REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

OS CRITÉRIOS DE INADMISSIBILIDADE DA PROVA DIGITAL EXTRAÍDA DE DISPOSITIVOS MÓVEIS POR QUEBRA DA CADEIA DE CUSTÓDIA NO PROCESSO PENAL

CRITERIA FOR THE INADMISSIBILITY OF DIGITAL EVIDENCE EXTRACTED FROM MOBILE DEVICES DUE TO BREACH OF CHAIN OF CUSTODY IN CRIMINAL PROCEDURE

Ciências Sociais Aplicadas • 06/11/2026

REGISTRO DOI: 10.70773/revistatopicos/793939732

Marcelo José Peres Gomes da Silva[1]

Fabrício Moraes de Almeida[2]

RESUMO

O presente artigo científico analisa os critérios jurídicos e técnico periciais de inadmissibilidade da prova digital extraída de dispositivos móveis apreendidos em razão da quebra da cadeia de custódia no processo penal brasileiro. A pesquisa, de abordagem qualitativa de natureza bibliográfica e documental, fundamenta-se na legislação processual penal, na doutrina especializada, em referenciais técnicos periciais e na jurisprudência do Superior Tribunal de Justiça. Examina as particularidades da obtenção e preservação de dados digitais, os mecanismos de controle de integridade, autenticidade e rastreabilidade, bem como as repercussões das irregularidades sobre a confiabilidade probatória e o exercício do contraditório. Já os resultados demonstram que a inobservância de procedimentos de custódia não implica, necessariamente, a inadmissibilidade da evidência, sendo indispensável avaliar a gravidade da falha, seus efeitos concretos e a possibilidade de verificação técnica posterior. Identificam-se três situações: irregularidades que não comprometem a confiabilidade da prova, deficiências passíveis de esclarecimento mediante exame complementar e rupturas que inviabilizam a verificação independente do material. Portanto, conclui-se que a inadmissibilidade se justifica quando o comprometimento da cadeia de custódia impede demonstrar, por meios tecnicamente verificáveis, a correspondência entre os dados originalmente obtidos e aqueles apresentados no processo, prejudicando sua confiabilidade e submissão ao contraditório.

Palavras-chave: Prova digital; Cadeia de custódia; Dispositivos móveis; Inadmissibilidade da prova; Processo penal.

ABSTRACT

This scientific article analyzes the legal and technical-expert criteria

for the inadmissibility of digital evidence extracted from seized mobile devices due to a breach in the chain of custody within the Brazilian criminal procedure. The research, adopting a qualitative approach of a bibliographic and documentary nature, is based on criminal procedural legislation, specialized doctrine, technical-expert references, and the jurisprudence of the Superior Court of Justice (STJ). It examines the particularities of obtaining and preserving digital data, the control mechanisms for integrity, authenticity, and traceability, as well as the repercussions of irregularities on evidentiary reliability and the exercise of the adversarial principle. The results demonstrate that failure to observe custody procedures does not necessarily imply the inadmissibility of the evidence; it is essential to evaluate the severity of the flaw, its concrete effects, and the possibility of subsequent technical verification. Three situations are identified: irregularities that do not compromise the reliability of the evidence, deficiencies that can be clarified through a complementary examination, and ruptures that render independent verification of the material unfeasible. Therefore, it is concluded that inadmissibility is justified when the impairment of the chain of custody prevents demonstrating, through technically verifiable means, the correspondence between the data originally obtained and those presented in the process, prejudicing its reliability and submission to adversarial scrutiny.
Keywords: Digital evidence; Chain of custody; Mobile devices; Inadmissibility of evidence; Criminal procedure.

1. INTRODUÇÃO

A crescente utilização de dispositivos móveis como fontes de evidências no processo penal brasileiro ampliou a relevância dos procedimentos destinados à preservação da prova digital. A extração

de dados desses equipamentos permite o acesso a informações potencialmente relevantes para a investigação e a persecução penal, mas envolve particularidades técnicas relacionadas à integridade, à autenticidade e à rastreabilidade do material obtido. Nesse contexto, a cadeia de custódia assume papel fundamental na documentação dos procedimentos de coleta, preservação, extração, armazenamento e análise, de modo a possibilitar a verificação da correspondência entre os dados originalmente obtidos e aqueles posteriormente apresentados no processo.

Embora os artigos 158-A a 158-F do Código de Processo Penal estabeleçam parâmetros para a preservação e a documentação da cadeia de custódia, a identificação de irregularidades nesses procedimentos suscita controvérsias quanto às suas consequências sobre a admissibilidade da prova digital. A questão assume particular relevância diante das características dos dados extraídos de dispositivos móveis, cuja confiabilidade depende de condições que permitam verificar sua origem, integridade e correspondência com o conteúdo originalmente obtido. Diante desse cenário, a pesquisa orienta-se pelo seguinte problema: quais critérios jurídicos e técnico periciais permitem reconhecer a inadmissibilidade da prova digital extraída de dispositivos móveis apreendidos em razão da quebra da cadeia de custódia no processo penal brasileiro?

Com o propósito de responder a essa questão, a pesquisa tem como objetivo geral identificar e sistematizar os critérios jurídicos e técnico periciais que fundamentam a inadmissibilidade da prova digital extraída de dispositivos móveis apreendidos em decorrência da quebra da cadeia de custódia. Especificamente, busca examinar as particularidades dessa modalidade probatória, analisar os parâmetros normativos e técnicos aplicáveis à sua preservação,

investigar as repercussões processuais das rupturas identificadas e avaliar o tratamento conferido à matéria pela jurisprudência do Superior Tribunal de Justiça. A articulação desses objetivos visa estabelecer parâmetros para distinguir irregularidades procedimentais de comprometimentos que inviabilizam a verificação confiável da evidência.

Metodologicamente, a investigação caracteriza-se como pesquisa qualitativa, de natureza bibliográfica e documental, desenvolvida mediante análise da legislação processual penal, da produção doutrinária especializada, de referenciais técnico periciais e de decisões do Superior Tribunal de Justiça. A abordagem adotada compreende o exame dos dispositivos legais relativos à cadeia de custódia, a identificação dos procedimentos técnicos aplicáveis à preservação e à extração de dados de dispositivos móveis e a análise dos fundamentos utilizados nos precedentes selecionados. A partir da articulação dessas fontes, busca-se sistematizar os critérios relevantes para a avaliação das consequências processuais decorrentes de falhas na preservação da evidência digital.

A relevância da pesquisa decorre da necessidade de conferir maior precisão à avaliação das consequências processuais das falhas na cadeia de custódia da prova digital, especialmente diante da complexidade técnica dos procedimentos de extração e preservação de dados de dispositivos móveis. A distinção entre desconformidades formais e rupturas capazes de comprometer a confiabilidade da evidência apresenta importância para a fundamentação das decisões judiciais e para o exercício efetivo do contraditório. Sob a perspectiva científica, o estudo contribui para a aproximação entre os parâmetros jurídico-processuais e os critérios

técnicos periciais, oferecendo uma sistematização voltada à análise da admissibilidade probatória.

Para alcançar os objetivos propostos, o artigo científico está estruturado em quatro tópicos, a saber: O primeiro examina as particularidades da prova digital no processo penal, com ênfase na extração de dados de dispositivos móveis apreendidos; O segundo aborda a cadeia de custódia e os parâmetros jurídicos e técnico periciais aplicáveis à preservação dessas evidências; O terceiro analisa as modalidades de ruptura da cadeia de custódia e suas repercussões processuais. Por fim, o quarto que examina a jurisprudência do Superior Tribunal de Justiça e sistematiza os critérios de inadmissibilidade da prova digital, considerando a gravidade das irregularidades, seus efeitos sobre a confiabilidade do material e a possibilidade de verificação técnica.

Logo após, conclusão e as referências.

2. A PROVA DIGITAL NO PROCESSO PENAL E A EXTRAÇÃO DE DADOS DE DISPOSITIVOS MÓVEIS APREENDIDOS

2.1. Prova Digital: Conceito e Particularidades

A crescente utilização de tecnologias digitais nas relações sociais fez com que informações produzidas, armazenadas ou transmitidas por sistemas computacionais passassem a assumir relevante função na reconstrução dos fatos no processo penal. Nesse contexto, a prova digital pode ser compreendida como aquela constituída por dados em formato digital, representados em sistema binário, existentes em suporte eletrônico ou transmitidos por redes de comunicação e capazes de representar fatos ou ideias relevantes para a atividade probatória. Em sentido técnico, a expressão refere-se

primordialmente à fonte de prova digital, embora também seja empregada para designar o elemento de prova obtido a partir desses dados (Saad; Rossi; Partata, 2024).

Destaca-se, que a prova digital apresenta características que a distinguem dos elementos probatórios tradicionalmente associados a suportes físicos. Entre elas destacam-se a imaterialidade, a volatilidade, o desprendimento em relação ao suporte em que os dados se encontram armazenados, a possibilidade de reprodução e a necessidade de intermediação tecnológica para que seu conteúdo possa ser compreendido. A imaterialidade decorre da própria natureza dos dados digitais, enquanto a volatilidade está relacionada à possibilidade de alterações, voluntárias ou involuntárias, mediante modificações na informação digital. Além disso, o conteúdo pode ser transferido entre diferentes suportes sem perder necessariamente sua essência informacional, circunstâncias que conferem à prova digital particularidades próprias quanto à sua obtenção, preservação e posterior utilização no processo penal (Saad; Rossi; Partata, 2024)

Neste giro, tem-se que a natureza digital desses elementos probatórios confere ao conjunto probatório características específicas, de imaterialidade ou invisibilidade, a volatilidade, a fragilidade e a dispersão. Tais atributos evidenciam que o dado digital não se confunde com o suporte físico em que eventualmente se encontra armazenado e pode estar sujeito a modificações, perda ou distribuição por diferentes ambientes tecnológicos. Essas particularidades justificam cuidados próprios em sua identificação, obtenção e preservação, especialmente porque a confiabilidade da prova dependerá da possibilidade de demonstrar que o conteúdo

posteriormente apresentado corresponde, de maneira verificável, àquele originalmente obtido (KIST, 2024).

A necessidade de intermediação tecnológica constitui outra particularidade relevante da prova digital, uma vez que os dados, em sua forma originária, não são diretamente perceptíveis pelos sentidos humanos, dependendo de dispositivos, sistemas e programas para que possam ser acessados e apresentados de maneira compreensível. Essa característica faz com que o conhecimento do conteúdo probatório esteja relacionado aos procedimentos empregados para sua obtenção e representação, tornando relevante distinguir a informação digital existente em determinada fonte dos meios utilizados para acessá-la e introduzi-la no processo. Tal distinção permite compreender que diferentes fontes digitais podem exigir formas igualmente distintas de obtenção da prova, aspecto que antecede a análise específica dos dados extraídos de dispositivos móveis apreendidos (Saad; Rossi; Partata, 2024).

2.2. Fontes Digitais e Meios de Obtenção da Prova Digital

A diversidade da prova digital decorre também da multiplicidade de fontes em que informações relevantes podem ser encontradas. Os dados podem estar armazenados em dispositivos eletrônicos, sistemas computacionais, servidores e serviços remotos, ou resultar de comunicações e atividades realizadas em ambientes digitais. A identificação da fonte assume importância porque não se confunde com o meio empregado para obtenção da prova: enquanto a fonte corresponde ao local, sistema ou suporte em que se encontram os dados de interesse, o meio de obtenção diz respeito ao procedimento jurídico e técnico utilizado para acessá-los e

incorporá-los à investigação ou ao processo. Essa distinção permite compreender que informações de natureza digital podem demandar procedimentos distintos conforme sua origem e as condições em que se encontram disponíveis (Saad; Rossi; Partata, 2024).

A distinção entre a fonte da prova e o meio empregado para sua obtenção assume especial relevância no ambiente digital. Saad, Rossi e Partata (2024) observam que a apreensão de um dispositivo eletrônico e o acesso aos dados nele armazenados constituem operações distintas, de modo que a obtenção física do suporte não se confunde com a obtenção das informações digitais nele contidas. Assim, um aparelho celular apreendido pode constituir o suporte em que se encontra determinada fonte de prova, enquanto o acesso e a extração de seu conteúdo representam etapa própria de obtenção dos elementos digitais de interesse. Essa diferenciação é relevante tanto para a definição dos procedimentos aplicáveis quanto para a posterior análise da regularidade da obtenção da prova.

Considerando a diversidade das fontes digitais e dos procedimentos empregados para sua obtenção, a presente pesquisa delimita seu objeto aos dados extraídos de dispositivos móveis apreendidos, especialmente *smartphones*. Nesse contexto, a distinção entre a apreensão do suporte físico e a aquisição de seu conteúdo digital assume relevância para a análise dos procedimentos técnicos utilizados, das condições de preservação da evidência e da possibilidade de verificar sua correspondência com o dispositivo de origem. Essa delimitação orienta o exame das particularidades da extração forense desenvolvido no tópico seguinte.

2.3. Dados Extraídos de Dispositivos Móveis Apreendidos

A obtenção de dados armazenados em dispositivos móveis não corresponde a uma operação tecnicamente uniforme. Na perícia digital, a extração forense pode assumir diferentes modalidades, entre as quais a extração física, a extração completa do sistema de arquivos, a extração lógica e a extração combinada, variando a quantidade e a natureza dos dados acessíveis em cada procedimento. A extração física aproxima-se da duplicação forense ao buscar uma imagem mais abrangente da unidade de memória do dispositivo, enquanto a extração lógica se restringe, em regra, aos arquivos acessíveis ao usuário, podendo não abranger determinados dados de aplicativos ou outros elementos existentes no equipamento. A extração combinada, por sua vez, associa modalidades distintas com o propósito de ampliar os resultados disponíveis para recuperação e análise. (Lorens, 2025, p. 238-239).

Especificamente, nos aparelhos celulares, a modalidade de extração empregada pode determinar a extensão e a natureza das informações recuperadas. Segundo Lourenço (2024, p. 210-215), diferentes técnicas de aquisição proporcionam níveis distintos de acesso ao conteúdo do dispositivo, de modo que a escolha do procedimento deve considerar as características do aparelho, do sistema operacional e os objetivos do exame. Consequentemente, os resultados obtidos devem ser analisados à luz do método empregado, uma vez que diferentes modalidades podem produzir conjuntos distintos de dados disponíveis para exame.

A definição do procedimento de extração exige, portanto, o conhecimento das características técnicas do dispositivo examinado. Figueiredo e França Júnior (2022, p. 88-89) destacam que elementos

de *hardware* e *software*, como modelo, sistema operacional, processador, capacidade de armazenamento e mecanismos de proteção, podem interferir nas possibilidades de acesso aos dados. Assim, a atividade pericial não se resume à utilização de uma ferramenta forense, mas pressupõe avaliação prévia das particularidades do aparelho para a seleção de um método de aquisição tecnicamente adequado.

A distinção entre a apreensão do dispositivo e a obtenção de seu conteúdo digital encontra respaldo técnico no relatório das Câmaras Técnicas de Cadeia de Custódia do Ministério da Justiça e Segurança Pública. O documento diferencia a coleta, correspondente à arrecadação física do material, da aquisição, que consiste na obtenção dos dados em formato binário, utilizando o termo extração como equivalente à aquisição. Ressalta, ainda, que o *hardware* pode constituir o próprio vestígio de interesse ou funcionar apenas como suporte físico da informação digital. Desse modo, a custódia do aparelho e os procedimentos de obtenção de seu conteúdo representam operações distintas, cuja diferenciação é essencial para compreender a preservação e a rastreabilidade da evidência digital (BRASIL, 2023, p. 361-362).

No exame dos dados digitais, importa também distinguir a cópia comum de arquivos da aquisição realizada mediante procedimentos forenses. Parodi (2024, p. 51-56) esclarece que a cópia ou imagem forense busca reproduzir o conteúdo da mídia de maneira tecnicamente verificável, mediante mecanismos de controle destinados a demonstrar a correspondência entre o material de origem e aquele submetido à análise, com preservação do original. Ressalta, contudo, que a obtenção de uma imagem forense integral nem sempre é tecnicamente possível, especialmente em

dispositivos móveis, cujas características, mecanismos de proteção e limitações de acesso podem restringir as modalidades de aquisição disponíveis. Nessas circunstâncias, a adequada documentação do procedimento efetivamente empregado assume especial relevância para a posterior verificação da evidência.

3. A CADEIA DE CUSTÓDIA E OS PARÂMETROS JURÍDICOS E TÉCNICO PERICIAIS DE PRESERVAÇÃO DA PROVA DIGITAL

3.1. Cadeia de Custódia: Conceito, Finalidade e Disciplina Legal

A cadeia de custódia recebeu disciplina expressa no Código de Processo Penal com a Lei nº 13.964/2019. Nos termos do art. 158-A, compreende o conjunto de procedimentos destinados a manter e documentar a história cronológica do vestígio, possibilitando o rastreamento de sua posse e de seu manuseio desde o reconhecimento até o descarte. O dispositivo estabelece, ainda, que a cadeia se inicia com a preservação do local do crime ou com procedimentos policiais ou periciais em que seja detectada a existência de vestígio, atribuindo responsabilidade por sua preservação ao agente público que o reconhecer como potencialmente relevante para a produção da prova pericial (BRASIL, 1941, art. 158-A).

O rastreamento legalmente previsto é desenvolvido pelo art. 158-B do Código de Processo Penal mediante etapas sucessivas de reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte do vestígio. A disciplina normativa evidencia que a cadeia de custódia acompanha o elemento probatório ao longo de todo o seu percurso, abrangendo desde sua identificação inicial até sua

destinação final e atribuindo relevância à documentação das sucessivas operações de coleta, transferência, exame e guarda (BRASIL, 1941, art. 158-B).

A continuidade desse rastreamento é reforçada pelos arts. 158-C a 158-F do Código de Processo Penal, que disciplinam a coleta, o acondicionamento, a guarda e a movimentação dos vestígios. Entre os mecanismos previstos, destacam-se o registro das circunstâncias de rompimento e substituição de lacres, a identificação das pessoas que tiveram acesso ao material armazenado e a documentação das ações realizadas durante sua tramitação. Essas exigências fornecem parâmetros normativos para a reconstrução posterior da posse, do acesso e das intervenções realizadas sobre o vestígio ao longo da cadeia de custódia (BRASIL, 1941, arts. 158-C a 158-F).

A cadeia de custódia relaciona-se diretamente à qualidade da prova, na medida em que possibilita verificar se a fonte probatória encontrada no local do crime ou em situação correlata corresponde àquela posteriormente submetida a exame e introduzida no processo. Para tanto, assume especial importância a documentação da história cronológica do vestígio entre sua identificação e submissão à análise pericial, permitindo a reconstrução posterior de sua existência e de seu percurso. (Saad Netto; Avolio; Borri, 2025, p. 105). Além de contribuir para a preservação física do vestígio, a cadeia de custódia permite documentar as intervenções realizadas e identificar as pessoas que tiveram contato com o material probatório ao longo de seu percurso, fornecendo elementos para a posterior reconstrução de sua história (Saad Netto; Avolio; Borri, 2025, p. 105-106).

A observância da cadeia de custódia não se resume ao cumprimento formal das etapas previstas nos arts. 158-A a 158-F do Código de Processo Penal. Sua finalidade também está relacionada à preservação da confiabilidade do elemento probatório e à possibilidade de verificar posteriormente sua identidade e seu percurso. Nesse contexto, a avaliação de eventuais falhas exige considerar não apenas a desconformidade procedimental, mas também suas repercussões concretas sobre a prova (Saad Netto; Avolio; Borri, 2025, p. 114-120).

A relevância da cadeia de custódia também se manifesta no exercício do contraditório, ao proporcionar às partes condições para examinar a confiabilidade da prova. Parodi (2024, p. 67-78) relaciona a documentação do percurso do vestígio à possibilidade de verificar sua origem, autenticidade e integridade, permitindo que o material probatório seja submetido a controle pelos sujeitos processuais. Sob essa perspectiva, a cadeia de custódia não constitui finalidade em si mesma, mas instrumento de preservação das condições necessárias à verificação e à contestação da prova no processo penal.

3.2. Particularidades da Cadeia de Custódia dos Vestígios Digitais

No âmbito dos vestígios digitais, a preservação da cadeia de custódia assume particular relevância diante da possibilidade de alteração, sobrescrita ou manipulação dos dados sem sinais necessariamente perceptíveis pela simples observação de seu conteúdo. Por essa razão, a confiabilidade da evidência exige condições para verificar tecnicamente sua origem, os procedimentos empregados na obtenção e as circunstâncias de sua preservação, não se esgotando na análise da informação apresentada (Saad Netto; Avolio; Borri, 2025, p. 124-126).

A aplicação dessas etapas aos vestígios digitais exige considerar as particularidades próprias dessa espécie de material. As Câmaras Técnicas de Cadeia de Custódia do Ministério da Justiça e Segurança Pública estabeleceram correspondência entre as fases previstas no art. 158-B do Código de Processo Penal e seu desenvolvimento no ambiente digital, distinguindo, inclusive, as situações relacionadas ao material físico que contém os dados daqueles referentes ao próprio vestígio digital submetido ao exame pericial. No reconhecimento, por exemplo, a identificação deve considerar não apenas os suportes usualmente apreendidos, mas também circunstâncias como a existência de dados criptografados, conexões ativas com fontes remotas e outros elementos capazes de interferir na identificação e posterior preservação do conteúdo de interesse (BRASIL, 2023, p. 363).

Nos dispositivos móveis, a preservação da cadeia de custódia apresenta uma particularidade adicional: a aquisição dos dados nem sempre pode ocorrer sem interação com o aparelho. Figueiredo e França Júnior observam que determinadas modalidades de extração exigem que o dispositivo esteja em funcionamento, circunstância em que a inicialização do sistema e as operações necessárias ao acesso às informações podem modificar seu estado. Assim, a preservação da evidência não pressupõe necessariamente a absoluta imutabilidade do aparelho, mas exige que as intervenções tecnicamente indispensáveis sejam controladas, reduzidas e documentadas, permitindo a posterior avaliação de seus efeitos (Figueiredo; França Júnior, 2022, p. 82-83).

Nesse contexto, a ABNT NBR ISO/IEC 27037:2013 relaciona a preservação da cadeia de custódia à manutenção de documentação capaz de registrar o percurso da potencial evidência digital e as

intervenções realizadas durante seu tratamento. A norma atribui relevância ao registro das transferências de custódia e das ações executadas sobre o material, de modo que seja possível identificar sua movimentação e reconstruir posteriormente as condições em que foi coletado, adquirido e preservado. A documentação constitui, assim, elemento técnico necessário à auditabilidade do tratamento conferido à evidência e à avaliação posterior de sua integridade e confiabilidade (ABNT, 2013, itens 6.1 e 6.6).

A estrutura legal da cadeia de custódia também não deve ser compreendida como sequência inflexível e invariável de atos. As Câmaras Técnicas de Cadeia de Custódia do Ministério da Justiça e Segurança Pública observam que, no tratamento de materiais com conteúdo digital, as etapas previstas no art. 158-B podem não ocorrer necessariamente na ordem em que são apresentadas pela legislação, a depender do contexto policial ou pericial em que o vestígio é reconhecido e submetido a tratamento. Essa particularidade reforça que a regularidade da cadeia deve ser examinada a partir da adequada documentação e da possibilidade de reconstrução do percurso efetivamente realizado, e não apenas pela reprodução formal de uma sequência abstrata de etapas (BRASIL, 2023, p. 366-367).

3.3. Integridade, Autenticidade, Identidade e Rastreabilidade

A finalidade atribuída à cadeia de custódia evidencia que integridade, autenticidade, identidade e rastreabilidade não constituem preocupações periféricas, mas propriedades diretamente relacionadas à possibilidade de demonstrar a correspondência entre o vestígio originalmente obtido e aquele

posteriormente examinado e apresentado no processo. (Saad Netto; Avolio; Borri, 2025, p. 105-106).

No âmbito da prova digital, a aferição dessas propriedades assume especial importância, pois integridade e autenticidade não decorrem da simples existência ou visualização de determinado arquivo, mensagem ou informação. A confiabilidade probatória pressupõe a existência de elementos que permitam verificar se os dados apresentados correspondem àqueles originalmente obtidos e se permaneceram preservados ao longo de seu percurso até sua utilização no processo. (Saad Netto; Avolio; Borri, 2025, p. 124-128).

Nesse exame, mostra-se relevante distinguir a integridade da integralidade da prova digital. Parodi relaciona a integridade à ausência de alterações indevidas no conteúdo do vestígio, enquanto a integralidade diz respeito à preservação do conjunto probatório em sua extensão necessária, sem supressões capazes de comprometer sua compreensão ou análise. Assim, determinado material pode permanecer íntegro quanto ao conteúdo efetivamente apresentado e, ainda assim, não ser integral, caso parte dos dados ou elementos necessários à sua contextualização não tenha sido preservada ou disponibilizada (Parodi, 2024, p. 79-81).

A correspondência entre o vestígio originalmente obtido e aquele posteriormente submetido ao processo também pode ser compreendida a partir do princípio da mesmidade. Kologeski relaciona esse princípio à necessidade de demonstrar que a prova apresentada permanece substancialmente a mesma ao longo de seu percurso, sem alterações capazes de comprometer sua integridade. No ambiente digital, essa verificação assume particular complexidade diante da facilidade de modificação dos dados, razão

pela qual a demonstração da mesmidade depende de mecanismos que permitam controlar objetivamente a permanência da evidência entre diferentes momentos de sua obtenção, preservação e análise (Kologeski, 2026, p. 35-36).

O controle da integridade dos dados obtidos em procedimentos de duplicação ou extração forense pode ser realizado mediante funções de resumo criptográfico, usualmente denominadas funções *hash*. Por meio desse mecanismo, determinado conjunto de dados é submetido a um algoritmo que produz um valor de tamanho definido, permitindo a posterior comparação dos resultados como instrumento de verificação da integridade do material digital. Entre as propriedades relevantes dessas funções encontram-se o determinismo, a resistência à inversão e a resistência a colisões, características que fundamentam sua utilização no controle de integridade de artefatos digitais submetidos à análise pericial. (Lorens, 2025, p. 240-241).

A utilidade probatória desse mecanismo se evidencia especialmente na comparação entre o vestígio digital e as cópias produzidas para exame. Kologeski explica que o cálculo e o registro dos valores *hash* em momentos distintos permitem verificar se os dados submetidos à análise permanecem correspondentes àqueles anteriormente preservados, de modo que a coincidência dos valores constitui elemento técnico de confirmação de integridade, enquanto sua divergência indica a ocorrência de alteração que deve ser identificada e investigada. Na atividade forense, esse procedimento pode ser aplicado tanto ao conjunto de dados quanto a arquivos individualmente considerados, permitindo diferentes níveis de controle sobre o material examinado (Kologeski, 2026, p. 30-33).

3.4. Auditabilidade, Repetibilidade, Reprodutibilidade e Verificabilidade Técnica

A confiabilidade da prova digital relaciona-se à possibilidade de controle posterior dos procedimentos utilizados para sua obtenção, preservação e apresentação, de modo que seja possível reconstruir o caminho percorrido pelo elemento probatório e examinar as condições em que foi produzido. A insuficiência de documentação acerca desses procedimentos pode dificultar ou impedir a verificação da autenticidade e da integridade dos dados, comprometendo a possibilidade de controle técnico da prova apresentada no processo. (Saad Netto; Avolio; Borri, 2025, p. 124-128).

Essa possibilidade de controle encontra parâmetros técnicos específicos na ABNT NBR ISO/IEC 27037:2013, que identifica como aspectos relevantes do tratamento da evidência digital a auditabilidade, a justificabilidade e, conforme as circunstâncias, a repetibilidade ou a reprodutibilidade dos procedimentos. A auditabilidade relaciona-se à possibilidade de avaliação independente das atividades realizadas, o que pressupõe documentação adequada das ações e das decisões adotadas. A repetibilidade refere-se à obtenção dos mesmos resultados mediante os mesmos procedimentos, instrumentos e condições, enquanto a reprodutibilidade considera a obtenção de resultados equivalentes mediante o mesmo método, porém com instrumentos ou condições diferentes. A justificabilidade, por sua vez, exige que as ações e os métodos empregados no tratamento da potencial evidência digital possam ser tecnicamente fundamentados (ABNT, 2013, itens 5.3.1-5.3.5).

A verificabilidade da prova digital pode envolver, ainda, o exame de informações técnicas associadas aos próprios arquivos e aos sistemas em que foram produzidos ou armazenados. Kologeski destaca que metadados podem registrar elementos como datas de criação e modificação, autoria, características do arquivo e outras informações relevantes, enquanto *logs* de sistemas e aplicativos podem documentar eventos relacionados ao acesso, à criação, à alteração ou à movimentação de dados. A análise conjunta desses registros permite identificar inconsistências cronológicas e outras divergências capazes de indicar a necessidade de investigação técnica mais aprofundada sobre a origem e o percurso da evidência digital (Kologeski, 2026, p. 36-39).

A possibilidade de controle técnico da prova digital depende da existência de documentação suficientemente detalhada acerca dos procedimentos empregados durante o exame pericial. O registro da metodologia utilizada, das ferramentas e respectivas versões, das intervenções realizadas e das condições em que os vestígios foram manipulados permite reconstruir posteriormente as etapas do exame e verificar a forma pela qual os resultados apresentados foram produzidos. (Lorens, 2025, p. 246-249).

3.5. Parâmetros Técnicos de Aquisição e Preservação

A aquisição de vestígios digitais deve ser conduzida mediante procedimentos que busquem preservar as características do material originalmente encontrado e reduzir intervenções capazes de alterar seu conteúdo. Sempre que tecnicamente possível, a análise deve ser realizada sobre cópia obtida por procedimento forense, preservando-se o vestígio original e documentando-se as operações realizadas durante sua aquisição e tratamento. A escolha

do método empregado deve considerar as características do dispositivo e as possibilidades técnicas de acesso aos dados nele armazenados. (Lorens, 2025, p. 237-240). Sob essa perspectiva, a ABNT NBR ISO/IEC 27037:2013 orienta que o procedimento de aquisição inclua método capaz de estabelecer a exatidão e a confiabilidade da cópia da evidência digital em relação à fonte original, devendo os métodos empregados e as atividades realizadas ser adequadamente documentados. A norma prevê, ainda, a verificação da fonte original e da cópia mediante função de verificação apropriada, inserindo o controle de integridade em um procedimento mais amplo de demonstração da correspondência entre o material adquirido e sua origem (ABNT, 2013, itens 5.2 e 5.4.4).

A utilização de funções *hash*, contudo, não deve ser compreendida como garantia absoluta ou autossuficiente da integridade da prova digital. Fisberg observa que esse mecanismo constitui importante instrumento de verificação, mas apresenta limitações e não soluciona, isoladamente, os diferentes problemas relacionados à admissibilidade dos vestígios digitais. Sua utilização deve ser compreendida em conjunto com os demais procedimentos de aquisição, preservação e documentação da evidência, permitindo avaliar tecnicamente a correspondência entre os dados examinados e aqueles originalmente obtidos (Fisberg, 2025).

No âmbito institucional brasileiro, as Câmaras Técnicas de Cadeia de Custódia do Ministério da Justiça e Segurança Pública também estabeleceram recomendações específicas para vestígios digitais. Entre elas, encontra-se a associação aos arquivos digitais obtidos durante a investigação de funções de resumo criptográfico (*hash*), com o respectivo registro nos autos, além da preservação dos

vestígios digitais processados em estrutura de custódia ou ambiente seguro. Essas recomendações demonstram a incorporação, no âmbito da política técnico-pericial nacional, de mecanismos destinados ao controle de integridade e à preservação dos vestígios digitais ao longo de seu tratamento (BRASIL, 2023, seção 2.9).

No âmbito específico dos dispositivos móveis, esses cuidados devem ser observados desde o momento da coleta, considerando que a conectividade do aparelho e sua interação com sistemas e redes podem ocasionar modificações nos dados antes mesmo da extração. A adoção de medidas destinadas ao isolamento das comunicações do dispositivo, associada ao registro de suas condições, identificação, acondicionamento e demais procedimentos realizados, busca reduzir a possibilidade de alteração do conteúdo e preservar as características do vestígio até a realização do exame pericial (Lourenço, 2024, p. 208-210).

A preservação do vestígio após sua coleta exige, ainda, a manutenção de registros capazes de documentar sua movimentação e as sucessivas intervenções realizadas até o exame. Figueiredo e França Júnior destacam a necessidade de registrar operações de abertura e novo lacre, bem como os atos de transporte e transferência do material entre responsáveis ou diligências, de forma que seja possível identificar quem teve acesso ao vestígio e reconstruir sua continuidade ao longo da cadeia de custódia. A relevância desses registros reside, portanto, menos na formalidade considerada isoladamente e mais na possibilidade de preservar a rastreabilidade das pessoas, intervenções e deslocamentos relacionados ao dispositivo apreendido (Figueiredo; França Júnior, 2022, p. 84-87). A movimentação da evidência digital não se limita, contudo, ao deslocamento físico do dispositivo. O relatório das

Câmaras Técnicas de Cadeia de Custódia do Ministério da Justiça e Segurança Pública observa que dados digitais podem ser transferidos eletronicamente entre sistemas ou unidades, circunstância que exige cautelas destinadas à preservação de suas características durante a transmissão. O documento exemplifica essa necessidade com o risco de arquivos multimídia sofrerem compressão no processo de transferência, além de ressaltar que as sucessivas transferências de posse devem ser devidamente documentadas. A rastreabilidade da prova digital abrange, assim, tanto o percurso físico do suporte quanto a circulação eletrônica dos próprios dados (BRASIL, 2023, p. 365).

Além dos mecanismos de controle de integridade, a preservação da prova digital depende da documentação suficientemente detalhada das etapas realizadas durante sua obtenção. Pereira destaca a importância do registro das condições em que o dispositivo foi encontrado e coletado, incluindo sua identificação e o estado relevante do aparelho, bem como da documentação dos procedimentos empregados na obtenção dos dados e das operações realizadas sobre o vestígio. Esses registros permitem reconstruir posteriormente o tratamento conferido à evidência e verificar as condições em que os dados foram obtidos e preservados, contribuindo para sua rastreabilidade e para o controle técnico de sua autenticidade e integridade ao longo da cadeia de custódia (Pereira, 2024, p. 232-239).

A sistematização desses cuidados encontra referência técnica na ABNT NBR ISO/IEC 27037:2013, norma atualmente vigente que estabelece diretrizes para a identificação, coleta, aquisição e preservação de evidências digitais que possam possuir valor probatório. Seu campo de aplicação alcança, portanto, etapas

diretamente relacionadas ao tratamento inicial do vestígio digital e à manutenção de condições adequadas para sua posterior utilização e exame, fornecendo parâmetros técnicos para orientar o manuseio da evidência sem substituir a disciplina jurídica aplicável à sua admissibilidade (ABNT, 2013).

4. A QUEBRA DA CADEIA DE CUSTÓDIA DA PROVA DIGITAL E SUAS REPERCUSSÕES PROCESSUAIS

4.1. Caracterização da Quebra da Cadeia de Custódia

No âmbito dos vestígios digitais, a quebra da cadeia de custódia pode decorrer de falhas relacionadas à preservação do material, à ausência ou insuficiência de registros sobre sua manipulação e aos procedimentos empregados durante a aquisição e o exame pericial. Considerando a possibilidade de alteração dos dados durante o manuseio e a necessidade de reconstrução das operações realizadas, a documentação das intervenções, dos métodos e das ferramentas utilizadas assume particular relevância para que se possa verificar posteriormente as condições em que o vestígio foi obtido, preservado e analisado. (Lorens, 2025, p. 246-249).

Essa caracterização assume contornos específicos quando a evidência provém de aparelho celular, pois sua produção envolve etapas sucessivas de coleta, extração, análise e apresentação, submetidas à continuidade da cadeia de custódia. Lourenço destaca a necessidade de que os procedimentos realizados sobre o dispositivo sejam documentados de forma a permitir a identificação do vestígio, o conhecimento das intervenções executadas e a reconstrução do percurso dos dados até sua apresentação como prova. Nesse contexto, a deficiência de registros ou de

procedimentos que inviabilize essa reconstrução pode ultrapassar a mera desconformidade operacional e comprometer a possibilidade de demonstrar a correspondência entre os dados obtidos do dispositivo e aqueles posteriormente utilizados no processo (Lourenço, 2024, p. 206-221).

4.2. Irregularidade Formal e Comprometimento Material da Prova

A disciplina introduzida pela Lei nº 13.964/2019 estabeleceu procedimentos destinados à manutenção da cadeia de custódia, sem, contudo, prever expressamente uma consequência processual única para sua inobservância. Essa ausência de cominação específica contribuiu para o surgimento de diferentes construções doutrinárias acerca dos efeitos decorrentes da quebra da cadeia. (Saad Netto; Avolio; Borri, 2025, p. 107-108).

Nesse contexto, Meireles distingue a quebra formal da dimensão material da irregularidade, relacionando a primeira à inobservância dos requisitos aplicáveis ao tratamento da prova e a segunda aos efeitos produzidos pela falha sobre o elemento probatório e sua utilização no processo. A distinção evidencia que a identificação de uma desconformidade não esgota a análise da cadeia de custódia, sendo necessário considerar também as consequências concretamente decorrentes da irregularidade. (Meireles, 2026, p. 34). Essa diferenciação se insere em um debate doutrinário mais amplo acerca das consequências da quebra da cadeia de custódia. O panorama doutrinário apresentado pelos autores demonstra que a quebra da cadeia de custódia não recebe tratamento jurídico uniforme, coexistindo entendimentos que a aproximam da inadmissibilidade, da ilicitude ou nulidade e outros que condicionam sua repercussão à análise das circunstâncias concretas,

da confiabilidade do vestígio e do prejuízo produzido. (Saad Netto; Avolio; Borri, 2025, p. 108-113).

Em sentido convergente, a doutrina ressalta que a quebra da cadeia de custódia não deve ser compreendida como mera irregularidade administrativa quando a falha compromete a própria confiabilidade do vestígio. A repercussão processual depende da natureza e da gravidade da ruptura, especialmente quando a deficiência impede demonstrar a correspondência entre o elemento originalmente colhido e aquele posteriormente apresentado em juízo. Nessa perspectiva, a ausência de rastreabilidade ou a impossibilidade de aferição da integridade pode deslocar a discussão do plano meramente formal para o comprometimento material da prova (Silva, 2026, p. 38-41).

No caso dos dados provenientes de aparelhos celulares, essa diferenciação exige considerar os efeitos técnicos produzidos pela falha identificada. Lourenço demonstra que a produção da prova digital envolve procedimentos sucessivos de coleta, extração, análise e apresentação, nos quais a identificação do dispositivo, o registro das operações realizadas e a preservação de elementos de controle permitem acompanhar o percurso da evidência. Desse modo, a relevância de eventual deficiência deve ser examinada também à luz da possibilidade de reconstruir o procedimento realizado e verificar a correspondência entre os dados obtidos do aparelho e aqueles posteriormente submetidos à análise e apresentados no processo (Lourenço, 2024, p. 206-221).

Essa análise exige considerar, ainda, que determinadas alterações no estado do dispositivo podem decorrer da própria execução do procedimento tecnicamente necessário à obtenção dos dados.

Figueiredo e França Júnior observam que algumas modalidades de extração demandam o funcionamento e a interação com o aparelho, circunstâncias capazes de produzir modificações em seu sistema durante a atividade pericial. Desse modo, a ocorrência de alteração no vestígio digital não deve ser tomada, isoladamente, como demonstração de comprometimento material da prova, tornando-se necessário examinar a natureza da intervenção realizada, sua necessidade técnica, sua documentação e seus efeitos sobre a possibilidade de verificar a integridade e a confiabilidade dos dados obtidos (Figueiredo; França Júnior, 2022, p. 82-83).

Embora direcionado ao exame do local da infração, o Código de Processo Penal também contempla, no art. 169, parágrafo único, a necessidade de que alterações constatadas pelos peritos sejam registradas no laudo e tenham suas consequências discutidas tecnicamente. A previsão reforça, em perspectiva normativa geral da atividade pericial, que a constatação de uma modificação não esgota sua avaliação probatória, sendo igualmente relevante documentar sua ocorrência e examinar os efeitos que dela decorreram (BRASIL, 1941, art. 169, parágrafo único).

4.3. Repercussões Sobre Integridade, Autenticidade, Rastreabilidade e Verificabilidade

No contexto da prova digital, a quebra da cadeia de custódia adquire especial relevância quando a falha identificada repercute sobre a possibilidade de demonstrar a integridade, a autenticidade e a confiabilidade dos dados apresentados no processo. A deficiência na documentação dos procedimentos empregados na obtenção e preservação do material pode impedir a adequada reconstrução de seu percurso e dificultar a verificação posterior acerca da

correspondência entre o dado originalmente obtido e aquele efetivamente apresentado como prova. (Saad Netto; Avolio; Borri, 2025, p. 124-128). Sob uma perspectiva complementar, Meireles destaca que a contaminação da prova digital pode ocorrer em diferentes momentos de seu tratamento, abrangendo falhas na coleta e no armazenamento, bem como alterações decorrentes do compartilhamento ou da transferência inadequada dos dados entre dispositivos. Tais ocorrências evidenciam que a preservação da integridade não se limita ao momento inicial da obtenção da evidência, devendo ser observada ao longo de seu tratamento e de sua circulação. (Meireles, 2026, p. 35-36).

A repercussão de falhas na cadeia de custódia digital deve considerar, ainda, a existência de elementos técnicos que permitam verificar posteriormente a integridade do material examinado e reconstruir os procedimentos realizados. A ausência ou insuficiência de registros acerca das intervenções, dos métodos e das ferramentas empregadas pode dificultar a demonstração das condições em que os dados foram adquiridos e analisados, especialmente quando não se dispõe de mecanismos adequados de controle de integridade e de documentações capazes de permitir a conferência do material e das operações realizadas. (Lorens, 2025, p. 240-241; 246-249).

4.4. Contraditório, Acesso à Prova e Possibilidade de Contraprova

A preservação da cadeia de custódia também se relaciona ao exercício do contraditório, na medida em que o controle da prova pressupõe a existência de elementos suficientes para que as partes possam examinar sua origem, seu percurso e os procedimentos empregados em sua obtenção e preservação. A deficiência desses registros pode restringir a possibilidade de questionamento técnico

do elemento probatório e dificultar a realização de contraprova acerca de sua integridade e autenticidade. (Saad Netto; Avolio; Borri, 2025, p. 121-129).

O controle técnico da prova pericial encontra fundamento também no próprio Código de Processo Penal. O art. 159 assegura às partes a possibilidade de formular quesitos e indicar assistente técnico, bem como de requerer esclarecimentos dos peritos e apresentar pareceres técnicos. De particular relevância para o exame da prova digital, o § 6º prevê que, mediante requerimento, o material probatório que serviu de base à perícia seja disponibilizado, sob a guarda do órgão oficial e na presença de perito oficial, para exame pelos assistentes técnicos. A disciplina legal estabelece, assim, fundamento para que o contraditório sobre a prova pericial alcance não apenas o resultado expresso no laudo, mas também o material que lhe serviu de suporte, quando preservado e disponível para exame (BRASIL, 1941, art. 159, §§ 3º-6º).

A preocupação com a confiabilidade do vestígio não se restringe, contudo, à prova produzida pelos órgãos estatais. Os autores também examinam a preservação da cadeia de custódia em relação a vestígios apresentados pela defesa, evidenciando que a possibilidade de aferição da autenticidade e da integridade constitui aspecto relevante para o controle da prova independentemente de sua origem, consideradas as particularidades existentes entre a atividade defensiva e a atuação dos órgãos oficiais de investigação e perícia (Saad Netto; Avolio; Borri, 2025, p. 121-123). No âmbito específico da perícia em aparelhos celulares, a documentação técnica também se manifesta na forma de apresentação dos resultados obtidos. Lourenço inclui entre os elementos relevantes do laudo pericial a identificação do aparelho e das mídias associadas, os

softwares utilizados no exame e as evidências efetivamente relatadas. O registro dessas informações permite relacionar o resultado apresentado ao dispositivo examinado e aos recursos técnicos empregados em sua obtenção, fornecendo elementos objetivos para a compreensão e a posterior análise do procedimento pericial (Lourenço, 2024, p. 220-221).

Essa necessidade de controle assume especial relevância quando o elemento apresentado consiste em mera captura de tela. Silva observa que o *print screen* registra essencialmente a representação visual exibida no dispositivo, sem necessariamente preservar os elementos técnicos associados à fonte digital da qual a informação se origina. A ausência desses elementos pode dificultar a verificação da origem, do contexto e da integridade do conteúdo apresentado, bem como a demonstração de sua correspondência com o vestígio digital original. Nessas circunstâncias, a limitação não se restringe à forma de apresentação da informação, podendo repercutir sobre a possibilidade de exame técnico independente e de produção de contraprova (Silva, 2026, p. 42-44).

Essa preservação também alcança os dados já adquiridos e armazenados após o processamento pericial. O relatório das Câmaras Técnicas de Cadeia de Custódia prevê o armazenamento do material, inclusive para fins de contra perícia, e ressalta que soluções de custódia digital ou híbrida devem observar requisitos capazes de manter a integridade e a confiabilidade dos vestígios digitais preservados. A possibilidade de reexame depende, portanto, não apenas da existência formal de uma cópia ou do dispositivo original, mas também das condições em que esses elementos permanecem armazenados e disponíveis para posterior verificação técnica (BRASIL, 2023, p. 365-366).

Sob a perspectiva do exercício defensivo desse controle, a complexidade técnica da prova digital também repercute sobre as condições necessárias ao exercício de sua impugnação. Meireles destaca que o questionamento da validade desse tipo de elemento probatório pode demandar conhecimento técnico especializado, sobretudo quando a controvérsia envolve a demonstração de sua integridade, autenticidade ou das condições em que os dados foram obtidos e preservados. Nesse contexto, a possibilidade de exame dos aspectos técnicos da evidência assume relevância para que eventuais questionamentos sobre sua confiabilidade possam ser adequadamente formulados no processo (Meireles, 2026, p. 60-61).

Essa possibilidade de impugnação pressupõe, em termos práticos, condições para que a evidência possa ser submetida a exame técnico independente. Pereira relaciona a contraprova digital à revisão dos elementos originais e dos procedimentos de coleta e cadeia de custódia, bem como ao exame de metadados, registros e outros dados técnicos capazes de permitir a conferência dos resultados apresentados. O autor contempla, ainda, a realização de testes independentes e a elaboração de análise técnica própria como instrumentos de confronto da prova produzida. A efetividade do contraditório técnico depende, portanto, não apenas do acesso ao conteúdo probatório, mas da disponibilidade de elementos suficientes para que a defesa possa examinar, por meios próprios, a origem, o tratamento e a integridade da evidência (Pereira, 2024, p. 239-240).

Para que esse exame independente seja efetivamente realizado, a análise técnica deve poder alcançar o próprio vestígio e os elementos necessários à verificação dos procedimentos realizados. Parodi (2024) destaca a relevância da atividade pericial para o exame

de provas digitais e relaciona o exercício do contraditório à possibilidade de análise técnica do material probatório, especialmente quando sua confiabilidade depende da aferição de aspectos que não podem ser constatados pela simples visualização do conteúdo. Nessa perspectiva, a disponibilização apenas do resultado ou da informação extraída pode não oferecer, por si só, condições equivalentes às existentes quando permanecem acessíveis o vestígio e os elementos técnicos necessários à verificação de sua integridade, integralidade e do tratamento a ele conferido (Parodi, 2024, p. 91-96).

A preservação do dispositivo original pode assumir relevância adicional quando a extração realizada não alcança integralmente o conteúdo nele existente. O relatório das Câmaras Técnicas de Cadeia de Custódia do Ministério da Justiça e Segurança Pública reconhece que ferramentas disponíveis em determinado momento podem não permitir a obtenção completa dos dados de aparelhos celulares e observa que o desenvolvimento posterior de novas técnicas de extração pode viabilizar acesso antes indisponível. Nessa perspectiva, a manutenção do aparelho sob custódia pode preservar a possibilidade de exame técnico futuro, circunstância que repercute diretamente sobre as condições de reanálise e de produção de contraprova (BRASIL, 2023, p. 653-654).

A possibilidade de impugnação técnica pode ser ainda mais severamente afetada quando o próprio vestígio digital original deixa de estar disponível para exame. Silva destaca que o descarte prematuro ou a perda da fonte da evidência pode inviabilizar a realização de análise independente destinada a verificar a autenticidade e a integridade do material posteriormente apresentado no processo. Nessas situações, a deficiência assume

especial relevância porque não se limita à ausência de documentação de determinada etapa, podendo tornar impossível reproduzir ou conferir tecnicamente o procedimento realizado e, consequentemente, restringir a produção de contraprova pela defesa (Silva, 2026, p. 44-47).

4.5. Consequências Processuais: Inadmissibilidade, Nulidade e Valoração

A inexistência de consequência legal expressamente determinada para toda e qualquer ruptura da cadeia de custódia torna necessária a diferenciação entre as possíveis repercussões processuais do vício. A doutrina examinada registra posições distintas quanto à inadmissibilidade, nulidade e valoração, revelando que a mera constatação de desconformidade no percurso do vestígio não conduz necessariamente a uma solução processual uniforme. (Saad Netto; Avolio; Borri, 2025, p. 107-113).

Essa controvérsia também é identificada por Kologeski (2026), que apresenta duas orientações acerca das consequências jurídicas da quebra da cadeia de custódia. Uma delas atribui maior rigor à preservação do percurso probatório, relacionando sua ruptura à inadmissibilidade da prova; a outra admite solução mais flexível, segundo a qual a consequência deve ser definida a partir da gravidade da falha e de sua repercussão sobre a confiabilidade do elemento probatório. Nessa segunda perspectiva, a quebra da cadeia de custódia não conduz necessariamente à exclusão automática da prova, podendo sua repercussão variar conforme o comprometimento concretamente produzido (Kologeski, 2026, p. 41-43).

Ao examinar as consequências jurídicas da quebra da cadeia de custódia, Reis apresenta diferentes posições doutrinárias acerca da inadmissibilidade, da ilicitude, da nulidade e da valoração da prova. A análise evidencia que a deficiência na documentação do percurso probatório não recebe tratamento jurídico uniforme, sendo necessário distinguir a mera irregularidade procedimental das situações em que o comprometimento da evidência inviabiliza sua utilização confiável no processo penal (Reis, 2025, p. 148-151). Em perspectiva mais rigorosa, Meireles associa determinadas falhas na cadeia de custódia digital à nulidade ou à inadmissibilidade da prova, especialmente quando atingem sua autenticidade, integridade ou confiabilidade. Ao tratar de situações de contaminação, alteração e deficiência na preservação dos dados, o autor sustenta que a repercussão processual pode ultrapassar a mera irregularidade quando o comprometimento alcança atributos necessários à confiabilidade do elemento probatório. (Meireles, 2026, p. 33-38).

Parte da literatura recente sustenta compreensão mais rigorosa acerca das consequências processuais decorrentes da inobservância da cadeia de custódia digital. Lima, Dias e Silva defendem que deficiências nos procedimentos de documentação, coleta e preservação capazes de comprometer a integridade do vestígio repercutem sobre a própria admissibilidade da prova, relacionando a ausência de procedimentos técnicos adequados à impossibilidade de sua utilização válida no processo penal. Essa compreensão evidencia uma das controvérsias centrais da matéria, pois exige determinar se toda desconformidade tecnicamente relevante conduz à exclusão da prova ou se a consequência processual depende da natureza da falha, de seus efeitos concretos e da

possibilidade de controle posterior do elemento probatório (Lima; Dias; Silva, 2026, p. 145-158).

Ao desenvolver especificamente as nulidades processuais aplicáveis à prova digital, Meireles diferencia as nulidades absolutas das relativas, atribuindo às primeiras de maior gravidade por atingirem aspectos essenciais do ato, enquanto as segundas admitiriam correção ou convalidação conforme a natureza do vício e a existência de prejuízo. Transportada para o campo da prova digital, essa diferenciação evidencia que a consequência processual não deve ser definida apenas pela constatação de uma falha, mas também pela natureza do requisito atingido, pela gravidade do comprometimento e pela possibilidade de reparação de seus efeitos. (Meireles, 2026, p. 39-40). Em perspectiva aplicada à prova digital, Pereira identifica diferentes situações suscetíveis de fundamentar questionamentos quanto à validade da evidência, entre elas a violação da cadeia de custódia, a obtenção sem a necessária autorização legal, a utilização de métodos ou ferramentas não reconhecidos, deficiências na documentação dos procedimentos realizados e indícios de manipulação ou contaminação do material. A relevância dessas ocorrências, contudo, deve ser examinada a partir de sua repercussão sobre a regularidade da obtenção e do tratamento da evidência e, especialmente, sobre as condições de demonstração de sua integridade e confiabilidade (Pereira, 2024, p. 240-241).

A definição dessas consequências exige considerar, ainda, o prejuízo concretamente produzido pela irregularidade. Parodi sustenta que a quebra da cadeia de custódia não deve ser examinada de maneira abstrata ou exclusivamente formal, devendo-se verificar se a falha comprometeu a integridade ou a integralidade da prova e se

produziu restrição efetiva ao exercício do contraditório e da ampla defesa. Nessa perspectiva, a repercussão processual da irregularidade depende de sua capacidade de afetar a confiabilidade do elemento probatório ou de impedir que a parte interessada disponha de condições adequadas para examiná-lo e contestá-lo (Parodi, 2024, p. 80-87).

A controvérsia assume contornos particulares na cadeia de custódia da prova digital, pois Silva identifica posições distintas acerca da natureza e das consequências jurídicas de sua ruptura. A discussão envolve desde compreensões que tratam determinadas falhas como irregularidades sujeitas à demonstração de prejuízo até entendimentos mais rigorosos quando a deficiência compromete atributos necessários à confiabilidade do vestígio. Nesse cenário, a definição da consequência processual exige examinar a repercussão concreta da falha sobre a possibilidade de demonstrar a identidade e a integridade do elemento probatório e de submetê-lo a controle pelas partes (Silva, 2026, p. 38-41).

Essa diferenciação também pode ser observada sob o prisma da valoração da prova. Nem toda desconformidade identificada no percurso da evidência digital elimina, por si só, sua aptidão para integrar o conjunto probatório. Quando a falha ainda permite reconstruir o procedimento adotado, verificar a origem dos dados e aferir sua integridade por outros elementos técnicos disponíveis, sua repercussão pode permanecer no plano da confiabilidade e do peso atribuído à prova. Diversamente, quando a deficiência impede a verificação da autenticidade, da integridade ou da própria correspondência entre o material examinado e aquele originalmente obtido, deixa de existir base técnica suficiente para o controle da evidência, aproximando a controvérsia do campo da

inadmissibilidade. (Saad Netto; Avolio; Borri, 2025, p. 114-120; Meireles, 2026, p. 33-40).

Desse modo, a consequência processual da quebra da cadeia de custódia da prova digital não pode ser determinada exclusivamente pela identificação da etapa ou formalidade descumprida. A análise deve alcançar os efeitos concretos da falha sobre a confiabilidade do vestígio, considerando se permanecem disponíveis condições para verificar sua identidade, integridade, autenticidade e percurso e para submetê-lo a efetivo controle técnico pelas partes. É a intensidade desse comprometimento, e não a irregularidade considerada isoladamente, que permite distinguir situações com repercussão predominantemente valorativa daquelas potencialmente capazes de afetar a própria admissibilidade da prova (Saad Netto; Avolio; Borri, 2025, p. 114-131).

5. OS CRITÉRIOS DE INADMISSIBILIDADE DA PROVA DIGITAL EXTRAÍDA DE DISPOSITIVOS MÓVEIS POR QUEBRA DA CADEIA DE CUSTÓDIA

5.1. A Jurisprudência do Superior Tribunal de Justiça Sobre Cadeia de Custódia Digital

O exame jurisprudencial desenvolvido por Saad Netto, Avolio e Borri evidencia a progressiva incorporação, pelo Superior Tribunal de Justiça, das particularidades inerentes à cadeia de custódia da prova digital, especialmente quanto à necessidade de preservação de elementos que permitam aferir a integridade, a autenticidade e a confiabilidade dos dados apresentados no processo. Nesse contexto, a análise da regularidade da prova deixa de se limitar à constatação formal do procedimento empregado e passa a considerar a

possibilidade concreta de controle sobre a origem, a obtenção e a preservação do elemento digital. (Saad Netto; Avolio; Borri, 2025, p. 124-131).

A relevância jurisprudencial da matéria também é evidenciada pelo levantamento realizado por Reis, que identificou, em pesquisa no sítio eletrônico do Superior Tribunal de Justiça, 1.374 decisões monocráticas e 27 acórdãos relacionados aos termos “cadeia de custódia” e “prova digital”, publicados entre dezembro de 2020 e o início de maio de 2025. Embora os resultados não correspondam necessariamente a pronunciamentos específicos sobre a inadmissibilidade de provas extraídas de dispositivos móveis, o levantamento demonstra a presença da temática na atividade jurisdicional da Corte e reforça a pertinência da investigação dos critérios empregados na apreciação das falhas de custódia digital (Reis, 2025, p. 139-141).

A jurisprudência sobre cadeia de custódia da prova digital, contudo, ainda revela divergências quanto às consequências atribuídas às falhas verificadas nos procedimentos de obtenção e preservação dos vestígios. Saad Netto, Avolio e Borri identificam a existência de posições substancialmente distintas no Superior Tribunal de Justiça e apontam a necessidade de harmonização dos critérios empregados pela Corte, especialmente diante das cautelas adicionais exigidas pela volatilidade da prova digital. A questão evidencia que a identificação de uma irregularidade na cadeia de custódia não encerra, por si só, a análise jurídica, tornando necessário estabelecer parâmetros capazes de definir em quais circunstâncias a deficiência constatada efetivamente compromete a utilização processual da prova (Saad Netto; Avolio; Borri, 2026, p. 18-21).

Essa orientação pode ser observada no AgRg no RHC 143.169/RJ, julgado pela Quinta Turma do Superior Tribunal de Justiça, em que se discutiu a confiabilidade de provas digitais diante da ausência de documentação suficiente acerca dos procedimentos empregados em sua obtenção e preservação. Ao examinar o caso, o Tribunal destacou a necessidade de adoção de medidas destinadas a assegurar a integridade das fontes probatórias e permitir o controle posterior de sua confiabilidade, atribuindo ao Estado o ônus de demonstrar a higidez dos elementos que pretende utilizar no processo. Diante da inexistência de registros capazes de documentar adequadamente o tratamento conferido aos dados digitais, reconheceu-se o comprometimento da cadeia de custódia e a inadmissibilidade das provas dela decorrentes (BRASIL, 2023).

Esse entendimento foi aprofundado no AgRg no HC 828.054/RN, julgado pela Quinta Turma em 2024, em caso envolvendo dados obtidos de aparelho celular apreendido e posteriormente apresentados por meio de capturas de tela. O Superior Tribunal de Justiça destacou que a volatilidade dos dados digitais exige procedimentos capazes de preservar integralmente os vestígios e permitir a identificação de eventuais alterações, atribuindo especial relevância à documentação das etapas de obtenção da evidência e à possibilidade de controle posterior do material. Diante da ausência de procedimentos que assegurassem a idoneidade e a integridade dos dados extraídos, reconheceu-se a quebra da cadeia de custódia e a inadmissibilidade da prova digital (BRASIL, 2024a).

A compreensão acerca da necessidade de controle efetivo da prova foi aprofundada no AgRg no RHC 184.003/SP, também julgado pela Quinta Turma, ao examinar controvérsia envolvendo a integridade de arquivos digitais disponibilizados à defesa. Embora houvesse

valores *hash* associados ao material, parte dos arquivos se encontrava corrompida ou inacessível, circunstância que impedia a comparação necessária à verificação de sua correspondência com os dados originalmente obtidos. O Superior Tribunal de Justiça reconheceu, nesse contexto, que a mera existência de registros de *hash* não assegura, isoladamente, a integridade da evidência quando o próprio material necessário à conferência não se encontra disponível em condições adequadas de exame, concluindo pela inadmissibilidade das provas comprometidas (BRASIL, 2024b).

Em sentido complementar, o AgRg no HC 1.080.226/PI, julgado pela Sexta Turma em 2026, evidencia que a ausência de determinadas cautelas técnicas não conduz, isoladamente, ao reconhecimento da quebra da cadeia de custódia. No caso, questionavam-se dados obtidos de aparelho celular de terceiro mediante manuseio manual e capturas de tela, apontando-se, entre outras deficiências, a ausência de geração de código *hash* e de procedimentos técnicos padronizados de preservação. O Tribunal afastou a nulidade ao considerar as circunstâncias concretas da obtenção da prova, a inexistência de demonstração objetiva de adulteração ou manipulação do conteúdo, a possibilidade de contraditório sobre os procedimentos realizados, o acesso da defesa aos dados disponibilizados e a existência de outros elementos probatórios que corroboravam o conteúdo extraído. O precedente demonstra, assim, que a ausência isolada de determinado mecanismo técnico não equivale necessariamente ao comprometimento material da evidência, exigindo-se a análise de seus efeitos concretos sobre a confiabilidade da prova e o exercício da defesa (BRASIL, 2026a).

Uma solução distinta foi adotada no AgRg no HC 1.014.212/ES, julgado pela Sexta Turma em 2026, em controvérsia envolvendo

capturas de tela de conversas em aplicativo de mensagens e outros elementos digitais relevantes para a imputação. Diante de questionamentos substanciais acerca da integridade e da autenticidade do material e da ausência de documentação técnica suficiente para demonstrar sua preservação, o Superior Tribunal de Justiça considerou necessária a realização de perícia complementar. A providência não foi determinada para excluir automaticamente a prova, mas para suprir o deficit técnico identificado e possibilitar a verificação de sua fidedignidade e o efetivo exercício do contraditório. O precedente evidencia, portanto, que a existência de dúvida relevante sobre a integridade da evidência não conduz necessariamente à inadmissibilidade imediata quando ainda subsistem condições para submetê-la a exame técnico capaz de esclarecer sua confiabilidade (BRASIL, 2026b).

A análise conjunta desses precedentes revela que o tratamento conferido pelo Superior Tribunal de Justiça à cadeia de custódia da prova digital não se estrutura sobre a exigência automática de determinada ferramenta ou formalidade técnica. A jurisprudência examinada atribui relevância às condições concretas de demonstração da integridade, autenticidade e correspondência entre o dado originalmente obtido e aquele apresentado no processo, bem como à possibilidade de controle técnico e exercício do contraditório. Nesse contexto, a insuficiência dos procedimentos de preservação pode conduzir à inadmissibilidade quando inviabiliza a verificação confiável da evidência, ao passo que irregularidades cuja repercussão possa ser afastada ou tecnicamente esclarecida não produzem necessariamente a mesma consequência (BRASIL, 2023; BRASIL, 2024a; BRASIL, 2024b; BRASIL, 2026a; BRASIL, 2026b).

5.2. Critérios Técnico-Jurídicos de Comprometimento da Prova

A aferição do comprometimento da prova digital por quebra da cadeia de custódia exige a consideração conjunta de elementos jurídicos e técnico periciais. A partir da doutrina examinada, podem ser identificados como fatores relevantes a possibilidade de demonstrar a identidade do elemento probatório, a preservação de sua integridade e autenticidade, a rastreabilidade de seu percurso, a existência de documentação acerca dos procedimentos empregados em sua obtenção e preservação e a possibilidade de posterior controle técnico sobre os dados apresentados. (Saad Netto; Avolio; Borri, 2025, p. 105-131). Esses elementos não devem ser compreendidos isoladamente como requisitos cuja ausência produza, de forma automática, a inadmissibilidade da prova. Sua relevância está na possibilidade de avaliar concretamente se a falha identificada comprometeu a confiabilidade do elemento digital ou inviabilizou sua adequada verificação e submissão ao contraditório, permitindo distinguir desconformidades de menor relevância de rupturas capazes de atingir materialmente a prova. (Saad Netto; Avolio; Borri, 2025, p. 114-131).

Sob a perspectiva técnico pericial, a avaliação do comprometimento da prova digital deve considerar se os procedimentos adotados permitem demonstrar as condições em que os dados foram adquiridos, preservados e examinados. Para essa aferição, mostram-se relevantes a preservação do vestígio original, a utilização de procedimentos adequados de aquisição, a existência de mecanismos de controle de integridade, a documentação das intervenções realizadas e o registro dos métodos, ferramentas e respectivas versões empregados no exame, elementos que

contribuem para a possibilidade de reconstrução e verificação posterior da atividade pericial (Lorens, 2025, p. 237-241; 246-249).

Em dispositivos móveis, a avaliação das intervenções realizadas deve considerar também as condições técnicas concretas em que ocorreu a aquisição dos dados. Figueiredo e França Júnior demonstram que determinadas modalidades de extração podem exigir o funcionamento e a interação com o aparelho e que a escolha do procedimento depende das características de seu *hardware, software* e mecanismos de proteção. Nesse contexto, a identificação de uma alteração no estado do dispositivo deve ser acompanhada da análise de sua origem, finalidade e necessidade técnica, bem como da existência de registros que permitam conhecer o procedimento executado e avaliar seus efeitos sobre os dados obtidos (Figueiredo; França Júnior, 2022, p. 82-83; 88-89).

A presença desses elementos evidencia que a avaliação da confiabilidade da prova digital não deve se restringir à simples apresentação ou visualização de seu conteúdo. Meireles ressalta a necessidade de que existam informações capazes de demonstrar a autenticidade e a integridade da evidência, bem como de documentar aspectos relevantes de sua obtenção e tratamento. Nessa perspectiva, a análise do comprometimento da prova alcança também as condições que permitem verificar sua origem e o estado em que foi preservada, fornecendo elementos para o controle da correspondência entre a informação apresentada no processo e a evidência digital da qual ela deriva (Meireles, 2026, p. 58-60).

A possibilidade de estabelecer essa correspondência depende, ainda, da preservação de condições que permitam retornar tecnicamente à fonte da evidência e examinar o percurso pelo qual

o conteúdo foi obtido. A análise desenvolvida por Silva evidencia que a indisponibilidade do vestígio original, a insuficiência de elementos de rastreabilidade ou a perda de informações necessárias à conferência do material podem adquirir relevância substancial quando impedem verificar se o dado apresentado no processo corresponde àquele efetivamente obtido da fonte. Desse modo, mais do que identificar isoladamente a ausência de determinada formalidade, importa aferir se permanecem disponíveis elementos suficientes para submeter a evidência a verificação técnica independente (Silva, 2026, p. 38-47).

A verificação da confiabilidade da evidência digital pode decorrer, nesse contexto, da análise conjugada de diferentes elementos técnicos. Kologeski (2026), aborda a comparação de valores *hash* como mecanismo de controle de integridade e destaca também a utilidade de metadados e registros de sistemas para a identificação de informações relacionadas à criação, modificação, acesso e percurso dos dados. Considerados conjuntamente e em associação com a documentação do procedimento realizado, esses elementos podem fornecer parâmetros para examinar a permanência da evidência ao longo de seu tratamento e identificar eventuais inconsistências que demandem investigação técnica mais aprofundada (Kologeski, 2026, p. 30-39).

De fato, essa distinção é ilustrada por Reis ao confrontar duas situações de preservação da prova digital: na primeira, a ausência de geração do código *hash* no momento da apreensão não compromete necessariamente a confiabilidade da evidência quando o dispositivo é devidamente identificado, acondicionado e lacrado, com documentação de sua custódia e posterior verificação pericial; na segunda, a geração imediata do *hash* não supre a

ausência de registros sobre o acondicionamento, a guarda e o manuseio do dispositivo até o exame. Os exemplos demonstram que o controle de integridade dos dados e a rastreabilidade do vestígio constituem dimensões complementares, de modo que a utilização de um recurso técnico isolado não substitui a documentação necessária à reconstrução do percurso probatório (Reis, 2025, p. 152-153).

Neste giro, a avaliação do comprometimento da prova deve considerar, ainda, se o material preservado e disponibilizado apresenta extensão suficiente para permitir sua adequada contextualização e controle. A distinção formulada por Parodi entre integridade e integralidade evidencia que a ausência de alteração do conteúdo apresentado não resolve, isoladamente, a questão da confiabilidade quando apenas parcela da evidência se encontra disponível. A incompletude assume relevância especialmente quando a ausência de dados relacionados impede compreender o contexto do elemento selecionado, verificar sua correspondência com a fonte ou realizar exame técnico sobre aspectos potencialmente relevantes à interpretação da prova. Assim, a integralidade constitui fator adicional a ser considerado não como requisito autônomo de admissibilidade, mas na medida em que sua deficiência repercuta concretamente sobre a confiabilidade e a possibilidade de controle do elemento probatório (Parodi, 2024, p. 79-87).

A possibilidade de verificação técnica também se mostra relevante quando subsistem dúvidas acerca da confiabilidade do material, mas ainda existem condições para submetê-lo a exame. No AgRg no HC 1.014.212/ES, a Sexta Turma do Superior Tribunal de Justiça considerou necessária a realização de perícia complementar diante

de questionamentos sobre a integridade e a autenticidade de elementos digitais relevantes para a imputação. A solução adotada evidencia que a dúvida quanto à higidez da prova não conduz necessariamente à sua imediata exclusão quando ainda é possível realizar exame técnico capaz de esclarecer sua confiabilidade. Desse modo, a própria possibilidade de verificação posterior constitui elemento relevante para distinguir situações em que a deficiência pode ser tecnicamente esclarecida daquelas em que a ruptura tornou inviável qualquer controle confiável sobre a evidência (BRASIL, 2026b).

5.3. Gravidade da Ruptura, Possibilidade de Verificação e Eventual Saneamento

A gravidade da quebra da cadeia de custódia deve ser examinada a partir das consequências concretamente produzidas sobre o elemento probatório. A inobservância de determinado procedimento não apresenta, necessariamente, a mesma relevância em todas as situações, razão pela qual a análise deve considerar se a falha permite, apesar de sua ocorrência, a reconstrução do percurso do vestígio e a aferição de sua identidade, integridade e confiabilidade. (Saad Netto; Avolio; Borri, 2025, p. 114-120). A possibilidade de verificação posterior da prova digital pode ser aferida, sob a perspectiva técnico-pericial, pela existência de elementos que permitam reconstruir as operações realizadas e controlar a integridade do material submetido a exame. A documentação dos procedimentos, das intervenções e das ferramentas empregadas, associada a mecanismos de verificação de integridade, fornece parâmetros para avaliar se, apesar de determinada irregularidade, ainda subsistem condições técnicas para examinar a correspondência entre o vestígio obtido e os dados

posteriormente analisados e apresentados no processo. (Lorens, 2025, p. 240-241; 246-249).

Além disso, a ruptura pode ser aferida, nessa perspectiva, também pela extensão em que a falha preserva ou elimina as condições necessárias ao controle posterior da evidência. A análise desenvolvida por Silva demonstra particular preocupação com situações em que deficiências de rastreabilidade, perda da fonte original ou insuficiência dos elementos de preservação impedem a reconstrução do percurso do vestígio e sua submissão a exame independente. Diferentemente de uma desconformidade cuja ocorrência e efeitos ainda possam ser tecnicamente verificados, a impossibilidade de retornar à fonte ou de conferir a correspondência entre o material originalmente obtido e aquele apresentado no processo pode conferir à ruptura caráter materialmente mais grave (Silva, 2026, p. 38-47). Nesta seara, a existência de uma ruptura não impede, por outro lado, que se investigue se permanecem elementos capazes de sustentar a confiabilidade do vestígio. Ao apresentar a orientação que admite tratamento mais flexível das falhas na cadeia de custódia, Kologeski relaciona a definição de suas consequências à gravidade da irregularidade e à possibilidade de ainda se reconhecer confiabilidade no material probatório. Essa perspectiva reforça a necessidade de distinguir situações em que a falha deixa subsistentes condições de controle da evidência daquelas em que o comprometimento impede verificar adequadamente sua integridade e correspondência com o vestígio originalmente obtido (Kologeski, 2026, p. 42-43).

De tal forma que essa diferenciação pode ser aprofundada a partir da possibilidade de controle posterior do elemento probatório. Parodi relaciona a avaliação do vício à existência de condições

efetivas para que a parte examine a prova e confronte tecnicamente os elementos utilizados contra ela, de modo que a análise do prejuízo não se esgota na identificação formal da irregularidade. Sob essa perspectiva, assume maior gravidade a deficiência que impede ou restringe de maneira relevante a verificação da integridade ou da integralidade do material e, consequentemente, compromete as condições necessárias ao exercício do contraditório sobre a própria prova (Parodi, 2024, p. 82-87).

A análise do eventual saneamento exige distinguir a correção de vícios processuais da recuperação das condições técnicas necessárias à verificação da prova digital. Embora determinados vícios relativos possam admitir correção ou convalidação no âmbito da teoria das nulidades, conforme sua natureza e seus efeitos, essa possibilidade não significa que uma deficiência na cadeia de custódia seja tecnicamente reversível. Quando a falha inviabiliza a reconstrução do procedimento ou a verificação da autenticidade e da integridade dos dados, a regularização formal do ato não restabelece, por si só, a confiabilidade do vestígio (Meireles, 2026, p. 39-40).

A jurisprudência do Superior Tribunal de Justiça acrescenta a essa distinção a possibilidade de esclarecimento técnico posterior quando ainda subsistem condições materiais para a verificação da evidência. No AgRg no HC 1.014.212/ES, diante de dúvida razoável acerca da integridade e da autenticidade dos dados digitais, o Tribunal determinou a realização de perícia complementar em vez de reconhecer imediatamente sua inadmissibilidade. A solução evidencia que a existência de questionamento relevante sobre a confiabilidade da prova não se confunde, necessariamente, com comprometimento técnico irreversível, devendo-se considerar se os

vestígios e demais elementos disponíveis ainda permitem exame capaz de esclarecer sua fidedignidade e assegurar o contraditório. Diversamente, quando a falha torna impossível reconstruir o procedimento, confrontar os dados ou aferir sua integridade e autenticidade, a possibilidade de verificação posterior deixa de constituir alternativa apta a superar a deficiência identificada (BRASIL, 2024b; BRASIL, 2026b).

A relevância prática dessa distinção pode ser observada em episódio recente envolvendo materiais digitais apreendidos em investigação relacionada à produção do filme *Dark Horse*. Em setembro de 2026, foi divulgado que o Instituto de Criminalística de São Paulo recusou inicialmente 27 dispositivos eletrônicos encaminhados pela Polícia Civil em razão de falhas no acondicionamento, embora os selos de segurança permanecessem íntegros. Segundo as informações divulgadas, as condições das embalagens possibilitariam, em tese, acesso aos dispositivos sem o rompimento dos lacres. O material foi devolvido para correção do acondicionamento e posteriormente reenviado e aceito para realização da perícia. O episódio ilustra que a identificação de deficiência na cadeia de custódia não se confunde necessariamente com a demonstração de efetiva manipulação ou alteração do vestígio, exigindo a análise da natureza da falha, do risco produzido, das condições de verificação da integridade e da possibilidade de saneamento antes da produção da prova pericial (Cassela, 2026).

5.4. Sistematização dos Critérios de Inadmissibilidade

A sistematização dos critérios de inadmissibilidade da prova digital extraída de dispositivos móveis por quebra da cadeia de custódia exige distinguir a inobservância procedimental do

comprometimento efetivo das condições de confiabilidade da evidência. A partir dos parâmetros normativos, técnico periciais e jurisprudenciais examinados, verifica-se que a consequência processual da ruptura não decorre exclusivamente da ausência de determinada formalidade ou ferramenta, mas de sua repercussão sobre a possibilidade de demonstrar a identidade, a integridade, a autenticidade e a rastreabilidade dos dados obtidos. Nesse contexto, a inadmissibilidade assume especial pertinência quando as deficiências constatadas impedem estabelecer, por meios tecnicamente verificáveis, a correspondência entre o conteúdo originalmente extraído do dispositivo e aquele posteriormente apresentado no processo, comprometendo sua submissão ao contraditório (BRASIL, 1941, arts. 158-A a 158-F; BRASIL, 2023; BRASIL, 2024a; BRASIL, 2024b).

Destarte, a aplicação desses parâmetros permite diferenciar três situações. Na primeira, a irregularidade não compromete a confiabilidade da evidência, pois subsistem elementos suficientes para reconstruir seu percurso e verificar sua integridade, hipótese em que a falha não determina, por si só, a inadmissibilidade. Na segunda, existem dúvidas relevantes sobre a autenticidade ou a integridade dos dados, mas permanecem disponíveis o vestígio e os elementos necessários à realização de exame técnico complementar, cuja conclusão poderá esclarecer a aptidão probatória do material. Na terceira, a deficiência impede a reconstrução confiável da obtenção ou preservação dos dados e inviabiliza sua verificação independente, configurando comprometimento material que pode justificar a inadmissibilidade da prova. Essa diferenciação encontra respaldo nas soluções adotadas pelo Superior Tribunal de Justiça, que considera as circunstâncias concretas da ruptura e a possibilidade efetiva de

controle da evidência (BRASIL, 2024a; BRASIL, 2024b; BRASIL, 2026a; BRASIL, 2026b).

Desse modo, a definição da inadmissibilidade exige a análise conjunta da natureza e da gravidade da ruptura, de seus efeitos sobre a confiabilidade dos dados e da possibilidade de verificação técnica posterior. A ausência de registros de custódia, a insuficiência da documentação pericial, a indisponibilidade do vestígio original e as falhas nos mecanismos de controle de integridade assumem relevância na medida em que comprometam a identificação da fonte, a reconstrução do percurso probatório ou a realização de exame independente. Assim, o critério determinante não reside na constatação isolada de uma desconformidade, mas na impossibilidade de demonstrar, por elementos tecnicamente verificáveis, a correspondência entre a evidência obtida e aquela submetida ao processo, com repercussão sobre sua confiabilidade e sobre o exercício do contraditório (BRASIL, 2023; BRASIL, 2024a; BRASIL, 2024b; BRASIL, 2026b).

6. CONCLUSÃO

De forma geral, a presente pesquisa examinou os critérios de inadmissibilidade da prova digital extraída de dispositivos móveis apreendidos em decorrência da quebra da cadeia de custódia no processo penal brasileiro. A análise da legislação processual, dos parâmetros técnicos periciais e da jurisprudência do Superior Tribunal de Justiça permitiu identificar que a inobservância dos procedimentos de preservação não determina, isoladamente, a exclusão da evidência. A consequência processual depende da repercussão concreta da irregularidade sobre a possibilidade de demonstrar a identidade, a integridade, a autenticidade e a

rastreabilidade dos dados, especialmente quanto à correspondência entre o conteúdo originalmente obtido e aquele apresentado no processo.

Portanto, os resultados evidenciaram que a avaliação da quebra da cadeia de custódia exige considerar a natureza da irregularidade, a extensão de seus efeitos e as condições de verificação da evidência. Nesse sentido, falhas procedimentais que não inviabilizam a reconstrução do percurso probatório distinguem-se de deficiências cuja repercussão ainda pode ser esclarecida mediante exame técnico complementar. Diversamente, quando a ruptura impede a identificação confiável da origem dos dados, a demonstração de sua integridade ou a verificação independente do material apresentado, resta comprometida a própria possibilidade de aferir sua autenticidade e submetê-lo ao contraditório. A jurisprudência examinada revelou, portanto, a necessidade de uma avaliação concreta dessas circunstâncias, afastando tanto a exclusão automática por mera desconformidade formal quanto a aceitação de evidências cuja confiabilidade não possa ser tecnicamente demonstrada.

Infere-se, assim, que a inadmissibilidade da prova digital extraída de dispositivos móveis apreendidos encontra fundamento no comprometimento das condições necessárias à verificação de sua confiabilidade, quando a ruptura da cadeia de custódia impede demonstrar, de maneira tecnicamente verificável, a correspondência entre os dados originalmente obtidos e aqueles submetidos à apreciação judicial. A contribuição da pesquisa consiste na sistematização de parâmetros que permitem distinguir irregularidades procedimentais, deficiências passíveis de esclarecimento técnico e rupturas que inviabilizam o controle da

evidência. Essa distinção oferece critérios para uma apreciação fundamentada da admissibilidade probatória, compatível com as particularidades da prova digital e com as exigências do contraditório e do devido processo legal.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT - Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27037:2013: tecnologia da informação - técnicas de segurança - diretrizes para identificação, coleta, aquisição e preservação de evidência digital.** Rio de Janeiro: ABNT, 2013. Disponível em: https://abntcatalogo.com.br/sebrae/norma.aspx?Q=NDlLZHR1a1ZUajNiNEhXZFI1WVpNWE1EVWRBUXUxNkdGSVNyT3dLL05qUT0=. Acessado em: 15 set. 2026.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. **Código de Processo Penal.** Brasília, DF: Presidência da República, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acessado em: 10 set. 2026.

BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Segurança Pública. **Compilado dos relatórios técnicos finais: Câmaras Técnicas de Cadeia de Custódia: discussão, diagnóstico e recomendações pós Lei n. 13.964/2019.** Brasília, DF: Ministério da Justiça e Segurança Pública, 2023. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/cadeia-de-custodia-1/relatorio_final_compilado_publicacao.pdf. Acesso em: 13 set. 2026.

BRASIL. Superior Tribunal de Justiça (5. Turma). **Agravo Regimental no Habeas Corpus n. 828.054/RN.** Relator: Ministro Joel Ilan Paciornik. Julgado em 23 abr. 2024. Diário da Justiça Eletrônico,

Brasília, DF, 29 abr. 2024. Disponível em: https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=%28%28AGRHC+INPATH%28CLAS%29+OR+%22AgRg+no+HC%22+INPATH%28CLAP%29%29+AND+828054+INPATH%28NUM%29%29+OR+%28NEAR%28%28%28AGRHC+OR+%22AgRg+no+HC%22%29%2C828054%29%2C0%2CTRUE%29+INPATH%28SUCE%29%29. Acessado em: 16 set. 2026.

BRASIL. Superior Tribunal de Justiça (5. Turma). **Agravo Regimental no Recurso em Habeas Corpus n. 143.169/RJ.** Relator: Ministro Messod Azulay Neto. Relator para acórdão: Ministro Ribeiro Dantas. Julgado em 7 fev. 2023. Diário da Justiça Eletrônico, Brasília, DF, 2 mar. 2023. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202100573956&dt_publicacao=02/03/2023. Acessado em: 12 set. 2026.

BRASIL. Superior Tribunal de Justiça (5. Turma). **Agravo Regimental no Recurso em Habeas Corpus n. 184.003/SP.** Relatora: Ministra Daniela Teixeira. Relator para acórdão: Ministro Ribeiro Dantas. Julgado em 10 dez. 2024. Diário da Justiça Eletrônico Nacional, Brasília, DF, 26 dez. 2024. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202503860194&dt_publicacao=23/04/2026. Acessado em: 12 set. 2026.

BRASIL. Superior Tribunal de Justiça (6. Turma). **Agravo Regimental no Habeas Corpus n. 1.014.212/ES.** Relator: Ministro Carlos Pires Brandão. Julgado em 10 fev. 2026. Diário da Justiça Eletrônico Nacional, Brasília, DF, 20 fev. 2026. Disponível em: https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?

livre=%28%28AGRHC+INPATH%28CLAS%29+OR+%22AgRg+no+HC%22+INPATH%28CLAP%29%29+AND+1014212+INPATH%28NUM%29%29+OR+%28NEAR%28%28%28AGRHC+OR+%22AgRg+no+HC%22%29%2C1014212%29%2C0%2CTRUE%29+INPATH%28SUCE%29%29. Acessado em: 12 set. 2026.

BRASIL. Superior Tribunal de Justiça (6. Turma). **Agravo Regimental no Habeas Corpus n. 1.080.226/PI.** Relator: Ministro Antonio Saldanha Palheiro. Julgado em 7 abr. 2026. Diário da Justiça Eletrônico Nacional, Brasília, DF, 14 abr. 2026. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202600907600&dt_publicacao=14/04/2026. Acessado em: 12 set. 2026.

CASSELA, Vinícius. **Perícia aponta falha em lacre de 27 dispositivos apreendidos em operação contra produtora de 'Dark Horse'.** Globo.com, canal G1. Brasília 13/09/2026. Disponível em: https://g1.globo.com/politica/noticia/2026/09/13/pericia-aponta-falha-em-lacre-de-27-dispositivos-apreendidos-em-operacao-contra-produtora-de-dark-horse.ghtml. Acesso em: 13 set. 2026.

FIGUEIREDO, Jorge Ramos de; FRANÇA JÚNIOR, Fausto Faustino de. **Extração forense avançada de dados em dispositivos móveis: técnicas aplicadas ao ambiente Android.** v. 1: Conceitos, fundamentos técnicos, diretrizes, métodos e documentos legais. Rio de Janeiro: Brasport, 2022. 128 p. ISBN 978-65-88431-60-3.

FISBERG, Yuri. **Função ‘hash’ e a integridade da prova digital.** Revista Brasileira de Direito Processual Penal, v. 11, n. 3, e1227, set./dez. 2025. DOI: 10.22197/rbdpp.v11i3.1227. Disponível em:

https://rbdpp.emnuvens.com.br/RBDPP/article/view/1227. Acessado em: 17 set. 2026.

KOLOGESKI, André. **Código hash: integridade digital, cadeia de custódia e prova eletrônica no direito brasileiro.** 1. ed. [S. l.]: [s. n.], 2026.

LIMA, Paula Siqueira; DIAS, Cristiane Berenice; SILVA, Wesley Roberto Mariano da. **Prova penal digital e cadeia de custódia: requisitos técnicos, exigências jurídicas e controle de admissibilidade.** Revista Científica do UBM, v. 28, n. 55, p. 145-158, 2026. DOI: 10.52397/rcubm.v0in.55.3095. Disponível em: https://revista.ubm.br/index.php/revistacientifica/article/view/3095. Acessado em: 17 set. 2026.

LOURENÇO, Marcus Vinicius. **Produção da prova digital em aparelho celular: coleta, extração e apresentação.** In: MAIA, Juliana Kryssia Lopes; SALDIAS, Sergio Andrés Hernández (org.). *Cadeia de custódia, metodologias e prova digital: conhecimento prático interdisciplinar*. Rio de Janeiro: Lumen Juris, 2024. p. 205-222.

MAIA, Juliana Kryssia Lopes; HERNÁNDEZ SALDIAS, Sergio Andrés (org.). **Cadeia de custódia, metodologias e prova digital: conhecimento prático interdisciplinar.** 1. ed. Rio de Janeiro: Lumen Juris, 2024. 308 p.

MEIRELES, Steverson Marcus Salgado. **Nulidade das provas digitais: cadeia de custódia, contraditório e devido processo legal na era digital.** [S. l.]: [s. n.], 2026. E-book Kindle.

PARODI, Lorenzo. **Perícia defensiva em provas digitais no processo penal: origem, custódia, integralidade e integridade.** 1.

ed. São Paulo: Revista dos Tribunais, 2024.

PEREIRA, Thiago Silva. **Informação única e prova digital.** In: MAIA, Juliana Kryssia Lopes; SALDIAS, Sergio Andrés Hernández (org.). *Cadeia de custódia, metodologias e prova digital: conhecimento prático interdisciplinar*. Rio de Janeiro: Lumen Juris, 2024. p. 223-247.

REIS, Rodrigo Casimiro. Verdade e prova penal: a cadeia de custódia na era digital. [S. l.]: Amanuense, 2025.

SAAD NETTO, Cláudio; AVOLIO, Luiz Francisco Torquato; BORRI, Luiz Antonio. **A cadeia de custódia da prova digital: dissensos e consensos entre teoria e práxis.** Boletim IBCCRIM, São Paulo, v. 34, n. 403, p. 18-21, 2026. DOI: 10.5281/zenodo.19697006. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/2761. Acessado em: 17 set. 2026.

SAAD NETTO, Cláudio; AVOLIO, Luiz Francisco Torquato; BORRI, Luiz Antonio. **Nulidades no processo penal e a cadeia de custódia.** São Paulo: Revista dos Tribunais, 2025.

SAAD, Marta; ROSSI, Helena Costa; PARTATA, Pedro Henrique. **A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais.** Revista Brasileira de Direito Processual Penal, v. 10, n. 3, 2024. DOI: 10.22197/rbdpp.v10i3.1071. Disponível em: https://revista.ibraspp.com.br/RBDPP/article/view/1071. Acesso em: 13 set. 2026.

SILVA, Gabriel Monari. **A cadeia de custódia da prova digital: a fragilidade do vestígio eletrônico e a necessidade de rigor**

procedimental. [S. l.]: Independently published, 2026.

---

[1] Engenheiro da Computação, Perito Forense Digital e Investigador Cibernético. Especialista em Direito Cibernético, Redes de Computadores e Comunicação de Dados, MBA em Gestão, Empreendedorismo e Desenvolvimento de Negócios. Pós-graduando em Neurociência, Comunicação e Desenvolvimento Humano. Graduando em Direito pela Universidade Estácio de Sá – Estácio. Faculdade De Pimenta Bueno – FAP. Currículo Lattes: http://lattes.cnpq.br/7399200236075562. E-mail: acesse o artigo original para visualizar o e-mail.

[2] PhD in Physics (UFC), with post-doctorate in Scientific Regional Development (DCR/CNPq). MBA in Software Engineering/Systems Analysis and Development/Electrical Engineering – UniÚnica. Professor of the Doctoral and Master Program in Regional Development and Environment (PGDRA/UFRO). E-mail: acesse o artigo original para visualizar o e-mail. ORCID: https://orcid.org/0000-0003-4173-4636.