A CADEIA DE CUSTÓDIA DE PROVAS DIGITAIS E AS LACUNAS NA LEGISLAÇÃO

Nicoly Helena de Souza[1]
Orientador (a): Giselle Batista Leite[2]

Resumo: O presente Trabalho de Conclusão de Curso aborda a cadeia de custódia das provas digitais no Processo Penal, tema de crescente relevância diante do avanço tecnológico que transformou a forma de obtenção e valoração das provas. As provas digitais, por sua natureza intangível e facilmente alterável, impõem desafios à legislação processual penal brasileira, ainda moldada sob um paradigma analógico. Conforme ressalta Badaró (2021), a integridade das evidências digitais depende de protocolos técnicos rigorosos, sob pena de comprometimento de sua validade judicial. O estudo analisa criticamente a insuficiência normativa existente para garantir a confiabilidade e a rastreabilidade das provas digitais, bem como as consequências jurídicas dessa lacuna, que se traduzem em insegurança e risco de nulidade probatória. A distinção entre prova física e digital é destacada como elemento central para compreender a inadequação das regras do Código de Processo Penal (CPP), concebidas para vestígios materiais. Essa deficiência tem sido reconhecida em precedentes do Superior Tribunal de Justiça (STJ), que apontam falhas na observância da cadeia de custódia digital como fundamento para exclusão de provas. O objetivo geral é demonstrar a fragilidade do ordenamento jurídico diante da ausência de regulamentação específica, evidenciando a necessidade de parâmetros técnicos e jurídicos que assegurem a confiabilidade probatória. A metodologia adotada foi a pesquisa bibliográfica e documental, pautada em doutrinadores como Renato Marcão (2023) e Aury Lopes Jr. (2025). Conclui-se pela necessidade de aperfeiçoamento legislativo e procedimental, com destaque para o Projeto de Lei nº 4.939/2020 e a adoção de normas da ABNT, Procedimentos Operacionais Padrão (POPs) e da Ata Notarial como instrumentos para mitigar riscos de nulidade e assegurar a integridade das provas digitais no Processo Penal.

Palavras-chave: Cadeia de Custódia; Prova Digital; Integridade da Prova; Inadmissibilidade de Prova; Lacuna Legislativa.

Sumário: Introdução; Provas digitais no processo penal; 1. Desafios técnicos; 1.1. Reconhecimento jurisprudencial da validade da prova digital; 1.2. Cadeia de custódia da prova no ordenamento jurídico; 2. Princípios aplicáveis à cadeia de custódia; 2.1. Especificidades da cadeia de custódia digital; 2.2. Lacunas na legislação brasileira e impactos práticos das lacunas legais; 3. Impactos práticos e a invalidação da prova digital; 3.1. Caminhos para o aperfeiçoamento normativo e procedimental; 4. Boas práticas nacionais; 4.1. Conclusão; Referências.

[1] Discente do Curso de Direito da Faculdade Afya Sete Lagoas.
[2] Doutoranda em Proteção dos Direitos Fundamentais (UIT). Mestre em Intervenção Penal e Garantismo (PUC Minas). Pós-graduada em Direito Público (ANAMAGES). Professora universitária. Advogada. E-mail: giselle.leite@afya.com.br.

INTRODUÇÃO

O presente trabalho tem como tema a cadeia de custódia das provas digitais no Processo Penal, inserido em um contexto de profunda transformação tecnológica que expandiu o conceito tradicional de prova antes restrito a elementos físicos e materiais. Com a incorporação crescente de tecnologias da informação no cotidiano social e institucional, as provas digitais passaram a ocupar papel central na persecução penal, exigindo análise jurídica e técnica diferenciada em razão de sua natureza desmaterializada, volátil e facilmente manipulável, conforme adverte Badaró (2021). A fragilidade dessas evidências, aliada à ausência de protocolos específicos de coleta e conservação, suscita questionamentos quanto à sua confiabilidade e validade processual, gerando um novo campo de tensão entre tecnologia e devido processo legal.

Nesse cenário, surge o problema que orienta a presente pesquisa: a legislação processual penal brasileira revela-se insuficiente para assegurar a integridade e a autenticidade das provas digitais, ocasionando insegurança jurídica e risco de nulidade probatória, como reconhecido em precedentes do Superior Tribunal de Justiça (STJ). A problemática torna-se ainda mais relevante à medida que a dinâmica da criminalidade digital desafia os instrumentos tradicionais de produção e controle de prova, exigindo respostas normativas compatíveis com a realidade tecnológica contemporânea.

O objetivo geral deste trabalho é demonstrar a distinção entre provas físicas e digitais, evidenciando a fragilidade do ordenamento jurídico brasileiro diante da ausência de regulamentação específica sobre a cadeia de custódia digital e a necessidade de criação de procedimentos técnicos aptos a preservar a confiabilidade das evidências eletrônicas. Como objetivos específicos, busca-se: (i) distinguir a natureza, a forma de obtenção e os riscos inerentes às provas digitais em comparação com as provas físicas; (ii) examinar o tratamento jurisprudencial conferido pelo STJ à validade das provas digitais; (iii) explorar a estrutura normativa da cadeia de custódia e seus princípios orientadores; (iv) identificar lacunas legais e seus reflexos práticos no processo penal; e (v) propor mecanismos de aperfeiçoamento, com base em boas práticas técnicas e legislativas.

O marco teórico adota a análise da prova digital sob a perspectiva do Processo Penal contemporâneo, com ênfase nas vulnerabilidades relacionadas à sua volatilidade e à necessidade de rastreabilidade. Argumenta-se que a inobservância de procedimentos técnicos e jurídicos adequados compromete a cadeia de custódia, afetando diretamente a confiabilidade, a autenticidade e a admissibilidade da prova digital. A pesquisa fundamenta-se

em doutrinadores como Renato Marcão (2023), Aury Lopes Jr. (2025), Gustavo Badaró (2021), Cristiane Vieira da Silva e José Augusto Bezerra Lopes (2025), além de decisões paradigmáticas do STJ. A metodologia adotada é bibliográfica e documental, voltada à análise crítica da insuficiência normativa e da defasagem do sistema processual penal brasileiro em relação aos avanços tecnológicos e às demandas de celeridade e segurança jurídica.

Por fim, o trabalho organiza-se em seções interdependentes. A primeira apresenta o conceito e as características da prova digital, contrapondo-a à prova física. A segunda analisa os desafios técnicos e o reconhecimento jurisprudencial da validade da prova digital. A terceira aborda a estrutura da cadeia de custódia prevista no Código de Processo Penal e destaca suas limitações frente à realidade digital. Na sequência, são discutidos os impactos práticos dessa lacuna, como nulidades e insegurança jurídica. Por fim, propõem-se caminhos para o aperfeiçoamento legislativo e técnico, com destaque para o Projeto de Lei Federal nº 4.939/2020, as normas da ABNT, os Procedimentos Operacionais Padrão (POPs) e a Ata Notarial, instrumentos capazes de mitigar riscos e consolidar um padrão mínimo de preservação probatória compatível com o Processo Penal digital.

1. Provas digitais no processo penal

No âmbito do Processo Penal a prova pode ser entendida como um conjunto de elementos probatórios para o livre convencimento motivado do julgador, ou seja, tudo aquilo que as partes irão apresentar para o juiz, para convencê-lo a respeito da ação penal. Renato Marcão argumenta que “trata-se de uma reconstrução histórica subjetivo-objetiva que tem por escopo demonstrar as razões e a dinâmica do fato passado” (Marcão, 2023, p.194).

O termo prova, originado do latim *probatio*, refere-se ao processo de verificação e exame que constitui o "panorama mais seguro para se ter uma noção do que se passou no plano da realidade" (Nucci, 2024, p.403). Ainda segundo Guilherme de Souza Nucci, a prova está relacionada ao convencimento. Ou seja, se a prova for convincente, presume-se que o fato ocorreu conforme retratado.

Aury Lopes argumenta que as provas são os meios através dos quais se fará essa reconstrução do fato passado crime (Lopes Júnior, 2025, p.399). O tema probatório é sempre a afirmação de um fato (passado), não sendo as normas jurídicas, como regra, tema de prova (Lopes Júnior, 2025, p.399). Nessa perspectiva, as provas buscam reconstruir o crime, buscando compreender o que de fato aconteceu.

Contudo, com o avanço tecnológico, surgiu uma nova espécie de provas, as provas digitais. Com isso, o conceito de prova tornou-se mais abrangente, exigindo uma análise específica sobre suas particularidades. Nesse novo cenário, a prova digital para Cristiane Vieira da Silva e José Augusto Bezerra Lopes, pode ser entendida como:

> Um conjunto probatório constituído a partir de arquivos digitais, sob posse do investigado, de terceiros, ou que tenham sido transmitidos por meio de redes de comunicação, contendo dados que possam contribuir para o esclarecimento dos fatos investigados. O foco recai sobre o arquivo digital em si, enquanto elemento autônomo de prova. A principal singularidade da prova digital está na sua natureza não física: trata-se de uma cadeia numérica que pode ser facilmente replicada, modificada e disseminada, exigindo o uso de ferramentas tecnológicas para ser acessada e interpretada. Entretanto, não se pode afirmar de forma absoluta que toda prova digital é necessariamente perecível, pois muitas vezes os dados armazenados digitalmente passam por procedimentos de conservação (Viera, Augusto, 2025, p.10).

Cristalino é a distinção entre a prova digital e a prova física, tornando-se um novo desafio ao processo penal, esse desafio baseia-se na facilidade em que as provas digitais podem ser facilmente corrompidas, ou modificadas através de poucos comandos. Nesse cenário, fica evidente a necessidade de peritos especializados em tecnologias para a aplicação de técnicas forenses para a correta preservação das provas, para não acontecer a perda das evidências digitais.

Para averiguar a autenticidade das provas, utiliza-se a função chamada *hash*, que tem por finalidade verificar a integridade de cada arquivo, atribuindo a cada documento uma espécie de impressão digital única. Segundo a ESET (2025), o *hash* assegura "que o objeto não será alterado ao longo do tempo por meio de um registro eletrônico. Esse registro é fundamental para averiguar a originalidade do objeto em questão". Nesse mesmo sentido, a AKAD Tecnologia [s.d.] destaca que "se um único byte do arquivo for alterado, o valor do *hash* muda completamente", evidenciando a confiabilidade do método como instrumento de verificação da integridade digital.

Embora tecnicamente eficaz, o *hash* não supre sozinho as exigências jurídicas, sem uma regulamentação específica, para coleta, acondicionamento e armazenamento dessas provas, o simples registro do *hash* não é suficiente para garantir a efetividade da prova digital. Isso deixa claro que a fragilidade da prova digital não está apenas na tecnologia, mas também na ausência de normas no ordenamento jurídico brasileiro (Data Certify, 2025).

Gustavo Badaró comenta sobre como as provas digitais podem ser frágeis e difíceis de garantir sua autenticidade:

> No que toca à sua "desmaterialização", não se trata de provas pensáveis como objetos físicos dotados de evidente corporeidade. E é exatamente dessa impalpabilidade que decorre os caráteres de volatilidade e fragilidade da própria prova digital, razão pela qual há necessidade de uma maior preocupação com a possibilidade de falsificação ou destruição. Há, na prova digital, uma congênita mutabilidade. Em suma, trata-se de uma fonte de prova que pode ser facilmente contaminada, sendo sua gestão muito delicada por apresentar um alto grau de vulnerabilidade a erros (Badaró, 2021, p.01).

Fica evidente, portanto, a distinção de prova física e digital, o Data Certify (2025) e Gustavo Badaró (2021), deixam claro que a prova digital apresenta vulnerabilidades relativas à sua desmaterialização e volatilidade. Sem a adoção de procedimentos forenses adequados, rastreabilidade e normatização específica, o simples uso do *hash* não garante a autenticidade, integridade ou efetividade probatória. Essa diferença exige um tratamento jurídico e técnico especializado, que reconheça as especificidades de cada prova, para garantir a autenticidade das mesmas.

1.1 Desafios técnicos

Um dos desafios técnicos mais complexos da prova digital é sua fragilidade, uma vez que pode ser facilmente adulterada, o que compromete todo o processo investigativo ao ameaçar a autenticidade e a integridade da evidência. Importante mencionar que esse desafio se torna mais complexo pela falta de mecanismos adequados no sistema brasileiro, como a ausência de ferramentas de análise e dispositivos aptos a verificar a autenticidade dessas provas (Paciarelli, 2024).

A falta de mecanismos adequados no sistema brasileiro, tem consequências diretas na validade das provas, isto é evidenciado na decisão do Agravo Regimental no Recurso em Habeas Corpus 828054 - RN (2023/0189615-0), julgado pela Quinta Turma do Superior Tribunal de Justiça – STJ, por unanimidade: "são inadmissíveis no processo penal as provas obtidas de celular quando não forem adotados procedimentos para assegurar a idoneidade e a integridade dos dados extraído".

A exemplo, segundo o acórdão da mencionada decisão, "o aparelho telefônico foi encaminhado para extração de dados via *Kit Cellebrite*" (aparelho que consiste em realizar a recuperação de dados, mensagens fotos, vídeos em telefone e computador) para a Polícia Civil do Rio Grande do Norte. No entanto, devido à falta de atualização do aparelho, não foi possível realizar a leitura do dispositivo. Como resultado, o tribunal concluiu que não era possível conferir a autenticidade das provas, pois não havia elementos probatórios suficientes

(AgRg no Habeas Corpus nº 828054,2024,p.6).

Torna-se evidente que há um desafio técnico no sistema jurídico brasileiro diante da ausência de tecnologias e infraestrutura de equipamentos, que podem levar a inadmissibilidade das provas, impedindo a análise de informações potencialmente relevantes para o processo.

1.2 Reconhecimento jurisprudencial da validade da prova digital

Para o STJ, a prova digital deve ser completa e íntegra para ser admitida em juízo, sendo que a corrupção parcial dos arquivos compromete sua integralidade e inviabiliza sua utilização. Além disso, o simples registro de *hashes* dos arquivos extraídos não garante, por si só, a integridade da prova digital (AgRg no Recurso em Habeas Corpus nº 184003 - SP nº 184003 STJ,2024,p.1).

Diante dos desafios técnicos já expostos, coube ao STJ estabelecer parâmetros para admissibilidade da prova digital no processo penal.

Em decisão de 13/03/2025, no Agravo Regimental no Recurso em Habeas Corpus nº 738418- SP, do STJ, o tribunal destacou que a prova deve ser garantida sob quatro pilares fundamentais: "A higidez da prova digital deve ser garantida sob os aspectos de audibilidade, repetibilidade, reprodutibilidade e justificabilidade[3]." (AgRg no Habeas Corpus nº 738418,2022,p.11). Na prática, quando esses critérios não são atendidos, a prova torna-se invalidada. Nesse acórdão o Tribunal declarou a imprestabilidade da prova impugnada (conversas de WhatsApp) e determinou seu desentranhamento dos autos (AgRg no Habeas Corpus nº 738418,2025,p.17).

Diante disso, quando se trata de provas digitais com a observância das decisões do STJ observa-se que a grande defasagem no processo penal em se tratando de provas digitais se dá pela falta de uma legislação específica para a cadeia de custódia digital, vez que não há especificações de qual forma esses vestígios devem ser coletados e armazenados. Essa lacuna gera consequências graves, como a quebra da autenticidade por falha de procedimento, visto no acórdão nº 738418/SP e por falha de infraestrutura percebido nos acórdãos nº 828054/RN,184003/ SP.

---

[3] A ABNT NBR ISO/IEC 27037:2013 define a audibilidade como o propósito de determinar se o método científico, técnica ou o procedimento foi adequadamente seguido. O conceito de repetibilidade é quando os mesmos resultados de testes são produzidos utilizando os mesmos procedimentos e métodos de medição, e pode ser repetido a qualquer tempo depois do teste original. Reprodutibilidade, quando os mesmos resultados são produzidos utilizando diferentes instrumentos, diferentes condições; e a qualquer tempo, e a justificabilidade tem como objetivo justificar todas as ações e métodos utilizados para o tratamento da evidência digital.

2. Cadeia de custódia da prova no ordenamento jurídico

Em dezembro de 2019, o pacote Anticrime, por meio da Lei Federal n. 13.964/2019, trouxe inovações ao Código de Processo Penal, destacando-se o artigo 158 -A:

> Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte (Brasil, 2019).

Assim, a cadeia de custódia deve ser entendida como:

> A sucessão encadeada de pessoas que tiveram contato com a fonte de prova real, desde que foi colhida, até que seja apresentada em juízo. É o conjunto de pessoas, uma após a outra (p. ex.: o investigador, o delegado de polícia, o perito, o escrivão do cartório etc.), que teve contato com tal coisa (p. ex.: uma arma, um líquido, um tufo de fios de cabelo). Esse conjunto de pessoas e os momentos específicos em que cada uma delas teve contato com a evidência precisam ser registrados, isto é, documentados, para que se saiba, exatamente, quem teve contato com a coisa e quando isso ocorreu (Badaró, 2021, p.02).

Nesse viés, a cadeia de custódia está embasada em elementos probatórios, desde a coleta até o seu descarte. Sendo de suma importância, cada movimentação ser documentalmente registrada. A cadeia de custódia visa coletar vestígios do crime. O artigo 158-A, §1° diz "que o início da cadeia de custódia dá-se com a preservação do local de crime ou com procedimentos policiais ou periciais nos quais seja detectada a existência de vestígio". (Brasil, 2019). Quando se trata de uma cadeia de custódia documentais, torna-se mais fácil de manter a autenticidade dessas provas.

Na mesma perspectiva da cadeia de custódia, no artigo 158-B, detalha cada fase do rastreamento do vestígio, desde seu reconhecimento até o seu descarte. As etapas são definidas da seguinte forma:

> I) Reconhecimento: ato de distinguir um elemento como de potencial interesse para a produção da prova pericial;
> II)Isolamento: ato de evitar que se altere o estado das coisas, devendo isolar e preservar o ambiente imediato, mediato e relacionado aos vestígios e local de crime;
> III)Fixação: descrição detalhada do vestígio conforme se encontra no local de crime ou no corpo de delito, e a sua posição na área de exames, podendo ser ilustrada por fotografias, filmagens ou croqui, sendo indispensável a sua descrição no laudo pericial produzido pelo perito responsável pelo atendimento;
> IV)Coleta: ato de recolher o vestígio que será submetido à análise pericial, respeitando suas características e natureza;
> V) Acondicionamento: procedimento por meio do qual cada vestígio coletado é embalado de forma individualizada, de acordo com suas características físicas, químicas e biológicas, para posterior análise, com anotação da data, hora e nome de

> quem realizou a coleta e o acondicionamento;
> VI) Transporte: ato de transferir o vestígio de um local para o outro, utilizando as condições adequadas (embalagens, veículos, temperatura, entre outras), de modo a garantir a manutenção de suas características originais, bem como o controle de sua posse;
> VII)Recebimento: ato formal de transferência da posse do vestígio, que deve ser documentado com, no mínimo, informações referentes ao número de procedimento e unidade de polícia judiciária relacionada, local de origem, nome de quem transportou o vestígio, código de rastreamento, natureza do exame, tipo do vestígio, protocolo, assinatura e identificação de quem o recebeu;
> VIII)Processamento: exame pericial em si, manipulação do vestígio de acordo com a metodologia adequada às suas características biológicas, físicas e químicas, a fim de se obter o resultado desejado, que deverá ser formalizado em laudo produzido por perito;
> IX)Armazenamento: procedimento referente à guarda, em condições adequadas, do material a ser processado, guardado para realização de contraperícia, descartado ou transportado, com vinculação ao número do laudo correspondente;
> X)Descarte: procedimento referente à liberação do vestígio, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial. (Brasil, 2019).

Nesse aspecto, observa-se que o legislador criou de forma minuciosa a cadeia de custódia de provas físicas, desde a coleta até o seu descarte, visando garantir a integridade dos vestígios. Contudo, constata-se que há uma escassez no que tange a cadeia de custódia de provas digitais, tornando-se uma lacuna na atual legislação processualista penal. A aplicação dessas mesmas etapas das provas digitais.

Ressalta-se que há um projeto de Lei Federal n° 4939/2020 da Câmara dos Deputados Federais, em tramitação desde 2020 que tem por finalidade criar uma cadeia de custódia de provas digitais específica, no artigo 19 o projeto estabelece que a obtenção da prova deve preservar cinco pilares fundamentais:

> Art. 19 Os meios de obtenção da prova digital serão implementados por perito oficial ou assistente técnico da área de informática, que deverão proceder conforme as boas práticas aplicáveis aos procedimentos a serem desenvolvidos, cuidando para que se preserve a integridade, a completude, a autenticidade, a auditabilidade e a reprodutibilidade dos métodos de análise (Leal, 2020).

A justificação do projeto reconhece que "a evidência digital tem natureza e comportamento distinto das conhecidas evidências físicas", o que revela a "premente necessidade de complementar as normas vigentes" (Leal, 2020, p.17).

À vista disso, analisa-se que o projeto tem por finalidade garantir a confiabilidade das provas, solucionando os desafios no qual observa-se acima, sendo eles: a falta de profissionais competentes para realizar a coleta de forma adequada, a ausência de procedimentos específicos, como visto no caso do Acórdão que analisou a falha no equipamento de extração de dados.

Esse projeto de lei, tem por foco a criação de um sistema legal próprio para a prova digital, estabelecendo protocolos técnicos e garantias processuais, que visam preencher as atuais lacunas na atual legislação, trazendo maior efetividade e segurança jurídica. Sendo o principal ponto de discussão do STJ, frente à integridade das provas.

2.1 Princípios aplicáveis à cadeia de custódia

De modo geral, a ausência de legislação processual sobre cadeia de custódia de provas digitais, afeta não só o processo penal, mas todos os âmbitos do Direito. Verifica essa realidade, no estudo desenvolvido por José Antônio Ribeiro de Oliveira Silva (2022), que, embora voltado ao processo do trabalho, apresenta conclusões de grande relevância para a compreensão dos estudos a respeito da cadeia de custódia, e visão que pode ser aplicada ao processo penal.

A observância da cadeia de custódia assegura o cumprimento dos princípios constitucionais, sendo eles o devido processo legal, a ampla defesa, o direito ao contraditório, trazendo uma efetividade e segurança jurídica[4].

Para Silva a confiabilidade das provas somente será proporcionada se atendidas duas premissas:

> Somente será proporcionada se atendidas duas premissas básicas: (i) que resulte bem clara a origem do documento digital, ou seja, a sua autenticidade, verificável quando não pairar dúvidas sobre a sua autoria, por assim dizer; (ii) que se possa verificar a integridade das informações, dos dados constantes do documento digital (Silva, 2022, p.10).

Nesse aspecto, há também outros princípios aplicáveis à cadeia de custódia para garantir efetividade processual, como o princípio da autenticidade, o qual segundo Silva (2022), a autenticidade é um dos requisitos essenciais da prova digital a que diz respeito à identificação da autoria, permitindo ao julgador verificar que o autor aparente é realmente o responsável pelo conteúdo. Isso quer dizer que o princípio da autenticidade tem por finalidade

[4] Legale Educacional (2025) define o devido processo legal, como um conjunto de garantias processuais estabelecidas para assegurar que nenhuma pessoa seja privada de seus direitos fundamentais sem uma condução processual justa e adequada.
O Tribunal de Justiça do Distrito Federal (2024), define o princípio do contraditório como uma garantia de que as partes sejam informadas sobre todos os atos processuais, e tenham a oportunidade de se manifestar a respeito. Isso inclui o direito de conhecer as alegações e provas apresentadas pela parte contrária, bem como o direito de resposta. Já o princípio da ampla defesa assegura que as partes possam utilizar todos os meios legais e provas necessárias para defender seus direitos. Projuris (2022) conceitua segurança jurídica como um princípio segundo o qual o Estado deve agir como garantidor dos direitos fundamentais dos cidadãos.

saber ao certo o autor que produziu aquele conteúdo, bem como as circunstâncias em que foi gerado, evitando fraudes e falsificações que possam comprometer a confiabilidade da prova. Essa observância é essencial para garantir a identificação do agente, prevenindo erros processuais e garantindo a legitimidade da persecução penal.

Destaca-se também o princípio da integridade que segundo Silva (2022), consiste na exigência de que a prova digital permaneça completa e sem qualquer adulteração desde o momento de sua coleta até a apresentação em juízo, garantindo sua autenticidade e valor probatório.

Ainda sob a perspectiva de provas, Silva, destaca que:

> A doutrina tem recomendado que a extração dos dados seja acompanhada por notário e descrita com precisão numa ata notarial, ou que, pairando dúvidas sobre a integridade da prova digital (Silva, 2022, p. 14).

Ainda que formulado sob a ótica do processo trabalhista, o entendimento de Silva (2022) revela-se aplicável ao processo penal, pois evidencia que a observância do princípio da integridade é essencial para assegurar a autenticidade e fidedignidade da prova digital.

Outro princípio aplicável à cadeia de custódia de prova digital é o da suficiência, segundo a Associação Brasileira de Normas Técnicas ABNT NBR ISO/IEC 27037:2013[5], a suficiência deve-se coletar vestígios suficientes para permitir o exame ou investigação adequados. Além disso, a confiabilidade é essencial, pois a evidência digital deve comprovar que "é o que diz ser", garantindo que representa a informação original e que sua autenticidade não foi comprometida. Por fim, a pertinência é um ponto crucial, onde a ABNT menciona que a evidência só terá valor se for capaz de "provar ou refutar" de maneira clara e direta um elemento central do caso em análise.

Essa exigência de preservação e identificação em todos os autos do processo é o que garantirá que a prova digital seja lícita ao processo. A inobservância dos procedimentos que garantem a integridade e autenticidade acarreta a quebra da cadeia de custódia,

[5] Destaca-se que a norma ABNT NBR ISO/IEC 27037:2012 é referência internacional para identificação, coleta, aquisição e preservação de evidências forenses digitais em todas as etapas no processo de investigação. Faz parte das normas da família ISO 27000 - Gestão da Segurança da Informação, sendo a mais relevante na área de perícia forense digital. Em vigor no Brasil desde janeiro de 2014, a norma define e descreve as diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Apesar de não se tratar de norma obrigatória, por não haver, ainda, um reconhecimento explícito em lei, é, de fato, a única norma elaborada por organismos competentes e reconhecida no Brasil que trata sobre o tema, além de ser a norma que, em sua versão internacional (ISO), descreve os procedimentos adotados nos ordenamentos de vários países.

comprometendo a confiabilidade da prova, ensejando na sua inadmissibilidade processual[6].

Por fim, é imprescindível destacar que toda e qualquer prova apresentada no processo deve estar em conformidade com o que está expressamente previsto na Constituição da República Federativa do Brasil 1988. A produção e valoração são regidas por princípios constitucionais, notadamente o contraditório e a ampla defesa, que asseguram às partes a oportunidade de participar ativamente da formação do elemento probatório e de se manifestar sobre ele.

2.2 Especificidades da cadeia de custódia digital

A cadeia de custódia digital se revela um processo intrinsecamente mais complexo do que a custódia da prova física tradicional. Sua particularidade reside no fato de que o vestígio original começa, muitas vezes, como um fenômeno analógico que precisa ser transformado em dados numéricos para existir como prova. Consequentemente, o objeto da prova digital só se manifesta no mundo físico analógico após a devida extração desses dados. Diferentemente do objeto material, que é palpável, o dado digital reside em números binários (Lopes Jr., *et.al,*2025).

Conforme mencionado anteriormente, a cadeia de custódia possui 10 (dez) etapas expressamente previstas no artigo 158-B do Código de Processo Penal. Nesse aspecto, foram criadas com base em provas materiais e vestígios físicos. Sobre essa limitação Beatriz de Carvalho Rodrigues (2024) observa que:

> As regras procedimentais apresentadas nesse artigo são, nitidamente, destinadas a objetos e materiais reais, corpóreos, físicos. Por exemplo, a etapa do transporte apresenta a exigência de um veículo, temperatura adequada e outras coisas que, claramente, são necessárias apenas para objetos físicos. Não há previsão de etapas especiais para as provas digitais (Rodrigues, 2024, p.30).

A autora acrescenta que, sob um ponto de vista legal, o "legislador enxerga os vestígios como objetos ou materiais que são visíveis" (Rodrigues, 2024, p.31)**.** O que evidencia uma lacuna normativa na regulamentação das provas digitais. No mesmo embasamento a Beatriz de Carvalho, diz que:

> A solução para esse questionamento ainda está em voga, todavia, há alguns procedimentos a serem seguidos. Um exemplo é a norma ABNT/ISO 27037. A

[6] (Campos, Cunha, 2017) Argumentam que a inadmissibilidade da prova é o regime jurídico que impede o ingresso e a consideração de um elemento probatório no processo, por ter sido obtido ou produzido em afronta a garantias constitucionais ou legais.

> norma descreve e define as “Diretrizes para a identificação, coleta, aquisição e preservação da evidência digital”. Em linhas gerais, a normativa 32 define quatro aspectos-chave para o manuseio da evidência digital: audibilidade, justificabilidade e repetibilidade ou reprodutibilidade (Rodrigues, 2024, p.31).

Complementarmente, a Norma Complementar n° 21 (IN01/DSIC/GSIPR) padroniza as fases da coleta, acondicionamento, manuseio e descarte das provas digitais. Enquanto a NC n° 21 foca nas diretrizes processuais, a norma técnica ABNT NBR ISO/IEC 27037 tem como objetivo o tratamento das evidências em suas etapas essenciais, sendo: a) Preparação, b) Coleta, c) Preservação e d) Comunicação.

Segundo a Polícia Federal (2015, p.15), a preparação constitui a fase inicial do tratamento da evidência digital, consistindo na formalização das equipes técnicas responsáveis, no treinamento de agentes e na definição das metodologias e ferramentas a serem utilizadas. Essa etapa tem como objetivo reduzir o risco de contaminação da prova e assegurar que a fase procedimental da coleta seja conduzida de forma adequada. A fase da coleta, conforme previsto na mesma norma, refere-se à obtenção dos dispositivos computacionais envolvidos e geração de cópia da evidência digital, sendo do disco inteiro, partições específicas ou arquivos selecionados. A Polícia Federal (2015, p.26) recomenda que sempre que possível evitar métodos que alterem a evidência digital.

Na fase de preservação, a Polícia Federal (2015) orienta que sejam observados procedimentos destinados à manutenção da integridade e, quando cabível, do sigilo dos dados coletados. Dentre as recomendações, destacam-se a utilização de algoritmos de *hash* para autenticação, o acondicionamento adequado das mídias e a adoção de medidas de proteção contra impactos físicos, calor e umidade. Ademais, é imprescindível a lavratura do termo de custódia, no qual devem constar as condições do lacre, os valores de *hash* e a identificação das mídias preservadas.

Embora o *hash* constitua ferramenta técnica essencial para a verificação da integridade dos dados, sua aplicação isolada não se revela suficiente para assegurar a autenticidade probatória (Data Certify, 2025).

Por fim, a comunicação das evidências às autoridades competentes, determina que seja elaborado um “relatório de comunicação de incidente de segurança, devendo o material ser encaminhado para autoridade competente, preocupando sempre com a privacidade e sigilo dos dados custodiados. ” (Polícia Federal, p.33, 2015).

Conclui-se que, desse modo, a adoção dessas quatro fases (preparação, coleta, preservação e comunicação), conforme as diretrizes da Polícia Federal (2015), visa suprir a ausência de normatização específica do Código de Processo Penal para o ambiente digital.

Esse rigor técnico assegura integridade e autenticidade da prova aumentando sua admissibilidade em juízo.

3. Lacunas na legislação brasileira e impactos práticos das lacunas legais

A Lei 13.964/2019, representou um avanço importante na coleta, preservação e integridade dos elementos probatórios. No entanto, como observa Alex Cardoso de Sousa "a supracitada lei nasceu obsoleta, já que o legislador foi silente em aspectos fundamentais do procedimento" (Sousa, 2025, p.8) uma vez que o texto legal não acompanhou as particularidades das evidências digitais.

A legislação não previu as consequências processuais decorrentes da violação da cadeia de custódia digital, fazendo com que a tarefa de suprir essa lacuna fosse feita à doutrina e às decisões judiciais. O fato de não haver legislação específica, gera entendimentos distintos e violação das provas, gerando insegurança jurídica no tratamento e na valoração das evidências digitais (Sousa, 2025).

As falhas legislativas decorrem na ausência de lei específica para a coleta dos vestígios digitais, o STJ vem reconhecendo a inadmissibilidade de provas digitais quando inexistem registros documentais da forma como foram coletadas e preservadas (Maia, 2024).

Como observa Gustavo Badaró (2021), a ausência de regulamentação específica sobre a cadeia de custódia digital deixa o sistema processual penal brasileiro em defasagem frente aos avanços tecnológicos, comprometendo a integridade e a confiabilidade das provas.

Com isso as lacunas na legislação, tem como resultado a invalidade das provas, tendo como consequências, as falhas do devido processo legal, essa conclusão se dá, devido aos casos supracitados acima, onde os tribunais decidiram não aceitar tais provas digitais.

3.1 Impactos Práticos e a Invalidação da Prova Digital

Gabriela Almeida Araruna Pires Rebelo, em publicação diz que:

> A legislação não aborda o impacto da não preservação da cadeia de custódia. Em outras palavras, embora os artigos da lei abordem aspectos relevantes, não há nenhuma determinação legislativa sobre o momento processual adequado para examinar a regularidade ou irregularidade da cadeia de custódia, nem qualquer explicitação sobre as consequências que devem ser atribuídas aos elementos probatórios cuja custódia tenha sido interrompida. A falta de observância das consequências decorrentes dessa quebra resulta em uma insegurança jurídica no âmbito do processo penal (Rebelo, 2023, p.45).

Essa ausência de determinação legislativa gera inseguranças jurídicas, uma vez que as

provas podem ser descartadas, pela ausência de regulamentação sobre falhas procedimentais.

Diante do que foi exposto, percebe-se que há uma clara ausência de leis ou diretrizes eficazes capazes de observar a quebra da cadeia de custódia. Rebelo (2023), afirma que é de incumbência do Estado:

> Assegurar que todas as provas sejam adequadamente acondicionadas custodiadas e posteriormente submetidas à perícia, a fim de viabilizar o contraditório diferido em relação a essas provas ou permitir o questionamento acerca de sua credibilidade (Rebelo, 2023, p.45).

A quebra da cadeia de custódia digital, ocorre segundo Rebelo quando:

> Não há um registro documental adequado dos procedimentos adotados pelas autoridades policiais para garantir a integridade, autenticidade e confiabilidade dos elementos informáticos. Por exemplo, se o conteúdo extraído dos dispositivos for analisado por terceiros antes mesmo de ser periciado pela polícia, ou se não houver um registro documental adequado sobre o processo de coleta e preservação dos dispositivos, bem como sobre as pessoas que tiveram acesso a eles, os momentos em que tais contatos ocorreram e o percurso administrativo interno percorrido pelos aparelhos desde a apreensão pela polícia. (Rebelo, 2023, p.45).

Como consequência tais falhas comprometem a admissibilidade da prova em juízo, surtindo como efeito prejuízo para as partes na ação penal e frustrando o objetivo da persecução penal. Nesse sentido, Geraldo Prado ressalta que "violada a cadeia de custódia da prova digital incide imperiosa proibição de valoração da prova assim obtida" (Prado, 2021, s.p).

Portanto, a ausência de normativas específicas e a quebra da cadeia de custódia das provas digitais não apenas geram insegurança jurídica, mas confrontam diretamente a legitimidade do processo penal. Geraldo Prado afirma "que a cadeia de custódia das provas digitais é uma garantia de natureza constitucional"(Prado, 2021, s.p).

4. Caminhos para o aperfeiçoamento normativo e procedimental

A partir das lacunas e fragilidades verificadas na legislação brasileira quanto à cadeia de custódia de provas digitais torna-se indispensável propor medidas que assegurem maior autenticidade e integridade das provas.

O aperfeiçoamento da legislação deve caminhar juntamente com o avanço tecnológico para evitar a quebra da cadeia de custódia. Nesse sentido, conforme destacam Aury Lopes *et al* (2025) é essencial que o sistema jurídico e os orgãos de persecução penal adotem e observem com rigor os Procedimentos Operacionais Padrão (POPs) e ISOs, assegurando a extração mais completa e fidedigna possível dos dados.

A Perícia Criminal, 2024, do Ministério da Justiça e Segurança Pública aborda procedimentos operacionais sendo eles:

> 5.01Exame pericial de mídias de armazenamento computacional: orientar o profissional de perícia da área de informática a realizar exames que envolvam dados contidos em mídias de armazenamento computacional (como discos rígidos, SSDs, pen drives, cartões de memória,;
> 5.02Exame pericial de dispositivos computacionais móveis: orientar o profissional de perícia da área de informática a realizar exames que envolvam dados contidos em dispositivos computacionais móveis (como telefones celulares, smartphones e tablets);
> 5.03Exame pericial de local de informática: orientar o profissional de perícia criminal a realizar exames em locais de crime que envolvam equipamentos computacionais, com o objetivo de fixar, coletar e preservar os vestígios digitais e/ou físicos;
> 5.04Exame pericial de local de internet: orientar o profissional de perícia criminal a realizar exames em locais virtuais (internet) que envolvam conteúdo, dados ou metadados de páginas web, redes sociais, aplicativos ou serviços online, com o objetivo de fixar, coletar e preservar esses vestígios digitais;
> 5.05Apreensão de dispositivos computacionais móveis: orientar os peritos criminais, auxiliares e outros profissionais da Segurança Pública que atuam na Cadeia de Custódia a realizarem a apreensão de dispositivos computacionais móveis (celulares, smartphones e tablets) no local de crime, garantindo a preservação da evidência digital e a correta aplicação da Cadeia de Custódia (Dsusp, 2024, p.11-47).

Para que os padrões técnicos dos POPs se tornem uma garantia processual efetiva, o Poder Judiciário deve adotar a observância dessas diretrizes rigorosas como critério indispensável de validade da prova digital. Assim, o Judiciário não apenas fiscaliza o cumprimento do artigo 158-B do CPP, mas eleva a qualidade da prova, assegurando o pleno contraditório ao permitir que a defesa audite a base técnica do vestígio (Lopes Jr., *et al*, 2025).

A fragilidade do sistema reside na distinção fundamental entre os tipos de prova: a) a prova analógica: refere-se a algo físico e contínuo e sua cadeia de custódia foca no rastreamento e preservação de um objeto material previamente existente (CPP, artigo 158-A); já a b) prova digital é feita de números binários (0 e 1). Sua existência física depende da transformação de um fenômeno (analógico) em dados discretos, por isso, sua cadeia de custódia deve documentar a técnica e o *software* utilizados na captura, priorizando a preservação dos dados brutos originais, pois o objeto da prova somente existe no mundo físico após sua extração adequada (Lopes Jr, *et al,* 2025).

No cenário nacional, destaca-se o Projeto de Lei Federal n°4.939/2020 da Câmara dos Deputados Federais que propõe a criação de uma cadeia de custódia específica para as provas digitais. O projeto visa estabelecer princípios como integridade, a completude, a autenticidade, a auditabilidade e a reprodutibilidade, buscando oferecer diretrizes técnicas claras para a coleta e preservação da prova (Leal, 2020). Sua aprovação resultaria no suprimento das lacunas existentes no processo penal.

Por fim, faz-se imprescindível o treinamento e especialização dos peritos, pois a ausência de conhecimento técnico adequado compromete a correta aplicação dos POPs e das diretrizes da cadeia de custódia desde o momento da apreensão, tornando ineficaz qualquer tentativa posterior de validação judicial da prova. Essa necessidade é comprovada ao se observar o panorama recente do setor forense, a exemplo, a revisão da Interpol (Reedy, 2023), que abrange o período de revisão de 2019 a 2022, revelou que no Brasil há considerável descentralização dos serviços forenses públicos e a diversidade de perfis dos analistas que incluem fonoaudiólogos, físicos e odontólogos geram obstáculos à uniformidade dos procedimentos. Como resultado, o estudo apontou que 40% dos analistas forenses multimídia no Brasil estão inicialmente despreparados para lidar com as tecnologias e instrumentos da área.

Diante disso, verifica-se que a cadeia de custódia digital depende não apenas de normas específicas, mas também da efetiva adoção de protocolos técnicos, da capacitação profissional e uniformização dos procedimentos. A legislação em vigor, ainda se mostra insuficiente para acompanhar as evidências digitais e garantir autenticidade dos elementos probatórios. Assim, torna-se essencial estabelecer diretrizes uniformes que garantam a integridade, rastreabilidade e a audibilidade das provas digitais.

4.1 Boas práticas nacionais

Diante do que foi dito anteriormente, as boas práticas para a cadeia de custódia da prova digital baseiam-se na adoção de normas técnicas brasileiras, ABNT NBR ISO/IEC 27037:2013. Essa norma estabelece diretrizes para a identificação, coleta, aquisição e preservação da prova digital. Sua especificidade reside em fornecer um método para garantir a integridade, a autenticidade e a rastreabilidade do vestígio desde o momento de sua descoberta, assim a norma orienta o cálculo da função *hash* a assinatura digital única do arquivo.

Ademais, menciona-se também a norma complementar n° 21 (NC n. 21/IN01/DSIC/GSIPR) do Gabinete de Segurança Institucional que estabelece diretrizes para o registro, coleta e preservação de evidências. Ao detalhar os procedimentos necessários para garantir a autenticidade e a integridade dos dados coletados, ela auxilia os peritos e as autoridades na aplicação dos princípios da cadeia de custódia, suprindo, em parte, a lacuna de uma legislação processual penal.

Além disso, a aplicação dos Procedimentos Operacionais Padrão (POPs), elaborados

pelo Ministério da Justiça e Segurança Pública é essencial para a preservação da prova digital na prática. Tais procedimentos determinam a documentação detalhada de cada fase da perícia, assegurando maior confiabilidade e auditabilidade, permitindo reconstruir todo o percurso da prova e identificar quem teve acesso a ela. Dessa forma, a aplicação rigorosa dos POPs, aliada à observância do artigo 158-B do Código de Processo Penal, fortalece a autenticidade e a confiabilidade da prova digital (Diretoria do Sistema único de Segurança Pública, 2024).

A adoção da Ata Notarial pode ser uma boa prática para a formalização e preservação de provas digitais. Prevista no artigo 384 do Código de Processo Civil[7], ela é o instrumento pelo qual o tabelião, dotado de fé pública, narra e atesta a existência, o conteúdo e o método de coleta de um fato digital. A Ata Notarial confere à prova os atributos de fé pública sendo essencial para documentar a cadeia de custódia da prova digital antes que ela possa ser alterada ou contestada judicialmente (Silva, 2022)**.**

A utilização de boas práticas da Norma ABNT, Procedimentos da Polícia Federal/MJSP , Ata Notarial, juntamente com a criação da Cadeia de Custódia de Provas Digitais específica (PL Federal nº 4.939/2020) é o caminho para o aperfeiçoamento e a segurança da prova digital no cenário jurídico brasileiro. Isso porque a adoção dessas práticas consolida um padrão técnico capaz de assegurar que a prova digital chegue ao juiz com sua integridade preservada. Cada uma dessas práticas supre uma etapa essencial da cadeia de custódia, desde a identificação e coleta, armazenamento, até a certificação pública de sua existência e conteúdo.

CONCLUSÃO

Em conclusão, este estudo buscou aprofundar a compreensão acerca da Cadeia de Custódia das Provas Digitais no Processo Penal, compreendendo-a como um dos principais desafios contemporâneos diante do avanço tecnológico e da crescente digitalização das relações humanas e jurídicas. A pesquisa evidenciou que, embora a Lei Federal nº 13.964/2019 tenha introduzido avanços ao prever formalmente a cadeia de custódia no ordenamento jurídico, seu conteúdo revela-se insuficiente e anacrônico frente à realidade digital. As dez etapas descritas no artigo 158-B do Código de Processo Penal foram concebidas para vestígios materiais, deixando desassistidas as provas eletrônicas, cuja

[7] Artigo 384 CPC: A existência e o modo de existir de algum fato podem ser atestados ou documentados, a requerimento do interessado, mediante ata lavrada por tabelião. Parágrafo único. Dados representados por imagem ou som gravados em arquivos eletrônicos poderão constar da ata notarial.

natureza volátil e desmaterializada demanda protocolos específicos de preservação, armazenamento e validação.

O trabalho atingiu o objetivo proposto ao demonstrar a distinção essencial entre provas físicas e digitais e ao evidenciar as deficiências normativas que comprometem a integridade e a confiabilidade das evidências eletrônicas no processo penal. Constatou-se que a insuficiência regulatória brasileira gera insegurança jurídica, abrindo margem para nulidades probatórias e decisões conflitantes nos tribunais. O estudo identificou, ainda, que o Poder Judiciário tem suprido parcialmente essa lacuna ao exigir que as provas digitais observem os quatro pilares técnicos da confiabilidade probatória: auditabilidade, repetibilidade, reprodutibilidade e justificabilidade, mas tais exigências esbarram em limitações estruturais e operacionais do sistema. Entre essas limitações, destacam-se a carência de infraestrutura tecnológica adequada, a defasagem de equipamentos e *softwares*, a descentralização dos serviços periciais e a falta de capacitação continuada de profissionais, fatores apontados em decisões judiciais, como no acórdão nº 828.054/RN, e em relatórios técnicos que indicam o despreparo inicial de parte significativa dos peritos em informática forense.

Diante desse cenário, o estudo propõe um conjunto de medidas voltadas à superação dessas fragilidades. Destaca-se, em primeiro plano, a necessidade de aprovação do Projeto de Lei Federal nº 4.939/2020, que representa importante avanço rumo à regulamentação específica da cadeia de custódia digital. Além disso, recomenda-se a implementação de Procedimentos Operacionais Padrão (POPs), a adoção das normas da ABNT NBR ISO/IEC 27037:2013 e o fortalecimento da capacitação técnica de peritos e operadores do direito. A utilização da Ata Notarial também se mostra uma boa prática para garantir a fé pública quanto à existência, integridade e conteúdo da prova digital no momento da coleta.

Conclui-se, portanto, que a criação e regulamentação de uma cadeia de custódia digital são indispensáveis para assegurar a validade e a integridade das provas digitais, prevenindo nulidades e fortalecendo a confiabilidade do processo penal. Com a adoção de padrões técnicos compatíveis com a complexidade das evidências digitais, o Processo Penal brasileiro poderá consolidar a segurança jurídica, assegurar a efetividade da justiça e resguardar, de forma plena, os direitos e garantias constitucionais fundamentais, especialmente o devido processo legal e a presunção de inocência.

REFERÊNCIAS

ABNT. NBR ISO/IEC 27037:2013: **Diretrizes para identificação, coleta, aquisição e preservação de evidência digital**. Rio de Janeiro, 2013.

AKAD. **Ferramenta de verificação de autenticidade - cálculo de hash: como funciona a validação por hash?**. São Paulo: AKAD TECNOLOGIA, [s.d] Disponível em: https://akad.com.br/verifica_hash.php. Acesso em: 09 set. 2025.

ALVARES, Marcelo Felipe Maia Hor-Meyll. Direito Digital e a manutenção da cadeia de custódia em evidências digitais do tipo SSD. **Revista do Ministério Público Militar**, Brasília, v. 51, n. 44, p. 236-258, 09 set. 2024. Disponível em: https://revista.mpm.mp.br/rmpm/article/view/440/414. Acesso em: 10 nov. 2025.

BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim IBCCRIM**, São Paulo, v. 29, n. 343, jun. 2021. ISSN 1676-3661. Disponível em: https://www.publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1325/627Acesso em: 11 set. 2025.

BRASIL. Câmara dos Deputados. Projeto de Lei n. 4.939, de 15 de outubro de 2020. **Dispõe sobre as diretrizes do direito da Tecnologia da Informação e as normas de obtenção e admissibilidade de provas digitais na investigação e no processo, além de outras providências**. Autor: Deputado Hugo Leal. Brasília, DF: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1936366&filename=PL%204939/2020. Acesso em: 11 set. 2025.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, [1988]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 set. 2025.

BRASIL. Decreto-Lei n. 3.689, de 13 de outubro de 1941. **Código de Processo Penal**. Diário Oficial da União, Rio de Janeiro, 13 out. 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 13 set. 2025.

BRASIL. Lei n. 13.105, de 16 de março de 2015. **Código de Processo Civil**. Diário Oficial da União, Brasília, DF, 17 mar. 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 10 set. 2025.

BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Segurança Pública. **Procedimentos Operacionais Padrão: informática forense**. Volume 5. Brasília, DF: SENASP, 2024. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/analise-e-pesquisa/pop/pop-pericia-criminal-2024-informatica-forense-vol-5-pdf.pdf.

BRASIL. Superior Tribunal de Justiça (5. Turma). **Agravo Regimental no Habeas Corpus n. 828.054/RN**. Disponível em: https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=integra&documento_sequencial=242041837&registro_numero=202301896150&peticao_

numero=202300906480&publicacao_data=20240429&formato=PDF. Acesso em: 13 set. 2025.

BRASIL. Superior Tribunal de Justiça (5. Turma). **Agravo Regimental no Recurso em Habeas Corpus n. 184.003/SP**. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202302482249&dt_publicacao=26/12/2024. Acesso em: 13 set. 2025.

BRASIL. Superior Tribunal de Justiça (6. Turma). **Agravo Regimental no Habeas Corpus n. 738.418/SP**. Disponível em: https://sintesecriminal.com/wp-content/uploads/2025/04/nulidade-provas-whatsapp.pdf. Acesso em: 13 set. 2025.

DATACERTIFY. **Por que o hash, por si só, não é suficiente?**. [S.l.]: DataCertify, 7 maio 2025. Disponível em: https://www.datacertify.com.br/por-que-o-hash-por-si-so-nao-e-suficiente/. Acesso em: 14 set. 2025.

ESET. **Hash: como usar e garantir a integridade dos seus arquivos**. [S.l.]: ESET Brasil, 6 fev. 2023. Disponível em: https://www.eset.com/br/artigos/hash-o-que-e-como-funciona/. Acesso em: 14 set. 2025.

FACHINI, Tiago. O que é segurança jurídica? Princípio e aplicações. **Projuris Blog**, 22 fev. 2022. Disponível em: https://www.projuris.com.br/blog/seguranca-juridica/. Acesso em: 14 set. 2025.

FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos. Apontamentos sobre a cadeia de custódia da prova digital no Brasil. **Revista Científica do UNIVEM**, Marília, v. 11, n. 2, p. 288-305, nov. 2020. Disponível em: https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/Em_Tempo_n.20.02.pdf.

LEGALE. **O devido processo legal no Direito Brasileiro**. Legale Blog, 5 jun. 2025. Disponível em: https://legale.com.br/blog/devido-processo-legal-conceito-e-importancia-no-direito-brasil/. Acesso em: 19 out. 2025.

LOPES JR., Aury. **Direito processual penal**. 22. ed. São Paulo: Saraiva Jur, 2025. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788553625673. Acesso em: 10 out. 2025.

LOPES JR., Aury *et al.* Prova penal digital: relatórios do Cellebrite podem ser insuficientes? **Consultor Jurídico**, São Paulo. Disponível em: https://www.conjur.com.br/2025-out-10/prova-penal-digital-relatorios-do-cellebrite-podem-ser-insuficientes/. Acesso em: 12 out. 2025.

MARCÃO, Renato. **Curso de processo penal**. 8. ed. São Paulo: Saraiva Jur, 2023. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786555598872. Acesso em: 13 out. 2025.

NUCCI, Guilherme de Souza. **Curso de direito processual penal**. 21. ed. Rio de Janeiro: Forense, 2024. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786559649280. Acesso em: 11 out. 2025.

PACIARELLI, Luiz Roberto. **Da prova digital no processo judicial**. 2024. [Número total de páginas] f. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica de Minas Gerais, Faculdade Mineira de Direito, Belo Horizonte, 2024. Orientador: Prof. Dr. Vicente de Paula Maciel Júnior. Disponível em: https://bib.pucminas.br/teses/Direito_LuizRobertoPaciarelli_31405_TextoCompleto.pdf. Acesso em: 10 out. 2025.

PRADO, Geraldo. **Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital**. Geraldo Prado, 22 jan. 2021. Disponível em: https://geraldoprado.com.br/artigos/breves-notas-sobre-o-fundamento-constitucional-da-cadeia-de-custodia-da-prova-digital/. Acesso em: 20 out. 2025.

REBELO, Gabriela Almeida Araruna Pires. **Cadeia de custódia de provas digitais**. 2023. 57 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal do Ceará, Faculdade de Direito, Fortaleza, 2023. Orientador: Prof. Nestor Eduardo Araruna Santiago. Disponível em: https://repositorio.ufc.br/bitstream/riufc/80580/1/2023_tcc_gaaprabelo.pdf. Acesso em: 25 out. 2025.

REEDY, Paul. Interpol review of digital evidence for 2019–2022. **Forensic Science International: Synergy**, [s. l.], v. 6, n. 100313, 2023. DOI: 10.1016/j.fsisyn.2022.100313. Disponível em: https://www.sciencedirect.com/science/article/pii/S2589871X22000985?via%3Dihub. Acesso em: 13 out. 2025.

RODRIGUES, Beatriz de Carvalho e Silva Brun. **A forma como garantia: uma análise da cadeia de custódia de provas digitais no processo penal brasileiro**. 2024.Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal do Pampa, Sant'Ana do Livramento, 2024. Orientador: João Beccon de Almeida Neto. Disponível em: https://repositorio.unipampa.edu.br/server/api/core/bitstreams/86bf4a53-2f26-44da-ab82-272f997afb29/content. Acesso em: 14 set. 2025.

SILVA, Cristiane Vieira; LOPES, José Augusto Bezerra. O uso de provas digitais no processo penal. **Revista Ibero-Americana de Humanidades, Ciências e Educação (REASE)**, São Paulo, v. 11, n. 5, p. 1084-1095, maio 2025. Disponível em: <https://periodicorease.pro.br/rease/article/view/19071/11208>. Acesso em: 18 out. 2025.

SILVA, José Antônio Ribeiro de Oliveira. A prova digital: um breve estudo sobre seu conceito, natureza jurídica, requisitos e regras de ônus da prova. **Rev. TST**, São Paulo, v. 88,

n. 2, p. 200-217, abr./jun. 2022. Disponível em: https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/207378/2022_silva_jose_prova_digital.pdf?sequence=1&isAllowed=y. Acesso em: 19 set. 2025.

SILVEIRA, Flávio. Diretrizes para a coleta e preservação de evidências digitais – NC nº 21. In: **COLÓQUIO DO CTIR GOV**, [9.], 2015, Brasília, DF. [Apresentação]. Disponível em: https://www.gov.br/ctir/pt-br/centrais-de-conteudo/palestras-em-pdf/coloquios/9o-coloquio-ctir-gov-2013-2015/1coloquio2015_palestra03_dpf_flaviosilveira.pdf. Acesso em: 11 out. 2025.

SOUSA, Alex Cardoso de. **A quebra da cadeia de custódia da prova digital e os reflexos no âmbito do processo penal**. 2025. Monografia (Graduação em Direito) – Universidade Federal do Ceará, Faculdade de Direito, Fortaleza, 2025. Orientador: Prof. Dr. Nestor Eduardo Araruna Santiago. Disponível em: https://repositorio.ufc.br/bitstream/riufc/81528/1/2025_tcc_acsousa.pdf. Acesso em: 29 out. 2025.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS. Contraditório X Ampla Defesa. **TJDFT: Direito Fácil,** 3 jun. 2024. Publicado por ACS. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/contraditorio-x-ampla-defesa. Acesso em: 15 out. 2025.