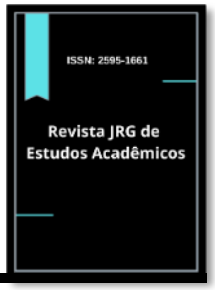
B1 ISSN: 2595-1661

ARTIGO DE REVISÃO

Listas de conteúdos disponíveis em Portal de Periódicos CAPES

Revista JRG de Estudos Acadêmicos

Página da revista:
https://revistajrg.com/index.php/jrg



Os avanços e desafios das investigações digitais diante das evidências disponibilizadas pelas mídias

The advances and challenges of digital investigations regarding the evidence provided by media

DOI: 10.55892/jrg.v7i15.1685
ARK: 57118/JRG.v7i15.1685

Recebido: 29/11/2024 | Aceito: 02/11/2024 | Publicado *on-line*: 03/12/2024

Odelino Oliveira Fonseca [1]
https://orcid.org/ 0009-0007-6565-926X
http://lattes.cnpq.br/5074899075914738
Faculdade Serra do Carmo (FASEC), TO, Brasil
E-mail: Odelino.direito@gmail.com

Ramilla Mariane Silva Cavalcante [2]
https://orcid.org/0000-0002-4714-7558
http://lattes.cnpq.br/5925550878581026
Faculdade Serra do Carmo (FASEC), TO, Brasil
E-mail: ramillacavalcante@mail.uft.edu.br

Resumo

O presente artigo examina os avanços e desafios das investigações digitais entre 2014 e 2024, destacando como as tecnologias emergentes impactaram o processo de coleta e análise de provas digitais. O problema central da pesquisa refere-se à necessidade de adaptação das práticas forenses e das legislações para enfrentar o crescimento de crimes cibernéticos e garantir a validade jurídica das evidências digitais. O objetivo principal é analisar as transformações nas práticas investigativas digitais, identificando as tecnologias utilizadas, as lacunas na legislação e os principais obstáculos na preservação da cadeia de custódia. A metodologia utilizada consiste em uma revisão de literatura, com abordagem qualitativa e objetivo descritivo, investigando fontes acadêmicas e jurídicas sobre técnicas e regulamentações da investigação digital. Conclui-se que, embora os avanços tecnológicos tenham proporcionado ferramentas mais eficazes, persistem desafios relacionados à volatilidade das provas digitais e à adaptação legal. A implementação de protocolos rigorosos e o fortalecimento da cadeia de custódia são essenciais para assegurar a integridade das evidências e a eficácia das investigações cibernéticas.

Palavras-chave: Investigação digital. Cadeia de custódia. Crimes.

[1] Graduando em Direito pela Faculdade Serra do Carmo (FASEC).
[2] Mestre pela Universidade Federal do Tocantins (UFT), Especialista em Direito Processual (UNISUL) e Direito Eleitoral (UFT). Advogada e professora da UFT e Faculdade Serra do Carmo (FASEC).

Abstract
This article examines the advances and challenges of digital investigations between 2014 and 2024, highlighting how emerging technologies have impacted the process of collecting and analyzing digital evidence. The central issue of the research concerns the need for forensic practices and legislation to adapt in response to the growth of cybercrimes and to ensure the legal validity of digital evidence. The primary objective is to analyze the transformations in digital investigative practices, identifying the technologies used, gaps in legislation, and the main obstacles in preserving the chain of custody. The methodology employed consists of a literature review with a qualitative approach and a descriptive objective, investigating academic and legal sources on digital investigation techniques and regulations. It is concluded that, although technological advances have provided more effective tools, challenges persist regarding the volatility of digital evidence and legal adaptation. The implementation of rigorous protocols and the strengthening of the chain of custody are essential to ensure the integrity of evidence and the effectiveness of cyber investigations.

Keywords: *Digital investigation. Chain of custody. Crimes.*

1. Introdução

Com a ascensão tecnológica, comportamentos e atitudes sofreram alterações quando se observa a agilidade promovida principalmente no ato comunicacional, seja por aplicativos ou redes sociais, que conjuntamente com a celeridade realizada, trouxeram contribuições significativas na resolução de problemas, otimização e atendimento às urgências e emergências que são exigidas hodiernamente.

Contudo, em contrapartida às vantagens ofertadas pelas tecnologias, subsiste um lado obscuro a ser observado, uma vez que o uso das elencadas ferramentas digitais agrega oportunidades para a validação de uma cibercriminalidade que afronta os princípios do Estado Democrático de Direito, bem como o ordenamento jurídico brasileiro que leva a execução de processos investigativos no universo digital.

Nesse cenário, as investigações digitais emergem como uma resposta fundamental para a coleta e análise de provas dos crimes cibernéticos na seguridade dos direitos de cidadania fundamentado nas legislações brasileiras. Todavia, a complexidade dessas investigações requer profissionais altamente qualificados e especializados, capazes de manejar ferramentas e técnicas de forense computacional, um campo que visa encontrar e preservar evidências digitais em dispositivos eletrônicos (Caloyannides, 2001; Carrier, 2003).

Enquanto a tecnologia facilita a identificação de padrões e provas, ela também apresenta desafios significativos, especialmente quando crimes cibernéticos evoluem tão rapidamente quanto os métodos de investigação. Crimes como fraudes digitais e ataques de malware tornam essencial uma abordagem que inclua tanto a adaptação de leis quanto o aprimoramento contínuo das práticas forenses para garantir a validade das provas no contexto jurídico (Rodrigues & Foltran Jr., 2010).

Nos últimos anos, o intervalo de 2014 a 2024 destacou-se por mudanças notáveis na tecnologia e na legislação que impactaram as investigações digitais. Desde o fortalecimento de regulamentações internacionais de proteção de dados, como o GDPR, até a criação de novas técnicas de análise forense, esse período

ilustra tanto os avanços quanto os desafios enfrentados no combate aos crimes digitais (Tauchert & Amaral, 2015).

Desse modo, verifica-se um crescente aumento na ação criminal utilizando as tecnologias, em que os crimes digitais assim denominados exigem normatizações e ampliações para o seu combate na sociedade, assegurando o acesso virtual sem práticas ou ações ilícitas, visto que os cidadãos possuem diversas contas de e-mails, redes sociais, aplicativos bancários e outros formatos de utilização. Além do mais, o uso dos artefatos tecnológicos não delineia idades específicas, ou seja, todos os sujeitos podem utilizar.

Neste contexto, norteia-se que a investigação digital se refere a busca pelas comprovações criminais ocorridas pelo uso da informática, ao realizar malwares, vazamento de dados, sites falsos, envio de informações sigilosas, fraudes, e terrorismos e outros atos das mídias digitais considerados crimes cibernéticos.

Outrossim, no campo das investigações digitais compete aos profissionais do Direito conhecer esse universo, pois os comportamentos sociais são realizados com apenas um clique, mascarados por crimes contra a dignidade humana ou infração de situações que devem gerar penas a serem cumpridas.

Portanto, o principal objetivo deste tipo de perícia forense pode ser definido como a coleta de vestígios relacionados ao crime investigado, os quais possibilitem a formulação de conclusões sobre o caso (Reis, 2003). Nesse viés, a adaptação das leis e a criação de novas regulamentações são essenciais para enfrentar os crimes cibernéticos de maneira eficaz, trazendo resoluções por práticas criminais, visto que a evolução caminha com o aparato da justiça pelo mundo digital.

Na fase de pesquisa e coleta de informações são utilizadas ferramentas forenses e devem ser criadas imagens (cópias físicas) dos discos rígidos dos computadores que são considerados suspeitos de terem sido utilizados no ato ilícito (Carrier, 2003).

Para tanto, o objetivo geral da presente pesquisa consistiu em analisar a efetividade nas investigações criminais no período do decênio de 2014 a 2024, por meio da revisão bibliográfica. Enquanto os objetivos específicos foram ordenados em: *Evidenciar conceitos e definições sobre as tecnologias da informação; Descrever as normatizações da aplicação da cadeia de custódia na investigação digital; Relacionar as técnicas de investigação digital em tempos contemporâneos; Apresentar o cenário do período de 2014 a 2024 da realização das investigações digitais.*

Os procedimentos metodológicos adotados são de uma pesquisa com revisão de literatura, com abordagem qualitativa e objetivo-descritivo. Além disso, os resultados alcançados serão discutidos pelos resultados alcançados no recorte de 2014 a 2024.

Nesse sentido, apresenta-se os aportes que direcionaram a pesquisa com revisão bibliográfica de maneira sistematizada para o leitor compreender o objeto temático, visto que socialmente existe uma ausência em materiais de natureza científica do assunto em tempos contemporâneos.

2. Metodologia

A pesquisa desenvolvida no artigo caracteriza-se como uma revisão bibliográfica, com abordagem qualitativa e objetivo descritivo. A escolha por essa metodologia se deu para explorar os avanços e desafios das investigações digitais entre os anos de 2014 e 2024, buscando compreender como as tecnologias

emergentes e as regulamentações impactaram as práticas forenses e a coleta de provas digitais.

Foram utilizadas fontes acadêmicas e jurídicas, abrangendo estudos sobre as técnicas de investigação digital e as normatizações aplicáveis, com ênfase na cadeia de custódia. A revisão bibliográfica foi conduzida de maneira sistematizada, de modo a proporcionar uma visão abrangente do tema, especialmente pela carência de materiais científicos sobre investigações digitais contemporâneas.

O recorte temporal de 2014 a 2024 foi adotado para permitir uma análise das transformações ocorridas nesse período, considerando tanto os avanços tecnológicos quanto os desafios enfrentados pela área jurídica no combate aos crimes cibernéticos.

3. Tecnologias da informação

Ao realizar uma busca por bibliografias sobre as Tecnologias da Informação (TI), observou-se que a sua inserção no meio social foi avançando de forma gradativa, em alguns casos transformando o ato humanístico refém dessa utilização, principalmente nas funcionalidades exercidas profissionalmente.

Todavia, não é algo tão recente, uma vez que a tecnologia sempre existiu, desde o início dos tempos ela já estava entre nós, só que em formas diferentes que nós não conseguíamos enxergar. Há 3.500 anos a.C. foi criada a roda, e na Idade Média os chineses inventaram a pólvora e os fogos de artifício. No século XVIII, mais precisamente no ano de 1712, Thomas Newcomen desenvolve o motor a vapor. Podemos dizer que a tecnologia e a inovação sempre existiram, não foi uma criação de 20 anos, todas essas descobertas são cruciais para chegar à tecnologia que hoje existe e não para de se desenvolver (Cavalcante 2011).

A tecnologia evoluiu muito rápido, com um intervalo de 80 anos desde o momento em que foi criado o primeiro automóvel até a chegada do homem na lua. Isso mostra o quanto o ser humano evoluiu e ainda pode evoluir, cuja rapidez dificulta a adaptação da geração atual com as tecnologias que surgiram. Daqui quarenta ou cinquenta anos, isso pode se tornar até um problema, em que os cidadãos se sintam excluídos do meio em que vivem (Cavalcante, 2011). Alguns autores definem a tecnologia como uma simbiose entre o “homem e a máquina, em que a segunda funciona como elemento cooperante e ativo durante os procedimentos de raciocínio dos sujeitos” (Faranhos, 2019, p. 25).

No contexto corporativo, as tecnologias da informação tornaram-se indispensáveis, impactando diretamente a competitividade e a eficiência das empresas, ao passo que otimizam processos e melhoram a tomada de decisão (Laudon, 2020). A implementação de sistemas de informação gerenciais e a automação de processos operacionais são apenas alguns exemplos de como a TI atua na otimização das operações e na estruturação das organizações modernas (Rezende; Abreu, 2018).

As tecnologias da informação também facilitam a comunicação e o trabalho colaborativo, especialmente com a expansão da internet e das redes de comunicação de dados. Ferramentas como e-mails, videoconferências e plataformas de colaboração em tempo real permitem que as equipes trabalhem em projetos compartilhados de qualquer lugar do mundo, o que reduz barreiras geográficas e aumenta a eficiência (Turban et al., 2018). O fenômeno do teletrabalho, que se intensificou a partir de 2020, exemplifica como as tecnologias da informação

possibilitaram que as organizações mantivessem a produtividade em momentos de distanciamento social" (Castells, 2018, p. 18).

Nesse contexto, a segurança da informação é um aspecto essencial para o uso eficaz das tecnologias da informação. Com o aumento das ameaças cibernéticas e dos ataques de hackers, a necessidade de garantir a segurança dos dados tornou-se uma prioridade. Medidas como criptografia, autenticação multifator e firewalls são fundamentais para proteger informações sensíveis e assegurar a privacidade dos usuários (Stallings, 2019). A segurança cibernética passou a ser uma preocupação central para empresas e governos, exigindo constantes investimentos e atualizações em tecnologias de proteção (Whitman; Mattord, 2017).

Além disso, as tecnologias da informação desempenham um papel vital na gestão do conhecimento, facilitando o armazenamento, o compartilhamento e o acesso a informações relevantes. Segundo Nonaka e Takeuchi (2008), o conhecimento é um recurso estratégico nas organizações, e a TI é essencial para gerenciar esse conhecimento de maneira eficaz. Ferramentas de gestão do conhecimento, como intranets e repositórios de dados, permitem que as empresas retenham o conhecimento e utilizem-no para melhorar processos e inovar (Davenport; Prusak, 2012).

Outro impacto significativo da TI é observado na análise de dados e na tomada de decisão baseada em dados. O desenvolvimento de tecnologias de Big Data e ferramentas de análise avançada possibilita que as organizações processem grandes volumes de informações e identifiquem padrões relevantes para a tomada de decisões (Marr, 2017). Essa abordagem, conhecida como data-driven decision making, permite que empresas respondam com agilidade às mudanças do mercado e atendam melhor as necessidades de seus clientes (Mcneely; Pope, 2018).

A inteligência artificial (IA) é uma das tecnologias da informação mais revolucionárias, com aplicação em setores como saúde, finanças e manufatura. A IA é capaz de realizar tarefas complexas e automatizar processos, tornando-se um importante diferencial competitivo. Em áreas como a medicina, por exemplo, algoritmos de aprendizado de máquina estão sendo utilizados para diagnosticar doenças e sugerir tratamentos, o que melhora a eficiência dos serviços de saúde (Russell; Norvig, 2021). Segundo Kurzweil (2019, s/n), a IA continuará a evoluir e desempenhar um papel cada vez mais importante na transformação digital.

As redes de Internet das Coisas (IoT) também representam um avanço notável nas tecnologias da informação, conectando dispositivos e sensores para coletar dados em tempo real. Na indústria, a IoT possibilita a manutenção preditiva e a automação de processos, reduzindo custos e melhorando a eficiência (Atzori; Iera; Morabito, 2017). No ambiente doméstico, dispositivos como assistentes virtuais e sistemas de automação residencial estão cada vez mais presentes, facilitando o cotidiano das pessoas (Evans, 2018).

Apesar dos avanços, o uso de tecnologias da informação traz desafios, especialmente no que diz respeito à privacidade e ao uso ético dos dados. A implementação de regulamentações como o GDPR na Europa e a LGPD no Brasil busca garantir que os dados dos usuários sejam tratados de maneira segura e ética (Kroenke; Auer, 2020). Contudo, o debate sobre a privacidade dos dados é constante, pois a coleta massiva de informações por grandes corporações levanta questões sobre o controle e a transparência desses dados (Zuboff, 2019).

De forma resumida, verifica-se que toda a evolução apresentada das tecnologias da informação traz alguns avanços e reflexões conceituais desse percurso de alterações e inserção social, evidenciando as crescentes relações

virtuais, e norteando que se trata de um ambiente utilizado não somente para o bem, mas, também, por aqueles que o manipulam com más intenções (Trivino, 2024). Pois, a autora infringe que o ciberespaço, como é conhecido o ambiente virtual, é palco do cometimento de diversos ilícitos, muitas vezes por indivíduos enrustidos na roupagem da invisibilidade ou do anonimato (Trivino, 2024, p. 11).

Contudo, ressalta-se que a gestão da TI, a segurança dos dados e a regulação ética do uso das informações devem ser tópicos de destaque na agenda de organizações e governos em todo o mundo, pois ao mesmo tempo que beneficia causam o aumento de crimes no território brasileiro.

4. Aplicação da cadeia de custódia na investigação digital

Como destacado anteriormente, o panorama demonstra uma ampliação em números em relação aos crimes utilizando as tecnologias, tão logo é necessária a penalidade com atos que possam trazer punições aos infratores.

Nesse contexto, a cadeia de custódia desempenha um papel fundamental na investigação digital, assegurando que as provas digitais coletadas sejam preservadas e manuseadas corretamente ao longo do processo investigativo. Nesta esteira, se tem o art. 158-A e seguintes, do Código de Processo Penal CPP, que versam sobre a cadeia de custódia e as etapas a serem seguidas para a manutenção e garantia da idoneidade do vestígio e da prova colhida durante os procedimentos policiais ou periciais (Mendonça, 2022).

Previsto no art. 4º do Código de Processo Penal Brasileiro, mostra-se relevante, com o fim de conceitua-lo, se dar a devida atenção ao substantivo que designa a atividade: apuração, esta que deriva do verbo apurar, o qual tem em sua etimologia o sentido de puro, de conhecer o certo, como bem define Aury Lopes Junior (2014) sendo dessa exposição que se extrai que o Inquérito não possui mais aquele caráter inquisitório por mais que sua instalação no ordenamento pátrio seja contemporânea a um período ditatorial que o Brasil vivia.

Além disso, no ano de 2019 ganha-se um reforço legal nesse panorama. A Lei nº 13.964 de 2019, também conhecida como Pacote Anticrime, estabelece que a cadeia de custódia dos vestígios compreende diversas etapas (reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processa mento, armazenamento e descarte) (Brasil, 2019).

A partir dessa homologação, na processualística moderna, o julgamento baseia-se:

> Nos elementos de convicção coligidos, os quais, regularmente admitidos no processo e submetidos ao crivo do contraditório e da ampla defesa, erigem-se em provas ou evidências3, com as quais se busca reconstituir historicamente determinado conjunto de fatos, com vistas a alcançar a verdade dita “processual” (Tourinho Filho, 2012, p. 58).

Para tanto, nesse ato processual, a prova digital (também chamada eletrônica, tecnológica ou e-evidence) pode ser definida como *"qualquer classe de informação (dados) que tenha sido produzida, armazenada ou transmitida por meios eletrônicos"* (Prado, 2021, on line).

A cadeia de custódia da prova corresponde, na linguagem jurídica, ao conjunto de procedimentos exigidos à preservação e rastreabilidade desses elementos de convencimento, caracterizando requisito de validade do resultado da atividade probatória primária, após a sua admissibilidade e valoração.

Nessa sequência de pensamento, Carrier e Spafford (2003, p. 2) destacam que a cadeia de custódia envolve *"o rastreamento detalhado da posse, controle,*

transferência e análise das provas desde o momento da coleta até a apresentação em tribunal". Essa prática é crucial para garantir a integridade dos dados digitais e para que as evidências possam ser aceitas juridicamente.

Prado (2014) apresenta a definição mais detalhada no qual a cadeia de custódia é a história cronológica escrita, ininterrupta e testemunhada, de quem teve a evidência desde o momento da coleta até que ela seja apresentada como prova no tribunal. A função da cadeia de custódia é garantir que a prova coletada seja analisada por meio de um procedimento que assegure sua autenticidade, impedindo alterações durante o manuseio e a extração de informações. Dessa forma, evita-se que qualquer modificação comprometa a integridade dos fatos e possa prejudicar o acusado.

Todavia, a necessidade de preservação de dados digitais que exigem atenção a diversos procedimentos, incluindo a documentação rigorosa de cada etapa do processo. Stallings (2019, p. 35) destaca que *"a documentação detalhada das etapas é necessária para manter a autenticidade das evidências".*

Isso é particularmente importante em contextos de crimes digitais, onde a alteração de dados pode ocorrer facilmente devido à natureza volátil das informações em sistemas eletrônicos. A coleta de provas digitais também deve seguir protocolos rígidos. Whitman e Mattord (2017, p. 45) afirmam que *"a coleta de evidências digitais requer o uso de ferramentas forenses apropriadas para evitar qualquer modificação dos dados originais".* Ferramentas como imagens de discos rígidos permitem a análise do conteúdo sem comprometer a integridade dos dados, criando uma cópia exata do dispositivo suspeito (Carrier, 2003).

Para garantir a validade das provas, a cadeia de custódia precisa ser mantida desde o momento da coleta até a apresentação das evidências em tribunal. Segundo Caloyannides (2001, p. 57), *"qualquer quebra na cadeia de custódia pode comprometer a admissibilidade das evidências".* A responsabilidade dos peritos digitais inclui a garantia de que as provas foram preservadas de maneira inalterada e que toda a manipulação dos dados foi documentada.

Além da preservação, a cadeia de custódia também exige que cada transferência de posse seja registrada. Tauchert e Amaral (2015, p. 12) explicam que *"cada transação e cada pessoa que teve acesso aos dados devem ser identificadas para manter a confiabilidade das provas digitais".* Essa prática é fundamental para evitar alegações de contaminação ou manipulação das evidências.

A análise forense digital exige que os peritos utilizem procedimentos rigorosos, especialmente no uso de ferramentas de análise que garantam a preservação das evidências originais. Para Carrier (2003, p. 8), *"o uso de ferramentas apropriadas permite que os investigadores analisem cópias das evidências, sem nunca comprometer os dados originais"* essa abordagem assegura que as provas se mantenham intactas ao longo de todo o processo investigativo.

A importância da documentação das etapas da cadeia de custódia também se estende à fase de análise dos dados. Rodrigues e Foltran Jr. (2010, p. 19) defendem que *"uma documentação detalhada na fase de análise é essencial para que o processo seja auditável e para que os dados coletados possam ser defendidos em tribunal".* Sem essa documentação, qualquer evidência pode ser questionada ou descartada.

A aplicação de práticas de cadeia de custódia em investigações digitais também auxilia na proteção dos direitos dos envolvidos. Segundo Reis (2003, p. 66), *"a cadeia de custódia assegura que o direito à privacidade seja mantido, garantindo que os dados sejam manuseados de maneira ética e segura".*

Esse cuidado evita abusos e protege a integridade das partes envolvidas, norteando a seguridade da dignidade que deve ser considerada como qualidade indissociável de todo e qualquer ser humano dentro dos aportes legais no território brasileiro.

5. As técnicas de investigação digital

Com o alto índice de informações e dados pelos meios tecnológicos a prática de crimes foi ampliada no cotidiano, exigindo a inserção de uma metodologia investigativa para validação de provas que afirmam a autenticidade do ato efetivado.

Surge, assim, a questão dos procedimentos adotados na cadeia de custódia das evidências, levantando preocupações sobre a integridade e confiabilidade do material coletado (Lobão Sobrinha, 2021, p. 7). Uma vez que a prática do ilícito estiver vinculada ao ambiente cibernético, trata-se, então, de “prova digital”.

O respeito à cadeia de custódia é imprescindível para a validação das provas obtidas pela Perícia Forense Computacional, devendo receber cada vez mais destaque nas demandas apresentadas às Cortes Superiores. Com os avanços da modernidade, torna-se essencial que o Direito se adapte às novas questões que surgem nesse contexto.

Segundo Lima (2018, p. 107) *“o Inquérito Policial possui natureza instrumental com dupla função: a) preservadora e b) preparatória”.* Da primeira, se extrai que o Inquérito Policial inibe a instauração de um processo penal infundado e temerário, pois muito pelo contrário, tem por finalidade a resguardar a liberdade do inocente e evitar onerosidade excessiva do Estado com investigações inócuas e desnecessárias.

As buscas tornam-se elementos informativos para validar e cumprir os aportes penais contra a ação realizada, garantido comprovações que podem viabilizar as soluções necessárias. Nesse sentido, as provas podem provir de pessoas ou de coisas, daí a tradicional classificação doutrinária: fontes de prova pessoais ou reais. A cadeia de custódia tem relação com as fontes de prova reais ("real evidences") (Badaró, 2017).

Ademais, pode-se dizer que a tecnologia é um poderoso instrumento de investigação. Todavia, não se pode olvidar que esse tipo de evidência possui características peculiares que vão variar de acordo com a fonte de prova, de modo que cada perícia guarda especificidades relevantes.

Na visão de Prado (2014, p. 70), a sociedade transforma-se diariamente em rápida velocidade e essa transformação é impulsionada pela extraordinária revolução que as inovações tecnológicas proporcionam. Viver é estar, portanto, conectado. Porém, o autor enfatiza que no campo dos métodos ocultos de investigação, as inovações trazidas pela tecnologia parecem capazes de atingir os objetivos perseguidos pela filosofia da consciência: garantir o acesso à realidade como objeto autônomo de conhecimento, não havendo uma vinculação com o sujeito (Prado, 2014, p. 69).

Outrossim, a responsabilidade pela manutenção da idoneidade das provas processuais, por meio da cadeia de custódia, é compartilhada entre todos os agentes do Estado envolvidos na investigação criminal. Desde o policial nas ruas, que identifica o delito, passando pelos investigadores, até o perito criminal responsável por validar as evidências nos exames periciais, todos desempenham um papel fundamental nesse processo (Lobão Sobrinha, 2021).

Cabe às autoridades garantirem uma estrutura física adequada, com espaços seguros, salubres e organizados para a guarda e manutenção das

evidências, assegurando que a *"cadeia de custódia seja respeitada e que as provas possam ser utilizadas de forma confiável tanto pela acusação quanto pela defesa ao longo de todo o processo judicial"* (Medeiros, 2020, p. 20).

Visto que, as provas digitais podem ser extraídas de uma ampla variedade de dispositivos, incluindo os mais comuns, como celulares, computadores, HDs, CDs, DVDs, pen drives e cartões de memória. No entanto, também é possível obter informações cruciais por meio da análise de dados em equipamentos de rede, como modems, pontos de acesso (Access Points), roteadores e switches.

Cabe destacar também que os aparelhos digitais podem ser utilizados como ferramenta de apoio para o cometimento de crimes, bem como pode ser meio para o cometimento do crime. Nesses casos, o computador está associado ao modus operandi do crime. Assim, em muitos casos, *"exames forenses nesses equipamentos são uma excelente prova técnica, e os laudos produzidos tornam-se peças fundamentais para o convencimento do juiz na elaboração da sentença"* (Eleutério; Machado, 2019, p. 13).

Para efetivação das técnicas de investigação o equipamento é utilizado como meio para a prática do crime, tornando a execução possível apenas com o uso do dispositivo eletrônico. Trata-se de crimes intrinsecamente vinculados à tecnologia, nos quais os dispositivos desempenham um papel central na realização das atividades ilícitas.

Muitos pedófilos e usuários baixam e compartilham fotos e vídeos com esse tipo de conteúdo, caracterizando crime conforme a legislação vigente, especialmente o artigo 241-A do Estatuto da Criança e do Adolescente. Sem o computador e a Internet, tais condutas seriam inviáveis (Eleutério; Machado, 2019, p. 14).

Dentro dessa perspectiva, vale ressaltar que a legislação brasileira atual ainda não abrange todos os crimes cibernéticos. Esse desafio ocorre devido ao constante aperfeiçoamento das práticas ilícitas, como o roubo de dados e informações, conhecido como *phishing,* e a criação de programas específicos para roubo de senhas, os chamados *malwares.*

A perícia deve atentar-se tanto para a estrutura física do dispositivo quanto para o seu conteúdo, pois somente ao preservar a integridade de ambos é possível obter evidências de forma adequada. Nesse sentido, é importante destacar as características específicas das provas digitais.

Segundo Eleutério e Machado (2019, p. 46), *"as principais peculiaridades são: fragilidade, facilidade de cópia, sensibilidade ao tempo de vida e sensibilidade ao tempo de uso".* A contextualização afirmada pelos autores atestam que mesmo com todos os avanços e modernização as provas digitais podem sofrer perdas, causando prejuízos sem não forem resguardadas.

6. Avanços e desafios no período de 2014 a 2024 nas investigações digitais

O período entre 2014 e 2024 foi marcado por avanços significativos no campo das investigações digitais, com o desenvolvimento de tecnologias mais sofisticadas e ferramentas de análise que aumentaram a precisão e a eficácia na coleta de evidências digitais.

A implementação de tecnologias como inteligência artificial, blockchain e análise de big data ampliou as capacidades das equipes de investigação, permitindo a identificação mais rápida de padrões criminosos e a obtenção de provas mais robustas (Marr, 2017). Contudo, a evolução das tecnologias também trouxe desafios, especialmente no que diz respeito à preservação e à validade das evidências digitais.

O não cumprimento dessas regulamentações pode comprometer a admissibilidade das provas em tribunal, tornando o processo ainda mais complexo. Para tanto, algumas medidas precisam ser descritas pela seguridade legal que foi homologada para preservação e zelo da dignidade dos cidadãos, dentre as quais estão as menções feitas por Teffé (2017, p. 75) em relação a imagem:

> O direito à imagem como a faculdade de se utilizar a própria imagem, usando, dispondo ou reproduzindo-a, com ou sem caráter comercial, corolário lógico desta definição é a possibilidade, pelo titular do direito, de obstar reproduções indevidas de sua imagem por terceiros, de modo a resguardar este direito enquanto expressão dos interesses existenciais do indivíduo na condição de ser. (Teffé, 2017, p. 75)

Porém, a autora menciona neste contexto alguns aclaramentos no que concerne ao mundo comercial a respectiva imagem:

> Se o uso da imagem estiver ligado a intuito comercial ou econômico, mantém-se a regra do consentimento, inclusive com presunção de prejuízo à pessoa exposta, nos termos da Súmula n. 403 do STJ: "Independe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais". Se se tratar de uso para fins didáticos, científicos, jornalísticos e culturais, por outro lado, a regra tende a ser relativizada (Teffé, 2017, p. 183).

Neste contexto, Trivino (2024, p. 35) corrobora destacando que a violação do direito de imagem em seus termos *"clássicos",* ou seja, a *"utilização ou divulgação de materiais envolvendo imagem de certa pessoa sem sua autorização, independentemente de ser pela internet, cabe reparação ao indivíduo lesado",* a menos que a divulgação da imagem do indivíduo esteja amparada na legislação ou em hipóteses permitidas pela jurisprudência.

Na sequência um avanço pode ser mencionado nas questões de correspondência e telefonia que podem ser comprovadas, visto que Schreiber, Ribas e Mansur (2021, p. 251) destacam que o direito brasileiro vem consagrando proteção à correspondência desde sua primeira Constituição, em 1824, que, em texto limitado ("é inviolável o sigilo da correspondência e das telecomunicações telegráficas e telefônicas") buscava resguardar o merecido sigilo de informações.

Doravante, nas palavras enfatizadas por Alexandre de Moraes (2005, p. 161):

> O preceito que garante o sigilo de dados engloba o uso de informações decorrentes da informática. Essa nova garantia, necessária em virtude da existência de uma nova forma de armazenamento e transmissão de informações, deve coadunar-se com as garantias de intimidade, honra e dignidade humanas, de forma que se impeçam interceptações ou divulgações por meios ilícitos. (Moraes. 2005, p. 161)

Continuamente, frisa-se que outro avanço das investigações se faz considerando os dados e as informações pessoais enquanto uma *"expressão da personalidade de um indivíduo, existe relação intrínseca entre eles e a privacidade, e entre eles e a dignidade humana, por esse motivo, dados e informações sobre as pessoas são sigilosos e devem ser protegidos pelo direito",* com responsabilização daquele que, sem autorização, acessar ou utilizar dados de terceiros sem permissão (Trivino, 2024, p. 43).

Dentre os avanços relevantes foi a regulamentação da cadeia de custódia, especialmente com a promulgação do Pacote Anticrime no Brasil em 2019. A partir

dessa legislação, foram estabelecidos critérios específicos para a preservação e rastreabilidade das provas digitais, garantindo que a integridade das evidências seja mantida ao longo de todo o processo judicial. Essa evolução legislativa representa um importante marco na luta contra os crimes digitais, proporcionando mais segurança e confiabilidade ao material probatório (Brasil, 2019).

Entretanto no rol de desafios estão a perda ou a alteração de dados durante a coleta pode comprometer a integridade da prova e, consequentemente, a conclusão da investigação. Stallings (2019, p. 52) destaca que *"a preservação da integridade das evidências é essencial para sua aceitação em tribunal, especialmente em crimes que dependem exclusivamente de provas digitais".*

Além disso, o aumento do uso de criptografia e de redes de anonimato, como a darknet, tornou mais difícil para os investigadores rastrearem e identificar atividades ilícitas. Criminosos cibernéticos têm se aproveitado dessas tecnologias para ocultar suas ações e dificultar o trabalho das autoridades. Conforme observado por Whitman e Mattord (2017, p. 67), *"a criptografia e a anonimização representam barreiras significativas para a investigação digital, exigindo novas abordagens e ferramentas mais avançadas".*

Os avanços discorridos revelam que a inserção de aportes e discussões em relação ao decênio demonstram que investigações podem e devem ser executadas para o fortalecimento da cadeia de custódia e o desenvolvimento contínuo de tecnologias forenses, fundamentais para garantir a validade das provas digitais e a eficácia do combate aos crimes cibernéticos.

6. Conclusão

Ao chegar nas palavras que fecham o presente estudo, verifica-se que o avançar célere das tecnologias da informação possibilitou ao cidadão diversas interfaces, sejam elas relacionadas ao campo pessoal ou profissional, mas trouxe situações de insegurança em relação aos crimes efetivados, ampliando-se estratégias no campo das investigações digitais nesse último decênio.

Além disso, impulsionou o pensar em políticas públicas para resguardar a dignidade dos cidadãos com os resultados apresentados nas comprovações que podem ser atestadas no ordenamento jurídico brasileiro a partir das ações investigativas para proteger imagens, dados pessoais, redes sociais e outros aplicativos que são utilizados continuamente na sociedade tecnológica.

As tipificações penais devem ser promovidas nos processos de investigação digital, bem como a cadeia de custódia, pois os crimes cibernéticos neste percurso tecnológico devem ser combatidos e diminuídos, uma vez que essa alteração social é um caminho sem regressão com a internet.

Com os dados encontrados, é possível promover uma conscientização sobre as práticas digitais e os riscos associados aos crimes cibernéticos, beneficiando a sociedade em geral ao promover uma cultura de responsabilidade no uso da tecnologia, além de incentivar práticas seguras tanto no ambiente doméstico quanto no corporativo.

O conhecimento sobre investigações digitais e cadeia de custódia é fundamental para o profissional do Direito, pois assegura que ele esteja preparado para lidar com os desafios impostos pelos crimes digitais e pela crescente relevância das provas digitais em processos judiciais.

Além do mais, a apresentação dos resultados discursivos pela temática promove a socialização da execução da organização a ser feita para comprovar o crime efetivado pelas evidências digitais, correlacionando os aportes em relação a

cadeia de custódia, como fator de essencialidade para assegurar todo o aparato legal da prova diante da importância de solucionar prática criminal.

É de suma importância que o profissional do Direito esteja atualizado com as regulamentações específicas sobre proteção de dados e privacidade, a exemplo do Regulamento Geral de Proteção de Dados (GDPR) e a Lei Geral de Proteção de Dados (LGPD), com impacto direto nas investigações digitais.

Isso é particularmente relevante em casos de crimes cibernéticos, cujo manejo inadequado das provas pode violar direitos fundamentais, como o direito à privacidade, e comprometer o resultado do processo. O advogado que possui esse conhecimento pode proteger melhor os direitos de seus clientes e garantir que as investigações sigam os padrões legais adequados.

Por fim, menciona-se a importância de propagar para a sociedade a existência das investigações digitais e sua efetividade para garantir os direitos e princípios dos cidadãos que são vitimas de malícias criminais pelo uso das tecnologias.

Referências

ATZORI, L.; IERA, A.; MORABITO, G. The Internet of Things: A survey. **Computer Networks,** v. 54, n. 15, p. 2787-2805, 2017. Disponível em: https://doi:10.1016/j.comnet.2010.05.010. Acesso em: 10 set. 2024.

BADARÓ, G. H. R. I. A Cadeia de Custódia e sua Relevância para a Prova Penal. In: SIDI, R.; LOPES, A. B. (Orgs.). **Temas Atuais da Investigação Preliminar no Processo Penal.** Belo Horizonte: Editora D'Plácido, 2017. p. 522.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019.** Institui o Pacote Anticrime. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm. Acesso em: 10 nov. 2024.

CALOYANNIDES, M. A. **Computer Forensics and Privacy.** Artech House, Inc. 2001.

CARRIER, B., SPAFFORD, E. H. **Getting Physical with the Digital Investigation Process.** International Journal of Digital Evidence, Fall 2003, Volume 2, Issue 2, 2003.

CASTELLS, M. **A Sociedade em Rede.** São Paulo: Paz e Terra, 2018.

CAVALCANTE E SILVA. **A importância da revolução industrial no mundo da tecnologia**. 2011. Disponível em: https://www.unicesumar.edu.br/epcc-2011/wp content/uploads/sites/86/2016/07/zedequias_vieira_cavalcante2.pdf .Acesso em: 22. jun. 2024.

DAVENPORT, T. H.; PRUSAK, L. **Conhecimento Empresarial:** como as organizações gerenciam o seu capital intelectual. 17. ed. Rio de Janeiro: Elsevier, 2012.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a computação forense.** São Paulo: Novatec Editora, 2019.

EVANS, D. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. **Cisco Internet Business Solutions Group (IBSG).** 2018.

KROENKE, D. M.; AUER, D. J. **Database Concepts.** 9. ed. Boston: Pearson, 2020.
KURZWEIL, R. The Singularity is Near: When Humans Transcend Biology. New York: Penguin Books, 2019.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de Informação Gerenciais:** administrando a empresa digital. 16. ed. São Paulo: Pearson Prentice Hall, 2020.

LIMA, Renato Brasileiro de. **Manual de Processo Penal**. 6. ed. Salvador: JusPodivm, 2018. p.107.

LOBÃO SOBRINHA, Maria Quaranta de. **Cadeia de custódia das provas digitais:** a perícia técnica como instrumento das garantias. Monografia (Graduação em Direito). Universidade Federal de Sergipe. Sergipe, 2021.

LOPES JUNIOR, Aury. **Direito Processual Penal**. 11. ed. São Paulo: Saraiva, 2014. p.194.

MARR, B. **Data Strategy: How to Profit from a World of Big Data, Analytics and the Internet of Things.** London: Kogan Page, 2017.

MCNEELY, C. L.; POPE, A. W. Big Data as a Public Good: Digital Platforms, Technological Innovation, and the Circular Economy**. IEEE Access**, v. 6, p. 104000-104013, 2018.

MEDEIROS, Flávia. **Políticas de Perícia Criminal. Na garantia dos Direitos Humanos.** Friedrich Ebert Stiftung.2020. Disponível em: http://library.fes.de/pdf-files/bueros/brasilien/16396-20200811.pdf. Acesso em: 18 de out. 2024.

MENDONÇA, Matheus Henrique. **Breves exposições sobre a imprescindibilidade da cadeia de custódia forte nas provas digitais colhidas em sede policial.** 2022. Disponível em: https://jus.com.br/artigos/96452/breves-exposicoes-sobre-a-imprescindibilidade-da-cadeia-de-custodia-forte-nas-provas-digitais-colhidas-em-sede-policial/2. Acesso em: 14 de out. 2024.

MOORE, M. G.; KEARSLEY, G. **Distance Education:** A Systems View of Online Learning. 3. ed. Belmont: Wadsworth, 2012.

MORAES, Alexandre de. **Constituição do Brasil interpretada e legislação constitucional**. 5. ed. São Paulo: Atlas, 2005, p. 161.

NONAKA, I.; TAKEUCHI, H. **Criação do Conhecimento na Empresa**. Rio de Janeiro: Elsevier, 2008.

PRADO, G. L. M. **Prova penal e sistema de controles epistêmicos:** A quebra da cadeia de custódia das provas obtidas por métodos ocultos. São Paulo: Marcial Pons, 2014.

PRADO, G. L. M. **Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital,** 2021. Disponível em: https://geraldoprado.com.br/artigos/breves-notas-sobre-o-fundamento-constitucional-da-cadeia-de-custo dia-da-prova-digital/>. Acesso em: 15 out. 2024.

REIS, M. A. **Forense computacional e sua aplicação em segurança imunológica.** Dissertação (Mestrado em computação). Instituto de Computação. Universidade Estadual de Campinas, 2003.

RODRIGUES, Thalita Scharr. FOLTRAN JUNIOR, Dierone César. Análise de ferramentas forenses na investigação digital. **Revista de Engenharia e Tecnologia,** v. 2, n . 3, dez., 2010.

RUSSELL, S.; NORVIG, P. **Inteligência Artificial**. São Paulo: Elsevier, 2021.

STALLINGS, W. **Criptografia e Segurança de Redes:** Princípios e Prática. 7. ed. São Paulo: Pearson, 2019.

SCHREIBER, Anderson; RIBAS, Felipe; MANSUR, Rafael. Deepfakes: regulação e responsabilidade civil. **Revista Brasileira de Direito Civil – RBDCivil**, Belo Horizonte, v. 27, p. 251-277, jan.-mar. 2021.

TAUCHERT, Maicon Rodrigo; AMARAL Suely Galvão. **O avanço tecnológico do Judiciário como facilitador do acesso à justiça.** 2015. Disponível em: https://jus.com.br/artigos/44341/o-avanco-tecnologico-do-judiciario-como-facilitador-do-acesso-a-justica. Acesso em 1 jun. 2024.

TEFFÉ, Chiara Spadaccini de. Considerações sobre a proteção do direito à imagem na internet. **Revista de Informação Legislativa**, Brasília, v. 213, n. 54, p. 175, mar. 2017. Disponível em: https://www12.senado.leg.br/ril/edicoes/54/213/ril_v54_n213_p173. Acesso em: 24 nov. 2024.

TRIVINO, Aline Melsone Marcondes. **Crimes cibernéticos:** como a nova tecnologia desafia o direito penal brasileiro. Dissertação (Mestrado em Direito). Pontifícia Universidade Católica de São Paulo (PUC-SP). São Paulo, 2024.

TOURINHO FILHO, F. D. C. **Manual de processo penal.** 15. ed. São Paulo: Saraiva, 2012, p. 58-59

TURBAN, E. et al. **Information Technology for Management:** On-Demand Strategies for Performance, Growth and Sustainability. New York: Wiley, 2018.

WHITMAN, M. E.; MATTORD, H. J. **Principles of Information Security**. 6. ed. Boston: Cengage Learning, 2017.

ZUBOFF, S. **The Age of Surveillance Capitalism:** The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.