Revista Brasileira de Direito e Gestão Pública
www.gvaa.com.br/revista/index.php/RDGP/
ISSN: 2358-2405

A cadeia de custódia da prova digital no inquérito policial: Desafios técnicos, operacionais e reflexos jurídicos

The chain of custody of digital evidence in police investigations: Technical and operational challenges and legal implications

Anderson Gomes de Oliveira[1] e Paulo Roberto Dantas de Souza Leão[2]

v. 14/ n. 2 (2026)
Abril/Junho

Aceito para publicação em 10/04/2026.

[1]Graduando em Direito pela Universidade Federal do Rio Grande do Norte, Natal, Rio Grande do Norte. ORCID: 0009-0008-7694-3765. E-mail: anderson.oliveira.706@ufrn.edu.br;
[2]Doutorando em Direito pela Universidad del Pais Vasco, Vizcaya, Espanha. Advogado e Professor Adjunto IV da Universidade Federal do Rio Grande do Norte, Natal, Rio Grande do Norte. ORCID: 0009-0005-5602-5180. E-mail: pauloleao61@gmail.com.

https://www.gvaa.com.br/revista/index.php/RDG

RESUMO: A expansão da criminalidade cibernética e a massificação dos dispositivos eletrônicos impuseram novos desafios à persecução penal, exigindo a transição da prova material corpórea para a prova digital. O presente artigo tem como objetivo analisar os desafios técnicos, operacionais e os reflexos jurídicos inerentes à cadeia de custódia da prova digital no âmbito do inquérito policial. A pesquisa adota uma metodologia qualitativa, consubstanciada em revisão bibliográfica e análise de jurisprudência recente do Superior Tribunal de Justiça (STJ) e do Supremo Tribunal Federal (STF). Constatou-se que as instituições de segurança pública enfrentam severas limitações estruturais, como o subdimensionamento de pessoal, a falta de ferramentas periciais adequadas e a dificuldade no armazenamento de grandes volumes de dados (Big Data). Conclui-se que a inobservância das normativas técnicas e do espelhamento forense (código hash) gera a quebra da cadeia de custódia, o que afasta a presunção de legitimidade da atuação estatal e resulta na ilicitude material da evidência. A consolidação jurisprudencial do "fim do print" como prova isolada reforça a necessidade inadiável de aparelhamento do Estado, salvaguardando o contraditório e o devido processo legal, admitindo-se a flexibilização do rigor técnico apenas para as provas fornecidas por particulares, em especial pela vítima.
Palavras-chave: Prova digital. Cadeia de custódia. Processo penal. Investigação cibernética. Prova penal.

ABSTRACT: The expansion of cybercrime and the massification of electronic devices have imposed new challenges on criminal prosecution, requiring a transition from physical material evidence to digital evidence. This article aims to analyze the technical, operational challenges, and legal consequences inherent to the chain of custody of digital evidence within the scope of the police inquiry. The research adopts a qualitative methodology, based on a bibliographic review and an analysis of recent jurisprudence from the Superior Court of Justice (STJ) and the Supreme Federal Court (STF). It was found that public security institutions face severe structural limitations, such as understaffing, a lack of adequate forensic tools, and difficulties in storing large volumes of data (Big Data). It is concluded that the failure to observe technical regulations and forensic imaging (hash code) results in a break in the chain of custody, which removes the presumption of legitimacy of state action and leads to the material inadmissibility of the evidence. The jurisprudential consolidation of the "end of the screenshot" as isolated evidence reinforces the urgent need for the State to be properly equipped, safeguarding the adversarial system and due process of law, while allowing technical rigor to be relaxed only for evidence provided by private individuals, especially by the victim.
Keywords: Digital evidence. Chain of custody. Criminal procedure. Cyber investigation.

1. CONSIDERAÇÕES INICIAIS

A revolução tecnológica observada nas últimas décadas transformou de forma significativa as dinâmicas sociais, econômicas e interpessoais. Como consequência direta desse processo, a criminalidade também se adaptou e passou, em larga medida, a operar no ambiente digital. Diversas condutas delitivas passaram a ser praticadas ou instrumentalizadas por meio de dispositivos eletrônicos, de modo que smartphones, computadores e sistemas de armazenamento em nuvem se consolidaram como relevantes repositórios de vestígios probatórios. Nesse cenário, a prova digital assume posição central na persecução penal contemporânea.

No âmbito do inquérito policial, sua relevância é particularmente evidente. Se, em períodos anteriores, a apuração criminal dependia predominantemente de testemunhos e vestígios físicos, as investigações atuais frequentemente se apoiam na quebra de sigilo de dados, no rastreamento de geolocalização e na extração de comunicações mantidas em aplicativos de mensagens instantâneas para a reconstrução da materialidade e da autoria delitivas. Ocorre que, diversamente dos vestígios materiais tradicionais, os dados digitais apresentam características próprias, como volatilidade, intangibilidade, alta replicabilidade e significativa suscetibilidade à alteração.

Em razão dessas peculiaridades, a manipulação de evidências digitais demanda rigor técnico específico e observância de protocolos próprios de preservação, circunstância que nem sempre se compatibiliza com a realidade estrutural dos órgãos de persecução penal. Nesse contexto, emerge o seguinte problema de pesquisa: em que medida as limitações técnicas e operacionais relacionadas ao armazenamento, à extração e à perícia de dados digitais comprometem a cadeia de custódia e a validade das provas digitais produzidas no inquérito policial?

Parte-se da hipótese de que a insuficiência de estrutura técnica adequada, aliada à ausência de padronização procedimental no tratamento das evidências digitais, fragiliza a cadeia de custódia e compromete a confiabilidade da prova produzida. Como consequência, tais deficiências podem afetar a admissibilidade do material probatório no processo penal, com potenciais repercussões sobre a higidez da persecução penal e sobre a própria efetividade da tutela jurisdicional.

A pesquisa desenvolve-se mediante metodologia jurídico-dogmática de natureza qualitativa, com emprego de revisão bibliográfica, análise documental e exame jurisprudencial. O referencial teórico foi construído a partir de doutrina especializada em Direito Processual Penal, Direito Digital e Computação Forense, em diálogo com a legislação aplicável — especialmente as alterações promovidas pela Lei nº 13.964/2019 no Código de Processo Penal. Ademais, procedeu-se à análise crítica de julgados recentes dos Tribunais Superiores, com ênfase na jurisprudência do Superior

Tribunal de Justiça, a fim de verificar a aplicação prática do regime jurídico da cadeia de custódia no tratamento da prova digital.

Estruturalmente, o artigo organiza-se em quatro eixos temáticos principais, além desta introdução e das considerações finais. Inicialmente, examina-se o conceito de prova digital, distinguindo-o da prova eletrônica e destacando suas características fundamentais. Em seguida, analisa-se a disciplina normativa da cadeia de custódia no Código de Processo Penal e sua adaptação ao contexto digital. Na sequência, investigam-se os principais desafios técnicos e operacionais enfrentados pelos órgãos de persecução penal no tratamento de evidências digitais. Por fim, são examinados os reflexos jurídicos decorrentes da quebra da cadeia de custódia digital, com especial atenção à confiabilidade do acervo probatório, às consequências processuais da irregularidade e ao atual posicionamento jurisprudencial sobre a matéria.

2. PROVAS DIGITAIS NO ÂMBITO DO INQUÉRITO POLICIAL

A expansão da tecnologia da informação e a disseminação do acesso à internet alteraram significativamente as relações sociais e, por consequência, as formas de manifestação da criminalidade. A investigação criminal no contexto contemporâneo demanda readequação metodológica por parte das autoridades policiais e do próprio sistema processual penal. O inquérito policial, historicamente orientado à coleta de vestígios físicos e à produção de prova testemunhal, passou a lidar com a necessidade de identificar, rastrear e preservar dados intangíveis dotados de relevância probatória (Lopes Junior, 2020). Nesse contexto, a adequada compreensão da prova digital mostra-se indispensável à análise de seus desafios operacionais e jurídicos.

2.1. CONCEITO DE PROVA DIGITAL

Sob perspectiva técnico-jurídica, a prova digital pode ser compreendida como toda informação armazenada, processada ou transmitida em formato binário que possua aptidão para demonstrar fatos juridicamente relevantes em investigação criminal ou processo penal (Sydow, 2020).

A doutrina especializada identifica como evidência digital os elementos que se manifestam no ambiente computacional ou telemático, abrangendo, entre outros, correios eletrônicos, metadados de arquivos, registros de conexão, históricos de geolocalização, logs de sistemas e comunicações mantidas em aplicativos de mensagens instantâneas, como WhatsApp e Telegram (Wendt; Jorge, 2022).

No plano normativo, a adesão brasileira à Convenção de Budapeste, promulgada pelo Decreto nº 11.491/2023, contribuiu para a delimitação conceitual da matéria ao incorporar a noção de "dado informático", definida como qualquer representação de fatos, informações ou conceitos em forma adequada para processamento por sistema computacional. A prova digital corresponde, nesse sentido, ao dado informático revestido de relevância jurídica e submetido ao regime processual probatório.

2.2. CARACTERÍSTICAS ESPECÍFICAS

Diversamente dos vestígios materiais tradicionais, a prova digital apresenta natureza imaterial, o que lhe confere particularidades técnicas próprias. Entre suas principais características destacam-se a volatilidade, a mutabilidade e o elevado volume de dados normalmente associado à sua coleta e processamento (Rocha, 2021).

Volatilidade: Determinados dados digitais possuem caráter altamente efêmero. Informações armazenadas em memória volátil, conexões de rede ativas e chaves criptográficas em uso podem ser perdidas imediatamente com o desligamento do equipamento. Além disso, dispositivos conectados à rede permanecem sujeitos à alteração ou exclusão remota de dados, inclusive por mecanismos de limpeza remota ("remote wipe") incorporados a sistemas operacionais contemporâneos (Wendt; Jorge, 2022).

A volatilidade da prova digital também se manifesta na própria dinâmica de atualização automática dos sistemas computacionais contemporâneos. Dispositivos conectados à internet frequentemente executam sincronizações em segundo plano, atualizações de aplicativos, sobrescrita de logs e limpeza automática de arquivos temporários, o que pode alterar o estado original da evidência mesmo sem qualquer intervenção humana direta. Em investigações envolvendo crimes cibernéticos, essa característica impõe às autoridades a necessidade de atuação célere e tecnicamente orientada, uma vez que o simples decurso do tempo pode comprometer de forma irreversível a preservação de dados relevantes à persecução penal.

Mutabilidade: Os dados digitais são tecnicamente suscetíveis à modificação, exclusão ou corrupção com relativa facilidade, inclusive sem sinais visíveis de adulteração ao observador leigo. Pequenas alterações em sua estrutura lógica são suficientes para modificar seu conteúdo e alterar os respectivos identificadores criptográficos de integridade (hash). Essa característica explica a crescente preocupação jurisprudencial com a autenticidade e rastreabilidade da prova digital, especialmente em hipóteses de coleta desacompanhada de procedimentos técnicos de preservação (Brasil, 2018).

RECURSO ORDINÁRIO EM HABEAS CORPUS. PENAL E PROCESSO PENAL. TRÁFICO DE DROGAS E ASSOCIAÇÃO AO TRÁFICO. AUTORIZAÇÃO JUDICIAL DE ESPELHAMENTO, VIA WHATSAPP WEB, DAS CONVERSAS REALIZADAS PELO INVESTIGADO COM TERCEIROS. ANALOGIA COM O INSTITUTO DA INTERCEPTAÇÃO TELEFÔNICA. IMPOSSIBILIDADE. PRESENÇA DE DISPARIDADES RELEVANTES. ILEGALIDADE DA MEDIDA. RECONHECIMENTO DA NULIDADE DA DECISÃO JUDICIAL E DOS ATOS E PROVAS DEPENDENTES. PRESENÇA DE OUTRAS ILEGALIDADES. LIMITAÇÃO AO DIREITO DE PRIVACIDADE DETERMINADA SEM INDÍCIOS RAZOÁVEIS DE AUTORIA E MATERIALIDADE. DETERMINAÇÃO ANTERIOR DE ARQUIVAMENTO DO INQUÉRITO POLICIAL. FIXAÇÃO DIRETA DE PRAZO DE 60 (SESSENTA) DIAS, COM PRORROGAÇÃO POR IGUAL PERÍODO. CONSTRANGIMENTO ILEGAL EVIDENCIADO. RECURSO PROVIDO.

1. Hipótese em que, após coleta de dados do aplicativo WhatsApp, realizada pela Autoridade Policial mediante apreensão judicialmente autorizada de celular e subsequente espelhamento das mensagens recebidas e enviadas, os Recorrentes tiveram decretadas contra si prisão preventiva, em razão da suposta prática dos crimes previstos nos arts. 33 e 35 da Lei n.º 11.343/2006.

2. O espelhamento das mensagens do WhatsApp ocorre em sítio eletrônico disponibilizado pela própria empresa, denominado WhatsApp Web. Na referida plataforma, é gerado um tipo específico de código de barras, conhecido como Código QR (Quick Response), o qual só pode ser lido pelo celular do usuário que pretende usufruir do serviço. Daí a necessidade de apreensão, ainda que por breve período de tempo, do aparelho telefônico que se pretende monitorar.

3. Para além de permitir o acesso ilimitado a todas as conversas passadas, presentes e futuras, a ferramenta WhatsApp Web foi desenvolvida com o objetivo de possibilitar ao usuário a realização de todos os atos de comunicação a que teria acesso no próprio celular. O emparelhamento entre celular e computador autoriza o usuário, se por algum motivo assim desejar, a conversar dentro do aplicativo do celular e, simultaneamente, no navegador da internet, ocasião em que as conversas são automaticamente atualizadas na plataforma que não esteja sendo utilizada.

4. Tanto no aplicativo, quanto no navegador, é possível, com total liberdade, o envio de novas mensagens e a exclusão de mensagens antigas (registradas antes do emparelhamento) ou recentes (registradas após), tenham elas sido enviadas pelo usuário, tenham elas sido recebidas de algum contato. Eventual exclusão de mensagem enviada (na opção "Apagar somente para Mim") ou de mensagem recebida (em qualquer caso) não deixa absolutamente nenhum vestígio, seja no aplicativo, seja no computador emparelhado, e, por conseguinte, não pode jamais ser recuperada para efeitos de prova em processo penal, tendo em vista que a própria empresa disponibilizadora do serviço, em razão da tecnologia de encriptação ponta-a-ponta, não armazena em nenhum servidor o conteúdo das conversas dos usuários.

5. Cumpre assinalar, portanto, que o caso dos autos difere da situação, com legalidade amplamente reconhecida pelo Superior Tribunal de Justiça, em que, a exemplo de conversas mantidas por e-mail, ocorre autorização judicial para a obtenção, sem espelhamento, de conversas já registradas no aplicativo WhatsApp, com o propósito de periciar seu conteúdo.

6. É impossível, tal como sugerido no acórdão impugnado, proceder a uma analogia entre o instituto da interceptação telefônica (art. 1.º, da Lei n.º 9.296/1996) e a medida que foi tomada no presente caso.

7. Primeiro: ao contrário da interceptação telefônica, no âmbito da qual o investigador de polícia atua como mero observador de conversas empreendidas por terceiros, no espelhamento via WhatsApp Web o investigador de polícia tem a concreta possibilidade de atuar como participante tanto das conversas que vêm a ser realizadas quanto das conversas que já estão registradas no aparelho celular, haja vista ter o poder, conferido pela própria plataforma online, de interagir nos diálogos mediante envio de novas mensagens a qualquer contato presente no celular e exclusão, com total liberdade, e sem deixar vestígios, de qualquer mensagem passada, presente ou, se for o caso, futura.

8. O fato de eventual exclusão de mensagens enviadas (na modalidade "Apagar para mim") ou recebidas (em qualquer caso) não deixar absolutamente nenhum vestígio nem para o usuário nem para o destinatário, e o fato de tais mensagens excluídas, em razão da criptografia end-to-end, não ficarem armazenadas em nenhum servidor, constituem fundamentos suficientes para a conclusão de que a admissão de tal meio de obtenção de prova

> implicaria indevida presunção absoluta da legitimidade dos atos dos investigadores, dado que exigir contraposição idônea por parte do investigado seria equivalente a demandar-lhe produção de prova diabólica.
> 9. Segundo: ao contrário da interceptação telefônica, que tem como objeto a escuta de conversas realizadas apenas depois da autorização judicial (ex nunc), o espelhamento via Código QR viabiliza ao investigador de polícia acesso amplo e irrestrito a toda e qualquer comunicação realizada antes da mencionada autorização, operando efeitos retroativos (ex tunc).
> 10. Terceiro: ao contrário da interceptação telefônica, que é operacionalizada sem a necessidade simultânea de busca pessoal ou domiciliar para apreensão de aparelho telefônico, o espelhamento via Código QR depende da abordagem do indíviduo ou do vasculhamento de sua residência, com apreensão de seu aparelho telefônico por breve período de tempo e posterior devolução desacompanhada de qualquer menção, por parte da Autoridade Policial, à realização da medida constritiva, ou mesmo, porventura – embora não haja nos autos notícia de que isso tenha ocorrido no caso concreto –, acompanhada de afirmação falsa de que nada foi feito.
> 11. Hipótese concreta dos autos que revela, ainda, outras três ilegalidades: (a) sem que se apontasse nenhum fato novo na decisão, a medida foi autorizada quatro meses após ter sido determinado o arquivamento dos autos; (b) ausência de indícios razoáveis da autoria ou participação em infração penal a respaldar a limitação do direito de privacidade; e (c) ilegalidade na fixação direta do prazo de 60 (sessenta) dias, com prorrogação por igual período.
> 12. Recurso provido, a fim de declarar a nulidade da decisão judicial que autorizou o espelhamento do WhatsApp via Código QR, bem como das provas e dos atos que dela diretamente dependam ou sejam consequência, ressalvadas eventuais fontes independentes, revogando, por conseguinte, a prisão preventiva dos Recorrentes, se por outro motivo não estiverem presos.

A mutabilidade da evidência digital não decorre apenas de adulteração dolosa. Alterações involuntárias também podem ocorrer durante o manuseio inadequado do dispositivo apreendido, seja pela simples inicialização do equipamento, pela conexão a sistemas operacionais comuns ou pela abertura indevida de arquivos antes da realização da imagem forense. Tais intervenções podem modificar metadados relevantes — como data de último acesso, data de modificação e registros de sistema — comprometendo a confiabilidade histórica do vestígio e dificultando a reconstrução cronológica dos fatos investigados.

Volume massivo de dados (Big Data): A apreensão de um único dispositivo eletrônico pode resultar na coleta de expressiva quantidade de informações digitais, incluindo anos de registros de comunicação, arquivos multimídia, dados de localização e históricos de navegação. O tratamento desse volume informacional impõe dificuldades relevantes à atividade pericial, tanto na etapa de extração quanto na de triagem e análise do conteúdo, gerando sobrecarga operacional aos órgãos de persecução penal (Sydow, 2020).

O problema do volume massivo de dados não se limita ao armazenamento físico do material coletado. A própria filtragem e seleção do conteúdo juridicamente relevante constitui desafio metodológico significativo, uma vez que a extração integral de dispositivos eletrônicos frequentemente produz grande quantidade de informações sem pertinência investigativa, incluindo dados pessoais de terceiros e conteúdos protegidos por sigilo constitucional. Desse modo, o

tratamento do Big Data forense demanda não apenas infraestrutura tecnológica robusta, mas também critérios técnicos de triagem e proporcionalidade na delimitação do escopo pericial, em atenção aos princípios da necessidade e da intervenção mínima na esfera privada do investigado.

2.3. DISTINÇÃO ENTRE PROVA DIGITAL E PROVA ELETRÔNICA

Embora frequentemente utilizadas como sinônimos na prática forense, as expressões "prova digital" e "prova eletrônica" não são tecnicamente equivalentes. A distinção possui relevância prática para a correta compreensão dos limites jurídicos da busca e apreensão e do tratamento pericial dos vestígios.

Segundo Wendt e Jorge (2022), a prova eletrônica corresponde ao suporte físico apto a armazenar, processar ou transmitir dados, isto é, ao hardware. Enquadram-se nessa categoria os smartphones, computadores, discos rígidos, pen drives e demais dispositivos apreendidos durante diligências investigativas.

Por sua vez, a prova digital refere-se ao conteúdo lógico armazenado nesses suportes, compreendendo os dados, arquivos, registros e comunicações extraíveis do equipamento apreendido (Rocha, 2021).

A distinção não possui apenas relevância conceitual. Sob perspectiva constitucional e processual, a apreensão lícita do suporte físico não autoriza automaticamente o acesso irrestrito ao conteúdo nele armazenado. A jurisprudência dos Tribunais Superiores tem reconhecido, como regra, que o acesso investigativo aos dados internos de dispositivos eletrônicos depende de autorização judicial específica, ressalvadas hipóteses excepcionais legalmente admitidas, em observância às garantias da intimidade, da privacidade e da proteção de dados pessoais (Brasil, 2017).

> PENAL E PROCESSO PENAL. RECURSO EM HABEAS CORPUS. FURTO E QUADRILHA. APARELHO TELEFÔNICO APREENDIDO. VISTORIA REALIZADA PELA POLÍCIA MILITAR SEM AUTORIZAÇÃO JUDICIAL OU DO PRÓPRIO INVESTIGADO. VERIFICAÇÃO DE MENSAGENS ARQUIVADAS. VIOLAÇÃO DA INTIMIDADE. PROVA ILÍCITA. ART. 157 DO CPP. RECURSO EM HABEAS CORPUS PROVIDO.
> 1. Embora a situação retratada nos autos não esteja protegida pela Lei n. 9.296/1996 nem pela Lei n. 12.965/2014, haja vista não se tratar de quebra sigilo telefônico por meio de interceptação telefônica, ou seja, embora não se trate violação da garantia de inviolabilidade das comunicações, prevista no art. 5º, inciso XII, da CF, houve sim violação dos dados armazenados no celular do recorrente (mensagens de texto arquivadas - WhatsApp).
> 2. No caso, deveria a autoridade policial, após a apreensão do telefone, ter requerido judicialmente a quebra do sigilo dos dados armazenados, haja vista a garantia, igualmente constitucional, à inviolabilidade da intimidade e da vida privada, prevista no art. 5º, inciso X, da CF. Dessa forma, a análise dos dados telefônicos constante dos aparelhos dos investigados, sem sua prévia autorização ou de prévia autorização judicial devidamente motivada, revela a ilicitude da prova, nos termos do art. 157 do CPP. Precedentes do STJ.

> 3. Recurso em habeas corpus provido, para reconhecer a ilicitude da colheita de dados do aparelho telefônico dos investigados, sem autorização judicial, devendo mencionadas provas, bem como as derivadas, serem desentranhadas dos autos.

Assim, a licitude da prova digital pressupõe não apenas a regular apreensão do suporte eletrônico, mas também a observância das exigências constitucionais e processuais pertinentes à extração e utilização do conteúdo digital dele derivado.

3. A CADEIA DE CUSTÓDIA NO CÓDIGO DE PROCESSO PENAL

A reconstrução histórica de um fato delituoso no processo penal não admite flexibilização irrestrita dos meios de obtenção da prova. Para que determinado elemento probatório legitime a atuação estatal sobre a esfera de liberdade do indivíduo, é necessário que sua produção e preservação estejam submetidas a mecanismos de controle técnico e jurídico aptos a assegurar sua confiabilidade (Prado, 2019). Nesse contexto, a cadeia de custódia consolida-se como instrumento essencial de garantia da autenticidade, integridade e rastreabilidade dos vestígios criminais.

3.1. EVOLUÇÃO LEGISLATIVA E PREVISÃO LEGAL (LEI Nº 13.964/2019)

Até o final de 2019, o Código de Processo Penal brasileiro não continha disciplina legal sistematizada acerca da cadeia de custódia. A preservação dos vestígios era regulada predominantemente por construções doutrinárias, princípios processuais e atos normativos infralegais, a exemplo da Portaria nº 82/2014 da Secretaria Nacional de Segurança Pública (Senasp), que estabelecia diretrizes técnicas para a atividade pericial, mas sem força normativa equivalente à lei formal para fins de invalidação processual (Lima, 2020).

Esse cenário foi substancialmente alterado com a promulgação da Lei nº 13.964/2019, denominada Pacote Anticrime, responsável por introduzir os artigos 158-A a 158-F no Código de Processo Penal. O art. 158-A passou a conceituar expressamente a cadeia de custódia como o "conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado […] para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte".

Com a positivação legislativa do instituto, a preservação da integridade probatória deixou de constituir mera recomendação de boas práticas administrativas para assumir a condição de dever processual legalmente imposto. Conforme observa Lopes Jr. (2020), a cadeia de custódia desempenha função de garantia epistêmica, na medida em que busca assegurar que o vestígio submetido à

apreciação judicial corresponda, efetivamente, ao mesmo elemento originalmente identificado na investigação, sem contaminações ou alterações indevidas.

3.2. ETAPAS DA CADEIA DE CUSTÓDIA

Ao disciplinar a cadeia de custódia no art. 158-B do Código de Processo Penal, o legislador brasileiro optou por um modelo analítico e procedimentalizado, estabelecendo as fases sucessivas que compõem o ciclo de preservação do vestígio probatório desde sua identificação até o descarte final. A sistematização legal dessas etapas atende à necessidade de assegurar a rastreabilidade integral do vestígio, permitindo a reconstrução documental de toda sua trajetória material e funcional no curso da persecução penal.

A finalidade subjacente à positivação dessas fases consiste em possibilitar o controle intersubjetivo da confiabilidade da prova, permitindo que magistrado, acusação e defesa verifiquem, de maneira objetiva, se o elemento probatório apresentado em juízo corresponde efetivamente ao mesmo vestígio originalmente identificado durante a investigação criminal. Sob essa perspectiva, cada etapa da cadeia de custódia desempenha função própria e complementar dentro de um sistema integrado de preservação da higidez probatória.

A primeira fase é o reconhecimento, consistente na identificação inicial de determinado elemento como potencial vestígio de interesse investigativo ou pericial. Trata-se de momento cognitivo preliminar em que o agente estatal, a partir da análise do contexto fático, distingue quais objetos, substâncias, documentos ou registros podem possuir relevância para a reconstrução do fato delituoso. O reconhecimento adequado é etapa fundamental, pois falhas nesse momento podem levar tanto à perda de vestígios relevantes quanto à apreensão indevida de elementos desnecessários ou juridicamente irrelevantes.

Na sequência, ocorre o isolamento, destinado à preservação imediata do estado original do vestígio e à prevenção contra contaminações, adulterações ou interferências externas. Em crimes materiais tradicionais, essa fase se concretiza por meio do isolamento físico do local do crime; no plano digital, manifesta-se mediante medidas técnicas destinadas a impedir alterações remotas ou automáticas nos dados armazenados em dispositivos eletrônicos. O isolamento constitui medida preventiva essencial, pois a integridade da prova pode ser comprometida antes mesmo de sua coleta formal.

A terceira etapa corresponde à fixação, entendida como o registro minucioso das condições em que o vestígio foi encontrado. Sua finalidade é documentar de forma objetiva o estado original do elemento probatório antes de qualquer manipulação técnica, geralmente mediante descrição escrita,

registros fotográficos, vídeos, croquis ou outros meios idôneos de documentação. A fixação permite futura reconstrução do contexto originário do vestígio e funciona como mecanismo de controle sobre eventuais alegações de alteração posterior.

Superada essa fase, procede-se à coleta, que consiste no recolhimento técnico do vestígio para fins de preservação e posterior exame pericial. A coleta deve ser realizada por agente tecnicamente capacitado, mediante observância de protocolos específicos compatíveis com a natureza do vestígio, justamente para evitar contaminações, degradações ou modificações involuntárias durante o manuseio inicial.

Após sua coleta, o vestígio é submetido ao acondicionamento, etapa voltada à sua embalagem e armazenamento inicial em recipiente adequado às suas características físicas, químicas, biológicas ou digitais. O acondicionamento deve impedir deterioração, extravio, contaminação cruzada e qualquer alteração indevida das propriedades do vestígio durante sua circulação institucional. Trata-se de fase especialmente relevante porque muitos vícios de preservação probatória decorrem de falhas logísticas posteriores à coleta.

Em seguida, realiza-se o transporte, correspondente à movimentação física do vestígio entre locais ou órgãos responsáveis por sua guarda e processamento. Durante essa fase, devem ser mantidas as condições adequadas de preservação e segurança, com documentação formal de remessa e recebimento. O transporte inadequado pode comprometer integralmente a confiabilidade do material coletado, especialmente em vestígios sensíveis ou tecnologicamente frágeis.

A sétima etapa é o recebimento, momento em que se formaliza a transferência da posse e responsabilidade pelo vestígio entre os agentes ou órgãos envolvidos em sua custódia. Tal ato deve ser documentalmente registrado, com identificação dos responsáveis pela entrega e recepção, horário, condições do material e eventuais intercorrências. O recebimento constitui importante marco de rastreabilidade, pois permite delimitar objetivamente a cadeia de responsabilidade sobre o vestígio.

Superadas as etapas de custódia logística, ingressa-se no processamento, fase correspondente ao exame pericial propriamente dito. É nesse momento que o vestígio é tecnicamente analisado, manipulado e submetido aos procedimentos científicos necessários à extração de informação probatória relevante. Trata-se de uma das fases mais sensíveis da cadeia de custódia, pois a manipulação técnica do material deve ocorrer de forma controlada, documentada e metodologicamente reproduzível.

Após o processamento, sobrevém o armazenamento, que consiste na guarda segura do vestígio em ambiente apropriado, pelo tempo necessário à persecução penal ou até ulterior determinação judicial. Mesmo após a conclusão da perícia, a preservação do material continua sendo necessária para viabilizar eventual contraprova, perícia complementar ou reanálise judicial futura.

Por fim, a cadeia de custódia encerra-se com o descarte, etapa em que o vestígio é liberado, devolvido, destruído ou inutilizado, conforme sua natureza e mediante observância das formalidades legais pertinentes. Ainda que represente a fase terminal do ciclo probatório, o descarte também deve ser documentado, justamente para preservar a completude histórica da cadeia de custódia.

A previsão legal dessas dez etapas evidencia que o legislador buscou estruturar verdadeiro microssistema normativo de preservação probatória, orientado pela lógica da rastreabilidade contínua e da documentação integral do percurso do vestígio. Não obstante, parcela significativa da doutrina observa que o modelo normativo positivado foi concebido primordialmente com base na realidade da prova material clássica, especialmente vestígios físicos e biológicos, razão pela qual sua transposição para o ambiente digital demanda releitura técnico-interpretativa adaptada às peculiaridades da prova informática (Sydow, 2020).

3.3. APLICAÇÃO DA CADEIA DE CUSTÓDIA ÀS PROVAS DIGITAIS

A incidência da cadeia de custódia sobre provas digitais exige adaptação metodológica das etapas legalmente previstas, em razão da natureza peculiar dos dados informáticos (Cancela, 2021). No ambiente digital, a preservação do vestígio não se exaure na apreensão física do equipamento eletrônico, sendo igualmente necessária a adoção de medidas aptas a garantir a integridade lógica dos dados nele armazenados.

Nesse cenário, a atuação dos órgãos de persecução penal deve observar parâmetros técnicos específicos de informática forense, inclusive diretrizes internacionais, como aquelas estabelecidas pela norma ISO/IEC 27037:2014, voltada à identificação, coleta, aquisição e preservação de evidências digitais.

Na etapa de isolamento, por exemplo, a simples apreensão de smartphone ou computador não é suficiente para preservar a integridade do vestígio digital. Faz-se necessária a imediata restrição de conectividade do dispositivo, mediante técnicas como utilização de invólucros de isolamento eletromagnético (Faraday bags), ativação de modo avião ou outras medidas equivalentes, com o objetivo de impedir alterações remotas, sincronizações automáticas ou comandos externos de exclusão de dados.

Quanto à coleta e ao processamento, a prática pericial recomenda a realização de extração forense mediante técnicas de espelhamento físico ou lógico dos dados, preferencialmente em ambiente controlado e com utilização de bloqueadores de escrita (write-blockers), instrumentos destinados a impedir alterações involuntárias dos metadados durante a aquisição pericial.

Adicionalmente, constitui medida técnica de elevada relevância a geração de código hash da mídia ou arquivo periciado. O hash consiste em identificador criptográfico obtido por algoritmo matemático, cuja principal função é permitir a verificação objetiva da integridade do conteúdo examinado. Qualquer alteração, ainda que mínima, no arquivo ou conjunto de dados produz hash distinto, tornando possível aferir tecnicamente eventual modificação superveniente do vestígio digital (Fisberg, 2021).

No âmbito jurisprudencial, o Superior Tribunal de Justiça tem progressivamente reconhecido a necessidade de observância rigorosa da cadeia de custódia em matéria de prova digital. No julgamento do RHC 99.735/SC, por exemplo, a Corte reputou inadequada a utilização de espelhamento de mensagens por meio de WhatsApp Web desacompanhado de procedimentos periciais idôneos, destacando a facilidade de alteração, exclusão ou manipulação unilateral do conteúdo das conversas sem rastros técnicos ostensivos.

De igual modo, a jurisprudência recente da Corte Superior vem atribuindo crescente relevância à demonstração técnica da integridade dos dados digitais coletados, especialmente quando ausentes mecanismos formais de certificação de autenticidade ou quando surgem dúvidas objetivas acerca da higidez do material extraído. Nessas hipóteses, a deficiência na documentação técnica da coleta ou da preservação pode comprometer a força probatória da evidência e ensejar questionamentos acerca da regularidade da cadeia de custódia.

Assim, a cadeia de custódia aplicada às provas digitais não se reduz a formalidade burocrática ou mera rotina administrativa de apreensão de equipamentos. Trata-se de mecanismo processual de controle da confiabilidade probatória, cuja observância é indispensável para assegurar que a evidência digital submetida ao contraditório preserve sua autenticidade, integridade e aptidão demonstrativa. Sua violação, quando apta a comprometer a confiabilidade do vestígio, poderá repercutir diretamente sobre a admissibilidade e o valor probatório do elemento produzido.

4. DESAFIOS TÉCNICOS E OPERACIONAIS DAS PROVAS DIGITAS

A positivação normativa da cadeia de custódia nos arts. 158-A e seguintes do Código de Processo Penal impôs ao Estado deveres técnicos e metodológicos rigorosos para a preservação da confiabilidade probatória. Todavia, a implementação prática dessas exigências encontra obstáculos estruturais relevantes no âmbito da persecução penal brasileira. A migração progressiva dos vestígios criminais do plano físico para o ambiente digital revelou um cenário de tensão entre a sofisticação tecnológica dos meios de investigação e a limitada capacidade operacional dos órgãos responsáveis pela coleta, preservação e análise de evidências informáticas (Giacomolli, 2016).

Nesse contexto, os desafios enfrentados pelas instituições policiais e periciais não se restringem à dimensão normativa, mas abrangem dificuldades concretas de infraestrutura, capacitação técnica, atualização tecnológica e gestão do elevado volume de dados atualmente produzido e armazenado em dispositivos eletrônicos.

4.1. DIFICULDADES DE ARMAZENAMENTO DE GRANDES VOLUMES DE DADOS

Um dos primeiros entraves enfrentados na persecução penal digital refere-se à gestão do expressivo volume de informações coletadas durante investigações contemporâneas. A apreensão de múltiplos dispositivos eletrônicos em uma única operação policial — como smartphones, computadores, servidores locais e mídias removíveis — pode resultar na obtenção de dezenas de terabytes de dados brutos, cuja preservação demanda infraestrutura tecnológica compatível.

A magnitude prática desse problema já foi evidenciada em operações reais. Durante a Operação Seival 2, o setor de informática forense do Instituto Geral de Perícias de Santa Catarina informou a apreensão e cópia de mais de 20 terabytes de dados digitais em uma única atuação pericial, demonstrando como investigações complexas podem rapidamente gerar acervos informacionais de enorme dimensão (IGP-SC, 2023).

A dificuldade de armazenamento, contudo, não se resume à mera disponibilização de espaço em disco. A preservação adequada da prova digital exige sistemas seguros, redundantes e auditáveis, capazes de garantir integridade, disponibilidade e rastreabilidade dos dados ao longo de todo o trâmite investigativo e processual. Conforme orienta a norma técnica ABNT NBR ISO/IEC 27037:2014, a manutenção de evidências digitais deve ocorrer em ambientes controlados, protegidos contra falhas físicas, degradação de hardware, acessos indevidos e perdas acidentais.

Além disso, mídias de armazenamento eletrônico estão sujeitas a fenômenos de degradação progressiva, como corrupção silenciosa de dados (bit rot), falhas mecânicas e perda de setores magnéticos, circunstâncias que exigem políticas permanentes de redundância, replicação e verificação periódica de integridade dos arquivos armazenados. A adoção dessas medidas implica investimentos contínuos em servidores, sistemas de backup, climatização de ambientes e manutenção especializada, elevando significativamente os custos operacionais da custódia digital estatal (Velho; Costa; Morrone, 2021).

Dessa forma, a limitação orçamentária dos órgãos de segurança pública compromete diretamente a preservação prolongada e tecnicamente adequada das provas digitais, especialmente em investigações de maior complexidade ou duração.

4.2. EXTRAÇÃO DE DADOS E RISCOS À INTEGRIDADE DA PROVA

A etapa de extração e processamento dos dados constitui um dos momentos mais sensíveis da cadeia de custódia digital, pois é justamente nesse estágio que a evidência se torna mais vulnerável à contaminação, modificação ou perda. A literatura especializada identifica essa característica como dinâmica da evidência digital, expressão utilizada para designar a elevada suscetibilidade dos dados informáticos a qualquer interferência externa durante sua manipulação técnica (Velho; Costa; Morrone, 2021).

Em razão dessa fragilidade, a extração dos dados deve observar protocolos rigorosos de computação forense. Um dos mecanismos técnicos tradicionalmente empregados para preservação da integridade da mídia original é o uso de bloqueadores de escrita (write-blockers), dispositivos físicos ou lógicos que impedem qualquer gravação involuntária na mídia examinada durante o procedimento pericial. Sem esse mecanismo de proteção, o simples acesso do sistema pericial ao dispositivo pode modificar automaticamente metadados relevantes — como data de último acesso, logs de sistema ou registros temporários — alterando o estado originário da evidência.

Nos dispositivos móveis contemporâneos, o desafio técnico torna-se ainda mais acentuado em razão da crescente sofisticação dos sistemas de criptografia embarcada. Smartphones atuais operam com mecanismos avançados de proteção de dados, como criptografia integral de disco, enclaves seguros de hardware e autenticação biométrica integrada, o que frequentemente exige a utilização de ferramentas especializadas de extração forense.

Nesse cenário, órgãos periciais recorrem a plataformas profissionais de forensic extraction, capazes de realizar desde extrações lógicas até aquisições físicas mais profundas da memória interna dos aparelhos. Todavia, mesmo esses procedimentos não são isentos de risco técnico, especialmente quando envolvem tentativas de bypass de bloqueios criptográficos ou exploração de vulnerabilidades do sistema operacional, hipóteses em que pode haver alteração involuntária do conteúdo original da prova.

Para mitigar tais riscos, consolidou-se como boa prática pericial a utilização de algoritmos hash como instrumento de verificação de integridade. O hash funciona como identificador matemático único do conjunto de dados extraído: qualquer modificação, ainda que mínima, gera alteração no código hash correspondente. Por essa razão, sua documentação no momento da aquisição e posterior conferência durante o exame pericial constituem importantes mecanismos de validação técnica da autenticidade da prova digital.

4.3. LIMITAÇÕES ESTRUTURAIS DA POLÍCIA JUDICIÁRIA

As dificuldades relacionadas à prova digital não decorrem apenas da complexidade tecnológica da evidência, mas também da insuficiência estrutural dos órgãos responsáveis por sua gestão. A realidade de muitas unidades policiais brasileiras ainda é marcada por déficit de pessoal especializado, carência de equipamentos adequados e ausência de protocolos operacionais uniformes para tratamento de vestígios digitais.

A realidade de muitas unidades policiais brasileiras ainda é marcada por déficit de pessoal especializado, carência de equipamentos adequados e ausência de padronização plena dos fluxos operacionais de tratamento de vestígios digitais. Tal cenário é reconhecido institucionalmente por órgãos de segurança pública, que apontam aumento exponencial da demanda por perícias cibernéticas sem correspondente expansão proporcional da capacidade técnico-operacional estatal (FBSP, 2024; Polícia Científica do Paraná, 2025).

O déficit de recursos humanos qualificados possui impacto direto sobre a cadeia de custódia. A apreensão inicial dos dispositivos frequentemente é realizada por agentes não especializados em computação forense, os quais, embora aptos à atividade policial ostensiva ou investigativa geral, nem sempre dispõem de treinamento técnico específico para adoção das cautelas necessárias à preservação de vestígios digitais.

Essa limitação operacional pode gerar falhas logo nos primeiros momentos da apreensão, como o acondicionamento inadequado de aparelhos eletrônicos, ausência de isolamento eletromagnético dos dispositivos ou manipulação indevida do equipamento antes da perícia técnica. Tais condutas, ainda que praticadas sem dolo, possuem potencial para comprometer a integridade da evidência e fragilizar sua confiabilidade probatória.

Some-se a isso o fato de que a distribuição de recursos tecnológicos costuma ocorrer de forma desigual entre as unidades policiais, concentrando equipamentos e treinamento especializado em grandes centros urbanos ou em investigações de maior repercussão, o que produz assimetrias relevantes na qualidade da persecução penal digital em âmbito nacional.

4.4. ATUAÇÃO DA PERÍCIA DIGITAL E GARGALOS TÉCNICOS

A crescente dependência da persecução penal em relação à prova digital produziu significativo aumento da demanda sobre os órgãos de perícia criminal, especialmente os setores especializados em informática forense. Entretanto, o crescimento do volume de vestígios digitais submetidos à análise não foi acompanhado, em igual medida, pela expansão da capacidade operacional dos institutos periciais, gerando acúmulo progressivo de material pendente de processamento.

Esse represamento técnico, frequentemente referido como backlog pericial, constitui um dos principais gargalos da persecução penal contemporânea. Em muitos casos, dispositivos apreendidos permanecem por meses — e, em situações mais complexas, por período ainda superior — aguardando análise técnica, o que retarda a conclusão do inquérito policial e impacta diretamente a duração razoável da investigação e do processo.

Além da insuficiência quantitativa de peritos e laboratórios especializados, o problema é agravado pela rápida obsolescência das ferramentas de informática forense. O desenvolvimento contínuo de novos sistemas operacionais, protocolos de segurança e padrões de criptografia impõe atualização permanente dos softwares e hardwares utilizados na extração de dados, sob pena de perda de capacidade técnica para acesso às informações armazenadas.

Ocorre que a aquisição e renovação desses instrumentos depende, em regra, de procedimentos administrativos complexos e disponibilidade orçamentária compatível, circunstâncias que frequentemente impedem a atualização tempestiva do aparato tecnológico estatal. Como consequência, não raramente dispositivos apreendidos tornam-se temporariamente inacessíveis à perícia oficial, não por ausência de relevância investigativa, mas por insuficiência material de meios técnicos para seu processamento.

Desse modo, os gargalos periciais e estruturais revelam que a efetividade da cadeia de custódia digital não depende exclusivamente de previsão normativa adequada, mas também de investimentos institucionais permanentes em tecnologia, capacitação profissional e infraestrutura pericial.

5. REFLEXOS JURÍDICOS DAS FALHAS NA CADEIA DE CUSTÓDIA DIGITAL

A inobservância dos protocolos técnicos de coleta, preservação e processamento da prova digital ultrapassa o campo das meras irregularidades administrativas e projeta efeitos diretos sobre a validade do acervo probatório produzido no processo penal. Isso porque, diante da elevada mutabilidade e replicabilidade dos dados informáticos, a ausência de observância à cadeia de custódia compromete a possibilidade de aferição da autenticidade, integridade e rastreabilidade da evidência digital.

Nessas hipóteses, a fragilidade metodológica do procedimento de coleta ou extração pode comprometer a confiabilidade epistêmica da prova, reduzindo sua aptidão para fundamentar decisões estatais restritivas de liberdade. Por essa razão, a jurisprudência brasileira tem progressivamente reconhecido que falhas relevantes na cadeia de custódia digital podem ensejar inadmissibilidade probatória, nulidade processual ou, ao menos, mitigação do valor persuasivo da evidência produzida (Badaró, 2021).

5.1. CONFIABILIDADE, AUTENTICIDADE E CONTROLE JURISDICIONAL DA PROVA DIGITAL

No processo penal contemporâneo, a aptidão demonstrativa da prova digital depende não apenas de sua existência material, mas de sua autenticidade verificável e de sua submissão a procedimentos tecnicamente auditáveis. Em outras palavras, não basta que determinado dado seja apresentado em juízo: é necessário que exista segurança objetiva quanto à sua origem, integridade e forma de obtenção.

A crescente centralidade da prova digital em investigações complexas tem evidenciado, inclusive em casos de elevada repercussão nacional, tensões institucionais entre a custódia jurídica do material apreendido e a necessidade de submissão desse material a protocolos técnicos especializados de perícia forense. Episódios recentes envolvendo a apreensão de grande volume de dispositivos eletrônicos em investigações conduzidas sob supervisão do Supremo Tribunal Federal demonstram que a mera guarda física judicial do hardware apreendido não substitui, por si só, a necessidade de posterior extração pericial adequada, com observância de protocolos de integridade e documentação técnica.

Nesse contexto, consolida-se o entendimento de que a custódia jurídica do suporte físico não se confunde com a validação técnica do conteúdo digital nele armazenado. A confiabilidade probatória da evidência depende da realização de procedimentos periciais aptos a demonstrar, de forma auditável, que os dados extraídos correspondem fielmente ao conteúdo originalmente apreendido.

5.2. CONSEQUÊNCIAS PROCESSUAIS DA QUEBRA DA CADEIA DE CUSTÓDIA DIGITAL

A quebra da cadeia de custódia digital pode gerar relevantes consequências processuais, especialmente quando impede a verificação objetiva da integridade ou autenticidade da prova produzida. Nesses casos, a jurisprudência tem reconhecido que a ausência de documentação mínima sobre os procedimentos empregados na extração e preservação dos dados compromete a confiabilidade do material probatório.

Todavia, é importante observar que a mera irregularidade formal não conduz automaticamente à nulidade da prova. A tendência jurisprudencial predominante é no sentido de que a violação da cadeia de custódia deve ser analisada casuisticamente, verificando-se se a falha comprometeu

concretamente a confiabilidade da evidência ou gerou prejuízo demonstrável ao contraditório e à ampla defesa.

Quando a ruptura metodológica impede a demonstração segura da autenticidade da prova digital, o ônus argumentativo do órgão acusador torna-se significativamente mais gravoso, pois passa a incumbir à acusação demonstrar, por outros elementos técnicos ou contextuais, que a prova permaneceu íntegra e confiável apesar da falha procedimental. Não se trata propriamente de inversão formal do ônus da prova, mas de enfraquecimento substancial da presunção de regularidade da atividade estatal de coleta e preservação probatória.

Nessas hipóteses, persistindo dúvida razoável acerca da integridade da evidência, sua utilização para fundamentar condenação penal tende a ser juridicamente inviável, em observância ao princípio do in dubio pro reo e às garantias constitucionais do devido processo legal.

5.3. FRAGILIDADE DOS PRINTS, MENSAGERIA INSTANTÂNEA E DISTINÇÃO QUANTO ÀS PROVAS PRODUZIDAS POR PARTICULARES

A volatilidade das plataformas de mensagens forçou o STJ a adotar um paradigma de extrema desconfiança em relação a provas descontextualizadas. O precedente histórico da Sexta Turma no julgamento do Recurso em Habeas Corpus nº 99.735/SC declarou a invalidade probatória do espelhamento do WhatsApp Web realizado por policiais sem preservação da cadeia de custódia. A Corte fundamentou que a plataforma permite a exclusão unilateral ("apagar para todos") sem deixar rastros aparentes, ferindo de morte a confiabilidade do acervo caso a extração não obedeça às normativas técnicas.

Esse movimento culminou no que a doutrina contemporânea chama de "o fim do print" como prova isolada. Em decisões supervenientes e paradigmáticas, a exemplo do Habeas Corpus nº 1.036.370/PR (julgado no final de 2025), o STJ sedimentou que condenações fundamentadas exclusivamente em capturas de tela produzidas por agentes de segurança, desprovidas da documentação técnica e da coleta de metadados prevista no art. 158-B do CPP e nas normas da ISO/IEC, padecem de nulidade material insuperável.

Todavia, é crucial destacar um importante distinguishing (distinção) no entendimento jurisprudencial: a assimetria na exigência de preservação em relação às provas produzidas por particulares. O rigor do STJ imposto aos órgãos de persecução estatal não se estende aos cidadãos comuns. No julgamento do AgRg no AREsp 2.967.267/SC, com aplicação frequente em crimes de violência doméstica, a Quinta Turma pacificou que prints de conversas apresentados pela própria vítima ou por seus familiares são válidos e lícitos.

> DIREITO PROCESSUAL PENAL. EMBARGOS DE DECLARAÇÃO. APLICAÇÃO DA SÚMULA 7 DO STJ. PREMISSAS FÁTICAS. PROVA DIGITAL. ESCLARECIMENTOS. EMBARGOS PARCIALMENTE ACOLHIDOS. EFEITOS INFRINGENTES NÃO CONCEDIDOS.
> I. CASO EM EXAME
> 1. Embargos de declaração opostos contra acórdão da Quinta Turma do STJ que negou provimento ao agravo regimental, mantendo decisão monocrática que não conheceu do recurso especial em razão da incidência da Súmula 7 do STJ.
> 2. O embargante alegou omissão e obscuridade na aplicação da Súmula 7 do STJ, sustentando que o acórdão utilizou premissas fáticas para validar a prova digital e afastar o dissídio jurisprudencial, mas invocou o óbice sumular para impedir a análise da violação ao art. 158-A do Código de Processo Penal. Apontou contradição entre o uso de fatos para fundamentar a decisão e a vedação ao reexame probatório. Alegou, ainda, omissão quanto à distinção entre provas digitais colhidas por particular e por autoridade policial, com violação ao contraditório, ampla defesa e paridade de armas.
> Requereu efeitos modificativos para reformar o julgado.
> II. QUESTÃO EM DISCUSSÃO
> 3. A questão em discussão consiste em saber se o acórdão embargado incorreu em omissão, obscuridade ou contradição ao aplicar a Súmula 7 do STJ para não conhecer do recurso especial, ao utilizar premissas fáticas para validar a prova digital e afastar o dissídio jurisprudencial, e ao não enfrentar alegações de violação ao contraditório, ampla defesa e paridade de armas.
> III. RAZÕES DE DECIDIR
> 4. A Súmula 7 do STJ impede o reexame de provas, mas não veda a utilização de premissas fáticas definitivamente assentadas pelas instâncias ordinárias para realizar o adequado enquadramento jurídico.
> 5. O acórdão embargado não procedeu ao reexame do conjunto probatório, mas utilizou as premissas fáticas estabelecidas pelo Tribunal de origem para demonstrar que o acolhimento da tese defensiva dependeria de revisão das circunstâncias fáticas, atraindo o óbice da Súmula 7 do STJ.
> 6. Não há omissão, obscuridade, contradição ou erro material no acórdão embargado, que enfrentou de forma suficiente a matéria e apresentou os motivos necessários para fundamentar seu convencimento.
> 7. A distinção entre provas digitais colhidas por autoridade policial e por particulares foi realizada exclusivamente no âmbito do cotejo analítico próprio do juízo de admissibilidade do dissídio jurisprudencial, não constituindo fundamento determinante do acórdão embargado.
> 8. A ausência de similitude fática entre o caso concreto e os paradigmas apresentados, bem como a não demonstração do cotejo analítico exigido pelo art. 1.029, §1º, do CPC, impedem o conhecimento do recurso especial pela alínea "c" do art. 105, III, da Constituição Federal.
> IV. DISPOSITIVO E TESE
> 9. Resultado do Julgamento: Embargos de declaração parcialmente acolhidos, sem efeitos infringentes, para prestar esclarecimentos, mantendo-se inalterado o resultado do julgamento.

O fundamento jurídico para tal flexibilização baseia-se na constatação de que não se pode exigir do particular o conhecimento formal ou os recursos para a realização de complexas extrações periciais via hash. Desde que os referidos prints sejam confirmados em juízo sob o crivo do contraditório e não apresentem indícios patentes de fraude ou edição, eles não configuram violação à cadeia de custódia, sendo admitidos para a formação do convencimento judicial (Sydow, 2020).

6. CONSIDERAÇÕES FINAIS

A persecução penal na era digital impôs ao ordenamento jurídico brasileiro relevantes desafios metodológicos e estruturais. Conforme demonstrado ao longo deste estudo, a progressiva substituição dos vestígios materiais tradicionais por evidências digitais alterou substancialmente a dinâmica probatória no processo penal, exigindo das instituições estatais não apenas adaptação normativa, mas também aprimoramento técnico compatível com a complexidade da computação forense contemporânea.

A positivação da cadeia de custódia no Código de Processo Penal, por meio da inserção dos arts. 158-A a 158-F pela Lei nº 13.964/2019, representou avanço normativo significativo ao estabelecer parâmetros legais para a preservação da autenticidade, integridade e rastreabilidade dos vestígios probatórios. Todavia, a pesquisa evidenciou que a existência de um marco normativo formal não elimina, por si só, os entraves práticos enfrentados na persecução penal. Persistem limitações estruturais relevantes nas Polícias Judiciárias e nos órgãos periciais, especialmente quanto à insuficiência de recursos humanos especializados, à escassez de ferramentas tecnológicas adequadas e à dificuldade de gerenciamento seguro de grandes volumes de dados digitais.

No plano jurisprudencial, verificou-se progressivo amadurecimento dos tribunais superiores quanto às especificidades da prova digital e à necessidade de observância rigorosa da cadeia de custódia em sua obtenção e preservação. A jurisprudência do Superior Tribunal de Justiça, em especial, tem demonstrado crescente preocupação com a confiabilidade de evidências digitais produzidas sem observância de protocolos técnicos mínimos de extração, preservação e documentação, particularmente em relação a dados obtidos de aparelhos celulares e aplicações de mensageria instantânea.

Também se constatou que a fragilidade inerente aos dados digitais — marcada por sua volatilidade, mutabilidade e facilidade de replicação — exige que o controle de integridade da prova vá além da mera apreensão física do dispositivo eletrônico. A preservação adequada da prova digital demanda procedimentos técnicos específicos, como isolamento do equipamento, extração forense adequada, documentação completa dos atos praticados e, sempre que cabível, utilização de mecanismos de verificação de integridade, como funções hash e técnicas de espelhamento pericial.

A análise permitiu concluir, ainda, que a quebra da cadeia de custódia digital não conduz automaticamente à ilicitude da prova em toda e qualquer hipótese, devendo seus efeitos ser examinados à luz do caso concreto, em consonância com a orientação jurisprudencial predominante. Não obstante, quanto maior a gravidade da falha na preservação da integridade ou da rastreabilidade do vestígio digital, maior tende a ser o comprometimento de sua confiabilidade e, consequentemente, de sua aptidão probatória no processo penal.

Por fim, conclui-se que a efetividade da persecução penal em ambiente digital depende da harmonização entre evolução normativa, capacitação técnica e aparelhamento estrutural das instituições responsáveis pela investigação criminal. Sem investimentos consistentes em tecnologia forense, qualificação profissional e padronização de protocolos operacionais, a crescente dependência da prova digital poderá transformar-se, paradoxalmente, em fator de insegurança jurídica e de fragilização da atividade persecutória estatal.

Em síntese, a cadeia de custódia digital não constitui mera formalidade procedimental, mas elemento essencial à confiabilidade epistemológica da prova penal contemporânea. Sua observância adequada representa pressuposto indispensável para a legitimidade da atividade probatória e para a compatibilização entre eficiência investigativa e preservação das garantias fundamentais no processo penal.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27037**: tecnologia da informação — técnicas de segurança — diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Rio de Janeiro: ABNT, 2014.

BADARÓ, G. H. **Processo penal**. 9. ed. São Paulo: Thomson Reuters Brasil, 2021.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 8 abr. 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: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 8 abr. 2026.

BRASIL. Superior Tribunal de Justiça. Agravo Regimental no Agravo em Recurso Especial nº 2.967.267/SC. 5ª Turma. Relator: Min. Messod Azulay Neto. **Diário da Justiça Eletrônico Nacional**, Brasília, DF, nov. 2025.

BRASIL. Superior Tribunal de Justiça. Habeas Corpus nº 1.036.370/PR. 5ª Turma. Relator: Min. Joel Ilan Paciornik. **Diário da Justiça Eletrônico Nacional**, Brasília, DF, set. 2025.

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1.706.113/DF (2017/0250966-3). Terceira Turma. Relatora: Min. Nancy Andrighi. Julgado em: 5 dez. 2017. **Diário da Justiça Eletrônico**, Brasília, DF, 13 dez. 2017.

BRASIL. Superior Tribunal de Justiça. Recurso em Habeas Corpus nº 99.735/SC. 6ª Turma. Relatora: Min. Laurita Vaz. Julgado em: 27 nov. 2018. **Diário da Justiça Eletrônico**, Brasília, DF, 12 dez. 2018.

CANCELA, A. G. Os standards metodológicos de produção da prova na prova digital e a importância da cadeia de custódia. **Revista do IBCCRIM**, São Paulo, v. 29, n. 343, p. 7-9, jun. 2021.

COSTA, J. A. L. da. Caso Master: prova sem perito, o STF e o processo penal. **JOTA**, Brasília, DF, 15 jan. 2026. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/caso-master-prova-sem-perito-o-stf-e-o-processo-penal. Acesso em: 8 abr. 2026.

FISBERG, Y. Função 'hash' e a integridade da prova digital. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 11, n. 3, 2025. DOI: https://doi.org/10.22197/rbdpp.v11i3.1227.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Raio X das forças de segurança pública do Brasil**. São Paulo: FBSP, 2024. Disponível em: https://forumseguranca.org.br. Acesso em: 8 abr. 2026.

GIACOMOLLI, N. J. **O devido processo penal**: abordagem conforme a Constituição Federal e o Pacto de São José da Costa Rica. 3. ed. São Paulo: Atlas, 2016.

INSTITUTO GERAL DE PERÍCIAS DE SANTA CATARINA. **Setor de informática forense do IGP apreende mais de 20 terabytes de dados copiados durante Operação Seival 2**. Florianópolis: IGP-SC, 2023. Disponível em: https://blog.neotel.com.br/sem-categoria/setor-de-informatica-forense-do-igp-apreende-mais-de-20-terabytes-de-dados-copiados-durante-operacao-seival-2/. Acesso em: 9 abr. 2026.

JESUS, D. de; MILAGRE, J. A. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

LIMA, R. B. de. **Manual de processo penal**: volume único. 8. ed. Salvador: Juspodivm, 2020.

LOPES JR., A. **Direito processual penal**. 17. ed. São Paulo: Saraiva Educação, 2020.

PRADO, G. **A cadeia de custódia da prova no processo penal**. 3. ed. São Paulo: Marcial Pons, 2019.

ROCHA, J. B. **Provas digitais no processo penal**. 2. ed. São Paulo: Tirant lo Blanch, 2021.

SYDOW, S. T. **Crimes informáticos e suas provas**. 3. ed. Salvador: Juspodivm, 2020.

VELHO, J. A.; COSTA, P. E.; MORRONE, Â. **Tratado de computação forense**. Campinas: Millennium, 2021.

WENDT, E.; JORGE, H. V. N. **Inteligência digital**: investigação de crimes cibernéticos. 4. ed. São Paulo: Brasport, 2022.