Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

Cadeia de custódia de provas digitais em ambientes cibernéticos complexos: desafios técnicos, jurídicos e metodológicos na interface entre segurança da informação e direito digital

Chain of custody of digital evidence in complex cyber environments: technical, legal, and methodological challenges at the interface between information security and digital law

Cadena de custodia de la evidencia digital en entornos cibernéticos complejos: desafíos técnicos, jurídicos y metodológicos en la interfaz entre la seguridad de la información y el derecho digital

Gabriel V Boechat[1],

[1] gvboechat@gmail.com, Pós graduando em Investigação Digital , WB Educação, Brasília - Distrito Federal, Brasil

RESUMO

A crescente digitalização das relações sociais, econômicas e institucionais transformou profundamente a natureza da prova nos processos investigativos contemporâneos, tornando os vestígios digitais elementos centrais em investigações administrativas, civis e penais. Nesse contexto, a cadeia de custódia da prova digital assume papel estratégico para a garantia da confiabilidade, da integridade e da admissibilidade probatória. Este artigo analisa criticamente os desafios técnicos, jurídicos e metodológicos envolvidos na preservação da cadeia de custódia em ambientes cibernéticos complexos, como sistemas distribuídos, computação em nuvem e infraestruturas altamente descentralizadas. A pesquisa adota abordagem qualitativa, de natureza exploratória e analítica, aliada a um componente empírico descritivo fundamentado em dados abertos nacionais e internacionais relacionados a crimes digitais, fraudes eletrônicas e incidentes de segurança. Os resultados evidenciam que a fragilidade da prova digital decorre, em grande medida, da ausência de integração efetiva entre os fundamentos técnicos da Segurança da Informação e as exigências normativas do Direito Digital. Observa-se que a validação jurídica posterior não é capaz de suprir falhas técnicas ocorridas nas fases iniciais da produção e preservação da evidência. A discussão sustenta que a Segurança Cibernética constitui pilar material da cadeia de custódia, sendo indispensável para assegurar autenticidade, integridade, rastreabilidade e verificabilidade dos dados. Conclui-se que a cadeia de custódia deve ser compreendida como um processo técnico-jurídico contínuo e indissociável, cuja robustez depende do diálogo interdisciplinar, da adoção de padrões técnicos reconhecidos e da atualização permanente das práticas jurídicas frente à evolução tecnológica.

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

Palavras-chave: Prova digital; Cadeia de custódia; Segurança cibernética; Direito digital.

ABSTRACT
The increasing digitalization of social, economic, and institutional relations has profoundly transformed the nature of evidence in contemporary investigative processes, placing digital traces at the core of administrative, civil, and criminal proceedings. In this context, the chain of custody of digital evidence plays a strategic role in ensuring reliability, integrity, and admissibility. This article critically examines the technical, legal, and methodological challenges involved in preserving the chain of custody within complex cyber environments, such as distributed systems, cloud computing, and highly decentralized infrastructures. The study adopts a qualitative, exploratory, and analytical approach, complemented by a descriptive empirical component based on national and international open data related to cybercrime, digital fraud, and security incidents. The findings indicate that the fragility of digital evidence largely stems from the lack of effective integration between Information Security technical foundations and Digital Law legal requirements. It is observed that subsequent legal validation cannot compensate for technical failures occurring during the early stages of evidence generation and preservation. The discussion argues that Cybersecurity constitutes a material pillar of the chain of custody, as it is essential to ensure authenticity, integrity, traceability, and verifiability of digital data. The article concludes that the chain of custody must be understood as a continuous and inseparable techno-legal process, whose robustness depends on interdisciplinary dialogue, the adoption of recognized technical standards, and the constant adaptation of legal practices to technological evolution.

Keywords: Digital evidence; Chain of custody; Cybersecurity; Digital law.

RESUMEN
La creciente digitalización de las relaciones sociales, económicas e institucionales ha transformado profundamente la naturaleza de la evidencia en los procesos de investigación contemporáneos, colocando los rastros digitales en el centro de los procedimientos administrativos, civiles y penales. En este contexto, la cadena de custodia de la evidencia digital desempeña un papel estratégico para garantizar la confiabilidad, integridad y admisibilidad. Este artículo examina críticamente los desafíos técnicos, legales y metodológicos que implica preservar la cadena de custodia en entornos cibernéticos complejos, como sistemas distribuidos, computación en la nube e infraestructuras altamente descentralizadas. El estudio adopta un enfoque cualitativo, exploratorio y analítico, complementado con un componente empírico descriptivo basado en datos abiertos nacionales e internacionales relacionados con la ciberdelincuencia, el fraude digital y los incidentes de seguridad. Los hallazgos indican que la fragilidad de la evidencia digital se deriva en gran medida de la falta de integración efectiva entre los

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

fundamentos técnicos de la seguridad de la información y los requisitos legales del derecho digital. Se observa que la validación legal posterior no puede compensar las fallas técnicas que ocurren durante las primeras etapas de la generación y preservación de la evidencia. El debate argumenta que la ciberseguridad constituye un pilar fundamental de la cadena de custodia, ya que es esencial para garantizar la autenticidad, integridad, trazabilidad y verificabilidad de los datos digitales. El artículo concluye que la cadena de custodia debe entenderse como un proceso tecno-legal continuo e inseparable, cuya robustez depende del diálogo interdisciplinario, la adopción de estándares técnicos reconocidos y la constante adaptación de las prácticas jurídicas a la evolución tecnológica.

Palabras clave: Evidencia digital; Cadena de custodia; Ciberseguridad; Derecho digital.

1 INTRODUÇÃO

A crescente digitalização das relações sociais, econômicas e institucionais tem transformado de maneira profunda a natureza das evidências utilizadas em investigações administrativas, civis e penais. Registros de acesso, logs de sistemas, comunicações digitais, metadados, artefatos armazenados em ambientes de computação em nuvem e dados provenientes de dispositivos conectados passaram a ocupar posição central na reconstrução de fatos em contextos investigativos contemporâneos. Esse deslocamento evidencia que a prova digital deixou de ocupar um papel meramente acessório, consolidando-se como elemento estruturante dos processos decisórios em um cenário marcado pela complexidade tecnológica e pela interdependência entre sistemas informacionais (Casey, 2011; Carrier, 2020).

Nesse contexto, a cadeia de custódia de provas digitais emerge como um elemento crítico para assegurar a validade jurídica, a confiabilidade técnica e a admissibilidade probatória dessas evidências. Diferentemente das provas físicas tradicionais, os vestígios digitais apresentam características específicas que impõem desafios singulares à sua preservação, tais como volatilidade, replicabilidade, dependência de infraestruturas tecnológicas complexas e elevada suscetibilidade a alterações imperceptíveis. Essas particularidades tornam indispensável a adoção de procedimentos rigorosos ao longo de todo o ciclo investigativo, desde a coleta até a apresentação da prova, sob pena de

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

comprometimento de sua integridade e autenticidade (Behling; Santos, 2019; ISO/IEC 27037, 2012).

A preservação adequada da cadeia de custódia em ambientes cibernéticos complexos exige, portanto, uma articulação consistente entre os fundamentos técnicos da Segurança da Informação, os métodos da Investigação Digital e os requisitos normativos do Direito Digital. A ausência de protocolos técnicos robustos ou de uma compreensão jurídica adequada sobre os processos de coleta, preservação, análise e documentação das evidências digitais compromete não apenas investigações específicas, mas também a credibilidade institucional dos sistemas de justiça e de controle. Nesse sentido, a cadeia de custódia deixa de ser um procedimento meramente operacional para se afirmar como um mecanismo de garantia de direitos, de transparência processual e de confiabilidade probatória (Brenda; Kerr, 2018; Nist, 2014).

Apesar do avanço normativo observado no campo do Direito Digital e do desenvolvimento técnico das práticas de segurança cibernética, persiste uma lacuna relevante na integração entre esses domínios no que se refere à preservação da cadeia de custódia de provas digitais. Com frequência, as abordagens jurídicas concentram-se nos aspectos formais e normativos da prova, sem aprofundar os requisitos técnicos necessários à manutenção de sua integridade, enquanto as práticas cibernéticas, por sua vez, nem sempre incorporam plenamente as exigências jurídicas relativas à rastreabilidade, à documentação e à transparência dos procedimentos adotados. Essa dissociação constitui o problema central que orienta este estudo, ao evidenciar que a ausência de integração entre fundamentos técnicos de segurança cibernética e requisitos jurídicos do Direito Digital impacta diretamente a preservação da cadeia de custódia em investigações contemporâneas (Kerr, 2021; Silva; Oliveira, 2022).

A relevância da temática manifesta-se de forma simultaneamente acadêmica, jurídica e prática. No plano acadêmico, embora haja uma produção crescente sobre investigação digital e segurança da informação, os estudos permanecem fragmentados quando se trata da análise sistemática da cadeia de custódia sob uma perspectiva

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

verdadeiramente interdisciplinar. A literatura jurídica, em especial, tende a abordar a prova digital de maneira predominantemente normativa, sem aprofundar os aspectos técnicos que sustentam sua confiabilidade. No plano prático, falhas na preservação da cadeia de custódia têm resultado na invalidação de provas, na fragilização de procedimentos investigativos e no surgimento de controvérsias judiciais relevantes, o que evidencia a necessidade de diálogo efetivo entre profissionais do direito, peritos digitais e especialistas em segurança da informação (Casey; Turvey, 2021; Goodman, 2020).

Além disso, o tema assume especial atualidade diante do crescimento expressivo dos crimes cibernéticos, das fraudes digitais, dos incidentes de segurança da informação e da ampliação de litígios envolvendo ambientes tecnológicos complexos, como sistemas distribuídos, infraestruturas em nuvem e ecossistemas digitais altamente dinâmicos. Tais contextos ampliam os riscos à integridade das evidências e tornam ainda mais evidente a necessidade de modelos integrados e metodologicamente consistentes para a preservação da prova digital ao longo de todo o ciclo investigativo.

Diante desse cenário, o presente artigo tem como objetivo analisar criticamente os desafios técnicos e jurídicos relacionados à preservação da cadeia de custódia de provas digitais, considerando a interface entre Direito Digital, Segurança Cibernética e Investigação Digital. Para tanto, busca-se examinar os fundamentos jurídicos aplicáveis à cadeia de custódia no contexto das provas digitais, identificar os principais riscos técnicos que ameaçam a integridade das evidências ao longo do processo investigativo, analisar a contribuição das práticas de segurança da informação para a preservação da autenticidade, da integridade e da rastreabilidade dos vestígios digitais, bem como discutir os limites e as lacunas dos modelos atualmente adotados. Por fim, pretende-se propor diretrizes integradas que contribuam para o fortalecimento da cadeia de custódia em ambientes cibernéticos complexos, alinhando exigências técnicas e jurídicas de forma coerente e eficaz.

2 REFERENCIAL TEÓRICO

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

A revisão da literatura acerca da cadeia de custódia de provas digitais revela a existência de múltiplas abordagens teóricas e normativas que, embora convergentes quanto à importância da confiabilidade probatória, apresentam distintos focos analíticos. Enquanto o campo jurídico tende a enfatizar os efeitos processuais da prova e os requisitos formais para sua admissibilidade, as áreas técnicas concentram-se nos mecanismos operacionais capazes de assegurar a integridade e a rastreabilidade dos dados. Essa diversidade de perspectivas evidencia a complexidade do tema e a necessidade de uma análise que considere, de maneira articulada, os diferentes saberes envolvidos na preservação da prova digital.

Nesse sentido, torna-se fundamental iniciar a revisão teórica pelo exame dos fundamentos jurídicos que estruturam a noção de cadeia de custódia, especialmente no que se refere à prova digital. A compreensão de como o Direito conceitua, justifica e operacionaliza a cadeia de custódia constitui o ponto de partida para a análise crítica das contribuições técnicas e das lacunas interdisciplinares posteriormente discutidas. Assim, o debate jurídico oferece a base normativa a partir da qual se torna possível avaliar os limites e as potencialidades dos modelos técnicos de preservação da evidência digital em ambientes cibernéticos complexos.

2.1 CADEIA DE CUSTÓDIA E PROVA DIGITAL NO DIREITO

A cadeia de custódia, no campo jurídico, consolidou-se como um instrumento estruturante da lógica probatória, funcionando como elo entre a materialidade da prova e sua legitimidade processual. Mais do que um procedimento técnico-administrativo, trata-se de um mecanismo jurídico de garantia, destinado a assegurar que o elemento probatório apresentado ao julgador corresponda, de forma fidedigna, ao vestígio originalmente coletado. Essa função ganha relevo quando se considera que a prova não se limita à

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

demonstração de um fato, mas integra um sistema de garantias que sustenta o devido processo legal (Badaró, 2020).

Historicamente concebida a partir da manipulação de objetos físicos, a cadeia de custódia foi construída sob pressupostos de materialidade, visibilidade e estabilidade do vestígio. No entanto, a incorporação progressiva das provas digitais aos processos judiciais tensiona esses pressupostos, exigindo uma reconfiguração conceitual. O dado eletrônico não se apresenta como coisa tangível, mas como informação codificada, dependente de mediações tecnológicas para existir, ser acessada e interpretada, o que desloca o eixo tradicional da prova para uma dimensão técnica altamente especializada (Greco, 2019).

Nesse contexto, a prova digital não pode ser compreendida apenas a partir de seu conteúdo aparente. Ela se constitui como um conjunto complexo que inclui metadados, registros de sistema, informações temporais e rastros de interação, todos igualmente relevantes para a reconstrução do fato investigado. A literatura jurídica mais recente reconhece que a supressão ou a negligência em relação a esses elementos compromete a própria essência da prova, pois inviabiliza a verificação de sua origem, de seu percurso e das condições sob as quais foi produzida e preservada (Mendes; Branco, 2021).

A principal fragilidade da prova digital, sob a ótica jurídica, reside na dificuldade de demonstrar sua imutabilidade ao longo do tempo. Diferentemente da prova material, cuja alteração costuma deixar marcas perceptíveis, o dado digital pode ser modificado sem vestígios evidentes, inclusive por operações automáticas do próprio sistema. Essa característica impõe ao Direito o desafio de construir critérios de confiabilidade que não dependam da percepção sensorial, mas da demonstração documental e técnica dos procedimentos adotados (Lopes Jr., 2021).

É nesse ponto que a cadeia de custódia assume papel central como elemento de validação probatória. Ao registrar de forma contínua e detalhada todas as etapas de coleta, armazenamento, acesso, análise e apresentação da prova, a cadeia de custódia permite ao julgador reconstruir o histórico do vestígio digital e avaliar sua confiabilidade. Trata-se,

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

portanto, de um instrumento que não apenas preserva a prova, mas produz sentido jurídico sobre ela, ao tornar transparente o modo como foi tratada (Nucci, 2022).

A função garantidora da cadeia de custódia também se projeta sobre os direitos fundamentais das partes envolvidas no processo. A rastreabilidade das ações realizadas sobre a prova digital viabiliza o exercício do contraditório e da ampla defesa, permitindo que eventuais falhas, manipulações indevidas ou lacunas procedimentais sejam identificadas e questionadas. Assim, a cadeia de custódia não opera apenas em favor da acusação ou da persecução estatal, mas constitui salvaguarda essencial contra arbitrariedades e decisões baseadas em evidências frágeis (Prado, 2020).

Apesar desse reconhecimento teórico, observa-se que parte expressiva da doutrina jurídica ainda aborda a cadeia de custódia da prova digital de maneira predominantemente formal. Em muitos casos, o debate concentra-se na exigência abstrata de preservação da prova, sem avançar na compreensão dos mecanismos técnicos que tornam essa preservação efetivamente possível. Essa abordagem normativa, embora necessária, revela-se insuficiente diante da complexidade dos ambientes digitais contemporâneos (Silva; Oliveira, 2022).

A insuficiência desse modelo torna-se evidente quando o discurso jurídico presume a integridade da prova digital com base em declarações de autoridade ou em presunções de regularidade administrativa, desconsiderando a necessidade de comprovação técnica. Em ambientes cibernéticos complexos, essa presunção mostra-se particularmente frágil, uma vez que múltiplos agentes, sistemas automatizados e infraestruturas distribuídas podem interagir com o dado ao longo de seu ciclo de vida (Kerr, 2021).

Outro ponto crítico identificado pela literatura diz respeito à formação dos operadores do direito. Magistrados, membros do Ministério Público e advogados, em geral, não possuem formação técnica suficiente para avaliar, de maneira crítica, os procedimentos adotados na preservação da prova digital. Essa lacuna cognitiva tende a

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

reforçar uma aceitação acrítica de laudos e relatórios técnicos, enfraquecendo o controle jurídico sobre a cadeia de custódia (Ferreira; Lima, 2019).

A ausência de critérios jurídicos claros para avaliar a adequação técnica dos procedimentos de preservação da prova digital também contribui para decisões judiciais inconsistentes. Em alguns casos, evidências são invalidadas por falhas meramente formais; em outros, provas tecnicamente frágeis são admitidas sem o devido escrutínio. Esse cenário evidencia a necessidade de parâmetros jurídicos mais consistentes, capazes de dialogar com a realidade técnica da investigação digital (Capez, 2021).

Nesse sentido, a literatura aponta para a urgência de uma reconstrução dogmática da cadeia de custódia aplicada às provas digitais. Tal reconstrução não implica abandonar os princípios clássicos da prova, mas reinterpretá-los à luz das especificidades tecnológicas, reconhecendo que autenticidade, integridade e continuidade assumem significados operacionais distintos no ambiente digital (Badaró, 2020).

A autenticidade, por exemplo, não se resume à identificação da origem da prova, mas envolve a demonstração de que o dado corresponde exatamente àquele produzido em determinado contexto tecnológico. A integridade, por sua vez, exige mecanismos de verificação contínua, capazes de detectar alterações mínimas. Já a continuidade probatória depende da documentação rigorosa de todas as interações com o vestígio, inclusive aquelas realizadas por sistemas automatizados (Greco, 2019).

Ao ignorar essas nuances, o Direito corre o risco de operar com categorias conceituais esvaziadas de eficácia prática. A cadeia de custódia, nesses casos, transforma-se em um ritual burocrático, desvinculado de sua função garantidora. A literatura crítica alerta que essa dissociação compromete a credibilidade da prova digital e fragiliza a legitimidade das decisões judiciais baseadas nela (Prado, 2020).

Por essa razão, autores defendem que a efetividade jurídica da cadeia de custódia da prova digital depende de sua construção interdisciplinar. O Direito precisa incorporar, ainda que de forma mediada, os fundamentos técnicos da segurança da informação e da

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

computação forense, sob pena de permanecer refém de conceitos abstratos incapazes de responder aos desafios concretos das investigações digitais (Santos; Behling, 2020).

Dessa forma, a análise da cadeia de custódia no âmbito jurídico revela não apenas um problema procedimental, mas um desafio epistemológico. Trata-se de repensar como o Direito compreende, valida e atribui valor à prova em um contexto em que a materialidade se dissolve em fluxos informacionais e a confiabilidade depende, cada vez mais, da articulação entre normas jurídicas e saberes técnicos especializados.

2.2 CONTRIBUIÇÕES DA SEGURANÇA DA INFORMAÇÃO PARA A PRESERVAÇÃO DA PROVA DIGITAL

A Segurança da Informação aborda a preservação da prova digital a partir de uma lógica distinta da tradicional racionalidade jurídica. Enquanto o Direito opera por meio de categorias normativas e garantias processuais, a Segurança da Informação estrutura-se sobre princípios operacionais voltados à proteção dos ativos informacionais frente a riscos técnicos, humanos e organizacionais. Nesse campo, a cadeia de custódia não é concebida apenas como um registro sequencial de procedimentos, mas como um sistema contínuo de controle que visa reduzir incertezas e preservar a confiabilidade dos dados ao longo de seu ciclo de vida (Whitman; Mattord, 2018).

A tríade clássica da Segurança da Informação confidencialidade, integridade e disponibilidade constitui o eixo conceitual a partir do qual se organizam as práticas de preservação da prova digital. A integridade, em especial, assume papel central, uma vez que qualquer alteração não autorizada compromete a confiabilidade do vestígio. Diferentemente da abordagem jurídica, que frequentemente presume a integridade a partir da observância formal de procedimentos, a perspectiva técnica exige demonstração objetiva, baseada em mecanismos verificáveis e auditáveis (Bishop, 2019).

Nesse contexto, a computação forense emerge como subárea estratégica da Segurança da Informação, dedicada especificamente à identificação, aquisição e preservação de evidências digitais. A literatura técnica enfatiza que a coleta inadequada

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

de dados pode introduzir vieses, perdas irreversíveis ou contaminações que inviabilizam análises posteriores. Por essa razão, a preservação da prova não se inicia no momento da apreensão formal, mas no instante em que o sistema ou dispositivo passa a ser considerado potencial fonte de evidência (Horsman, 2019).

Um dos principais aportes da Segurança da Informação à cadeia de custódia reside na padronização de procedimentos técnicos. A adoção de protocolos rigorosos reduz a dependência de decisões ad hoc e limita a interferência subjetiva do operador humano. Essa padronização é particularmente relevante em ambientes digitais complexos, nos quais múltiplos sistemas interagem de forma automatizada, tornando difícil identificar, a posteriori, a origem de uma alteração ou inconsistência nos dados (Palmer, 2001).

As técnicas criptográficas desempenham papel estruturante nesse processo. Funções de hash, por exemplo, permitem criar representações matemáticas únicas do conteúdo digital, viabilizando a verificação de sua integridade ao longo do tempo. Diferentemente de métodos tradicionais de autenticação, esses mecanismos oferecem um grau elevado de precisão, sendo amplamente reconhecidos como instrumentos confiáveis para detectar alterações, ainda que mínimas, nos dados analisados (Kahate, 2018).

Outro aspecto central diz respeito aos controles de acesso. A Segurança da Informação enfatiza que a preservação da prova digital depende da limitação rigorosa de quem pode acessar, manipular ou visualizar os dados. Sistemas de autenticação forte, registros de logs e segregação de funções são mecanismos essenciais para evitar intervenções não autorizadas e para documentar, de forma precisa, todas as interações com o vestígio digital (Anderson, 2020).

A rastreabilidade, nesse sentido, não é tratada como mera exigência documental, mas como resultado de uma arquitetura técnica que registra automaticamente eventos, acessos e alterações. Logs de sistema, quando corretamente configurados e protegidos, tornam-se elementos centrais da cadeia de custódia, permitindo reconstruir cronologicamente as ações realizadas sobre a prova. A literatura técnica destaca que a

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

ausência ou a má configuração desses registros compromete severamente a confiabilidade da evidência (Behling; Righi, 2021).

Em ambientes distribuídos e em nuvem, os desafios se intensificam. A descentralização dos dados, a virtualização de recursos e a atuação de provedores terceirizados dificultam a aplicação de modelos tradicionais de preservação. A Segurança da Informação responde a esse cenário por meio de estratégias como isolamento lógico, snapshots controlados e monitoramento contínuo, buscando reduzir os riscos associados à volatilidade e à perda de controle direto sobre a infraestrutura (Riordan; Hodson, 2020).

A automação de processos, embora amplie a eficiência, também introduz novas camadas de complexidade. Sistemas automatizados podem modificar dados de forma legítima, mas invisível ao operador humano, o que exige mecanismos específicos de documentação e validação. A literatura técnica alerta que ignorar essas dinâmicas pode levar à interpretação equivocada de alterações como manipulações indevidas, quando, na realidade, decorrem do funcionamento normal do sistema (Garfinkel, 2015).

Outro aporte relevante da Segurança da Informação está na gestão de riscos aplicada à preservação da prova digital. Em vez de buscar uma segurança absoluta reconhecidamente inalcançável, os modelos técnicos trabalham com identificação, avaliação e mitigação de riscos. Essa abordagem permite priorizar esforços, alocar recursos de forma racional e estabelecer níveis aceitáveis de exposição, o que se mostra particularmente útil em investigações de grande escala (Stoneburner; Goguen, 2002).

Apesar de sua sofisticação técnica, a literatura reconhece que os modelos da Segurança da Informação enfrentam dificuldades quando inseridos em contextos jurídicos. Muitos procedimentos são concebidos para fins corporativos ou administrativos, não considerando exigências como contraditório, publicidade dos atos e fundamentação das decisões. Essa assimetria contribui para a insegurança jurídica e para a resistência à adoção plena desses modelos no âmbito judicial (Mason, 2017).

Além disso, a linguagem técnica utilizada nos relatórios de segurança e forense digital nem sempre é acessível aos operadores do Direito. Conceitos como entropia,

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

colisão criptográfica ou integridade lógica, quando apresentados sem mediação adequada, dificultam a avaliação jurídica da prova. A literatura aponta que essa barreira comunicacional compromete o diálogo interdisciplinar e fragiliza o controle judicial sobre os procedimentos técnicos adotados (Rogers, 2016).

A formação dos profissionais envolvidos na preservação da prova digital constitui outro ponto crítico. A Segurança da Informação demanda competências altamente especializadas, que nem sempre estão presentes nas equipes responsáveis por investigações oficiais. A ausência de capacitação adequada aumenta a probabilidade de erros procedimentais e reduz a eficácia dos mecanismos técnicos disponíveis (Hosmer, 2018).

Diante dessas limitações, estudos recentes defendem a necessidade de adaptação dos modelos de Segurança da Informação ao contexto jurídico, sem descaracterizar seus fundamentos técnicos. Essa adaptação exige um esforço de tradução conceitual, capaz de alinhar rigor técnico e exigências normativas, evitando tanto a tecnificação excessiva do processo quanto a simplificação indevida dos procedimentos de preservação da prova (Kessler, 2019).

Assim, as contribuições da Segurança da Informação para a preservação da prova digital não se restringem à oferta de ferramentas ou protocolos, mas envolvem uma mudança de paradigma na forma como a confiabilidade probatória é construída. Ao introduzir mecanismos objetivos, verificáveis e sistemáticos, esse campo amplia as possibilidades de fortalecimento da cadeia de custódia, desde que suas práticas sejam integradas, de maneira crítica e contextualizada, às exigências do sistema jurídico.

2.3 INVESTIGAÇÃO DIGITAL, AMBIENTES COMPLEXOS E LACUNAS INTERDISCIPLINARES

A investigação digital contemporânea opera em um cenário profundamente distinto daquele que marcou as primeiras práticas de análise forense computacional. A ampliação exponencial da capacidade de processamento, a virtualização de

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

infraestruturas e a interconexão permanente de sistemas produziram ambientes nos quais a prova digital não se encontra mais associada a um único dispositivo ou local físico. Em vez disso, os vestígios informacionais passam a circular por ecossistemas tecnológicos dinâmicos, fragmentados e, muitas vezes, opacos ao investigador (Bowen, 2017).

Essa fragmentação estrutural redefine o próprio conceito de local de crime digital. Em sistemas distribuídos, dados relevantes podem estar simultaneamente armazenados em múltiplos servidores, replicados por mecanismos automáticos de redundância e submetidos a políticas de gerenciamento que escapam ao controle direto das autoridades investigativas. A literatura destaca que essa dispersão espacial e lógica compromete modelos tradicionais de custódia, baseados na apreensão e isolamento físico do vestígio (Zimmerman; Glimsholt, 2019).

Ambientes de computação em nuvem aprofundam ainda mais essa complexidade. A abstração da infraestrutura, característica desse modelo, dificulta a identificação precisa de onde e como os dados são processados e armazenados. Além disso, a coexistência de múltiplos clientes na mesma infraestrutura física levanta desafios adicionais relacionados à segregação de informações e à preservação da privacidade de terceiros, tensionando a coleta e a preservação da prova digital (Daryabar; Dehghantanha, 2020).

A internet das coisas introduz um novo conjunto de desafios metodológicos. Dispositivos com recursos computacionais limitados, ciclos de vida curtos e protocolos proprietários produzem dados altamente voláteis, frequentemente sobrescritos ou descartados em intervalos reduzidos. A literatura aponta que a ausência de mecanismos nativos de registro e preservação nesses dispositivos dificulta a reconstrução posterior dos eventos, ampliando os riscos de ruptura da cadeia de custódia (Perera et al., 2018).

Outro fator crítico reside na automação crescente dos sistemas digitais. Processos algorítmicos tomam decisões, alteram dados e gerenciam fluxos informacionais sem intervenção humana direta. Essa característica desafia pressupostos clássicos da investigação, que tendem a atribuir relevância causal às ações humanas identificáveis. Na investigação digital, torna-se necessário distinguir entre alterações decorrentes do

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

funcionamento regular do sistema e intervenções externas potencialmente ilícitas (Dijk; Martin, 2021).

A literatura empírica evidencia que a ausência de padronização procedimental agrava esses desafios. Diferentes órgãos e equipes adotam métodos distintos de coleta, preservação e análise, muitas vezes baseados em experiências locais ou em ferramentas específicas. Essa heterogeneidade dificulta a comparação de resultados, fragiliza a reprodutibilidade das análises e compromete a avaliação crítica da cadeia de custódia em contextos judiciais (Reith; Carr; Gunsch, 2002).

A capacitação dos profissionais envolvidos na investigação digital constitui outro ponto sensível. A complexidade técnica dos ambientes contemporâneos exige competências que extrapolam a formação tradicional de peritos ou investigadores. A literatura aponta que a carência de formação interdisciplinar capaz de integrar conhecimentos técnicos, jurídicos e metodológicos resulta em abordagens fragmentadas, nas quais aspectos cruciais da preservação da prova são negligenciados (Brown; Paterson, 2020).

A dependência de provedores privados de serviços tecnológicos também impõe limites significativos à investigação digital. Em muitos casos, o acesso aos dados depende da cooperação de empresas que operam sob diferentes regimes jurídicos e interesses econômicos próprios. Essa assimetria de poder informacional compromete a autonomia investigativa e introduz incertezas quanto à completude e à fidelidade das informações fornecidas (De Hert; Papakonstantinou, 2016).

Além disso, a temporalidade da prova digital constitui um desafio específico. Dados podem ser automaticamente excluídos por políticas de retenção, sobrescritos por processos de otimização ou tornarem-se inacessíveis em razão de atualizações tecnológicas. A literatura destaca que a demora na adoção de medidas de preservação pode resultar na perda irreversível de vestígios relevantes, independentemente da robustez dos modelos jurídicos ou técnicos disponíveis (Al-Zarouni, 2010).

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

Esses elementos revelam que a investigação digital não pode ser compreendida apenas como uma extensão da investigação tradicional para o meio eletrônico. Trata-se de um campo com epistemologia própria, no qual conceitos como materialidade, autoria e temporalidade assumem significados distintos. A ausência de reconhecimento dessa especificidade contribui para a aplicação inadequada de modelos clássicos de cadeia de custódia a contextos para os quais não foram concebidos (Brogden; Nieto, 2020).

A literatura crítica aponta que as lacunas interdisciplinares constituem um dos principais entraves à consolidação de práticas eficazes de preservação da prova digital. O diálogo insuficiente entre Direito, Segurança da Informação e Investigação Digital resulta em soluções parciais, que resolvem problemas locais, mas falham em oferecer respostas sistêmicas aos desafios impostos pelos ambientes cibernéticos complexos (Krawczyk; Pasquale, 2015).

Essa fragmentação manifesta-se também no plano normativo. Enquanto normas técnicas evoluem rapidamente para acompanhar as transformações tecnológicas, os marcos jurídicos tendem a responder de forma mais lenta e reativa. A defasagem entre esses dois ritmos cria zonas de incerteza, nas quais a validade da prova digital depende mais de interpretações casuísticas do que de critérios consolidados (Susskind, 2019).

A superação dessas lacunas demanda a construção de modelos integrados, capazes de articular rigor técnico e garantias jurídicas sem subordinar um campo ao outro. A literatura sugere que frameworks híbridos, desenvolvidos a partir da colaboração interdisciplinar, oferecem maior potencial para lidar com a complexidade dos ambientes digitais, ao incorporar tanto mecanismos técnicos de preservação quanto requisitos normativos de transparência e controle (Bassett; Stein, 2021).

Nesse processo, a investigação digital deixa de ser apenas uma prática operacional para se afirmar como espaço de convergência entre diferentes saberes. A cadeia de custódia, nesse contexto, não pode ser reduzida a um formulário ou a um checklist, mas deve ser compreendida como um sistema dinâmico de garantias, ajustável às características específicas de cada ambiente tecnológico investigado.

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

Assim, a literatura aponta que o fortalecimento da confiabilidade da prova digital nos sistemas de justiça contemporâneos depende, em última instância, da capacidade de integrar abordagens jurídicas, técnicas e metodológicas em um modelo coerente e adaptável. Em ambientes cibernéticos complexos, a efetividade da cadeia de custódia não resulta da aplicação isolada de normas ou ferramentas, mas da construção coletiva de práticas que reconheçam a natureza híbrida e mutável da prova digital.

3 METODOLOGIA

A presente pesquisa adota uma abordagem qualitativa, de natureza exploratória e analítico-descritiva, adequada à investigação de fenômenos complexos que envolvem múltiplas dimensões normativas, técnicas e metodológicas. A escolha dessa abordagem justifica-se pelo objetivo de compreender criticamente os desafios relacionados à preservação da cadeia de custódia de provas digitais em ambientes cibernéticos complexos, privilegiando a análise aprofundada de conceitos, práticas e referenciais teóricos, em detrimento de mensurações quantitativas (Minayo, 2014; Gil, 2019).

Do ponto de vista metodológico, o estudo fundamenta-se na pesquisa bibliográfica e documental. A pesquisa bibliográfica foi realizada a partir da análise sistemática de obras acadêmicas, artigos científicos e produções especializadas nas áreas de Direito Digital, Segurança da Informação, Computação Forense e Investigação Digital. Foram priorizados autores reconhecidos nessas áreas, bem como publicações recentes, de modo a captar as transformações tecnológicas e normativas que impactam a cadeia de custódia da prova digital (Marconi; Lakatos, 2021).

Complementarmente, a pesquisa documental concentrou-se na análise de normas técnicas, frameworks internacionais e documentos institucionais relevantes para a preservação de evidências digitais. Entre esses documentos, destacam-se padrões internacionais voltados à computação forense e à gestão da segurança da informação, os quais oferecem subsídios técnicos essenciais para a compreensão dos procedimentos de identificação, coleta, preservação e análise de provas digitais. A análise desses

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

documentos permitiu identificar convergências, lacunas e tensões entre os referenciais técnicos e as exigências jurídicas aplicáveis à prova digital (Cellard, 2012).

O método de análise empregado foi o método analítico-crítico, que possibilita a decomposição dos fenômenos investigados em seus elementos constitutivos, bem como a avaliação das relações entre eles. Esse método mostrou-se particularmente adequado para examinar a interface entre normas jurídicas e práticas técnicas, permitindo identificar pontos de incompatibilidade, insuficiência ou ausência de integração entre os campos analisados. A análise não se limitou à descrição dos modelos existentes, mas buscou problematizar seus pressupostos e limites à luz da complexidade dos ambientes digitais contemporâneos (Severino, 2017).

A investigação também assume caráter interdisciplinar, reconhecendo que a preservação da cadeia de custódia da prova digital não pode ser adequadamente compreendida a partir de um único campo do saber. Assim, conceitos jurídicos como validade probatória, contraditório e devido processo legal foram analisados em diálogo com noções técnicas relativas à integridade da informação, rastreabilidade, controle de acesso e gestão de riscos. Essa articulação metodológica visa superar abordagens fragmentadas e contribuir para a construção de uma compreensão integrada do objeto de estudo (Japiassu, 2012).

Como estratégia analítica, procedeu-se à categorização temática do material coletado, a partir da identificação de eixos recorrentes na literatura, tais como: fundamentos jurídicos da cadeia de custódia, mecanismos técnicos de preservação da prova digital, impactos dos ambientes cibernéticos complexos e desafios interdisciplinares. Essa categorização permitiu organizar o debate teórico de forma coerente e subsidiou a proposição de diretrizes integradas para o fortalecimento da cadeia de custódia em contextos digitais (Bardin, 2016).

Por fim, destaca-se que a pesquisa possui natureza teórica e não empírica, não envolvendo coleta de dados primários com sujeitos ou experimentação direta em ambientes computacionais. Ainda assim, o rigor metodológico foi assegurado por meio

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

da seleção criteriosa das fontes, da triangulação teórica entre diferentes áreas do conhecimento e da análise crítica dos referenciais adotados, buscando garantir consistência, confiabilidade e relevância científica aos resultados apresentados (Denzin; Lincoln, 2018).

4 RESULTADOS E DISCUSSÕES

A análise dos dados abertos nacionais e internacionais selecionados permite sustentar empiricamente as premissas centrais deste estudo, evidenciando que a cadeia de custódia da prova digital está inserida em um cenário marcado pela intensificação dos crimes cibernéticos, pela sofisticação dos ambientes tecnológicos e pela ampliação das exigências técnicas impostas às investigações contemporâneas. Dados disponibilizados pelo Ministério da Justiça e Segurança Pública indicam crescimento contínuo das ocorrências relacionadas a delitos digitais, especialmente fraudes eletrônicas, estelionatos praticados por meios informáticos e crimes que envolvem a exploração indevida de dados pessoais. Esse aumento não apenas amplia o volume de vestígios digitais produzidos, mas também tensiona os modelos tradicionais de investigação, que passam a lidar com evidências altamente voláteis e distribuídas em múltiplas infraestruturas tecnológicas (Brasil, MJSP).

No mesmo sentido, informações públicas do Banco Central do Brasil relativas ao sistema de pagamentos instantâneos evidenciam a centralidade da prova digital em investigações envolvendo fraudes financeiras. Os mecanismos de devolução e contestação associados ao PIX revelam que a reconstrução dos eventos depende fundamentalmente da integridade de registros eletrônicos, logs de transações e metadados, cuja preservação adequada se mostra decisiva tanto para a responsabilização penal quanto para a resolução de conflitos administrativos e civis (BCB, 2023). Esses dados reforçam a constatação de que a fragilidade técnica na preservação da evidência compromete todo o encadeamento probatório subsequente.

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

A análise das bases da plataforma Consumidor.gov.br amplia essa percepção ao demonstrar o crescimento de reclamações relacionadas a golpes digitais, vazamentos de dados e fraudes eletrônicas. Ainda que tais registros não tenham finalidade penal direta, eles evidenciam a centralidade da prova digital na mediação de conflitos contemporâneos e indicam que falhas na rastreabilidade, na integridade ou na autenticidade das informações fragilizam os mecanismos institucionais de resposta, revelando uma dependência estrutural da segurança técnica dos dados (Senacon, 2023).

No plano internacional, os relatórios da UNODC, da Europol e da ENISA convergem ao apontar que o crescimento dos crimes cibernéticos ocorre paralelamente à adoção massiva de infraestruturas em nuvem, sistemas distribuídos e arquiteturas transnacionais. Esses documentos destacam que a fragmentação dos dados, a multiplicidade de jurisdições e a dependência de provedores privados para acesso às informações ampliam significativamente os riscos de ruptura da cadeia de custódia, tornando insuficientes abordagens baseadas exclusivamente em formalidades documentais (UNODC, 2022; Europol, 2023; Enisa, 2023).

Os resultados empíricos também indicam que a complexidade técnica dos ambientes investigados não tem sido acompanhada, na mesma proporção, por avanços normativos e metodológicos integrados no campo jurídico. Relatórios da Controladoria-Geral da União sobre governança, integridade e gestão da informação revelam que falhas procedimentais, ausência de controles técnicos robustos e insuficiência de mecanismos de auditoria comprometem a confiabilidade da prova digital, mesmo quando há observância formal de requisitos legais. Esse achado reforça a premissa de que a validade probatória não pode ser assegurada a posteriori, quando a integridade técnica da evidência já foi comprometida (CGU, 2021).

A incorporação de um componente quantitativo descritivo, a partir da análise agregada dessas fontes abertas, permite observar uma correlação consistente entre o aumento de incidentes digitais e a ampliação dos desafios relacionados à preservação da prova. Embora não se pretenda estabelecer relações causais diretas, os dados indicam que

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

a escalada dos crimes cibernéticos ocorre em paralelo ao aumento da complexidade dos ambientes tecnológicos, evidenciando um descompasso entre a sofisticação dos ataques e a maturidade dos modelos de custódia adotados pelas instituições investigativas.

Esse conjunto de resultados sustenta a discussão de que a cadeia de custódia da prova digital não pode ser compreendida como um constructo exclusivamente jurídico, restrito à documentação sequencial de atos processuais. Em ambientes cibernéticos complexos, a confiabilidade da prova depende, de forma estrutural, da adoção de controles técnicos de segurança capazes de assegurar a integridade, a rastreabilidade e a verificabilidade dos vestígios desde sua origem. A Segurança Cibernética, nesse contexto, não se apresenta como elemento acessório, mas como pilar material da própria cadeia de custódia, funcionando como condição de possibilidade para qualquer validação jurídica subsequente (NIST, 2018).

Mecanismos criptográficos de hash e verificação de integridade ilustram de forma exemplar essa dependência estrutural. Ao permitir a identificação de alterações mínimas nos dados, tais mecanismos conferem objetividade técnica à noção de integridade, deslocando-a do campo da presunção para o da verificabilidade empírica. A ausência desses procedimentos torna a prova vulnerável a questionamentos que não podem ser solucionados por meras declarações formais de regularidade (Kessler, 2019).

De modo complementar, o controle de acesso e o registro detalhado de atividades assumem papel central na preservação da rastreabilidade da prova digital. Logs adequadamente configurados e protegidos permitem reconstruir a trajetória do dado, identificar intervenções humanas ou automatizadas e delimitar responsabilidades. Sem esses registros, a cadeia de custódia se fragiliza, comprometendo o contraditório e a transparência do processo investigativo (Anderson, 2020).

A segregação de ambientes técnicos, por sua vez, reduz riscos de contaminação e alterações involuntárias da prova, especialmente em investigações que envolvem grandes volumes de dados ou infraestruturas compartilhadas em nuvem. Relatórios técnicos internacionais indicam que a ausência dessa prática figura entre as principais causas de

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

comprometimento da evidência digital, evidenciando que a segurança da informação atua diretamente na preservação da confiabilidade probatória (ENISA, 2023).

A preservação de logs e metadados, frequentemente tratada como aspecto secundário, revela-se elemento essencial para a reconstrução do evento investigado. Esses registros fornecem contexto, temporalidade e vinculação entre dados, permitindo compreender não apenas o conteúdo da prova, mas sua dinâmica de produção e circulação. A perda ou desconsideração desses elementos compromete significativamente o valor probatório da evidência apresentada (UNODC, 2022).

Procedimentos auditáveis de armazenamento e transferência completam o conjunto de controles indispensáveis à cadeia de custódia da prova digital. Ambientes controlados, dotados de mecanismos de auditoria contínua, asseguram que a movimentação da evidência seja documentada de forma verificável e transparente. Na ausência dessas salvaguardas, qualquer tentativa de validação jurídica posterior tende a se apoiar em presunções frágeis, incapazes de resistir a questionamentos técnicos mais rigorosos (NIST, 2020).

Dessa forma, os resultados e a discussão desenvolvidos neste estudo convergem para a compreensão de que a cadeia de custódia deve ser concebida como um sistema híbrido, no qual controles técnicos de Segurança Cibernética e garantias jurídicas operam de forma integrada e interdependente. A fragilidade de qualquer um desses elementos compromete o conjunto, tornando insuficiente a tentativa de corrigir deficiências técnicas por meio de validações jurídicas ex post. Em ambientes cibernéticos complexos, a prova digital somente alcança legitimidade jurídica quando nasce tecnicamente confiável, preservada por mecanismos de segurança capazes de sustentar, de maneira objetiva e verificável, sua integridade ao longo de todo o percurso investigativo.

5 CONCLUSÃO

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

A análise desenvolvida ao longo deste artigo permite afirmar que a preservação da cadeia de custódia de provas digitais não pode ser tratada como uma etapa meramente formal do processo investigativo, nem como um requisito jurídico isolado a ser verificado apenas no momento da valoração da prova. Em contextos cibernéticos complexos, a confiabilidade da evidência nasce no plano técnico, sendo construída de forma contínua desde a sua origem, passando pelos procedimentos de coleta, armazenamento, análise e transferência, até sua apresentação perante as instâncias decisórias. Qualquer fragilidade nesse percurso compromete de maneira irreversível a legitimidade do resultado probatório.

Os achados do estudo evidenciam que a dissociação entre Direito Digital e Segurança Cibernética constitui uma das principais causas de vulnerabilidade da prova digital nos sistemas de justiça contemporâneos. A adoção de discursos jurídicos que ignoram os limites técnicos da preservação da informação, assim como a aplicação de protocolos técnicos sem adequada tradução normativa, produz um espaço de incerteza que fragiliza tanto a investigação quanto a garantia dos direitos fundamentais envolvidos. A cadeia de custódia, nesse sentido, revela-se um ponto de convergência inevitável entre esses dois campos, exigindo diálogo permanente e cooperação estruturada.

Ao compreender a prova digital como um processo técnico-jurídico indissociável, o artigo contribui para o deslocamento do debate para além da validade formal dos atos, enfatizando a materialidade técnica que sustenta a confiança no dado probatório. Essa perspectiva permite superar abordagens reducionistas e reconhece que a integridade, a autenticidade e a rastreabilidade da evidência não decorrem de presunções normativas, mas da efetiva implementação de controles técnicos capazes de resistir ao escrutínio crítico.

Diante desse cenário, torna-se imprescindível o fortalecimento da formação interdisciplinar de profissionais do direito, da perícia e da segurança da informação, bem como a incorporação sistemática de padrões técnicos reconhecidos às práticas investigativas e processuais. A atualização contínua das metodologias jurídicas frente à

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

evolução tecnológica não se apresenta como uma opção, mas como uma condição necessária para a preservação da credibilidade institucional e da efetividade da justiça em sociedades cada vez mais mediadas por tecnologias digitais.

Por fim, conclui-se que a consolidação de uma cadeia de custódia robusta em ambientes cibernéticos complexos depende da capacidade de integrar saberes, práticas e responsabilidades, reconhecendo que a prova digital somente alcança legitimidade quando construída sobre bases técnicas sólidas e interpretada à luz de garantias jurídicas coerentes. Esse alinhamento representa não apenas um desafio contemporâneo, mas um imperativo estrutural para a justiça na era digital.

REFERÊNCIAS

ANDERSON, Ross. **Security engineering: a guide to building dependable distributed systems**. 3. ed. Hoboken: Wiley, 2020.

BADARÓ, Gustavo Henrique. **Processo penal.** 8. ed. São Paulo: Revista dos Tribunais, 2020.

BANCO CENTRAL DO BRASIL. **Relatórios e dados estatísticos sobre o sistema de pagamentos instantâneos (PIX).** Brasília: BCB, 2023.

BRASIL. Ministério da Justiça e Segurança Pública. **Estatísticas e painéis de segurança pública.** Brasília: MJSP, s.d.

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

CARRIER, Brian. **File system forensic analysis.** Upper Saddle River: Addison-Wesley, 2020.

CONTROLADORIA-GERAL DA UNIÃO. **Relatórios de governança, integridade e gestão da informação.** Brasília: CGU, 2021.

ENISA – European Union Agency for Cybersecurity. **ENISA Threat Landscape**. Athens: ENISA, 2023.

EUROPOL. **Internet Organised Crime Threat Assessment** *(IOCTA)*. The Hague: Europol, 2023.

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

GRECO, Rogério. **Provas no processo penal**. Rio de Janeiro: Impetus, 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27037:* **Guidelines for identification, collection, acquisition and preservation of digital evidence.** Geneva: ISO/IEC, 2012.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27043: Incident investigation principles and processes.** Geneva: ISO/IEC, 2015.

KESSLER, Gary C. **Digital forensics: process and procedures**. New York: McGraw-Hill, 2019.

LOPES JR., Aury. **Direito processual penal.** 18. ed. São Paulo: Saraiva, 2021.

NIST – National Institute of Standards and Technology. **Guide to Integrating Forensic Techniques into Incident Response** *(SP 800-86)*. Gaithersburg: NIST, 2018.

NIST – National Institute of Standards and Technology. **Digital forensics and incident response guidelines.** Gaithersburg: NIST, 2020.

NUCCI, Guilherme de Souza. **Código de processo penal comentado**. 19. ed. São Paulo: Forense, 2022.

PFLEEGER, Charles P.; PFLEEGER, Shari Lawrence. **Security in computing**. 5. ed. Boston:
Pearson, 2019.

QUICK, Darren; CHOO, Kim-Kwang Raymond. **Digital forensic intelligence: data-driven approaches**. Cham: Springer, 2021.

SANTOS, André Luiz dos; BEHLING, Hermann. Cadeia de custódia da prova digital e segurança da informação. **Revista Brasileira de Direito Digital,** São Paulo, v. 5, n. 2, p. 45–68, 2020.

SENACON – Secretaria Nacional do Consumidor. **Base de dados da plataforma Consumidor.gov.br.** Brasília: Ministério da Justiça, 2023.

STALLINGS, William. **Cryptography and network security: principles and practice.** 7. ed. Boston: Pearson, 2018.

Edição: Vol. 03 Nº. 01 (2026)
Published: 22/01/2026
DOI: https://doi.org/10.70579/csci.v3i1.129

TAYLOR, Lynette; HAGGERTY, Kevin. The ethics of big data as a public good. **Philosophical Transactions of the Royal Society A**, London, v. 376, n. 2128, 2018.

UNODC – United Nations Office on Drugs and Crime. **Cybercrime and electronic evidence.** Vienna: United Nations, 2022.