II ENCONTRO NACIONAL DE DIREITO DO FUTURO - II ENDIF

DIREITO PENAL E TECNOLOGIA I

D598
Direito penal e tecnologia I [Recurso eletrônico on-line] organização II Encontro Nacional de Direito do Futuro: Escola Superior Dom Helder Câmara – Belo Horizonte;

Coordenadores: Camila Martins de Oliveira e Gabriela Emanuele de Resende – Belo Horizonte: Escola Superior Dom Helder Câmara - ESDHC, 2025.

Inclui bibliografia
ISBN: 978-65-5274-383-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: Justiça social e tecnológica em tempos de incerteza.
1. Direito do Futuro. 2. Justiça Social. 3. Justiça Tecnológica. I. II Encontro Nacional de Direito do Futuro (1:2025 : Belo Horizonte, MG).

CDU: 34

Dom Helder
CENTRO UNIVERSITÁRIO

II ENCONTRO NACIONAL DE DIREITO DO FUTURO - II ENDIF

DIREITO PENAL E TECNOLOGIA I

Apresentação

O II Encontro Nacional de Direito do Futuro (II ENDIF), organizado pelo Centro Universitário Dom Helder com apoio técnico do Conselho Nacional de Pesquisa e Pós-graduação em Direito – CONPEDI, reafirma-se como um espaço qualificado de produção, diálogo e circulação do conhecimento jurídico, reunindo a comunidade científica em torno de um propósito comum: pensar, com rigor metodológico e sensibilidade social, os caminhos do Direito diante das transformações que marcam o nosso tempo. Realizado nos dias 09 e 10 de outubro de 2025, em formato integralmente on-line, o evento assumiu como tema geral "Justiça social e tecnológica em tempos de incerteza", convidando pesquisadoras e pesquisadores a enfrentar criticamente os impactos da inovação tecnológica, das novas dinâmicas sociais e das incertezas globais sobre as instituições jurídicas e os direitos fundamentais.

Nesta segunda edição, os números evidenciam a força do projeto acadêmico: 408 trabalhos submetidos, com a participação de 551 pesquisadoras e pesquisadores, provenientes de 21 Estados da Federação, culminando na organização de 31 e-books, que ora se apresentam à comunidade científica. Essa coletânea traduz, em linguagem acadêmica e compromisso público, a vitalidade de uma pesquisa jurídica que não se limita a descrever problemas, mas busca compreendê-los, explicar suas causas e projetar soluções coerentes com a Constituição, com os direitos humanos e com os desafios contemporâneos.

A publicação dos 31 e-books materializa um processo coletivo que articula pluralidade temática, densidade teórica e seriedade científica. Os textos que compõem a coletânea passaram por avaliação acadêmica orientada por critérios de qualidade e imparcialidade, com destaque para o método double blind peer review, que viabiliza a análise inominada dos trabalhos e exige o exame por, no mínimo, dois avaliadores, reduzindo subjetividades e preferências ideológicas. Essa opção metodológica é, ao mesmo tempo, um gesto de respeito à ciência e uma afirmação de que a pesquisa jurídica deve ser construída com transparência, responsabilidade e abertura ao escrutínio crítico.

O II ENDIF também se insere em uma trajetória institucional já consolidada: a primeira edição, realizada em junho de 2024, reuniu centenas de pesquisadoras e pesquisadores e resultou na publicação de uma coletânea expressiva, demonstrando que o Encontro se consolidou, desde o início, como um dos maiores eventos científicos jurídicos do país. A

continuidade do projeto, agora ampliada em escopo e capilaridade, reafirma a importância de se fortalecer ambientes acadêmicos capazes de integrar graduação e pós-graduação, formar novas gerações de pesquisadoras e pesquisadores e promover uma cultura jurídica comprometida com a realidade social.

A programação científica do evento, organizada em painéis temáticos pela manhã e Grupos de Trabalho no período da tarde, foi concebida para equilibrar reflexão teórica, debate público e socialização de pesquisas. Nos painéis, temas como inteligência artificial e direitos fundamentais, proteção ambiental no sistema interamericano, proteção de dados e herança digital foram tratados por especialistas convidados, em debates que ampliam repertórios e conectam a produção acadêmica aos dilemas concretos vividos pela sociedade.

A programação científica do II ENDIF foi estruturada em dois dias, 09 e 10 de outubro de 2025, combinando, no período da manhã, painéis temáticos com exposições de especialistas e debates, e, no período da tarde, sessões dos Grupos de Trabalho. No dia 09/10 (quinta-feira), após a abertura, às 09h, realizou-se o Painel I, dedicado aos desafios da atuação processual diante da inteligência artificial ("Inteligencia artificial y desafios de derechos fundamentales en el marco de la actuación procesal"), com exposição de Andrea Alarcón Peña (Colômbia) e debate conduzido por Caio Augusto Souza Lara. Em seguida, às 11h, ocorreu o Painel II, voltado à proteção ambiental no Sistema Interamericano, abordando a evolução da OC-23 ao novo marco da OC-32, com participação de Soledad Garcia Munoz (Espanha) e Valter Moura do Carmo como palestrantes, sob coordenação de Ricardo Stanziola Vieira. No período da tarde, das 14h às 17h, desenvolveram-se as atividades dos Grupos de Trabalho, em ambiente virtual, com apresentação e discussão das pesquisas aprovadas.

No dia 10/10 (sexta-feira), a programação manteve a organização: às 09h, foi realizado o Painel III, sobre LGPD e a importância da proteção de dados na sociedade de vigilância, com exposições de Laís Furuya e Júlia Mesquita e debate conduzido por Yuri Nathan da Costa Lannes; às 11h, ocorreu o Painel IV, dedicado ao tema da herança digital e à figura do inventariante digital, com apresentação de Felipe Assis Nakamoto e debate sob responsabilidade de Tais Mallmann Ramos. Encerrando o evento, novamente no turno da tarde, das 14h às 17h, seguiram-se as sessões dos Grupos de Trabalho on-line, consolidando o espaço de socialização, crítica acadêmica e amadurecimento das investigações apresentadas.

Ao tornar públicos estes 31 e-books, o II ENDIF reafirma uma convicção essencial: não há futuro democrático para o Direito sem pesquisa científica, sem debate qualificado e sem compromisso com a verdade metodológica. Em tempos de incerteza — tecnológica, social,

ambiental e institucional —, a pesquisa jurídica cumpre um papel civilizatório: ilumina problemas invisibilizados, questiona estruturas naturalizadas, qualifica políticas públicas, tensiona o poder com argumentos e oferece horizontes normativos mais justos.

Registramos, por fim, nosso reconhecimento a todas e todos que tornaram possível esta obra coletiva — autores, avaliadores, coordenadores de Grupos de Trabalho, debatedores e equipe organizadora —, bem como às instituições e redes acadêmicas que fortalecem o ecossistema da pesquisa em Direito. Que a leitura desta coletânea seja, ao mesmo tempo, um encontro com o que há de mais vivo na produção científica contemporânea e um convite a seguir construindo, com coragem intelectual e responsabilidade pública, um Direito à altura do nosso tempo.

Belo Horizonte-MG, 16 de dezembro de 2025.

Prof. Dr. Paulo Umberto Stumpf – Reitor do Centro Universitário Dom Helder

Prof. Dr. Franclim Jorge Sobral de Brito – Vice-Reitor e Pró-Reitor de Graduação do Centro Universitário Dom Helder

Prof. Dr. Caio Augusto Souza Lara – Pró-Reitor de Pesquisa do Centro Universitário Dom Helder

A (IN) UTILIZAÇÃO DO CÓDIGO HASH NAS PROVAS DIGITAIS

THE (IN)USE OF THE HASH CODE IN DIGITAL EVIDENCE

Lívia Silveira Sousa

Resumo

A pesquisa objetiva evidenciar a relevância da documentação da cadeia de custódia no processo penal, com foco nas provas digitais e na utilização do algoritmo hash. A partir da Lei nº 13.964/2019, analisa-se sua aplicação como instrumento de preservação da integridade probatória. Assim, a ausência de regulamentação legislativa sobre vestígios digitais compromete a efetividade da cadeia de custódia. O estudo aborda o hash sob perspectiva técnica, demonstrando sua função essencial para evitar a invalidação de provas. Conclui-se que a observância da cadeia de custódia assegura a legitimidade penal. A metodologia é hipotético-dedutiva, qualitativa e jurídico-interpretativa.

Palavras-chave: Provas digitais, Documentação, Cadeia de custódia, Hash, Processo penal

Abstract/Resumen/Résumé

The research aims to demonstrate the relevance of chain of custody documentation in criminal proceedings, focusing on digital evidence and the use of the hash algorithm. Based on Law No. 13,964/2019, its application is analyzed as an instrument for preserving evidentiary integrity. The absence of legislative regulation regarding digital traces compromises the effectiveness of the chain of custody. The study addresses the hash from a technical perspective, demonstrating its essential role in preventing evidence invalidation. Compliance with the chain of custody ensures legal legitimacy. The methodology is hypothetical-deductive, qualitative, and legal-interpretative.

Keywords/Palabras-claves/Mots-clés: Digital evidence, Documentation, Chain of custody, Hash, Criminal procedure

1. INTRODUÇÃO

A presente pesquisa objetiva analisar o uso do código *hash* como mecanismo de garantia da confiabilidade e da integridade das provas digitais, assegurando a adequada documentação da cadeia de custódia. Ressalte-se que a necessidade de registrar formalmente os elementos probatórios digitais enfrenta obstáculos, sobretudo pela ausência de legislação que estabeleça de maneira obrigatória e tecnicamente procedimentalizada o tratamento desse tipo de vestígio. Tal lacuna tem gerado debates no campo jurídico, uma vez que a Lei nº 13.964/2019 (Pacote Anticrime), ao dispor sobre a documentação da cadeia de custódia da prova, restringiu-se a abordá-la de forma genérica e apenas no que se refere a vestígios físicos e materiais, sem contemplar as especificidades dos vestígios digitais.

A prova é essencial ao processo, pois verifica a veracidade dos fatos submetidos ao juízo para a formação de seu livre convencimento. O avanço tecnológico impacta diretamente a atividade processual, já que a crescente presença de meios digitais amplia os vestígios de natureza digital.

Nesse cenário, a prova digital consiste em dados e informações armazenados em dispositivos eletrônicos, relacionados a fatos físicos ou virtuais, como registros de celulares e computadores, capturas de tela, mensagens, vídeos e imagens.

Cumpre destacar que a prova digital possui características próprias que as distinguem das demais modalidades probatórias, o que reforça a necessidade de preservar sua integridade. Assim, já se encontram disponíveis mecanismos voltados à garantia de sua autenticidade, como o código *hash*.

Evidencia-se, ainda, que a inutilização de meios adequados para a preservação da evidência digital, como o código *hash*, compromete sua admissibilidade e pode violar princípios processuais, como o devido processo legal, a ampla defesa, o contraditório e o direito à prova, o que pode resultar em precedentes duvidosos e, até mesmo, em condenações injustas.

Por fim, o estudo em questão refere-se à vertente metodológica hipotético-dedutiva, de Severino (2007), Marconi e Lakatos (2009). Em relação ao raciocínio desenvolvido, o dialético prevalece e, quanto ao gênero da pesquisa, adotou-se a qualitativa. Já no tipo genérico de pesquisa, foi escolhido o tipo jurídico-interpretativo (Gustin; Dias; Nicácio, 2020).

2. A DOCUMENTAÇÃO DA CADEIA DE CUSTÓDIA E AS PROVAS DIGITAIS

A princípio, é importante destacar a definição e a finalidade da cadeia de custódia da prova. Esse instituto jurídico está previsto nos artigos 158-A e seguintes do Código de Processo Penal, introduzidos pela Lei nº 13.964/2019 (Pacote Anticrime), que regulamenta a documentação dos elementos probatórios. A cadeia de custódia consiste no registro detalhado de todas as etapas pelas quais um vestígio passa, desde sua coleta até o eventual descarte (Sousa, 2025).

Nesse sentido, a cadeia de custódia da prova tem como principal objetivo assegurar a integridade, a confiabilidade e a veracidade do vestígio, possibilitando sua inserção no processo penal de maneira segura e livre de vícios que possam comprometer a validade da prova ou gerar decisões judiciais controversas.

Todavia, observa-se que a regulamentação trazida pelo Pacote Anticrime aborda de forma genérica apenas os vestígios físicos e materiais, deixando de contemplar as particularidades técnicas envolvidas na cadeia de custódia da prova digital. Diante dessa lacuna normativa no ordenamento jurídico brasileiro e da necessidade de garantir a idoneidade da evidência digital, torna-se imprescindível a observância de normas técnicas específicas, como a ABNT ISO/IEC 27027:2013, que estabelece diretrizes para a coleta e preservação adequados desse tipo de vestígio, assegurando sua confiabilidade e admissibilidade no processo penal (Sousa, 2025).

A adequada documentação da prova digital é imprescindível, sobretudo por suas características específicas, como a imaterialidade, volatilidade e suscetibilidade à clonagem. A imaterialidade decorre do fato de a prova digital não possuir forma física palpável. A volatilidade relaciona-se à instabilidade e às constantes alterações a que está sujeita. A suscetibilidade de clonagem, por sua vez, refere-se à facilidade com que as informações podem ser copiadas e transferidas para outros dispositivos (Vaz, 2012, p. 66-70) (Sousa, 2025). Essas particularidades diferenciam a prova digital de maneira significativa em relação às provas físicas.

Diante dessas peculiaridades, torna-se evidente a necessidade de um cuidado redobrado na documentação da prova digital. Embora ainda não exista, no ordenamento jurídico brasileiro, um regramento legal específico e obrigatório que estabeleça padrões para esse tipo de prova, já se reconhece a adoção de mecanismos técnicos amplamente utilizados e aceitos, como o algoritmo *hash*.

3. O CÓDIGO *HASH* COMO MEIO DE DOCUMENTAÇÃO E CONFIABILIDADE DO ELEMENTO DIGITAL

O código *hash* teve sua origem na década de 1950, inicialmente no contexto das chamadas tabelas de dispersão, uma estrutura de dados projetada para armazenar e recuperar informações de maneira rápida e eficiente. Com o avanço da tecnologia, os algoritmos *hash* passaram por um processo de evolução, passando a ser utilizados não apenas na organização de dados, mas também como ferramentas essenciais para a garantia da integridade da informação, tornando-se componentes fundamentais na segurança de sistemas digitais (ElemarJR [s.d]).

Desse modo, um *hash* é uma função criptográfica que transforma um conjunto de dados em uma sequência única de caracteres. Essa sequência é geralmente expressa em formato hexadecimal, composta por uma combinação de números de 0 a 9 e letras de A a F (Avelar et al., 2024).

O referido meio de documentação do vestígio digital visa assegurar a integridade do dispositivo eletrônico, impedindo alterações no conteúdo desde a coleta. Para tanto, a autoridade responsável pela apreensão da prova digital deve realizar a cópia integral do documento, *bit* a *bit*. Assim, qualquer modificação ocorrida ao longo da investigação, ainda que mínima, resultará em um valor *hash* distinto daquele gerado na coleta (Almeida, 2011, p. 29) (Moreira, 2023) (STJ, AgRg no HC nº 143.169/RJ, 2021).

> Funções *hash* são algoritmos matemáticos determinísticos que mapeiam dados de comprimento aleatório em saída de tamanho fixo em base hexadecimal, dispersando os *bits* de entrada de forma não correlacionada às mudanças. Ou seja, uma pequena mudança na entrada, seja um simples caractere em uma frase inteira, ou um pixel em uma foto, acarreta uma saída completamente diferente, sendo essa característica conhecida como Efeito Avalanche (Silva; Silva, 2018, p. 20-21).

O Superior Tribunal de Justiça reconhece a utilização do código *hash*, diante de sua confiabilidade e relevância. *In verbis*:

> PENAL E PROCESSUAL PENAL. AGRAVO REGIMENTAL NO RECURSO ORDINÁRIO EM HABEAS CORPUS. OPERAÇÃO OPEN DOORS. FURTO, ORGANIZAÇÃO CRIMINOSA E LAVAGEM DE DINHEIRO. ACESSO A DOCUMENTOS DE COLABORAÇÃO PREMIADA. FALHA NA INSTRUÇÃO DO HABEAS CORPUS. CADEIA DE CUSTÓDIA. INOBSERVÂNCIA DOS PROCEDIMENTOS TÉCNICOS NECESSÁRIOS A GARANTIR A INTEGRIDADE DAS FONTES DE PROVA ARRECADADAS PELA POLÍCIA. FALTA DE DOCUMENTAÇÃO DOS ATOS REALIZADOS NO TRATAMENTO DA PROVA. CONFIABILIDADE COMPROMETIDA. PROVAS INADMISSÍVEIS, EM CONSEQUÊNCIA. AGRAVO REGIMENTAL PARCIALMENTE PROVIDO PARA PROVER TAMBÉM EM PARTE O RECURSO ORDINÁRIO. [...] 2. A principal finalidade da cadeia de custódia é garantir que os vestígios deixados no mundo material por uma infração penal correspondem exatamente àqueles arrecadados pela polícia, examinados e

> apresentados em juízo. 3. Embora o específico regramento dos arts. 158-A a 158-F do CPP (introduzidos pela Lei 13.964/2019) não retroaja, a necessidade de preservar a cadeia de custódia não surgiu com eles. Afinal, a ideia de cadeia de custódia é logicamente indissociável do próprio conceito de corpo de delito, constante no CPP desde a redação original de seu art. 158. Por isso, mesmo para fatos anteriores a 2019, é necessário avaliar a preservação da cadeia de custódia. **4. A autoridade policial responsável pela apreensão de um computador (ou outro dispositivo de armazenamento de informações digitais) deve copiar integralmente (*bit* a *bit*) o conteúdo do dispositivo, gerando uma imagem dos dados: um arquivo que espelha e representa fielmente o conteúdo original. 5. Aplicando-se uma técnica de algoritmo *hash*, é possível obter uma assinatura única para cada arquivo, que teria um valor diferente caso um único *bit* de informação fosse alterado em alguma etapa da investigação, quando a fonte de prova já estivesse sob a custódia da polícia. Comparando as *hashes* calculadas nos momentos da coleta e da perícia (ou de sua repetição em juízo), é possível detectar se o conteúdo extraído do dispositivo foi modificado.** [...] (STJ - AgRg no RHC: 143169 RJ 2021/0057395-6, Data de Julgamento: 07/02/2023, T5 - QUINTA TURMA, Data de Publicação: DJe 02/03/2023 – grifos meus).

Não obstante esse reconhecimento, a adoção do *hash* como meio de documentação probatória não pode ser imposta de forma obrigatória, tampouco servir como condição exclusiva para atestar a autenticidade da prova digital. Tal exigência violaria os princípios da liberdade probatória e da livre apreciação das provas pelo juízo, restringindo, de maneira indevida, o conjunto probatório assegurado pelo ordenamento jurídico brasileiro (Sousa, 2025).

Destaca-se que essa forma de documentação da prova digital apresenta desafios no que se refere à sua estruturação. Isso porque a coleta adequada do elemento probatório em meio tecnológico, com a utilização do código *hash*, exige elevado grau de instrução, rigor, técnica e competência específica. Essa incumbência recai sobre as autoridades encarregadas da coleta do vestígio, como policiais e peritos, competindo-lhes o dever de manter constante atualização no que tange a melhoria de práticas e atuação profissional (Sousa, 2025).

O cenário ideal para o processo penal brasileiro pressupõe a criação de uma legislação específica que regulamente, de forma padronizada e obrigatória, os procedimentos relativos à documentação da cadeia de custódia da prova digital. Tal normatização deve contemplar a adoção de métodos capazes de verificar a integridade e a autenticidade dos vestígios digitais, como a aplicação de algoritmos *hash*, a fim de assegurar que esses elementos probatórios sejam inseridos no processo judicial com a devida segurança jurídica, evitando, assim, a ocorrência de nulidades processuais.

Nesse contexto, torna-se evidente que a utilização de técnicas adequadas para a correta identificação, coleta, aquisição e preservação dos vestígios digitais impacta diretamente na *força probandi* da evidência. Cada etapa do manuseio da prova deve ser rigorosamente

documentada, especialmente diante das peculiaridades dos dados digitais, como sua vulnerabilidade a alterações, efemeridade e volatilidade (Badaró, 2021, p. 2) (Sousa, 2025).

A observância de rigor técnico, que em um cenário ideal seria estabelecida em norma legal, configura-se como condição indispensável para o correto detalhamento da cadeia de custódia dos vestígios digitais. Tal exigência visa resguardar a integridade do processo penal, prevenindo decisões judiciais fundadas em provas potencialmente adulteradas, seja por dolo, seja por erro técnico acidental.

A manipulação indevida dos vestígios, independentemente de sua origem intencional ou acidental, compromete de forma substancial a confiabilidade da evidência digital e, por conseguinte, sua admissibilidade como meio de prova. A aceitação de vestígios cuja cadeia de custódia não tenha sido devidamente documentada ou que apresente falhas nos requisitos de integridade e autenticidade inaugura precedentes duvidosos, capazes de gerar condenações questionáveis, fomentar a insegurança jurídica e fragilizar a credibilidade do sistema de justiça penal. Ademais, tal prática configura uma afronta direta a princípios basilares, como o devido processo legal e o direito à prova.

4. CONSIDERAÇÕES FINAIS

A Lei nº 13.964/2019, ao acrescentar os artigos 158-A e seguintes ao Código de Processo Penal, tratou da matéria de forma genérica, sem disciplinar especificamente a documentação da cadeia de custódia da prova digital. Todavia, a relevância desse elemento probatório para a persecução penal é incontestável, uma vez que, por meio dele, busca-se a verdade processual dos fatos, garantindo a efetividade do sistema de justiça criminal. Nessa perspectiva, as partes do processo também têm o direito de ver assegurada a licitude da prova, sendo que, no caso dos vestígios digitais, sua confiabilidade pode ser garantida por métodos de documentação, como a utilização do código *hash*.

Diante disso, o cenário ideal consistiria no estabelecimento, por norma legal, de critérios técnicos e obrigatórios para a coleta, aquisição e preservação do vestígio digital, sob pena de sua inutilização. Assim, seria possível assegurar, com elevado grau de confiabilidade, a integridade e a autenticidade da prova digital admitida no processo penal.

Destaca-se que lacuna normativa existente no ordenamento jurídico contribui para o aumento da insegurança jurídica, haja vista que a inexistência de um procedimento legal e

obrigatório acarreta divergências quanto à aceitação, no processo penal, de vestígios digitais não documentados ou documentados de forma deficiente.

Sob tal ótica, a ausência de previsão legal acaba por remeter à aplicação de normas técnicas, a exemplo da ABNT ISSO/IEC 27027:2013, que dispõe sobre diretrizes voltadas à documentação e à preservação da cronologia da prova digital. Todavia, por não possuir caráter vinculante, essa normativa não é observada de forma uniforme nos processos penais. Como consequência, a cadeia de custódia da prova digital nem sempre é rigorosamente respeitada, o que acarreta insegurança processual e viola princípios fundamentais – como o devido processo legal e o direito à prova –, diante da possibilidade de que elementos probatórios não devidamente verificados em sua integridade e confiabilidade resultem em precedentes duvidosos e condenações controvertidas, sejam absolutórias ou condenatórias.

Fica evidente, pois, as consequências da inutilização de técnicas que deveriam ser obrigatórias no ordenamento jurídico brasileiro para assegurar a confiabilidade do elemento probatório digital, como o uso do algoritmo *hash*. Torna-se, assim, imprescindível a adoção de métodos que garantam a integridade da prova digital, possibilitando sua inserção segura no processo e assegurando às partes transparência, autenticidade e integridade. Dessa forma, preserva-se, de modo efetivo, o direito constitucional ao devido processo legal.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Rafael Nader de. **Perícia Forense Computacional: Estudo das técnicas utilizadas para coleta e análise de vestígios digitais**, 2011. 48 f. Monografia (Graduação) – Faculdade de Tecnologia de São Paulo, São Paulo, 2011.

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

BADARÓ, Gustavo. **Processo Penal**. 9 ed. São Paulo: RT, 2021.

BADARÓ, Gustavo Henrique Righi Ivahy. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim IBCCRIM**, São Paulo, 2021.

BRASIL. **Decreto-Lei n. 3.689**, de 03 de outubro de 1941. Código de Processo Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 20 set. 2025.

BRASIL. **Lei nº 13.964**, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 20 set. 2025.

BRASIL. Superior Tribunal de Justiça. **AgRg no RHC n. 143.169/RJ**. Relator: Ministro Messod Azulay Neto, Relator para acórdão Ministro Ribeiro Dantas. Quinta Turma. Diário de Justiça Eletrônico, 02 de março de 2023. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202100573956&dt_publicacao=28/03/2023. Acesso em: 15 set. 2025

ELEMAR Jr. Tabelas Hash: Desvendando a Eficiência na Busca e Acesso a Dados. **ElemarJR**. Rio Grande do Sul, [*s.d*].

INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL. **Manual do Usuário para o Registro Eletrônico de Programas de Computador**. Rio de Janeiro: INPI, 2019. Disponível em: https://www.ufsm.br/app/uploads/sites/399/2019/07/Manual-INPI-Programa-de-Computador.pdf. Acesso em: 15 set. 2025.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 6. ed. São Paulo: Atlas, 2009.

MOREIRA, Rômulo de Andrade. Manutenção da Cadeia de Custódia da prova pelo STJ. **Revista Bonijuris**, Curitiba, ano 35, 682 ed., jun./jul. 2023.

OLIVEIRA, Vinicius Machado de. **ISO 27037 Diretrizes para identificação, coleta, aquisição e preservação de evidência digital**. Academia Forense Digital, [*S.l.*], 01 jan. 2019. Disponível em: https://academiadeforensedigital.com.br/iso-27037-identificacao-coleta-aquisicao-e-preservacao-de-evidencia/. Acesso em: 11 set. 2025.

ROCHA, Anacélia Santos et al. **O dom da produção acadêmica**: manual de normalização e metodologia da pesquisa. Belo Horizonte: Escola Superior Dom Helder Câmara, 2016. Disponível em: https://eje.treba.jus.br/pluginfile.php/1634/mod_page/content/66/dom_da_producao%20%281%29.pdf. Acesso em: 11 set. 2025.

SEVERINO, Joaquim Antônio. **Metodologia do trabalho científico**. 23. ed. rev. atual. São Paulo: Cortez, 2007.

SILVA, Johan Matos Coelho da; SILVA, Philipe Matos Coelho da. **Técnicas de detecção e classificação de malwares baseada na visualização de binários**, 2018. 80 f. Monografia (Graduação) - Faculdade de Tecnologia, Universidade de Brasília, Brasília, 2018.

SOUSA, Lívia Silveira. **A cadeia de custódia nas provas digitais**. 2025. 50f. Monografia (Graduação) – Faculdade de Direito, Centro Universitário Dom Helder, Belo Horizonte, 2025.

VAZ, Denise Provazi. **Provas digitais no processo penal**: formulação do conceito, definição das características e sistematização do procedimento probatório. Tese (Doutorado em Direito). 350f. São Paulo. Universidade de São Paulo, São Paulo, 2012.

VAZ, Millena Ferreira. A preservação da cadeia de custódia como pressuposto de admissibilidade da prova digital. **Revista da ESMESC**, v.30, n.36, p.323-350, 2023.