos utilizados para a prática de delitos. O uso de criptoativos, por exemplo, tornou-se uma preocupação crescente, especialmente no que se refere a lavagem de dinheiro e outras atividades ilícitas. Como destacado por Nogueira e Drumond (2024), a anonimização e descentralização das transações dificultam o rastreamento de operações fraudulentas, exigindo novas abordagens investigativas. No Brasil, a Lei nº 14.478, de 21 de dezembro de 2022, trouxe um marco regulatório para os criptoativos, estabelecendo novas penalidades para fraudes e lavagem de dinheiro, ampliando o escopo das investigações criminais e reforçando a necessidade de atualização constante das metodologias periciais (BRASIL, 2022).

Nesse contexto, ainda há uma lacuna significativa no ordenamento jurídico brasileiro, que carece de uma regulamentação específica e detalhada sobre a utilização de provas digitais no processo penal. Embora o Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018) estabeleçam diretrizes gerais para o uso e proteção de dados digitais, ainda persistem desafios jurídicos relevantes, especialmente no que diz respeito à admissibilidade, autenticidade e tratamento dessas provas no âmbito das investigações e dos processos criminais (Brasil, 2014; Brasil, 2018).

Além disso, a proteção dos direitos humanos se torna fundamental nas investigações criminais, exigindo que a aplicação de técnicas modernas esteja sempre alinhada aos preceitos constitucionais (França, 2023). O acesso a um vasto conjunto de materiais probatórios relacionados às atividades de um indivíduo, como e-mails, mensagens em aplicativos de celular e arquivos digitais armazenados em nuvem ou em dispositivos físicos, suscita questões complexas acerca do direito fundamental à privacidade e à intimidade, conforme previsto no artigo 5º, inciso X, da Constituição Federal:

> "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (Brasil, 1989).

Diante desse cenário, o presente artigo se propõe a analisar os desafios e limites da utilização de provas digitais nas investigações criminais à luz da legislação brasileira, com especial atenção à necessidade de equilibrar a eficácia investigativa com a proteção dos direitos fundamentais dos indivíduos.

2. A PROVA PENAL NA ERA DIGITAL

No contexto do processo penal, as provas desempenham um papel fundamental na formação do juízo de valor do magistrado, sendo essenciais para a construção de decisões fundamentadas. O termo "prova" origina-se do latim *probatio*, que significa demonstrar ou atestar (Nucci, 2018), e, no âmbito jurídico, refere-se aos elementos que permitem ao juiz verificar a veracidade ou falsidade dos fatos alegados pelas partes (Melo, Pinto, Jacinto, 2022; Garcia, 2009). Como as versões apresentadas pela acusação e pela defesa podem refletir interesses distintos, a função probatória se torna indispensável para garantir a imparcialidade e a justiça no processo.

No processo penal, é fundamental que o juiz examine com atenção as alegações apresentadas pelas partes, confrontando-as com as provas disponíveis, a fim de esclarecer dúvidas e resolver eventuais contradições. Tradicionalmente, os meios de prova mais utilizados eram os documentos físicos, os depoimentos testemunhais e as perícias. No entanto, com o avanço das tecnologias, surgiram as chamadas provas digitais, que têm se mostrado cada vez mais relevantes, tanto na fase investigativa quanto na instrução e julgamento do processo.As provas digitais, ou *digital evidence*, correspondem a informações armazenadas em formato binário em dispositivos eletrônicos ou transmitidas por redes de comunicação. Esses dados podem conter representações de fatos relevantes para a materialidade e autoria de crimes, sendo amplamente utilizados tanto no ordenamento jurídico brasileiro quanto no estrangeiro (França, 2023; Ramalho & Almeida, 2024). Diferentemente das provas convencionais, as evidências digitais possuem características que exigem um tratamento técnico específico, como a imaterialidade, a volatilidade e a suscetibilidade à adulteração (Vaz, 2012).

Por serem mais suscetíveis a alterações, as provas digitais precisam ser coletadas e preservadas com muito cuidado, seguindo procedimentos bem definidos. Nesse sentido, a cadeia de custódia é fundamental para garantir que essas evidências cheguem ao processo sem ter sofrido qualquer tipo de modificação ou contaminação que possa colocar em dúvida sua

validade. A perícia digital também tem um papel importante, pois é ela que analisa as provas, verifica se são autênticas, se houve alguma adulteração e até consegue recuperar dados apagados. Com o uso de ferramentas específicas, como a análise de metadados e softwares forenses, é possível detectar fraudes e garantir que o material analisado seja confiável e possa ser aceito legalmente no processo (Academia Forense Digital, [s.d.]; Badaró, 2021).

3. REGULAMENTAÇÃO E CADEIA DE CUSTÓDIA

O desenvolvimento das tecnologias da informação e comunicação trouxe novos desafios para o processo penal, sobretudo no que se refere à produção, conservação e utilização das provas digitais. No ordenamento jurídico brasileiro, admite-se a utilização tanto de provas típicas quanto atípicas, desde que observados os direitos fundamentais e os princípios que regem o devido processo legal (Capozzi, 2023). No entanto, considerando que as evidências digitais possuem natureza mais delicada e são facilmente manipuláveis, torna-se indispensável a existência de normas claras e rigorosas que assegurem sua autenticidade e confiabilidade no curso da persecução penal.

A cadeia de custódia, regulamentada pela Lei nº 13.964, de 2019, tornou-se um dos principais instrumentos de controle da integridade das provas digitais, estabelecendo um conjunto de procedimentos obrigatórios para documentar sua trajetória desde a coleta até o descarte. O Código de Processo Penal reforça essa necessidade nos artigos 158-A a 158-F, determinando que a preservação do vestígio deve ser realizada por peritos oficiais, sempre que possível (Brasil, 2019). O correto manuseio da prova digital inclui reconhecimento e isolamento do vestígio, impedindo que seu estado original seja alterado, fixação e coleta, documentando detalhadamente suas características por meio de laudos e registros fotográficos, acondicionamento e transporte, assegurando que os vestígios sejam armazenados em recipientes lacrados e rastreados, recebimento e processamento, garantindo que apenas profissionais habilitados realizem a análise forense da evidência, armazenamento e descarte, permitindo a realização de contraprovas e evitando a contaminação da prova (Brasil, 2019).

Além do Código de Processo Penal, outros regulamentos complementam essas diretrizes. A Portaria SENASP nº 82, de 2014, estabelece requisitos específicos para a coleta de vestígios, determinando o uso de equipamentos de proteção individual e a identificação numérica das evidências (Brasil, 2014). Já a ABNT NBR ISO/IEC 27037 recomenda que a identificação segura das provas digitais seja garantida por funções *hash*, como MD5 e SHA-

256, para evitar adulterações e assegurar a confiabilidade dos vestígios digitais (Associação Brasileira de Normas Técnicas, 2013).

A preservação da cadeia de custódia também se relaciona com os princípios da proteção de dados e da privacidade. A Lei Geral de Proteção de Dados, instituída pela Lei nº 13.709, de 2018, determina que o tratamento de informações digitais em investigações criminais deve obedecer a critérios de finalidade, necessidade e transparência (Brasil, 2018). Qualquer prova obtida sem respeito a essas diretrizes podem ser consideradas ilícitas, conforme o artigo 5º, inciso X, da Constituição Federal (Brasil, 1988).

Uma outra questão em relação à utilização da inteligência artificial no âmbito das investigações criminais diz respeito à admissibilidade das provas digitais. De acordo com Solanke e Biasiotti (2022), os algoritmos empregados nesses sistemas muitas vezes operam de forma opaca, sendo comparados a verdadeiras "caixas-pretas", cuja lógica interna não é facilmente acessível ou compreendida. Essa falta de transparência pode comprometer a capacidade do Poder Judiciário de avaliar a origem e a validade dos resultados apresentados, impactando diretamente sua aceitação como prova válida. Diante disso, é indispensável a criação de normas técnicas e jurídicas que estabeleçam critérios de transparência e assegurem a confiabilidade das ferramentas baseadas em inteligência artificial no processo penal.

Nesse contexto, a regulamentação adequada das provas digitais e a observância rigorosa da cadeia de custódia assumem papel essencial para a sua aceitação legítima no processo penal. O cumprimento dessas exigências não apenas reforça a validade e a integridade da investigação, mas também assegura a proteção dos direitos fundamentais das partes envolvidas, prevenindo eventuais abusos ou nulidades que possam comprometer a legalidade do procedimento.

3.1 Admissibilidade e preservação da cadeia de custódia das provas digitais

A admissibilidade das provas digitais no processo penal depende diretamente do respeito à cadeia de custódia, que tem a função de garantir que os vestígios coletados sejam autênticos e não tenham sido alterados. Para que esse tipo de prova tenha validade perante o Judiciário, é fundamental que ela seja obtida por meios legais e que, desde o momento da coleta até sua apresentação em juízo, seja possível verificar sua origem e assegurar que seu conteúdo permaneceu íntegro. O Código de Processo Penal, após a promulgação da Lei nº 13.964, de 2019, passou a disciplinar a cadeia de custódia nos artigos 158-A a 158-F, estabelecendo diretrizes rigorosas sobre o manuseio, o armazenamento e o transporte das provas digitais (Brasil, 2019). O procedimento inclui as seguintes etapas:

a) reconhecimento e isolamento, impedindo que o estado original do vestígio seja alterado;
b) fixação e coleta, documentando detalhadamente suas características por meio de laudos e registros fotográficos;
c) acondicionamento e transporte, garantindo que os vestígios sejam armazenados em recipientes lacrados e rastreados;
d) recebimento e processamento, assegurando que apenas profissionais habilitados realizem a análise forense da evidência;
e) armazenamento e descarte, permitindo a realização de contraprovas e evitando a contaminação da prova.

Além da cadeia de custódia, a integridade da prova digital deve ser protegida por técnicas que evitem manipulação indevida. Métodos como hashes criptográficos (MD5, SHA-256) são amplamente aceitos como meio de verificação da autenticidade dos dados digitais (Capozzi, 2023).

A jurisprudência brasileira tem reforçado a importância do cumprimento rigoroso da cadeia de custódia. O Superior Tribunal de Justiça, por meio da Súmula 588, determina que interceptações telefônicas só são admissíveis como prova se forem autorizadas judicialmente (Brasil, 2017). No mesmo sentido, o Supremo Tribunal Federal, no julgamento do Habeas Corpus 152.752/SP, reiterou que provas obtidas por meios ilícitos são inadmissíveis, conforme o artigo 5º, inciso LVI, da Constituição Federal (STF, 2018).

A ausência de preservação adequada da cadeia de custódia pode comprometer seriamente a validade das provas digitais no processo penal. Alterações não autorizadas em arquivos eletrônicos, como mensagens ou e-mails, são suficientes para que essas provas sejam desconsideradas judicialmente (Capozzi, 2023). Por esse motivo, é indispensável que tais evidências sejam mantidas íntegras e com procedência devidamente comprovada, de forma a garantir sua confiabilidade e admissibilidade no curso da persecução penal.

4. AS PROVAS DIGITAIS NO PROCESSO PENAL: PRINCIPAIS DESAFIOS

Embora as provas digitais ofereçam vantagens, como maior precisão e rastreabilidade, elas também trazem desafios, como a vulnerabilidade à manipulação e questões éticas relacionadas à privacidade e à sua admissibilidade em tribunal.

Guttman et al. (2022), em seu relatório sobre preservação de evidências digitais, discutem técnicas como o uso de *hashes* criptográficos para garantir que as provas não sejam adulteradas durante o processo de investigação. Além disso, enfatizam a importância da

manutenção rigorosa da cadeia de custódia para assegurar a autenticidade das provas apresentadas em tribunal.

Por outro lado, Solanke et al. (2022) abordam os desafios específicos do uso da inteligência artificial na análise de provas digitais. Eles destacam a opacidade dos modelos de IA, que muitas vezes funcionam como "caixas pretas", dificultando a explicação clara de como os resultados são alcançados. Essa falta de transparência pode ser um grande obstáculo na admissibilidade das provas, uma vez que é necessário comunicar de forma compreensível como a IA chegou às suas conclusões. Para melhor entendimento das diferenças e abordagens de Guttman et al. (2022) e Solanke e Biasiotti (2022), a Tabela 1 a seguir apresenta uma comparação entre os dois estudos."

Tabela 1: Comparativo entre os estudos de Guttman et al (2022) e Solanke e Biasiotti(2022).

	Guttman et al, (2022)	**Solanke e Biasiotti (2022)**
Foco Principal	Integridade e preservação das evidências digitais	Uso da inteligência artificial (IA) na análise forense digital
Desafios Primários	Preservação de evidências e manutenção da cadeia de custódia.	falta de transparência nos modelos de inteligência artificial e os impactos na confiabilidade dos resultados gerados
Ferramentas de Proteção	Hashes criptográficos a fim de manter a integridade das provas.	Padronização de algoritmos de IA para maior transparência.
Limitações na Admissibilidade	Dificuldade em provar a autenticidade das provas digitais caso a cadeia de custódia ter sido comprometida.	Dificuldade de explicar o funcionamento dos modelos de IA de maneira compreensível para o contexto jurídico.
Recomendações	Rigor técnico na preservação e documentação detalhada da cadeia de custódia.	Padronizar algoritmos de IA e aprimorar métodos de avaliação para aumentar a confiança nos resultados
Impacto em Investigações	Provas digitais podem ser comprometidas se não forem preservadas corretamente.	Resultados de IA podem ser mal interpretados se os algoritmos não forem devidamente avaliados e otimizados.
Contribuição para a Ciência Forense	Estabelecer critérios e métodos para a preservação e manipulação segura de provas digitais.	Técnicas para avaliação, padronização e otimização de modelos de IA para perícia forense.

Fonte: elaborada pelo autor

Embora os dois estudos abordem temas distintos, ambos convergem na necessidade de garantir a confiabilidade das provas digitais no âmbito forense. Enquanto Guttman et al. (2022) propõem diretrizes para a preservação e manipulação segura das evidências**,** Solanke e Biasiotti

(2022) enfatizam a importância da avaliação e otimização dos modelos de IA para que possam ser aceitos no meio jurídico. Dessa forma, a integração das duas abordagens torna-se essencial para aprimorar os métodos de investigação forense e assegurar a validade das provas no contexto digital.

5. CONCLUSÃO

As tecnologias digitais tem desempenhado um papel relevante na modernização das investigações criminais, ao proporcionar maior precisão na coleta de dados e facilitar o rastreamento de evidências. No entanto, juntamente com esses avanços, surgem obstáculos importantes relacionados à autenticidade das provas, à sua admissibilidade no processo penal e à garantia dos direitos fundamentais. Nesse contexto, a cadeia de custódia torna-se um instrumento indispensável, pois é por meio dela que se assegura a integridade e a fidedignidade das evidências digitais. A observância rigorosa desse procedimento é fundamental para afastar dúvidas sobre a prova e prevenir eventuais nulidades processuais (Capozzi, 2023).

Além disso, a crescente utilização de inteligência artificial na análise de provas digitais levanta questionamentos sobre transparência e confiabilidade dos algoritmos. Conforme discutido por Solanke e Biasiotti (2022), os modelos de inteligência artificial, muitas vezes, operam como sistemas de difícil interpretação, dificultando a compreensão dos processos decisórios e, consequentemente, sua aceitação em juízo. Assim, é fundamental que os critérios técnicos e jurídicos de validação dessas provas sejam constantemente aprimorados, garantindo que seu uso respeite os princípios do devido processo legal.

Diante dessas questões, torna-se imprescindível que as normativas e procedimentos que regulamentam a coleta e a preservação das provas digitais sejam continuamente aprimorados. A Lei Geral de Proteção de Dados, o Código de Processo Penal e a ABNT NBR ISO/IEC 27037 são marcos regulatórios essenciais para estabelecer diretrizes que garantam a legalidade e a confiabilidade dessas evidências (Brasil, 2018; Brasil, 2019; Associação Brasileira de Normas Técnicas, 2013).

Diante do cenário atual, é indispensável buscar um ponto de equilíbrio entre a efetividade das investigações criminais e a preservação dos direitos fundamentais. As provas digitais, embora representem um avanço significativo para o processo penal, demandam cuidados específicos tanto no aspecto técnico quanto jurídico, a fim de não comprometer garantias essenciais, como a privacidade e a integridade das informações. Nesse sentido, torna-se necessário o constante aprimoramento das normas legais e das ferramentas tecnológicas, de

modo a assegurar a confiabilidade das provas produzidas e fortalecer a legitimidade das decisões no âmbito da Justiça criminal.

6. REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. ABNT NBR ISO/IEC 27037:2013. Tecnologia da informação – Técnicas de segurança – Diretrizes para identificação, coleta, aquisição e preservação de evidências digitais. Rio de Janeiro: ABNT, 2013.

BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. Boletim IBCCRIM, São Paulo, ano 29, n. 343, p. 7, jun. 2021.

BRASIL. Constituição da República Federativa do Brasil de 1988. Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 1 out. 2024.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Diário Oficial da União, Brasília, DF, 13 out. 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 1 mar. 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 27 set. 2024.

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, 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 3 out. 2024.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Diário Oficial da União, Brasília, DF, 24 dez. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm. Acesso em: 3 out. 2024.

BRASIL. Lei nº 14.478, de 21 de dezembro de 2022. Dispõe sobre diretrizes para a prestação de serviços de ativos virtuais e a regulação dos criptoativos. Diário Oficial da União, Brasília, DF, 22 dez. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2021-2024/2022/lei/L14478.htm. Acesso em: 7 mar. 2025.

BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Segurança Pública. Portaria Senasp nº 82, de 16 de maio de 2014. Dispõe sobre os procedimentos de coleta, preservação e custódia de vestígios em investigações criminais. Diário Oficial da União, Brasília, DF, 19 maio 2014. Disponível em: https://www.gov.br/mj/pt-br. Acesso em: 15 out. 2024.

CAPOZZI, R. A. Provas Digitais e a Cadeia de Custódia. Academia Forense Digital, 2023. Disponível em: https://academiadeforensedigital.com.br/provas-digitais-e-a-cadeia-de-custodia/. Acesso em: 30 set. 2024.

FONTENELE LEMOS, D.; HOMSI CAVALCANTE, L.; GONÇALVES MOTA, R. A prova digital no direito processual brasileiro. Revista Acadêmica Escola Superior Do Ministério Público Do Ceará, v. 13, n. 1, p. 11–34, 2021. Disponível em: https://doi.org/10.54275/raesmpce.v13i1.147. Acesso em: 30 set. 2024.

FRANÇA, Rafael Francisco. Balancing Self-Incrimination and Public Safety: A Comparative Analysis of Compelled Smartphone Unlocking in Brazilian and U.S. Legal Systems. Revista Brasileira de Direito Processual Penal, v. 9, n. 3, p. 1-50, set./dez. 2023.

GUTTMAN, Barbara; WHITE, Douglas R.; WALRAVEN, Tracy. Preservation of Digital Evidence: Considerations for Evidence Handlers. National Institute of Standards and Technology (NIST), NIST Interagency Report 8387, Sep. 2022. Disponível em: https://doi.org/10.6028/NIST.IR.8387. Acesso em: 30 set. 2024.

MAUÉS, Marcelo Brito. Modelagem de ameaças antiforenses aplicada ao processo forense digital. 2016. 113 f. Dissertação (Mestrado em Engenharia Elétrica) – Universidade de Brasília, Brasília, 2016. Disponível em: http://repositorio.unb.br/handle/10482/23487. Acesso em: 3 out. 2024.

MEDEIROS NETO, J. S. Provas Digitais e o Princípio da Proibição de Provas Ilícitas. Revista Brasileira de Direito Digital, São Paulo, v. 4, n. 2, p. 45-68, 2018.

MPF – MINISTÉRIO PÚBLICO FEDERAL. Operação Lava Jato: entenda o caso. Disponível em: https://www.mpf.mp.br/grandes-casos/casos-historicos/lava-jato/entenda-o-caso. Acesso em: 4 out. 2024.

NUCCI, Guilherme de Souza. Código de Processo Penal Comentado. 2. ed. São Paulo: RT, 2003.

PARANÁ. Polícia Científica do Estado do Paraná. Relatório de Atividades da Computação Forense – Janeiro de 2024. Curitiba: Polícia Científica, 2024. Disponível em: https://www.policiacientifica.pr.gov.br/Noticia/Secao-de-Computacao-Forense-bate-recorde-de-pericias-em-vestigios-ciberneticos-em-2024. Acesso em: 30 set. 2024.

RAMALHO, J.; ALMEIDA, F. Apprehend Electronic Mail: The Code of Criminal Procedure and Cybercrime Law Regimes. Revista Jurídica Portucalense, p. 261–276, 2024. Disponível em: https://doi.org/10.34625/issn.2183-2705(35)2024.ic-13. Acesso em: 4 out. 2024.

SOLANKE, Abiodun A.; BIASIOTTI, Maria Angela. AI Forensics: Evaluating, Standardizing, and Optimizing Digital Analysis. KI – Künstliche Intelligenz, 2022. Disponível em: https://doi.org/10.1007/s13218-022-00763-9. Acesso em: 4 out. 2024.

VAZ, Denise Provasi. Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. 287 f. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012. Disponível em: https://teses.usp.br/teses/disponiveis/2/2137/tde-28052013-153123/pt-br.php. Acesso em: 4 out. 2024.