CADEIA DE CUSTÓDIA DA PROVA DIGITAL NO PROCESSO PENAL

Autora: Thaysa Mendes Marques[1]

Orientador: Prof. Dr. Karlos Alves Barbosa

RESUMO

Este artigo analisa a cadeia de custódia da prova digital no Processo Penal, destacando os desafios e a importância de garantir a integridade das evidências digitais. Com o avanço das tecnologias, os métodos de investigação têm evoluído, possibilitando novas formas de obtenção de provas, entretanto possibilitando novos riscos relacionados à manipulação e adulteração dessas evidências. O estudo analisa as regulamentações atuais sobre a cadeia de custódia da prova digital, destacando a importância de preservar a integridade das provas, para a obtenção de resultados justos e seguros no processo penal. A pesquisa também explora as melhores práticas e os protocolos necessários para garantir a confiabilidade da cadeia de custódia da prova digital no contexto jurídico.

Palavras-chave: Cadeia de custódia. Prova digital. Código de Processo Penal. Investigação Criminal. Quebra da cadeia de custódia.

ABSTRACT

This article analyzes the chain of custody for digital evidence in Criminal Procedure, highlighting the challenges and the importance of ensuring the integrity of digital evidence. As technology advances, investigative methods have evolved, offering new ways to obtain evidence, yet also introducing new risks related to the manipulation and tampering of such evidence. The study examines the current regulations on the digital evidence chain of custody, emphasizing the importance of preserving evidence integrity to achieve fair and reliable outcomes in criminal proceedings. The research also explores the best practices and protocols required to guarantee the reliability of the digital evidence chain of custody within the legal context.

Keywords: Chain of custody. Digital evidence. Code of Criminal Procedure. Criminal Investigation. Breach of chain of custody.

---

[1] Artigo Científico apresentado na disciplina de Trabalho de Conclusão de Curso II, da Faculdade de Direito da Universidade Federal de Uberlândia, como requisito parcial para obtenção do título de bacharel em Direito.

1.INTRODUÇÃO

O presente artigo irá abordar sobre as transformações importantes que o processo penal brasileiro passou nas últimas décadas no que diz respeito ao tratamento da prova, especialmente após a promulgação da Lei nº 13.964/2019, conhecida como "Pacote Anticrime". A partir dessa reforma, a cadeia de custódia ganhou previsão expressa no Código de Processo Penal, com os artigos 158-A a 158-F, estabelecendo parâmetros mais claros para a coleta, preservação e apresentação das provas no processo penal.

Ademais, com o avanço das tecnologias da informação, a prova digital passou a ocupar papel central nas investigações criminais e na instrução processual. Nesse contexto, dados extraídos de dispositivos eletrônicos, redes sociais, e-mails, sistemas de geolocalização e outras fontes digitais tornaram-se elementos cruciais para a responsabilização penal. No entanto, por se tratarem de informações altamente sensíveis e voláteis, essas provas exigem cuidados específicos para garantir sua integridade, autenticidade, confiabilidade e admissibilidade.

Neste cenário, a utilização correta da cadeia de custódia digital torna-se essencial para que as provas não percam sua validade jurídica. A manipulação inadequada, a ausência de documentação das etapas percorridas ou o uso de técnicas incorretas na extração e análise dos dados podem comprometer todo o processo, gerando a possibilidade de nulidade ou de injustiças processuais.

Além das exigências técnicas, a cadeia de custódia também se conecta com princípios constitucionais como o devido processo legal, a ampla defesa e o contraditório. Um processo penal que se pretende democrático e garantista não pode prescindir da verificação criteriosa das provas apresentadas, sobretudo quando produzidas por meio digital. Assim, é fundamental que autoridades policiais, membros do Judiciário e peritos estejam alinhados com boas práticas e protocolos claros, que assegurem o controle sobre cada fase do manuseio da prova digital.

Dessa forma, o presente trabalho tem por objetivo analisar a cadeia de custódia aplicada às provas digitais no processo penal brasileiro, abordando os desafios práticos de sua implementação, os impactos jurídicos decorrentes de sua violação e propondo melhorias nos protocolos existentes. Para tanto, serão

utilizados métodos de pesquisa bibliográfica e análise jurisprudencial, com foco na aplicação prática do tema à luz da legislação atual e de doutrinas especializadas.

2. PROVA DIGITAL

As provas permitem a reconstrução histórica e dinâmica dos fatos ocorridos. É a partir de sua análise que se aplica o Direito, sendo a prova conceituada como todo meio lícito e legítimo utilizado para demonstrar a veracidade de um fato alegado.

Conforme explica Renato Marcão (2023, p.194) “A prova produzida em juízo serve para a demonstração da verdade que se pretende ver formalmente reconhecida, para que dela decorram os efeitos jurídicos previstos em lei”. Esse convencimento trata-se do objetivo da prova que consiste na demonstração da veracidade ou falsidade das alegações feitas no processo pelas partes, em que aponta o fato pela acusação ou defesa para que possa ser esclarecido, para que o Juiz possa analisá-lo e formar seu convencimento no momento de proferir a decisão.

As provas digitais caracterizam-se como provas atípicas no processo penal. Sob a perspectiva de Gustavo Badaró (2025), como não possuem rito probatório preestabelecido pelo legislador, sua admissibilidade deve passar por um controle mais rigoroso, podendo ter a produção de provas atípicas, entretanto, não significa que possam ser inseridas no material probatório e valoradas pelo juiz.

Os meios de provas admitidos estão previstos no título VII do Código de Processo Penal, a partir do artigo 155 que estabelece a regra geral de valoração da prova, ou seja, expressa que o juiz deve formar sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão com base nos elementos informativos colhidos na investigação, salvo as peculiaridades das provas cautelares, não repetíveis e antecipadas.

Ademais, os seguintes artigos listam os meios de provas em espécie, sendo os principais: exame de corpo de delito, perícias em geral, interrogatório do acusado, confissão, declarações do ofendido, prova testemunhal, reconhecimento de pessoas e coisas, acareação, prova documental, indícios e busca e apreensão. A respeito, Aury Lopes Jr. (2025, p. 422) frisou que “indícios são concebidos como provas mais fracas, de menor confiabilidade e credibilidade, insuficientes para um juízo

condenatório, mas suficientes para decretação de medidas incidentais ou decisões interlocutórias".

Diante do contínuo avanço da tecnologia e o desenvolvimento da sociedade de informação, novos hábitos e transformações surgiram, especialmente no que se refere ao processamento e arquivamento de dados. O meio digital consolidou-se como a ferramenta mais usada no cotidiano para comunicação, interação e registro de atividades, passando a ter também relevante papel no campo jurídico, principalmente em relação ao surgimento da prova digital. Para Geraldo Prado (2021) essa evidência se caracteriza por ser "qualquer classe de informações (dados) que tenha sido produzida, armazenada ou transmitida por meios eletrônicos".

De acordo com Ricardo Capozzi (2025), essas evidências podem ser consideradas como instrumento probatório, utilizado para o convencimento do juízo, isto é, quaisquer informações com valor probatório, armazenado ou processado digitalmente. Nesse sentido, vale salientar que a prova digital possui caráter não material e uma linguagem não natural, podendo ser facilmente alterada, copiada ou até mesmo deletada, devido a sua congênita mutabilidade e sua vulnerabilidade a erros, torna-se indispensável o protocolo correto da completa e integral documentação da cadeia de custódia para assegurar a confiabilidade e evitar sua contaminação.

Sob essa perspectiva, vale destacar que as provas digitais são particularmente suscetíveis a manipulações imperceptíveis, o que demanda cuidados extras na sua obtenção e tratamento. A falta de rigor técnico e a ausência de procedimentos adequados podem comprometer a validade e a admissibilidade dessas provas no processo penal (Rodrigues, 2024).

As pessoas utilizam da tecnologia diariamente, sendo uma poderosa ferramenta para investigação criminal. Se um ato criminoso for praticado em meios digitais e deixar rastros ou vestígios, esses são considerados provas digitais. No entanto, deve-se atentar às peculiaridades e detalhes técnicos a serem seguidos no momento da extração das evidências. Conforme ressalta o autor Geraldo Prado (2021), a prova digital deve assegurar a transparência, controle, proporcionalidade e as condições concretas de efetivação do contraditório digital.

2.1.Meios de obtenção das provas digitais

As provas digitais são encontradas em uma vasta gama de meios eletrônicos que armazenam dados e arquivos. Entre as fontes mais comuns estão aparelhos celulares, computadores, câmeras de segurança, totens de reconhecimento facial e arquivos recebidos e enviados pela internet, cada qual demandando uma abordagem específica para a coleta das evidências.

Para acessar essa diversidade de fontes, a legislação processual penal prevê meios de obtenção específicos, como a utilização de ferramentas e metodologias apropriadas, cada um com seus próprios requisitos e procedimentos. Os principais meios são: a busca e apreensão de dispositivos eletrônicos, a quebra de sigilo de dados telemáticos armazenados, a interceptação do fluxo de comunicações e a coleta de dados em fontes abertas.

A busca e apreensão consiste em uma medida de coleta de provas, onde se inicia a cadeia de custódia no momento da apreensão física de determinado dispositivo, com seu devido acondicionamento e lacre, que busca assegurar a recolha e preservação de elementos úteis ao processo, conforme previsto no artigo 243 do Código de Processo Penal. Em relação aos dispositivos eletrônicos, o Marco Civil da Internet assegura a inviolabilidade e sigilo de dados (artigo 7º).

Ademais, a quebra de sigilo de dados telemáticos armazenados consiste em um meio de obtenção de acessos a dados que já foram armazenados e mantidos por provedores de aplicação, em que inicia a cadeia de custódia com o recebimento do material e a necessidade da verificação de sua integridade, conforme fundamenta o artigo 10 da Lei nº 12.965/14, que disciplina sobre o Marco Civil da Internet. Cabe ressaltar a diferença com a interceptação do fluxo de comunicações telemáticas, que consiste em um meio de obtenção em tempo real das comunicações, conforme disciplina o artigo 1º da Lei nº 9.296/96.

Já a coleta de dados em fontes abertas, consiste no meio de obtenção de mais fácil acesso e que dispensa a ordem judicial para ser obtido, pois este utiliza de dados publicamente acessíveis nas redes sociais sem violação de privacidade por utilizar de dados públicos.

Além dos meios de obtenção classicamente previstos, a realidade tecnológica impõe desafios complexos que testam os limites da legislação processual. O maior exemplo no Brasil contemporâneo é o sistema 'Smart Sampa' da cidade de São Paulo, que consiste no maior programa de monitoramento de segurança da América Latina, que usa o reconhecimento facial de câmeras inteligentes espalhadas pela cidade (públicas, de estabelecimento comerciais e residenciais que aderem ao programa) para auxiliar na busca de desaparecidos, identificação de foragidos da polícia e casos de violência urbana.

Este sistema representa um desafio para a cadeia de custódia. Em relação a falta de documentação da coleta da imagem em meio a milhares de câmeras, como garantir a integridade do arquivo contra manipulações e, principalmente, como a defesa pode auditar o algoritmo de reconhecimento facial. A ausência de protocolos claros para o manuseio dessas evidências representa um grave risco à validade da prova e ao próprio direito de defesa.

Ainda, em relação aos meios de obtenção de provas digitais possui o malware, que consiste na instalação de forma oculta no equipamento de um terceiro, por meio de um software malicioso, usado para acessar dados e coletar informações, o que fere os direitos fundamentais e garantias processuais dos investigados (Ribeiro; Cordeiro; Fumach, 2022).

Apesar de ser uma ferramenta potencialmente eficaz, o uso dessa tecnologia é atualmente ilícito no ordenamento jurídico brasileiro pela falta de previsão legal. Tal ilicitude evidencia a importância de se atentar ao caminho percorrido para a obtenção das provas digitais, pois os elementos probatórios obtidos por meios ilícitos e sem autorização do poder judiciário são inadmissíveis e não podem ser utilizados no processo penal.

Essa inadmissibilidade se fundamenta não apenas na ilicitude originária da coleta, mas também se estende a todas as provas dela decorrentes, em uma aplicação direta da Teoria dos Frutos da Árvore Envenenada (Fruit of the Poisonous Tree), conforme artigo 157, § 1º, do Código de Processo Penal. Nessa analogia, a instalação do *malware*, por ser um ato ilícito que viola a intimidade e o sigilo de dados sem autorização judicial, constitui a "árvore envenenada". Por consequência, qualquer informação ou evidência colhida por meio desse *software*, como

mensagens, arquivos ou senhas, representa um "fruto envenenado", tornando-se igualmente ilícita por derivação e, portanto, inadmissível seu uso no processo.

3.PRINCÍPIOS E NORMAS LEGAIS DA CADEIA DE CUSTÓDIA DA PROVA DIGITAL

A cadeia de custódia das provas digitais não se trata de uma consequência lógica do sistema de preservação do corpo de delito digital e sim uma garantia de natureza constitucional (Prado, 2021).

As provas, para serem inseridas ao processo, devem respeitar os princípios constitucionais de legalidade, do contraditório, da ampla defesa e da intimidade, conforme previsto nos incisos X, XII e LVI do artigo 5º da Constituição Federal.

Nesse contexto, o inciso X estabelece a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, protegendo a esfera mais pessoal do indivíduo. O inciso XII, por sua vez, garante a inviolabilidade do sigilo das comunicações de dados, permitindo sua quebra para fins de investigação criminal ou instrução processual penal somente mediante ordem judicial. Por fim, o inciso LVI consagra o princípio da vedação à prova ilícita, ao determinar que são inadmissíveis, no processo, as provas obtidas por meios ilícitos.

Além disso, no ordenamento jurídico brasileiro, vigora o princípio da atipicidade e o da liberdade da prova. O princípio da atipicidade dos meios de prova permite que se utilize de todos os meios de provas para demonstrar a verdade dos fatos, podendo ser meios não estabelecidos em lei, como provas atípicas, desde que estas sejam obtidas por meios legais e respeitem os direitos fundamentais e garantias processuais. conforme disciplina o artigo 369 do Código de Processo Civil que se aplica por analogia no Processo Penal (Capozzi,2025).

O princípio da liberdade da prova ou do livre convencimento motivado, previsto no artigo 155 do Código de Processo Penal, estabelece que o juiz é livre para apreciar e valorar as provas apresentadas no processo. Essa liberdade refere-se à análise do conjunto probatório admitido nos autos, podendo utilizar além dos meios de provas previstos em lei, outros métodos não tipificados, desde que sejam lícitos, moralmente legítimos e que sua decisão seja fundamentada.

Face a isso, é importante destacar o princípio da mesmidade, como ferramenta essencial, em que visa assegurar a integridade da prova digital. Segundo o Ministro Rogerio Schietti Cruz (2021), esse princípio pretende garantir a autenticação de uma prova, sendo um dos métodos que assegura ser o item apresentado aquilo que se afirma ser desde o seu início. Tem por objetivo garantir, por meio de técnicas criptográficas como o algoritmo hash, juntamente com softwares confiáveis e auditáveis, que o vestígio digital analisado seja idêntico ao original que foi coletado, livre de qualquer alteração.

A admissibilidade e a valoração da prova digital no processo penal brasileiro são regulamentadas por um conjunto de princípios e normas que visam garantir a autenticidade, integridade e confiabilidade das provas. Essa estrutura parte de uma regra geral sobre a necessidade da prova pericial e de protocolos técnicos detalhados, especialmente no que diz respeito à cadeia de custódia.

O tratamento da prova no processo penal inicia-se com o dever geral imposto pelo artigo 158 do Código de Processo Penal, que torna indispensável o exame de corpo de delito sempre que a infração deixar vestígios. No contexto digital, qualquer informação oriunda de meios eletrônicos é considerada por deixar vestígios e sua preservação é o primeiro passo para a persecução penal. Para assegurar a idoneidade do vestígio desde sua coleta até o descarte, o Pacote Anticrime (Lei nº 13.964/2019) instituiu a cadeia de custódia no ordenamento jurídico.

Em seu artigo 158-A do Código de Processo Penal, define esta como o conjunto de procedimentos que documentam a história cronológica e detalhada do vestígio. No seu §2º, estabelece que a responsabilidade pela preservação inicial é atribuída ao agente público que primeiro reconhecer o potencial probatório do elemento.

A rastreabilidade, conforme disciplinam os artigos 158-B e 158-D, visa proteger os vestígios de forma que não altere seu estado e preserve suas características, garantindo sua inviolabilidade e idoneidade ao impedir contaminações e controlar sua posse.

O artigo 3.5 da Portaria SENASP nº 82/2014 desempenha um papel fundamental ao detalhar os procedimentos práticos da cadeia de custódia,

materializando o princípio da rastreabilidade, determinando que cada vestígio seja registrado individualmente em formulário específico. A norma exige que constem dados essenciais como a descrição do vestígio, sua identificação numérica, o local e a data da coleta e, fundamentalmente, o registro de todos os agentes públicos que o manusearam, desde o coletor até o recebedor, incluindo as informações sobre a transferência de custódia. Tal procedimento visa criar um histórico documental completo, assegurando a rastreabilidade e a transparência de cada etapa da cadeia de custódia.

Ademais, a norma ABNT ISO/IEC 27037:2013 tem por finalidade normatizar o tratamento das evidências digitais, para obter sua admissibilidade e força probatória, abordando sobre as atividades essenciais de identificação, coleta, aquisição e a preservação de dados. Tem como objetivo guiar a persecução penal, auxiliar no suporte de procedimentos disciplinares internos e na comunicação de elementos probatórios entre diferentes jurisdições.

Sua aplicação estabelece diretrizes para padronizar as ações relacionadas ao manuseio das provas digitais, abrangendo sua identificação, aquisição, coleta e preservação do que pode ter valor probatório. O processo de tratamento das evidências digitais pode ser compreendido como um fluxo contínuo e metodológico, que salienta a importância da cadeia de custódia nessa primeira fase.

4. IMPLEMENTAÇÃO PRÁTICA DA CADEIA DE CUSTÓDIA DA PROVA DIGITAL

A cadeia de custódia é indispensável para análise de dados digitais, visa assegurar a autenticidade, integridade e confiabilidade dos elementos coletados durante uma investigação, possibilitando a documentação, ordem cronológica das evidências e os responsáveis pelo manuseio dos vestígios.

Uma vez estabelecidos os fundamentos legais e principiológicos da cadeia de custódia no capítulo anterior, torna-se essencial detalhar sua implementação prática no cenário investigativo. Foi formalmente instituída no processo penal brasileiro pela Lei nº 13.964/2019, com o artigo 158-A que define:

> Art. 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.
>
> § 1º 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.
>
> § 2º O agente público que reconhecer um elemento como de potencial interesse para a produção da prova pericial fica responsável por sua preservação.
>
> § 3º Vestígio é todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal.

Segundo Nucci (p.246, 2025), a cadeia de custódia é responsável por assegurar a preservação do local do crime, do reconhecimento primário dos elementos coletados até o seu descarte. Nesse contexto, a não realização da cadeia de custódia corretamente pode levar a nulidade relativa, passível de demonstração de prejuízo pela parte interessada.

Esse instituto do Código de Processo Penal, define e visa assegurar a documentação e as etapas da cadeia de custódia da prova digital desde o momento do reconhecimento do vestígio até o seu descarte final. Conforme estabelece o artigo é crucial o isolamento e preservação do local do crime para não perder a cronologia dos fatos, chamada de externa até chegar ao instituto médico legal ou onde será analisada que passará a ser chamada de interna, no procedimento do laboratório até seu descarte.

As etapas consistem em uma sucessão criteriosa, que se inicia com o reconhecimento de um elemento como de potencial interesse para a produção da prova pericial e o imediato isolamento do ambiente para evitar que se altere o estado das coisas. Em seguida, realiza-se a fixação, que é a descrição detalhada do vestígio em sua localização original, podendo ser ilustrada por fotografias ou filmagens, para então se proceder à coleta do material que será submetido à análise.

Uma vez recolhido, o vestígio passa pelo acondicionamento, no qual é embalado de forma individualizada com as devidas anotações, e pelo transporte, um

ato de transferência que deve garantir a manutenção de suas características originais e o controle de sua posse. A fase subsequente é o recebimento, que formaliza a transferência da posse da prova de maneira documentada, dando início ao processamento, que trata-se do exame pericial, em que os resultados são formalizados em um laudo. Por fim, o material segue para o armazenamento em condições adequadas, onde fica guardado para eventuais perícias, até o seu descarte final.

4.1.O papel dos peritos na preservação e garantia de autenticidade das provas digitais

A coleta dos vestígios deve ser realizada preferencialmente por peritos oficiais, os quais são os responsáveis pela coleta e análise de evidências digitais, ou seja, pelo procedimento da cadeia de custódia.

Dessa forma, é essencial que os peritos sigam as diretrizes claras e criteriosas, incluindo a documentação detalhada das etapas da cadeia de custódia, conforme estabelece a Associação Brasileira de Normas Técnicas na NBR ISO/IEC 27.037/2013.

Os peritos são responsáveis pelo laudo técnico, que consiste em uma completa descrição do sistema informático, instrumentos utilizados e o relatório obtido, além do laudo pericial. Segundo Eoghan Casey (2011, p.76-77), o laudo pericial deve conter: introdução, descrição da fonte de provas, resumo do exame, exame do sistema de arquivos, análise forense, descobertas forenses e a conclusão.

Ademais, devido a vulnerabilidades e a possibilidade de manipulação e omissão das provas pelos peritos responsáveis, foi regulamentado pela legislação processual penal o artigo 158-B, a fim de disciplinar a coleta de evidências e os procedimentos a serem seguidos nos locais de crime, instituiu um protocolo específico para o tratamento de vestígios. A norma visa garantir a idoneidade da prova, a fim de assegurar que o perito acesse a cena do crime acompanhado pela autoridade policial, de modo a mitigar os riscos de adulteração e assegurar a preservação do local do crime e de todos os elementos materiais encontrados.

Logo, vale salientar que o papel do perito no tratamento da prova digital transcende a mera análise técnica, assumindo a função de uma verdadeira garantia

processual para as partes. Isso ocorre porque o modelo de perícia oficial adotado no Brasil exige um nível de rigor e confiabilidade que assegure a idoneidade do material probatório.

4.2.Procedimento e práticas adequadas para garantir a integridade das provas digitais

O procedimento de aquisição de provas digitais, por apresentar alto grau de vulnerabilidade a erros, necessita de uma gestão delicada, a qual exige uma cadeia de custódia ainda mais detalhada que as provas tradicionais. Ademais, deve salientar que o método deve garantir a integridade, imutabilidade e a proteção dos vestígios, na perspectiva de uma repetibilidade da análise pericial, evitando interferências suscetíveis de alteração e falsificação da atividade probatória (Capozzi,2025).

A utilização de métodos inadequados na coleta contamina a evidência, que perde sua idoneidade. Por essa razão, o manuseio de vestígios voláteis, que podem ser facilmente contaminados, exigem a aplicação de técnicas rigorosas de autenticação para prevenir qualquer alteração.

Ressalta-se, ainda, o uso do Código Hash para garantir a integridade dos arquivos digitais. Trata-se de um algoritmo criptográfico que gera uma assinatura digital única para cada arquivo, funcionando como uma "impressão digital" da evidência no momento de sua coleta. A verificação dessa assinatura em etapas posteriores permite atestar matematicamente se o arquivo permaneceu íntegro. A ausência dessa validação pode não apenas comprometer a admissibilidade da prova, como também abrir margem para nulidades processuais e contestações defensivas.

As centrais de custódia são de suma importância para garantir a integridade das provas digitais, conforme aponta o artigo 158-E da Lei nº 13.964/19. Tem por objetivo armazenar as provas obtidas do local do crime e garantir a inviolabilidade das provas no decorrer do processo. Sendo assim, cabe ao Estado assegurar a total integridade e idoneidade da prova, como também provar que ela não foi violada em nenhum momento, assegurando que a produção da evidência tenha sido transparente e qualificada, validando todas as fases do processo (Fernandes, 2022).

Nesse contexto, Nucci define as centrais de custódia como sendo uma boa solução para concentrar, num só local, os vestígios, conferindo a segurança devida e o acesso controlado ao local do crime.

Entretanto, o autor afirma que embora o ideal seria o armazenamento dos vestígios coletados na central de custódia de cada comarca, na maioria das cidades brasileiras não é possível cumprir este progresso e inovações. Nesse sentido, devido a falta das centrais em determinados locais, os vestígios ficam sob responsabilidade dos peritos. Além disso, no artigo 158-F da citada lei, determina que após a análise do perito deve retornar à central de custódia para seu armazenamento.

5.A QUEBRA DA CADEIA DE CUSTÓDIA DA PROVA DIGITAL

É fundamental destacar que o escopo da cadeia de custódia é amplo, abrangendo todos os indícios e provas pertinentes à elucidação do crime. A quebra da cadeia de custódia da prova consiste na falha ou interrupção da trajetória das provas, como na identificação, manuseio e descarte das informações usadas na investigação, a qual prejudica a confiabilidade e o contraditório por não permitir a garantia da integralidade da prova.

Dentro dessa problemática, a violação da cadeia de custódia resulta na perda do valor probatório dos vestígios encontrados e caso utilizar de meios ilícitos para obter a prova, afeta a confiabilidade da prova, o que leva ao juiz não poder usá-la para fundamentar sua decisão. Nesse contexto, Geraldo Prado (2025) aborda que as consequências jurídicas da quebra da cadeia de custódia não se submetem a juízo de peso probatório, sequer de relevância da prova.

Ademais, pode afetar a confiabilidade da evidência, do mesmo modo, segundo Lopes Júnior (2023) compromete o contraditório por não permitir a garantia da integralidade da prova, assim como de sua confiabilidade, não permitindo a auditoria do procedimento cronologicamente realizado pelos agentes públicos.

Sobre o tema, o Superior Tribunal de Justiça (STJ) tem consolidado o entendimento de que a falta de procedimentos adequados da cadeia de custódia, para garantir sua integridade e idoneidade dos dados extraídos de dispositivos eletrônicos, leva à quebra de confiabilidade da prova. Essa quebra, por sua vez,

torna a evidência desprovida de força probatória, não sendo possível usá-la para fundamentar uma condenação.

Assim, no julgamento do Agravo Regimental no Habeas Corpus (AgRg no HC) nº 828.054-RN, do relator Ministro Joel Ilan Paciornik, pela Quinta Turma, é unânime em seu resultado, ocorrido em 23 de abril de 2024 e publicado no Diário da Justiça Eletrônico em 29 de abril de 2024, reitera a exigência de autenticidade e integridade da potencial evidência digital, além da inadmissibilidade da prova por quebra da cadeia de custódia e a relevância das etapas, como documentar e validar a extração e análise dos dados encontrados.

Nesse acórdão, o tribunal considerou a prova inadmissível, afirmando que a simples apreensão do dispositivo e a juntada de "prints" não suprem a necessidade de uma perícia técnica que retira os dados seguindo os protocolos da cadeia de custódia. Conforme a decisão, é o procedimento pericial formal que garante a integridade e a idoneidade da evidência, não podendo ser substituído por métodos informais que não permitem a auditoria da prova. Este julgado reforça que a cadeia de custódia não se esgota no ato da apreensão, mas abrange, de forma indispensável, todo o processo de manuseio e análise do vestígio digital.

O Superior Tribunal de Justiça vem consolidando o entendimento de que a cadeia de custódia se refere à garantia da idoneidade e rastreabilidade do vestígio, desde sua coleta até a análise judicial. Nessa perspectiva, qualquer interferência ou falha documentada nesse percurso pode levar à não confiabilidade da prova por sua quebra. Contrariando uma visão mais tradicional, a jurisprudência recente do STJ tem apontado que o ônus de demonstrar a integridade da prova é do Estado, e não da defesa o de provar sua contaminação.

6.CONSIDERAÇÕES FINAIS

O presente artigo se propôs a analisar a complexa e indispensável aplicação da cadeia de custódia às provas digitais no processo penal brasileiro. Conforme demonstrado, a crescente evolução da tecnologia impôs ao sistema de justiça o desafio de garantir a integridade e a autenticidade de evidências voláteis e sensíveis, tornando a regulamentação do Pacote Anticrime um marco fundamental, porém não exaustivo, para a segurança jurídica.

Face a isso, é importante destacar a adoção de procedimentos adequados para garantir a validade das evidências, pois a ausência de uma cadeia de custódia adequada ou de uma documentação detalhada sobre o manuseio do vestígio compromete fatalmente sua confiabilidade, tornando imprestável para a formação do convencimento judicial.

Ao longo da pesquisa, constatou-se que a eficácia da cadeia de custódia digital depende de uma série de fatores. Primeiramente pelos artigos 158-A a 158-F do Código de Processo Penal, que formalizou procedimentos. Segundo, o pilar técnico, que se revelou essencial, pois a lei por si só é insuficiente sem a aplicação de práticas forenses rigorosas como o espelhamento forense e o uso de funções de hash para garantir matematicamente a integridade da prova. Terceiro, o pilar humano, que abrange a responsabilidade compartilhada de todos os agentes, além da importância do contraditório técnico, exercido pela fiscalização do trabalho do perito oficial por meio do assistente técnico.

Ressalta-se o relevante ponto da análise, que recaiu sobre as consequências da quebra da cadeia de custódia. Demonstrou-se que a posição adotada pelo Superior Tribunal de Justiça transcende a mera irregularidade formal.

A falha na documentação e preservação do vestígio digital não acarreta a nulidade automática do processo, mas sim compromete a confiabilidade da prova, tornando-a imprestável para fundamentar uma decisão. Conclui-se, portanto, que a principal consequência jurídica da quebra, caso a evidência contaminada seja o único pilar da acusação, é a absolvição do réu por insuficiência probatória, reforçando o caráter garantista do processo penal.

Apesar dos avanços legislativos e jurisprudenciais, a dificuldade na implementação de centrais de custódia em todo o território nacional, conforme apontado por Nucci, e a carência de recursos técnicos e de capacitação contínua para os peritos, são desafios práticos que ainda colocam em risco a aplicação efetiva da cadeia de custódia. A teoria, portanto, ainda enfrenta obstáculos estruturais para sua plena efetivação.

Por fim, fica evidente que a cadeia de custódia da prova digital não é apenas um procedimento técnico, mas uma ferramenta indispensável para a proteção de

direitos fundamentais, sendo um pilar para a legitimidade e a justiça das decisões no processo penal da era digital, especialmente em relação às novas tecnologias, como provas geradas por inteligência artificial, buscando a garantia de um processo justo e equitativo.

7.REFERÊNCIAS

AGRAVO REGIMENTAL NO HABEAS CORPUS. AgRg no HC 828054/RN. Disponível em: https://processo.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=%28%28AGRHC.clas.+ou+%22AgRg+no+HC%22.clap.%29+e+%40num%3D%22828054%22%29+ou+%28%28AGRHC+ou+%22AgRg+no+HC%22%29+adj+%22828054%22%29.suce.

BRASIL. Decreto-lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em 26 de junho de 2025.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm . Acesso em 22 de julho de 2025.

BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. Boletim IBCCRIM – ano 29 – n. 343 – junho de 2021- ISSN 1676-3661.

CAPOZZI, Ricardo Andrian. Provas Digitais e a Cadeia de Custódia. Academia de Forense digital. Disponível em: https://academiadeforensedigital.com.br/provas-digitais-e-a-cadeia-de-custodia/. Acesso em: 08 de julho de 2025.

CASEY, Eoghan. Digital Evidence and Computer Crime. Disponível em: https://rishikeshpansare.wordpress.com/wp-content/uploads/2016/02/digital-evidence-and-computer-crime-third-edition.pdf

Cadeia de Custódia da Prova e Princípio da Mesmidade. STJ, HC 653.515. Rel. Min. Rogerio Schietti Cruz. Julgado em 23/11/2021. Acesso em: https://buscador.tudodepenal.com/julgados/cadeia-de-custodia-da-prova-e-principio-da-mesmidade/

FERNANDES, Vitor Ribeiro. FERNANDES, Vinicius Ribeiro. Cadeia de custódia: as centrais de custódia na preservação idônea da prova. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano. 07, Ed. 07, Vol. 02, pp. 111-118. Julho de 2022. ISSN: 2448-0959. Disponível em: https://www.nucleodoconhecimento.com.br/lei/cadeia-de-custodia**.** Acesso em: 20 de julho de 2025.

LOPES JÚNIOR, Aury. Direito Processual Penal. 22. ed – São Paulo: Saraiva Educação. 2025.

LOPES, André Magno. A cadeia de custódia da prova digital no processo penal brasileiro. Trabalho de Conclusão de Curso. Governador Valadares, 2023.

MARCÃO, Renato. Curso de Processo Penal. 8. ed. São Paulo: Saraiva, 2023.

MEDEIROS, Flavia. Democracia e Direitos Humanos, Políticas de perícia criminal na garantia dos direitos humanos. Friedrich Ebert Stifung, 2020. Disponível em: https://library.fes.de/pdf-files/bueros/brasilien/16396-20200811.pdf .

NUCCI, Guilherme de Souza. Código de Processo Penal Comentado. 24. ed. São Paulo: Editora Forense, 2025.

OLIVEIRA, Vinicius Machado. Artigo sobre ABNT NBR ISO/IEC 27037:2013. Academia de Forense Digital. Disponível em: https://academiadeforensedigital.com.br/iso-27037-identificacao-coleta-aquisicao-e-preservacao-de-evidencia/ . Acesso em: 22 de julho de 2025.

PORTARIA SENASP Nº 82, DE 16 DE JULHO DE 2014. Disponível em: https://diariofiscal.com.br/ZpNbw3dk20XgIKXVGacL5NS8haIoH5PqbJKZaawfaDwCm/legislacaofederal/portaria/2014/senasp82.htm . Acesso em: 22 de julho de 2025.

PRADO, Geraldo. Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital. Site Geraldo Prado, 22 de janeiro de 2021. Disponível em: https://geraldoprado.com.br/artigos/breves-notas-sobre-o-fundamento-constitucional-da-cadeia-de-custodia-da-prova-digital/?utm_source=chatgpt.com. Acesso em: 26 de junho de 2025.

RIBEIRO, Gustavo A. M.; CORDEIRO, Pedro Ivo R. V.; FUMACH, Débora M. O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. Revista Brasileira de Direito Processual Penal- 2022. Disponível em: https://www.scielo.br/j/rbdpp/a/rhHb6tynNX5rNH74mNGHSrj/?lang=pt . Acesso em 10 de julho de 2025.

RODRIGUES, Bruno. Garantindo a integridade das provas digitais: A importância da cadeia de custódia. Migalhas, 2024. Disponível em: https://www.migalhas.com.br/depeso/406806/garantindo-a-integridade-das-provas-digitais-a-cadeia-de-custodia . Acesso em: 22 de julho de 2025.

SMART SAMPA. Inteligência para deixar São Paulo mais segura. Disponível em: https://smartsampa.prefeitura.sp.gov.br/#programa . Acesso em 20 de agosto de 2025.