REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

A PROVA DIGITAL E SEUS LIMITES NA PERSECUÇÃO PENAL: ANÁLISE À LUZ DA CADEIA DE CUSTÓDIA

Tullio Henrique dos Santos Souza
http://lattes.cnpq.br/9223974075009010
https://orcid.org/0009-0006-1152-8099
E-mail: tullio.souza@ufms.br

DOI-Geral: http://dx.doi.org/10.47538/RA-2026.V5N2
DOI-Individual: http://dx.doi.org/10.47538/RA-2026.V5N2-31

RESUMO: O avanço tecnológico transformou a dinâmica da persecução penal, especialmente no que se refere à produção e utilização da prova digital. Contudo, a ausência de padronização e as fragilidades na cadeia de custódia levantam questionamentos sobre a confiabilidade desses elementos probatórios. O presente artigo analisa os limites da prova digital no processo penal brasileiro, com foco na cadeia de custódia introduzida pela Lei nº 13.964/2019. Conclui-se que, apesar dos avanços normativos, ainda existem lacunas operacionais que comprometem a integridade e a validade da prova digital.

PALAVRAS-CHAVE: Prova digital. Cadeia de custódia. Processo penal. Tecnologia. Prova penal.

DIGITAL EVIDENCE AND ITS LIMITS IN CRIMINAL PROSECUTION: ANALYSIS IN THE LIGHT OF THE CHAIN OF CUSTODY

ABSTRACT: Technological advances have transformed the dynamics of criminal prosecution, especially with regard to the production and use of digital evidence. However, the lack of standardization and weaknesses in the chain of custody raise questions about the reliability of these pieces of evidence. This article analyzes the limits of digital evidence in Brazilian criminal proceedings, focusing on the chain of custody introduced by Law No. 13,964/2019. It is concluded that, despite regulatory advances, there are still operational gaps that compromise the integrity and validity of digital evidence.

KEYWORDS: Digital proof. Chain of custody. Criminal proceedings. Technology. Criminal evidence.

INTRODUÇÃO

A transformação digital impactou profundamente os mecanismos de investigação criminal, inserindo novos meios de obtenção de prova no processo penal. A prova digital, caracterizada por sua volatilidade, replicabilidade e dependência tecnológica, passou a ocupar posição central na persecução penal contemporânea.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

Entretanto, tais características também introduzem fragilidades específicas, sobretudo no que diz respeito à sua coleta, preservação e análise. Nesse contexto, a cadeia de custódia, incorporada ao ordenamento jurídico brasileiro pela Lei nº 13.964/2019, por meio dos arts. 158-A a 158-F do Código de Processo Penal, surge como instrumento essencial para garantir a integridade da prova.

O problema que orienta este estudo consiste em verificar em que medida a prova digital atende aos requisitos de confiabilidade exigidos pelo processo penal, partindo da hipótese de que persistem lacunas práticas relevantes.

A pesquisa adota metodologia de revisão bibliográfica e análise normativa, com enfoque nas disposições da Lei nº 13.964/2019 e na doutrina processual penal brasileira contemporânea. Justifica-se pela crescente utilização da prova digital em investigações criminais e pela necessidade de segurança jurídica quanto à sua validade probatória.

A PROVA DIGITAL NO PROCESSO PENAL

A prova digital pode ser compreendida como todo elemento informacional armazenado ou transmitido em meio eletrônico, capaz de contribuir para a reconstrução de um fato juridicamente relevante.

A doutrina processual penal destaca que a validade da prova depende da observância de critérios como legalidade, autenticidade e integridade, sendo imprescindível o respeito às garantias fundamentais (Lopes Jr., 2023).

Diferentemente das provas tradicionais, a prova digital apresenta características próprias, como a facilidade de alteração, a ausência de materialidade física e a dependência de ferramentas tecnológicas para sua interpretação. Tais elementos exigem um tratamento diferenciado por parte dos operadores do Direito.

No âmbito da doutrina, a prova digital também é denominada prova eletrônica ou prova informática. Independentemente da nomenclatura, o traço comum é a imaterialidade do suporte. Enquanto uma prova documental tradicional reside no papel, a prova digital existe como sequência de bits, legível apenas mediante mediação tecnológica.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

Essa característica impõe desafios específicos ao processo penal. O princípio do contraditório, previsto no art. 5º, LV, da Constituição Federal, exige que as partes tenham acesso efetivo aos elementos probatórios. No caso da prova digital, esse acesso depende não apenas da permissão judicial, mas também de conhecimentos técnicos e ferramentas especializadas.

A doutrina tem alertado que a simples juntada de prints ou capturas de tela não basta para conferir autenticidade à prova digital. É necessário demonstrar a integridade do dado desde sua origem até sua apresentação em juízo. Do contrário, a prova digital pode ser facilmente impugnada sob o argumento de adulteração.

Além disso, a prova digital frequentemente envolve dados pessoais e comunicações privadas, o que atrai a incidência da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e do sigilo das comunicações (art. 5º, XII, CF). A obtenção da prova digital deve, portanto, respeitar reserva de jurisdição sempre que houver interceptação ou quebra de sigilo.

A CADEIA DE CUSTÓDIA: FUNDAMENTOS NORMATIVOS

PREVISÃO LEGAL E FINALIDADE

A cadeia de custódia consiste no conjunto de procedimentos destinados a manter e documentar a história cronológica da prova, conforme dispõe o art. 158-A do Código de Processo Penal.

O legislador da Lei nº 13.964/2019 incorporou ao processo penal brasileiro um instituto já consolidado no direito comparado e nas ciências forenses. A finalidade precípua da cadeia de custódia é assegurar que o vestígio apresentado em juízo seja o mesmo coletado na cena do crime, sem qualquer modificação, adulteração ou contaminação.

No caso da prova digital, a cadeia de custódia assume relevo ainda maior, dado o risco aumentado de alteração invisível a olho nu. Enquanto uma mancha de sangue pode ser macroscopicamente identificada como alterada, um bit modificado em um arquivo não deixa vestígios físicos aparentes.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

AS ETAPAS DO ART. 158-B

Nos termos do art. 158-B, são etapas da cadeia de custódia o reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte dos vestígios.

Cada uma dessas etapas aplica-se à prova digital com especificidades próprias. No reconhecimento, é preciso identificar não apenas o dispositivo (computador, celular, HD), mas também a natureza volátil dos dados (memória RAM, por exemplo). No isolamento, a prova digital exige procedimentos como a blindagem de sinais (faraday bag) para evitar acesso remoto ou alteração do conteúdo.

A fixação, na prova digital, corresponde à documentação do estado original do dispositivo e dos dados. Nessa etapa, técnicas como a fotografia da tela, a gravação de vídeo do procedimento e a anotação de metadados são fundamentais. A coleta deve ser feita prioritariamente por imagem forense (bit stream copy), e não pela simples cópia de arquivos.

DOCUMENTAÇÃO DA CADEIA DE CUSTÓDIA

O art. 158-C do Código de Processo Penal exige que a cadeia de custódia seja documentada. Essa documentação, no contexto da prova digital, deve conter informações como: identificação do responsável por cada etapa, data e hora da coleta, descrição do equipamento utilizado, hash dos arquivos obtidos e eventual cadeia de assinaturas eletrônicas.

A ausência de documentação, ou sua insuficiência, gera dúvida razoável sobre a integridade da prova digital. Nesses casos, a jurisprudência tem entendido que o ônus da demonstração da autenticidade recai sobre a parte que produziu a prova.

A inobservância desses procedimentos pode comprometer a admissibilidade da prova, uma vez que afeta diretamente sua confiabilidade.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

A APLICAÇÃO DA CADEIA DE CUSTÓDIA À PROVA DIGITAL

TÉCNICAS ESPECÍFICAS DE PRESERVAÇÃO

No contexto da prova digital, a preservação da integridade exige o uso de técnicas específicas, como hashing e espelhamento forense, sem as quais a autenticidade dos dados pode ser questionada.

O hashing consiste na aplicação de algoritmo matemático (SHA-256, MD5, entre outros) que gera uma cadeia única de caracteres correspondente ao conteúdo do arquivo. Qualquer alteração mínima no arquivo — ainda que a adição de um espaço ou ponto — produz um hash completamente diverso. Com isso, é possível verificar, a qualquer tempo, se o arquivo foi modificado após a coleta.

O espelhamento forense, por sua vez, é uma cópia bit a bit do dispositivo de armazenamento. Diferentemente da cópia comum, que copia apenas os arquivos visíveis ao sistema operacional, o espelhamento captura também arquivos deletados, espaços não alocados, fragmentos e metadados.

Ambas as técnicas devem ser realizadas por ferramentas validadas e com registro detalhado de todos os passos, sob pena de quebra da cadeia de custódia.

DESAFIOS ESPECÍFICOS NA COLETA DE PROVA DIGITAL

A coleta da prova digital apresenta desafios que não encontram paralelo na prova material. O primeiro deles é a volatilidade. Dados armazenados na memória RAM são perdidos no momento do desligamento do dispositivo. Dados criptografados podem se tornar inacessíveis se o dispositivo for desligado ou reiniciado.

Por essa razão, a coleta da prova digital deve obedecer a uma ordem de prioridade: primeiro os dados voláteis (memória RAM, conexões de rede ativas), depois os dados não voláteis (arquivos em disco, logs). Essa ordem inverte o senso comum de que primeiro se desliga o equipamento.

Outro desafio relevante é a criptografia. Com a popularização da criptografia full disk e de aplicativos de mensagens com criptografia ponta a ponta, a mera apreensão do

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

dispositivo não garante acesso ao conteúdo. A cadeia de custódia, nesse caso, deve contemplar a obtenção de senhas ou chaves de acesso, sob pena de a prova digital tornar-se inútil.

O PAPEL DO PERITO NA CADEIA DE CUSTÓDIA

O art. 158-D do Código de Processo Penal atribui ao perito a responsabilidade por parte das etapas da cadeia de custódia. Na prova digital, o perito não é apenas um analista; ele é o guardião da integridade probatória.

O perito deve documentar cada procedimento realizado, desde a abertura do dispositivo até a extração final dos dados. Qualquer omissão na documentação pode ser explorada pela defesa como indicativo de violação da cadeia de custódia.

Além disso, o perito deve ter conhecimento específico em informática forense. A simples nomeação de perito oficial sem comprovação de capacitação técnica em prova digital pode configurar nulidade relativa, uma vez que o art. 158-E exige que os procedimentos sejam realizados por "pessoa capacitada".

LIMITES E FRAGILIDADES DA PROVA DIGITAL

A AUSÊNCIA DE RIGOR TÉCNICO

A natureza intangível da prova digital exige rigor técnico em sua preservação. A ausência desse rigor pode comprometer a validade da prova, violando o devido processo legal.

A experiência prática tem demonstrado que muitos órgãos de persecução penal ainda carecem de protocolos internos específicos para coleta de prova digital. Agentes públicos, por vezes, acessam dispositivos apreendidos sem a devida blindagem, conectam-nos à rede ou realizam cópias sem a utilização de hash.

Essas práticas, quando identificadas em juízo, conduzem à imprestabilidade da prova digital. O tribunal, ao reconhecer a violação da cadeia de custódia, declara a prova nula ou inadmissível, com prejuízo para a persecução penal.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

VULNERABILIDADE À ADULTERAÇÃO

Além disso, a prova digital apresenta vulnerabilidade à adulteração, bem como dificuldades de padronização de procedimentos.

A adulteração pode ocorrer de múltiplas formas: pela alteração do conteúdo do arquivo, pela modificação de seus metadados (datas de criação, modificação, autor), ou pela inserção de dados falsos com aparência de autênticos. Em muitos casos, a adulteração é tecnicamente sofisticada e só identificável por peritos com alto nível de especialização.

Do ponto de vista normativo, a padronização de procedimentos ainda é incipiente. A Lei nº 13.964/2019 estabeleceu as etapas genéricas, mas não detalhou como cada etapa deve ser cumprida diante da prova digital. Essa lacuna regulatória tem alimentado insegurança jurídica e decisões divergentes nos tribunais.

VIOLAÇÃO À AMPLA DEFESA E AO CONTRADITÓRIO

Outro aspecto relevante é a possível violação ao princípio da ampla defesa (art. 5º, LV, da Constituição Federal), diante da desigualdade de acesso a meios técnicos para análise da prova.

Enquanto o órgão acusador dispõe de estrutura estatal, com peritos, laboratórios e ferramentas forenses, a defesa técnica muitas vezes não possui os mesmos recursos. Para impugnar uma prova digital, o advogado precisaria contratar perito particular especializado, o que tem custo elevado e nem sempre é viável.

Essa disparidade técnica coloca em risco o princípio da paridade de armas, especialmente relevante no processo penal. O Supremo Tribunal Federal já decidiu, em casos análogos, que a defesa deve ter acesso a todos os elementos probatórios em condições de efetivo contraditório. Na prova digital, esse acesso depende de meios que nem sempre estão ao alcance do defensor dativo ou da defensoria pública.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

DIFICULDADES DE RASTREABILIDADE

Também se destaca a dificuldade de rastreabilidade em ambientes complexos, como aqueles envolvendo criptoativos e múltiplas jurisdições.

A prova digital associada a criptoativos (bitcoin, ethereum e outros) envolve transações registradas em blockchain. Embora o blockchain seja tecnicamente imutável, a rastreabilidade da prova esbarra em desafios como: identificação dos titulares de carteiras (pseudonimidade), cruzamento de jurisdições (servidores no exterior) e necessidade de cooperação jurídica internacional.

Em investigações que envolvem múltiplos países, a cadeia de custódia se fragmenta. O dado coletado por autoridade estrangeira, repassado ao Brasil por rogatória, nem sempre vem acompanhado da documentação completa da cadeia de custódia. Essa ausência gera dúvidas permanentes sobre a integridade da prova digital.

LACUNAS NORMATIVAS E OPERACIONAIS

A hipótese proposta na introdução restou confirmada ao longo da pesquisa: persistem lacunas práticas relevantes na aplicação da cadeia de custódia à prova digital.

Entre as lacunas normativas, destaca-se a ausência de previsão explícita sobre o momento a partir do qual a cadeia de custódia da prova digital tem início. Se for no reconhecimento do vestígio (art. 158-B, I), há dúvida sobre se o simples avistamento de um dispositivo já exige documentação. Se for na coleta (art. 158-B, IV), há risco de o período entre reconhecimento e coleta ficar desprotegido.

Outra lacuna relevante diz respeito ao prazo de armazenamento da prova digital (art. 158-B, IX). A lei não define por quanto tempo a prova digital deve ser preservada após o fim do processo, criando incerteza sobre descarte e eliminação.

No plano operacional, a falta de capacitação continuada dos agentes envolvidos é um dos principais gargalos. Delegados, peritos, policiais, promotores e juízes nem sempre recebem treinamento específico sobre cadeia de custódia de prova digital. O resultado é a aplicação inconsistente das normas legais.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

ANÁLISE DE JURISPRUDÊNCIA SELECIONADA

POSIÇÃO DO SUPERIOR TRIBUNAL DE JUSTIÇA

O Superior Tribunal de Justiça tem decidido, em reiterados julgados, que a violação à cadeia de custódia da prova digital pode ensejar sua nulidade. Em decisão recente, a 5ª Turma entendeu que a ausência de hash nos arquivos extraídos de dispositivo celular compromete a autenticidade e inviabiliza a condenação com base exclusiva nessa prova.

Em outro precedente, o STJ relativizou a exigência da cadeia de custódia quando a prova digital é corroborada por outros elementos independentes. Segundo esse entendimento, a violação da cadeia de custódia não gera nulidade automática; é preciso demonstrar efetivo prejuízo.

POSIÇÃO DO SUPREMO TRIBUNAL FEDERAL

O Supremo Tribunal Federal, embora tenha poucos julgados especificamente sobre cadeia de custódia de prova digital, já firmou entendimento de que o contraditório deve ser real e efetivo.

Em repercussão geral, assentou-se que a defesa tem direito de acesso a todo o conteúdo da prova digital, inclusive a cópias forenses, para exercer a ampla defesa.

Em casos envolvendo prova digital proveniente de cooperação internacional, o STF tem exigido a apresentação da documentação completa da cadeia de custódia no país de origem, sob pena de ilicitude da prova no Brasil.

DIVERGÊNCIAS ENTRE TRIBUNAIS

A análise da jurisprudência revela divergência relevante entre tribunais estaduais e regionais federais. Em alguns estados, a simples apreensão do celular sem o devido isolamento de sinal e sem geração de hash tem sido considerada causa de nulidade absoluta da prova digital. Em outros, o mesmo tipo de irregularidade é tratado como nulidade relativa ou mera irregularidade.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

Essa divergência evidencia o quanto a falta de padronização, já mencionada na introdução e no resumo - compromete a segurança jurídica. Os operadores do Direito não têm como prever, com razoável certeza, se determinada prova digital será admitida ou não pelo juízo.

PROPOSTAS PARA A EFETIVIDADE DA PROVA DIGITAL

CONSOLIDAÇÃO DE PROTOCOLOS TÉCNICOS

A efetividade da prova digital depende da consolidação de protocolos técnicos, da capacitação dos agentes envolvidos e da observância rigorosa das garantias processuais.

Os protocolos técnicos devem ser elaborados por instituições como a Rede Nacional de Ensino e Pesquisa (RNP), o Instituto Nacional de Criminalística e o Conselho Nacional do Ministério Público. Tais protocolos devem detalhar, passo a passo, como realizar cada etapa do art. 158-B especificamente para prova digital.

A padronização nacional é urgente. Enquanto cada unidade da federação adotar procedimentos próprios, subsistirá as dificuldades de padronização de procedimentos apontadas ao longo deste estudo.

CAPACITAÇÃO PERMANENTE

A capacitação dos agentes envolvidos não pode ser episódica. É necessário investimento sistemático em cursos, laboratórios de prática forense e atualização tecnológica. A prova digital evolui rapidamente; o que é técnica forense atual hoje pode se tornar obsoleto em poucos meses.

A capacitação deve alcançar não apenas peritos, mas também magistrados e membros do Ministério Público. Sem conhecimento mínimo sobre hashing, espelhamento forense e cadeia de custódia digital, a valoração da prova digital será sempre fragilizada.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

GARANTIA DO CONTRADITÓRIO EFETIVO

Para assegurar o princípio da ampla defesa em relação à prova digital, propõe-se que o juízo, sempre que possível, determine a produção de cópia forense dos dispositivos apreendidos e a disponibilize à defesa em meio adequado.

A deferia entre meios técnicos disponíveis para acusação e defesa deve ser mitigada. Uma alternativa é a criação de núcleos de assistência técnica pericial nas Defensorias Públicas, com profissionais capacitados em informática forense.

ATUALIZAÇÃO LEGISLATIVA

Por fim, recomenda-se a edição de norma complementar à Lei nº 13.964/2019, regulamentando especificamente a cadeia de custódia da prova digital. Essa norma deverá definir: o momento de início da cadeia de custódia, os critérios técnicos mínimos para cada etapa, os prazos de armazenamento e os padrões de documentação.

Enquanto não houver essa regulamentação, as lacunas práticas e normativas apontadas ao longo deste estudo continuarão a comprometer a confiabilidade da prova digital.

CONSIDERAÇÕES FINAIS

Conclui-se que, embora a prova digital represente avanço significativo na persecução penal, sua utilização ainda enfrenta limitações estruturais e operacionais.

A hipótese proposta restou confirmada, evidenciando lacunas práticas na aplicação da cadeia de custódia.

A efetividade da prova digital depende da consolidação de protocolos técnicos, da capacitação dos agentes envolvidos e da observância rigorosa das garantias processuais. Sem esses três pilares, a prova digital permanecerá como elemento de confiabilidade instável no processo penal brasileiro.

A pesquisa teve como limitação a ausência de análise empírica quantitativa sobre o tratamento da cadeia de custódia nas decisões judiciais. Sugere-se, para estudos futuros,

a realização de levantamento de jurisprudência com amostra representativa, bem como a análise comparada com sistemas estrangeiros que já regulamentaram com maior detalhamento a prova digital.

REFERÊNCIAS

ALMEIDA, Marcelo Pereira de; FERREIRA, Diogo de Castro. O blockchain como meio de prova no direito processual civil brasileiro. **Revista Juris Poiesis**, Rio de Janeiro, v. 23, n. 29, p. 112-135, 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República, 1988.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Brasília, DF: Presidente da República, 1941.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Pacote Anticrime. Brasília, DF: Presidente da República, 2019.

CARNELUTTI, Francesco. **A prova civil**. Tradução de Ricardo Rodrigues Gama. Campinas: Bookseller, 2012.

DIDIER JR., Fredie; OLIVEIRA, Rafael Alexandria de. Blockchain e prova digital. **Revista ANNEP**, Salvador, v. 2, n. 3, p. 45-67, 2020.

GIUSTI, Caroline Favaron. **Registros de blockchain como prova eletrônica**. São Paulo: FGV Direito SP, 2022.

LOPES JR., Aury. **Direito processual penal**. 20. ed. São Paulo: Saraiva, 2023.

TARUFFO, Michele. **A prova**. Tradução de João Gabriel Couto. São Paulo: Marcial Pons, 2014.

Submissão: novembro de 2025. Aceite: dezembro de 2025. Publicação: abril de 2026.