PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

MONOGRAFIA JURÍDICA

O DESAFIO DO USO DAS PROVAS DIGITAIS NO PROCESSO PENAL:

A NECESSIDADE DE INVESTIGAÇÃO E A PROTEÇÃO DA PRIVACIDADE

ORIENTANDA: RAFAELA DE SOUSA SILVA

ORIENTADOR: PROF. ME. ERNESTO MARTIM S. DUNCK

GOIÂNIA

2026

RAFAELA DE SOUSA SILVA

O DESAFIO DO USO DAS PROVAS DIGITAIS NO PROCESSO PENAL:

A NECESSIDADE DE INVESTIGAÇÃO E A PROTEÇÃO DA PRIVACIDADE

Monografia Jurídica apresentada à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).

Prof. Orientador: Ernesto Martim S. Dunck

GOIÂNIA

2026

RAFAELA DE SOUSA SILVA

O DESAFIO DO USO DAS PROVAS DIGITAIS NO PROCESSO PENAL:

A NECESSIDADE DE INVESTIGAÇÃO E A PROTEÇÃO DA PRIVACIDADE

Data da Defesa: _____ de _____ de 2026

BANCA EXAMINADORA

_____ _____

Orientador: Prof. Me. Ernesto Martim S. Dunck Nota

_____ _____

Prof. Me. Eurípedes Clementino Ribeiro Junior Nota

Primeiramente, agradeço a Deus, pela força, sabedoria e perseverança que me permitiram chegar até aqui.

À minha família, por todo amor, apoio e incentivo ao longo dessa caminhada, sendo essencial em cada etapa da minha formação.

À minha amiga Viviane, pelo apoio, incentivo e companheirismo ao longo dessa trajetória, especialmente nos momentos mais desafiadores.

A todas as pessoas que estiveram ao meu lado durante essa caminhada, oferecendo apoio, incentivo e compreensão nos momentos mais difíceis.

Ao meu orientador, Prof. Me. Ernesto Martim S. Dunck, pela disponibilidade, orientação segura e valiosas contribuições ao desenvolvimento deste trabalho.

Aos professores do curso de Direito da Pontifícia Universidade Católica de Goiás, pela excelência na formação acadêmica e pelo compromisso com a qualidade do ensino jurídico.

Dedico este trabalho à memória do meu avô, Luiz Francisco Alves de Miranda, que sempre acreditou em mim, se orgulhou de cada passo da minha trajetória e nunca deixou de me incentivar, mesmo nos momentos mais difíceis.

Grande parte da pessoa que me tornei carrega os ensinamentos, o carinho e o amor que recebi dele ao longo da vida. Tenho a certeza de que ele estaria profundamente feliz e emocionado com esta conquista, celebrando este momento com o mesmo orgulho que sempre demonstrou por mim.

Embora sua ausência seja sentida diariamente, sua presença permanece viva em minha história, em minhas lembranças e em tudo aquilo que construo.

“Punir é necessário, punir é civilizatório, mas é preciso respeitar a regra do jogo.”

Aury Lopes Jr.

RESUMO

O presente trabalho analisa o uso das provas digitais no processo penal brasileiro, destacando seus desafios jurídicos, especialmente quanto à validade da cadeia de custódia e à proteção dos direitos fundamentais. A crescente digitalização das relações sociais ampliou o uso de dados eletrônicos como meio de prova, exigindo adaptação do sistema jurídico diante da volatilidade, fragilidade e facilidade de manipulação dessas evidências. Nesse contexto, examina-se a necessidade de observância de critérios rigorosos na coleta, preservação e valoração das provas digitais, a fim de garantir sua integridade e autenticidade. O estudo também aborda a tensão entre a eficiência da investigação criminal e a proteção da privacidade, considerando os limites constitucionais, o Marco Civil da Internet e a Lei Geral de Proteção de Dados. Por fim, analisa-se a importância do controle judicial e da cadeia de custódia como mecanismos essenciais para assegurar a legitimidade da prova digital e evitar violações de direitos fundamentais no processo penal contemporâneo.

Palavras-chave: provas digitais, processo penal, cadeia de custódia, privacidade, direitos fundamentais.

ABSTRACT

This study analyzes the use of digital evidence in the Brazilian criminal procedure, emphasizing its legal challenges, particularly regarding the validity of the chain of custody and the protection of fundamental rights. The increasing digitalization of social relations has expanded the use of electronic data as evidence, requiring the legal system to adapt to the volatility, fragility, and susceptibility to manipulation of such information. In this context, the research examines the need for strict criteria in the collection, preservation, and evaluation of digital evidence to ensure its integrity and authenticity. It also addresses the tension between effective criminal investigation and the protection of privacy, considering constitutional limits, the Internet Civil Framework, and data protection legislation. Finally, the study highlights the importance of judicial control and the chain of custody as essential mechanisms to ensure the legitimacy of digital evidence and to prevent violations of fundamental rights in contemporary criminal proceedings.

Keywords: digital evidence, criminal procedure, chain of custody, privacy, fundamental rights.

SUMÁRIO

INTRODUÇÃO

O avanço tecnológico e a crescente digitalização das relações sociais transformaram profundamente o modo como os fatos são produzidos, registrados e investigados no âmbito do processo penal. Nesse cenário, as provas digitais passaram a ocupar posição central na persecução penal, constituindo instrumentos relevantes para a elucidação de infrações, especialmente aquelas praticadas em ambientes virtuais.

Entretanto, a utilização dessas evidências impõe desafios jurídicos significativos, sobretudo em razão de suas características próprias, como volatilidade, fragilidade e elevada suscetibilidade à manipulação. Tais particularidades exigem não apenas adaptações técnicas, mas também uma releitura dos institutos processuais clássicos, especialmente no que se refere à validade jurídica do elemento probatório e à preservação de sua integridade.

Diante desse contexto, a cadeia de custódia digital destaca-se como requisito essencial para a admissibilidade e confiabilidade das provas no processo penal. Regulamentada pelos artigos 158-A a 158-F do Código de Processo Penal, ela estabelece um conjunto de procedimentos destinados a garantir a rastreabilidade dos vestígios digitais desde sua coleta até sua apresentação em juízo.

Contudo, sua aplicação prática ainda revela fragilidades relevantes, sobretudo em razão da ausência de padronização técnica e da complexidade inerente ao tratamento de dados digitais.

Paralelamente, a ampliação das ferramentas investigativas no ambiente digital intensifica a tensão entre a necessidade de eficiência na persecução penal e a proteção dos direitos fundamentais, especialmente a privacidade e a intimidade. O acesso a dados armazenados em dispositivos eletrônicos, registros de conexão e comunicações digitais representa significativa intervenção na esfera privada do indivíduo, exigindo rigoroso controle de legalidade e proporcionalidade.

Nesse sentido, o problema de pesquisa que orienta este trabalho consiste em verificar em que medida o processo penal brasileiro é capaz de assegurar a utilização das provas digitais sem comprometer a proteção dos direitos fundamentais, especialmente a privacidade, à luz dos mecanismos de controle da validade probatória.

Parte-se da hipótese de que, embora o ordenamento jurídico brasileiro tenha avançado na regulamentação das provas digitais, ainda persistem lacunas normativas e operacionais que comprometem a efetiva garantia da integridade probatória e da proteção da privacidade, sobretudo diante da ausência de protocolos técnicos uniformes e da dificuldade de controle sobre a manipulação de dados digitais.

Assim, o objetivo geral da pesquisa é analisar os desafios jurídicos relacionados à utilização das provas digitais no processo penal brasileiro, com foco na cadeia de custódia e na proteção dos direitos fundamentais. Como objetivos específicos, busca-se: compreender as características e especificidades das provas digitais; examinar os limites constitucionais à atuação estatal no acesso a dados digitais; e avaliar a eficácia da cadeia de custódia como mecanismo de garantia da legitimidade probatória.

Para tanto, adota-se abordagem qualitativa, com utilização do método dedutivo, a partir de pesquisa bibliográfica e documental, incluindo análise doutrinária, legislativa e jurisprudencial.

A estrutura do trabalho organiza-se em três seções: a primeira aborda a transformação do processo penal diante das provas digitais; a segunda analisa os direitos fundamentais e os limites à atuação estatal; e a terceira examina a cadeia de custódia digital e os desafios relacionados à sua efetividade, propondo uma reflexão crítica acerca da necessidade de aprimoramento do sistema jurídico.

Nesse contexto, a análise da cadeia de custódia digital não se apresenta como um fim em si mesma, mas como instrumento técnico-jurídico por meio do qual se busca compreender em que medida a validade da prova pode coexistir com a preservação dos direitos fundamentais, especialmente a privacidade.

I. PROVAS DIGITAIS E A TRANSFORMAÇÃO DO PROCESSO PENAL

A sociedade contemporânea, profundamente marcada pela digitalização das interações humanas, impôs uma redefinição significativa no panorama do processo penal. A vida cotidiana, mediada por dispositivos eletrônicos e redes de comunicação, gera uma vasta e contínua produção de registros informacionais, que se tornam vestígios relevantes para a elucidação de ilícitos.

Nesse cenário, o sistema de justiça criminal depara-se com a crescente centralidade das provas digitais, evidências que não encontram correspondência direta com o paradigma clássico da prova, historicamente fundado em vestígios físicos e na materialidade tangível. Essa transformação impõe uma verdadeira transformação estrutural do direito processual penal.

A prova digital desafia a lógica tradicional construída a partir da prova testemunhal e pericial física. Sua natureza intangível, volátil, mutável e ubíqua exige do Estado não apenas adaptação tecnológica, mas, sobretudo, uma reestruturação normativa e interpretativa dos institutos processuais. Nesse contexto, evidencia-se o dilema central da modernidade: ampliar a eficácia investigativa sem comprometer a proteção dos direitos fundamentais.

1.1. A EVOLUÇÃO DO CONCEITO DE PROVA E O DESAFIO DA DESMATERIALIZAÇÃO

A transição da prova física para a prova digital representa uma mudança estrutural no processo penal. Diferentemente dos vestígios materiais, os dados digitais são intrinsecamente voláteis e suscetíveis a alterações ou exclusões, o que impõe a adoção de mecanismos rigorosos de preservação, como a cadeia de custódia, a fim de garantir sua integridade e confiabilidade.

Nesse contexto, a Lei nº 13.964/2019 introduziu, no Código de Processo Penal, a disciplina da cadeia de custódia, estabelecendo, em seu art. 158-A, que:

> Considera-se cadeia de custódia 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. BRASIL (2019).

A partir dessa definição legal, verifica-se que a cadeia de custódia assume papel central na garantia da autenticidade e integridade da prova, funcionando como mecanismo de controle da atividade estatal. No entanto, sua aplicação no âmbito das provas digitais apresenta desafios adicionais, em razão das particularidades técnicas envolvidas.

Nesse sentido, Souza, Munhoz e Carvalho (2025, p. 220) afirmam que:

> O ambiente digital exige procedimentos específicos de preservação da prova, sob pena de comprometimento de sua validade, especialmente diante da facilidade de manipulação dos dados eletrônicos.

A observação dos autores evidencia que a simples previsão normativa é estruturalmente insuficiente para assegurar a confiabilidade da prova digital, sendo indispensável a adoção de protocolos técnicos adequados. Assim, a cadeia de custódia, no contexto digital, deve ser compreendida não apenas como exigência formal, mas como condição material de validade da prova.

A adaptação do sistema probatório, portanto, não se limita ao plano tecnológico, mas assume natureza eminentemente jurídica. Nesse cenário, o Marco Civil da Internet (Lei nº 12.965/2014) estabelece limites relevantes à atuação estatal, especialmente no que se refere ao acesso a dados digitais.

De acordo com Souza, Munhoz e Carvalho (2025, p. 220):

> Esta Lei é considerada uma espécie de ‘Constituição da Internet no Brasil’, regulamentando, entre outras, questões como liberdade de expressão, privacidade e responsabilidade civil.

Tal compreensão reforça a importância do Marco Civil como instrumento normativo de proteção de direitos fundamentais no ambiente digital, impondo limites à atuação investigativa do Estado.

Em complemento, o art. 22 do referido diploma legal dispõe que:

> A parte interessada poderá requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

A exigência de ordem judicial evidencia a incidência da cláusula de reserva de jurisdição, demonstrando que o acesso a dados digitais não pode ocorrer de forma arbitrária, devendo estar submetido a controle judicial rigoroso.

Nesse contexto, o dispositivo eletrônico, especialmente o smartphone, consolida-se como verdadeiro repositório da vida privada do indivíduo. Conforme leciona Lopes Jr. (2024), trata-se de uma verdadeira “extensão da vida privada”, em razão da quantidade e da sensibilidade das informações armazenadas.

Essa perspectiva evidencia que o acesso a dados digitais representa intervenção profunda na esfera íntima do indivíduo, exigindo fundamentação adequada e respeito aos limites constitucionais.

A jurisprudência do Supremo Tribunal Federal reforça essa compreensão. No julgamento do Recurso Extraordinário nº 926.883/MG, a Corte fixou o entendimento de que: “é ilícita a prova obtida mediante acesso, sem autorização judicial, a registros e conversas armazenados em aparelho celular apreendido.” STF (2024).

Diante disso, verifica-se que a evolução do conceito de prova no processo penal não se limita à incorporação de novas tecnologias, mas implica a necessidade de reestruturação dos mecanismos de controle e validação probatória. A prova digital, ao mesmo tempo em que amplia a capacidade investigativa do Estado, impõe a observância rigorosa de garantias fundamentais, sob pena de comprometimento da legitimidade da atividade jurisdicional.

1.2. CARACTERÍSTICAS E ESPECIFICIDADES DA PROVA DIGITAL

A compreensão das especificidades da prova digital constitui pressuposto essencial para seu adequado tratamento jurídico no processo penal. Trata-se de modalidade probatória que exige não apenas conhecimento técnico, mas também uma interpretação jurídica sensível às suas particularidades, especialmente diante de sua distinção em relação às provas tradicionais.

Nesse sentido, Linares Filho (2025, p. 22) define a prova digital como:

> A prova eletrônica pode ser compreendida como todo elemento de natureza probatória cuja origem, forma de representação ou método de obtenção esteja ancorado em sistemas computacionais, dispositivos digitais ou meios de comunicação eletrônica. Trata-se de um conceito técnico-jurídico que abrange uma gama extensa de evidências digitais, como arquivos de texto, planilhas, imagens, vídeos, áudios, e-mails, registros de navegação, dados armazenados em servidores remotos, metadados e mensagens trocadas por aplicativos de comunicação instantânea, como WhatsApp, Telegram, Signal e similares. A particularidade essencial da prova eletrônica reside em sua materialização digital, o que a diferencia das provas tradicionais por exigir, para sua adequada captação, preservação, análise e apresentação em juízo, o emprego de procedimentos técnicos rigorosos e conhecimentos especializados.

A definição apresentada evidencia que a prova digital não se limita a um suporte físico específico, abrangendo um amplo conjunto de dados produzidos em ambiente eletrônico. Essa característica amplia significativamente o espectro probatório, ao mesmo tempo em que impõe desafios relevantes quanto à sua preservação e valoração no processo penal.

Dentre suas principais características, destacam-se a volatilidade e a fragilidade. Conforme ensina Kist (2024, p. 57):

> A prova digital não necessita, para existir, de um suporte físico; esse é necessário apenas para que possa ser percebida e vista e, portanto, recolhida e utilizada posteriormente, na fase da valoração. E essa ausência de fixação material em um suporte físico torna a prova digital deveras frágil e volátil.

A partir dessa observação, observa-se que a ausência de materialidade física estável torna a prova digital altamente suscetível a alterações, exclusões e manipulações, muitas vezes imperceptíveis. Tal vulnerabilidade compromete diretamente sua confiabilidade, exigindo rigor técnico em todas as etapas de sua produção.

Em continuidade, o referido autor afirma que:

> Frágil na medida em que, se for manipulada de forma descuidada, poderá perder suas propriedades ou mesmo desaparecer. Essa manipulação pode ser feita pelo próprio usuário do sistema informático, acessando os dados ou editando-os e depois gravando o arquivo, ou então de forma automática pelo próprio sistema operacional. E, nos casos em que a prova é acessível de forma remota, um terceiro interessado na sua alteração ou eliminação poderá fazê-lo à distância.

Essa constatação demonstra que os riscos associados à prova digital não decorrem apenas da intervenção humana intencional, mas também de fatores

automáticos ou externos, o que amplia significativamente a complexidade de sua preservação.

Prosseguindo na mesma linha argumentativa, o referido autor sustenta que:

> Ela também é volátil, porque pode desaparecer como efeito de determinados eventos, provocados pelo usuário, intencionalmente ou não, ou outra causa, como a falta de bateria para alimentar o equipamento que contém o sistema informático e o desligamento desse, a gravação, automática ou não, de informação nova 'por cima' da anterior, ou então tratar-se de informação que, por natureza, é temporária e que, ao cabo de determinado período ou verificado certo evento, ela se apaga.

Dessa forma, a volatilidade revela-se como elemento estrutural da prova digital, exigindo atuação imediata e tecnicamente adequada para evitar a perda do vestígio.

Outro aspecto relevante refere-se à natureza sensível dos dados digitais. Kist (2024, p. 186) esclarece que "Vestígio é uma categoria conceitual específica, que não pode ser confundida com outras como as de evidência, indício e prova."

A partir dessa distinção, compreende-se que os dados digitais, enquanto vestígios, podem conter informações extremamente sensíveis, relacionadas à intimidade e à vida privada do indivíduo, o que reforça a necessidade de proteção jurídica reforçada.

Nesse contexto, a Lei Geral de Proteção de Dados estabelece, em seu art. 5º, II, que dado pessoal sensível é:

> Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. BRASIL (2018).

A incorporação dessa definição evidencia que os dados digitais não são meros elementos técnicos, mas manifestações diretas da esfera íntima do indivíduo, o que intensifica o potencial de violação de direitos fundamentais.

Outro elemento central na análise das provas digitais refere-se aos metadados. Nesse sentido, o Marco Civil da Internet dispõe que "O provedor responsável pela guarda somente será obrigado a disponibilizar os registros de conexão e de acesso a aplicações de internet mediante ordem judicial, na forma do disposto nesta Lei." BRASIL (2014).

A exigência de autorização judicial demonstra que, mesmo quando não há acesso direto ao conteúdo das comunicações, os metadados possuem elevado potencial invasivo, permitindo a reconstrução detalhada das atividades do indivíduo.

Diante dessas características, verifica-se que a prova digital não apenas amplia as possibilidades investigativas do Estado, mas também intensifica os riscos de violação de direitos fundamentais. Assim, sua utilização no processo penal exige não apenas adequação técnica, mas também rigor jurídico, especialmente no que se refere à observância da cadeia de custódia e aos limites constitucionais da atuação estatal.

1.3. A EXPANSÃO DA INVESTIGAÇÃO CRIMINAL NO AMBIENTE DIGITAL

A expansão das tecnologias digitais transformou significativamente a dinâmica da investigação criminal, ampliando o acesso a fontes de informação e potencializando a capacidade de reconstrução dos fatos. Nesse cenário, a utilização de dados digitais passou a ocupar posição central na atividade probatória, especialmente em razão da crescente digitalização das relações sociais.

No que se refere às comunicações digitais realizadas em tempo real, sua interceptação submete-se ao regime jurídico da Lei nº 9.296/1996. O artigo 2º do referido diploma estabelece que:

> Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses: I – não houver indícios razoáveis da autoria ou participação em infração penal; II – a prova puder ser feita por outros meios disponíveis; III – o fato investigado constituir infração penal punida, no máximo, com pena de detenção. Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada. BRASIL (1996).

A leitura do dispositivo evidencia que a interceptação constitui medida excepcional, condicionada ao preenchimento de requisitos rigorosos. Assim, sua aplicação ao ambiente digital exige interpretação ampliativa, de modo a abranger também as comunicações telemáticas, sob pena de esvaziamento da proteção constitucional ao sigilo das comunicações.

À luz das transformações impostas pela digitalização das relações sociais, Souza, Munhoz e Carvalho (2025, p. 113) asseveram que:

> Os juízes não mais estão se atendo às leis, pura e simplesmente, mas também às evidências do mundo moderno, como aquelas oferecidas pelas redes sociais. À medida que plataformas como Facebook, Instagram, Twitter e LinkedIn fazem cada vez mais parte do dia a dia das pessoas, nelas somos capazes de encontrar informações relevantes para comprovar ofensas, negócios, comentários e assim sucessivamente.

A partir dessa observação, verifica-se que as redes sociais passaram a desempenhar papel relevante na produção probatória, permitindo a identificação de comportamentos, intenções e contextos que auxiliam na reconstrução dos fatos.

Ainda no âmbito da doutrina especializada, os autores sustentam que Souza, Munhoz e Carvalho (2025, p. 113):

> O emprego de informações de redes sociais como provas em processos judiciais tem se tornado cada vez mais comum em decorrência de sua ampla disponibilidade e da crescente utilização das redes sociais em todo o mundo. As publicações, comentários e conversas em plataformas podem fornecer evidências valiosas para investigações criminais, especialmente em casos de crimes contra a honra praticados no ambiente digital.

Tal constatação evidencia que a prova digital, especialmente aquela oriunda de redes sociais, possui elevado valor probatório, mas sua utilização deve ser analisada com cautela, especialmente quanto à licitude de sua obtenção.

Nesse sentido, os mesmos autores afirmam que:

> As informações coletadas nas redes sociais podem ser apresentadas como prova em processos judiciais para revelar a intenção da parte autora, o contexto do diálogo, o histórico de comportamento da parte ré e assim por diante.

Dessa forma, embora tais elementos possam contribuir significativamente para a elucidação dos fatos, sua utilização não dispensa o controle judicial, sobretudo quando houver potencial violação de direitos fundamentais.

No plano jurídico, a limitação ao uso dessas provas encontra fundamento na vedação às provas ilícitas. O Código de Processo Penal, em seu art. 157 estabelece que:

> São também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras. BRASIL (1941)

A partir desse dispositivo, constata-se a adoção, no ordenamento jurídico brasileiro, da teoria dos frutos da árvore envenenada, segundo a qual a ilicitude da prova originária contamina as provas dela derivadas.

No contexto digital, essa teoria assume especial complexidade, tendo em vista a interdependência e o encadeamento das informações eletrônicas. A identificação do nexo causal entre a prova ilícita e as provas derivadas exige análise criteriosa, especialmente diante da facilidade de replicação e compartilhamento dos dados digitais.

Diante desse cenário, demonstra-se, portanto, que a expansão da investigação no ambiente digital, embora amplie significativamente a eficiência da persecução penal, também intensifica os desafios relacionados à proteção dos direitos fundamentais. Assim, impõe-se a necessidade de atuação estatal pautada por critérios rigorosos de legalidade, proporcionalidade e controle judicial, a fim de garantir a legitimidade da atividade probatória no processo penal contemporâneo.

II. PRIVACIDADE, DIREITOS FUNDAMENTAIS E LIMITES AO USO DAS PROVAS DIGITAIS

A utilização das provas digitais no processo penal impõe a necessidade de análise dos limites constitucionais à atuação estatal, especialmente no que se refere à proteção da privacidade e aos direitos fundamentais. Em uma sociedade marcada pela digitalização das relações sociais, a atuação investigativa passa a incidir diretamente sobre dados sensíveis, o que exige rigoroso controle jurídico.

Nesse contexto, torna-se imprescindível examinar de que forma o ordenamento jurídico brasileiro estabelece mecanismos capazes de equilibrar a eficiência da persecução penal com a preservação da esfera íntima do indivíduo, evitando intervenções estatais desproporcionais.

2.1. A PROTEÇÃO CONSTITUCIONAL DA PRIVACIDADE E DA INTIMIDADE

A Constituição Federal de 1988 consagra a privacidade e a intimidade como direitos fundamentais estruturantes do Estado Democrático de Direito, funcionando como limites materiais à atuação estatal. Nesse sentido, tais garantias não apenas protegem a esfera individual, mas também condicionam a legitimidade da atividade investigativa no âmbito do processo penal.

O artigo 5º, inciso X, da Constituição Federal dispõe que:

> São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação. BRASIL (1988).

A norma evidencia que a proteção da esfera privada constitui dimensão essencial da dignidade da pessoa humana, impedindo que o Estado interfira arbitrariamente na vida do indivíduo.

Em complemento, o artigo 5º, inciso XII, estabelece que:

> É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. BRASIL (1988).

A leitura sistemática desses dispositivos demonstra que o acesso estatal a dados e comunicações privadas possui natureza excepcional, estando condicionado ao cumprimento de requisitos estritos de legalidade, necessidade e proporcionalidade.

No plano doutrinário, José Afonso da Silva (2016, p. 209) esclarece que: “a intimidade se insere como esfera secreta da vida do indivíduo na qual este tem o poder legal de evitar os demais.”

A partir dessa conceituação, verifica-se que a intimidade constitui núcleo mais restrito da vida privada, estando diretamente relacionada à proteção da dignidade humana. Assim, qualquer intervenção estatal nessa esfera exige fundamentação adequada e respeito aos limites constitucionais.

Ainda no âmbito da doutrina constitucional, Mendes e Branco (2021, p. 1220) destacam que:

> No que se refere aos dados informáticos, a questão não se limita mais à mera proteção de dados armazenados em computadores pessoais ou em provedores de internet. Com o surgimento de tecnologias como *cloud computing* (computação nas nuvens), tornou-se possível o armazenamento de qualquer informação não apenas em discos rígidos em poder do usuário ou de seu provedor, como também em ambientes virtuais acessíveis pela internet de qualquer parte do mundo.

Tal constatação evidencia que a proteção da privacidade, no contexto digital, assume dimensão ampliada, exigindo do Estado uma atuação ainda mais cautelosa.

No plano normativo, a Emenda Constitucional nº 115/2022 incluiu o direito à proteção de dados pessoais no rol de direitos fundamentais, ao estabelecer que: “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.” BRASIL (1988).

Dessa forma, verifica-se que a proteção de dados pessoais passou a integrar o núcleo essencial dos direitos fundamentais, reforçando a necessidade de controle rigoroso da atuação estatal.

2.2. A TENSÃO ENTRE INVESTIGAÇÃO CRIMINAL E GARANTIAS FUNDAMENTAIS

A tensão entre a necessidade de uma persecução penal eficiente e a preservação das garantias fundamentais constitui um dos principais eixos

estruturantes do processo penal contemporâneo, assumindo especial relevância no contexto das provas digitais. O avanço tecnológico ampliou significativamente as possibilidades investigativas do Estado, permitindo o acesso a dados que revelam, com elevado grau de precisão, comportamentos, comunicações e aspectos íntimos da vida do indivíduo.

Antes de avançar na análise dessa tensão, torna-se necessário delimitar o conceito de prova digital. Nesse sentido, Vaz (2012, p. 45) define que:

> Qualquer informação de valor probatório contida em meio eletrônico ou transmitida por esse meio, que possua aptidão para demonstrar fatos juridicamente relevantes em qualquer tipo de infração penal.

A definição apresentada evidencia que a prova digital possui ampla aplicabilidade no processo penal, sendo capaz de demonstrar fatos em diversas espécies de infração penal. Tal amplitude reforça sua relevância prática, mas também intensifica os riscos de intervenção indevida na esfera privada do indivíduo.

No plano constitucional, a persecução penal eficiente encontra fundamento na própria Constituição Federal. O artigo 129, inciso I, estabelece que: “são funções institucionais do Ministério Público promover, privativamente, a ação penal pública, na forma da lei.” BRASIL (1988).

De igual modo, o artigo 144 da Constituição dispõe que: “a segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio.” BRASIL (1988).

A partir da conjugação desses dispositivos, verifica-se que a atuação estatal na investigação criminal possui fundamento constitucional legítimo. Entretanto, essa atuação não se desenvolve de forma ilimitada, devendo observar os direitos fundamentais como parâmetros de validade.

No âmbito da doutrina processual penal, Lopes Jr. (2022, p. 541) sustenta que:

> Em determinados casos, especialmente crimes praticados mediante tecnologias digitais, a prova digital constitui o único meio disponível para demonstração da autoria e materialidade delitivas.

A afirmação evidencia a centralidade da prova digital no processo penal contemporâneo, sobretudo em crimes informáticos. Todavia, essa relevância não autoriza a mitigação das garantias constitucionais, sendo indispensável a observância dos limites jurídicos à atuação estatal.

Sob a ótica jurisprudencial, o Supremo Tribunal Federal tem reafirmado a necessidade de controle judicial das medidas investigativas. Nesse sentido, no julgamento do Recurso Extraordinário nº 1.055.941/SP, consignou-se que: “é possível o acesso a dados digitais para fins de investigação criminal, desde que haja prévia autorização judicial devidamente fundamentada.” STF (2019).

A orientação jurisprudencial demonstra que o ordenamento jurídico brasileiro busca estabelecer um ponto de equilíbrio entre eficiência investigativa e proteção de direitos fundamentais, condicionando a validade da prova digital ao respeito aos parâmetros constitucionais.

Dessa forma, verifica-se que a tensão entre investigação criminal e garantias fundamentais não se resolve pela prevalência absoluta de um sobre o outro, mas pela construção de um modelo de atuação estatal pautado pela legalidade, proporcionalidade e controle jurisdicional efetivo.

2.3. PROVAS ILÍCITAS, LIMITES ÉTICOS E CONTROLE JUDICIAL DA OBTENÇÃO DE DADOS

A vedação às provas ilícitas constitui uma das garantias fundamentais mais relevantes no processo penal brasileiro, funcionando como instrumento de limitação do poder punitivo estatal e de proteção da dignidade da pessoa humana. No contexto das provas digitais, essa vedação assume especial relevância, em razão do elevado potencial invasivo dos meios tecnológicos utilizados na obtenção de dados.

Nesse sentido, a Constituição Federal estabelece, em seu artigo 5º, inciso LVI, que: “são inadmissíveis, no processo, as provas obtidas por meios ilícitos.” BRASIL (1988).

A norma constitucional evidencia que a validade da prova não depende apenas de sua utilidade, mas também da licitude dos meios empregados para sua obtenção. Assim, a utilização de provas ilícitas compromete não apenas o elemento probatório, mas a própria legitimidade do processo penal.

A vedação das provas ilícitas constitui expressão do devido processo legal, funcionando como limite ao poder punitivo estatal e impedindo que meios ilegais sejam utilizados para alcançar resultados probatórios.

Essa compreensão revela que a ilicitude probatória não pode ser analisada de forma isolada, devendo ser compreendida como violação estrutural às garantias fundamentais do indivíduo.

Em complemento, o Código de Processo Penal dispõe que:

> São também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras. BRASIL (1941).

A partir desse dispositivo, verifica-se a adoção da teoria dos frutos da árvore envenenada, segundo a qual a ilicitude da prova originária contamina as provas dela derivadas.

No contexto digital, essa teoria assume contornos ainda mais complexos, tendo em vista a interdependência dos dados eletrônicos e a facilidade de replicação das informações. A identificação do nexo causal entre a prova ilícita e suas derivadas exige análise rigorosa, especialmente diante da possibilidade de múltiplas fontes de obtenção de dados.

Nesse cenário, Wanderley (2019, p. 128) destaca que: “o acesso aos dados armazenados em smartphones pode revelar aspectos íntimos da vida privada que jamais seriam acessíveis mediante busca tradicional.”

Sob essa ótica, os dispositivos eletrônicos revelam-se como verdadeiros repositórios da vida privada, concentrando informações sensíveis que, se acessadas de forma indevida, podem resultar em grave violação de direitos fundamentais.

Dessa forma, o controle judicial assume papel central na validação das provas digitais, funcionando como mecanismo indispensável para garantir a legalidade, a proporcionalidade e a legitimidade das medidas investigativas.

Assim, verifica-se que a utilização das provas digitais no processo penal exige não apenas o cumprimento de requisitos legais, mas também a observância de limites éticos e constitucionais, sob pena de comprometimento da validade da prova e da própria legitimidade da atuação estatal.

III. CADEIA DE CUSTÓDIA DIGITAL E O DILEMA ENTRE EFICIÊNCIA INVESTIGATIVA E PRIVACIDADE

No contexto das provas digitais, a preservação da integridade probatória assume papel decisivo para a validade do processo penal. Isso se deve à natureza peculiar dos dados eletrônicos, caracterizados pela volatilidade, facilidade de modificação e alta suscetibilidade a interferências externas, fatores que comprometem sua estabilidade como fonte de prova.

Mais do que um mecanismo de controle técnico, a cadeia de custódia digital deve ser compreendida como espaço de tensão entre a eficiência da persecução penal e a proteção dos direitos fundamentais, na medida em que sua observância condiciona não apenas a validade da prova, mas também os limites da atuação estatal sobre a esfera privada.

Diferentemente das provas tradicionais, os vestígios digitais não possuem materialidade estática, sendo dependentes de suportes tecnológicos e processos técnicos para sua extração, armazenamento e análise. Essa condição impõe a necessidade de mecanismos rigorosos de controle que assegurem a fidelidade entre o dado originalmente obtido e aquele apresentado em juízo.

Nesse sentido, Linares Filho (2025, p. 22) destaca que:

> A cadeia de custódia digital desempenha um papel central, pois estabelece um encadeamento documental que comprova cada etapa do manuseio do vestígio eletrônico, identificando os responsáveis pela coleta, armazenamento, transporte, perícia e guarda da evidência.

A observação evidencia que não se trata apenas de formalidade procedimental, mas de condição estruturante da aptidão probatória. A ausência desse controle compromete a possibilidade de verificação da autenticidade e da integridade do vestígio, fragilizando sua confiabilidade.

Sob essa perspectiva, a problemática central desloca-se da mera obtenção da prova para a sua validade jurídica. A questão não é apenas “o que foi coletado”, mas “em que condições foi produzido, preservado e apresentado”. Essa mudança de enfoque é particularmente relevante no ambiente digital, em que pequenas intervenções podem alterar substancialmente o conteúdo informacional.

A inobservância de protocolos técnicos adequados não apenas compromete o valor probatório do elemento obtido, mas pode ensejar sua exclusão do processo, sobretudo quando houver violação de garantias fundamentais. Assim, a confiabilidade da prova digital passa a depender diretamente da regularidade dos procedimentos adotados ao longo de todo o seu percurso.

Para além da dimensão técnica, a discussão insere-se em um dilema estrutural do processo penal contemporâneo: a necessidade de equilibrar a eficiência investigativa com a proteção dos direitos fundamentais. Trata-se de tensão inerente ao modelo acusatório, especialmente diante da expansão das capacidades tecnológicas de investigação.

De um lado, o fortalecimento dos instrumentos de investigação é indispensável para o enfrentamento da criminalidade contemporânea, cada vez mais sofisticada e digitalizada. De outro, a ampliação descontrolada desses mecanismos pode resultar em violações à privacidade, à intimidade e ao devido processo legal.

Nesse cenário, a solução não reside na prevalência absoluta de um desses polos, mas na construção de um modelo de atuação estatal pautado pela legalidade, proporcionalidade e controle jurisdicional efetivo. A preservação da confiabilidade da prova digital, nesse contexto, emerge como elemento de equilíbrio entre eficiência e garantia.

3.1. CADEIA DE CUSTÓDIA DIGITAL COMO REQUISITO DE VALIDADE DA PROVA

A introdução dos artigos 158-A a 158-F no Código de Processo Penal, pela Lei nº 13.964/2019, representou avanço significativo ao estabelecer parâmetros normativos para o controle dos vestígios. Contudo, sua aplicação no âmbito digital revela desafios que ultrapassam a literalidade da norma, exigindo adaptação às especificidades tecnológicas.

Nesse contexto, Kist (2024, p. 538) conceitua o instituto como:

> Conjunto de procedimentos adotados e documentados, desde a descoberta dos vestígios, para manter a sua integridade e permitir o posterior rastreio da posse e do seu manuseio.

A definição evidencia que a validade da prova não decorre apenas de sua existência, mas da possibilidade de reconstrução de sua trajetória. Em outras palavras, a admissibilidade do elemento probatório está diretamente condicionada à transparência dos procedimentos que viabilizaram sua produção.

Linares Filho (2025) sustenta que a preservação da prova digital exige não apenas mecanismos técnicos adequados, mas também rigoroso controle jurídico sobre a atuação estatal ao longo de toda a persecução penal.

A observação demonstra que a confiabilidade da prova digital depende da conjugação entre técnica e legalidade. A ausência de qualquer desses elementos compromete sua validade, ainda que o dado em si seja relevante para a investigação.

A previsão legal das etapas — reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte — não deve ser compreendida como mero roteiro operacional, mas como sequência lógica destinada a garantir a integridade do vestígio.

A fase de reconhecimento, por exemplo, assume relevância estratégica no ambiente digital, em que as fontes de prova nem sempre são evidentes. Nesse sentido, Kist (2024, p. 223) adverte que:

> Antes da remoção, contudo, é imprescindível que o investigador reconheça todas as fontes de evidências digitais na cena do crime ou no local de busca. Já a preservação do vestígio exige atuação imediata e tecnicamente adequada.

Conforme Souza, Munhoz e Carvalho (2025, p. 58), “sempre é preciso que se inicie maneira rápida, evitando a perda de informações, especialmente se o objeto de coleta estiver sujeito à degradação ou remoção”. Essas etapas evidenciam que a regularidade procedimental não constitui formalidade dispensável, mas requisito material de confiabilidade probatória.

Além disso, a rastreabilidade emerge como elemento central desse controle, permitindo a verificação posterior da integridade e autenticidade dos dados. Contudo, a doutrina aponta limites a essa garantia. Nesse sentido, Linares Filho (2025, p. 34) adverte que:

> A rastreabilidade dos vestígios, que hoje se ancora na cadeia de custódia digital, poderá tornar-se insuficiente diante de estruturas computacionais que burlam os próprios fundamentos de certificação.

Nesse contexto, evidencia-se que a conformidade procedimental, no ambiente digital, não constitui garantia absoluta de confiabilidade, mas apenas condição mínima de validade probatória, revelando a insuficiência do modelo normativo diante das especificidades tecnológicas.

3.2. FRAGILIDADES, RISCOS E DESAFIOS NA PRESERVAÇÃO DE PROVAS DIGITAIS

A validade da prova digital no processo penal está diretamente condicionada à preservação de sua integridade e autenticidade, de modo a assegurar que o conteúdo apresentado em juízo corresponda fielmente ao dado originalmente coletado. Diferentemente das provas tradicionais, os vestígios digitais são altamente suscetíveis a alterações, muitas vezes imperceptíveis, o que exige a adoção de mecanismos técnicos rigorosos de verificação.

Nesse cenário, a manipulação de evidências digitais demanda não apenas conhecimento técnico especializado, mas também observância de limites jurídicos, especialmente quanto à legalidade da obtenção e ao respeito aos direitos fundamentais. Como observa Linares Filho (2025, p. 39):

> A manipulação de provas eletrônicas requer, portanto, não apenas competência técnica – como o uso adequado de ferramentas forenses para espelhamento de dispositivos e verificação de integridade digital por meio de algoritmos de *hash* –, mas sobretudo vigilância jurídica quanto aos limites do poder estatal de persecução penal.

A partir dessa perspectiva, a integridade probatória não se reduz a um requisito técnico, mas pressupõe a articulação entre procedimentos tecnológicos adequados e controle jurídico da atividade investigativa.

Entre os instrumentos técnicos utilizados para esse fim, destacam-se os algoritmos de *hash,* amplamente empregados na perícia digital para verificação da integridade dos dados. Sobre o tema, Souza, Munhoz e Carvalho (2025, p. 60) esclarecem que:

> O código *hash* é o resultado de um algoritmo matemático que produz uma sequência de caracteres pequena (normalmente de 32 a 256 caracteres) com base no conteúdo de um determinado arquivo. Caso seja feita qualquer alteração desse conteúdo, a sequência de caracteres sofre uma mudança drástica em seu conteúdo.

Esse mecanismo funciona como uma espécie de assinatura digital do arquivo, permitindo a identificação de qualquer modificação no conteúdo, ainda que mínima.

Os mesmos autores acrescentam que:

> Após verificar a confiança dos códigos *hash* preservados, deve-se comparar os códigos documentados com novos códigos gerados a partir do material recebido. Caso sejam idênticos, foi preservada a integridade do seu conteúdo. Caso sejam divergentes, podem ter ocorrido modificações nos arquivos que invalidam a confiança em seu conteúdo. Souza, Munhoz e Carvalho (2025, p. 60).

Percebe-se, portanto, que a integridade da prova digital depende não apenas da geração do código *hash,* mas da sua verificação contínua e da adequada documentação ao longo do percurso do vestígio.

Todavia, a utilização de ferramentas tecnológicas não é suficiente, por si só, para assegurar a confiabilidade da prova digital. Isso porque tais mecanismos incidem sobre o estado do arquivo em determinado momento, não sendo capazes de demonstrar, de forma isolada, a regularidade de todo o processo de obtenção e manuseio dos dados.

Nesse sentido, Linares Filho (2025, p. 39) ressalta que:

> A validade da prova eletrônica exige a preservação de sua autenticidade e integridade, de modo a garantir que o conteúdo apresentado ao juízo corresponde, sem qualquer alteração, ao material originalmente extraído do dispositivo ou sistema de origem.

A partir dessa compreensão, a integridade probatória deve ser entendida como resultado de um conjunto de procedimentos interdependentes, que envolvem técnica, documentação e controle jurídico.

Além disso, a confiabilidade da prova digital está diretamente relacionada à possibilidade de verificação independente por parte da defesa, elemento essencial para a efetividade do contraditório e da ampla defesa. A ausência de acesso aos dados originais ou aos métodos utilizados na sua análise compromete a legitimidade da prova e fragiliza o equilíbrio processual.

Evidencia-se, nesse cenário, que a conformidade procedimental não constitui garantia absoluta de confiabilidade, mas apenas condição mínima de validade probatória, revelando a insuficiência dos mecanismos atualmente empregados para assegurar, de forma plena, a integridade da prova digital.

Assim, a integridade da prova digital não decorre exclusivamente da aplicação de mecanismos tecnológicos, mas da integração entre técnica, procedimento e garantias fundamentais, sendo a cadeia de custódia o elemento estruturante dessa dinâmica. A inobservância de qualquer desses fatores compromete não apenas o valor probatório do vestígio, mas a própria legitimidade da decisão judicial.

Nesse sentido, a discussão sobre a integridade da prova digital não se esgota na dimensão técnica, mas revela, em sua essência, o próprio dilema estrutural do processo penal contemporâneo: a necessidade de assegurar a efetividade da investigação sem comprometer a proteção da privacidade e das garantias fundamentais.

3.3. O DILEMA ENTRE EFICIÊNCIA INVESTIGATIVA E PROTEÇÃO DA PRIVACIDADE

A análise da prova digital no processo penal não se limita à verificação de sua integridade técnica ou regularidade procedimental, exigindo, sobretudo, a consideração dos limites impostos pelos direitos fundamentais, especialmente aqueles relacionados à privacidade e à proteção de dados pessoais.

Nesse contexto, a doutrina contemporânea reconhece que a obtenção de dados digitais implica ingerências significativas na esfera privada do indivíduo, uma vez que tais elementos possuem elevada capacidade de revelar aspectos íntimos da vida pessoal. Conforme apontado por Saad, Rossi e Partata (2024, p. 3):

> Destacam-se as garantias expressamente positivadas pelo texto constitucional – como as inviolabilidades da intimidade, da vida privada, do domicílio e dos sigilos das diversas formas de comunicação, bem como a autodeterminação informativa.

A partir dessa perspectiva, evidencia-se que o uso de provas digitais exige não apenas observância de critérios técnicos, mas também a submissão a parâmetros constitucionais rigorosos, capazes de limitar o exercício do poder investigativo estatal.

Ao examinar a transformação da privacidade na sociedade da informação, Doneda (2020, p. 13) ressalta que “o tratamento de informações pessoais [...] possibilita o acesso à esfera privada”, sendo necessário impedir que tais dados sejam utilizados de forma descontrolada.

Essa compreensão revela que a proteção de dados pessoais não constitui mera extensão da privacidade clássica, mas sim uma dimensão autônoma de tutela da pessoa, especialmente relevante diante da massificação do tratamento de informações no ambiente digital.

Nesse cenário, o controle judicial assume papel central na legitimação das medidas investigativas que envolvem dados digitais, não se restringindo à verificação formal da legalidade, mas exigindo análise substancial quanto à proporcionalidade, necessidade e adequação da medida. A reserva de jurisdição, portanto, deve ser compreendida como mecanismo de contenção do poder estatal, evitando intervenções arbitrárias na esfera privada.

Ademais, a insuficiência normativa no tratamento das provas digitais contribui para a insegurança jurídica e amplia o risco de violações a direitos fundamentais. Como observa Provasi Vaz (2012, p. 10) “não se encontram definidos os limites de sua utilização, a forma de sua introdução no processo e os critérios para aferição de sua validade e de seu valor probatório”.

Essa lacuna evidencia a necessidade de construção de parâmetros jurídicos mais consistentes, aptos a orientar tanto a atuação investigativa quanto a atividade jurisdicional.

Paralelamente, a confiabilidade da prova digital encontra-se diretamente vinculada à observância da cadeia de custódia, cuja violação compromete a própria legitimidade do elemento probatório. Nesse sentido, Menezes, Borri e Soares (2018, p. 285) destacam que a cadeia de custódia:

> Garante a confiabilidade da prova produzida no processo penal desde seu nascedouro até o momento da valoração pelo magistrado, permitindo-se a verificação de sua cronologia existencial.

A quebra dessa cadeia, portanto, não representa mera irregularidade formal, mas sim fator capaz de afetar a credibilidade da prova e, consequentemente, a própria justiça da decisão judicial.

Diante desse panorama, impõe-se a adoção de critérios materiais para a validade da prova digital, tais como a necessidade da medida, sua adequação ao fim investigativo, a proporcionalidade em sentido estrito e a observância efetiva do contraditório e da ampla defesa.

Assim, a prova digital deve ser compreendida como instrumento que, embora essencial à persecução penal contemporânea, somente se legitima quando produzida e utilizada dentro de um modelo que harmonize eficiência investigativa e respeito às garantias fundamentais, sob pena de conversão do avanço tecnológico em mecanismo de fragilização de direitos.

Diante desse cenário, sustenta-se que a prova digital rompe com os paradigmas tradicionais do direito probatório, evidenciando a insuficiência do modelo normativo vigente e revelando que o tratamento das provas digitais não pode ser adequadamente resolvido pelas categorias tradicionais do processo penal, na medida em que estas se mostram incapazes de abarcar as especificidades técnicas, a volatilidade dos dados e os riscos ampliados de violação a direitos fundamentais inerentes ao ambiente digital.

CONCLUSÃO

O desenvolvimento da presente pesquisa evidenciou que a incorporação das tecnologias digitais ao contexto da persecução penal alterou substancialmente a dinâmica probatória, impondo novos desafios ao Direito Processual Penal. As provas digitais, marcadas por características próprias, como volatilidade, imaterialidade e elevada suscetibilidade à manipulação, afastam-se dos paradigmas tradicionais de prova e demandam tratamento jurídico específico.

Ao longo do trabalho, demonstrou-se que a legitimidade da prova digital não pode ser aferida de forma isolada sob o prisma da legalidade formal, devendo resultar da conjugação de múltiplos fatores. Nesse sentido, destacou-se que a integridade do vestígio digital depende da adoção de mecanismos técnicos adequados, como os algoritmos de *hash*, bem como da observância rigorosa da cadeia de custódia, responsável por assegurar a rastreabilidade e a confiabilidade do elemento probatório ao longo de todo o seu percurso.

Entretanto, a análise demonstrou que a dimensão técnica, por si só, não é suficiente para legitimar a prova digital. A obtenção e utilização de dados eletrônicos implicam ingerências relevantes na esfera privada do indivíduo, exigindo a incidência de limites constitucionais claros. Nesse contexto, assumem centralidade os direitos à privacidade, à intimidade e à proteção de dados pessoais, bem como os princípios da proporcionalidade, da legalidade e do devido processo legal.

Verificou-se, ainda, que o controle judicial desempenha papel essencial na contenção de eventuais excessos na atividade investigativa, devendo ultrapassar a análise meramente formal e alcançar a verificação material da necessidade, adequação e proporcionalidade das medidas adotadas. A ausência de critérios normativos suficientemente definidos contribui para a insegurança jurídica e potencializa o risco de violações a direitos fundamentais, revelando a insuficiência do atual arcabouço jurídico para lidar com as especificidades da prova digital.

Diante desse cenário, sustenta-se que a prova digital rompe com os paradigmas tradicionais do direito probatório, evidenciando a insuficiência do modelo normativo vigente e exigindo a construção de um regime jurídico próprio, apto a integrar, de forma sistemática, exigências técnicas, procedimentais e constitucionais.

Nesse sentido, algumas medidas concretas se mostram necessárias. A primeira diz respeito à edição de legislação específica sobre prova digital no processo

penal, que estabeleça, de forma sistemática, os requisitos de admissibilidade, os protocolos de coleta e preservação e os critérios de valoração das evidências eletrônicas, superando a fragmentação normativa atualmente existente entre o Código de Processo Penal, o Marco Civil da Internet e a Lei Geral de Proteção de Dados.

A segunda refere-se à padronização técnica dos procedimentos periciais digitais, por meio de regulamentação administrativa vinculante aos órgãos de segurança pública e perícia oficial, de modo a uniformizar a aplicação da cadeia de custódia e reduzir a margem de contaminação probatória.

A terceira concerne ao fortalecimento do controle judicial, que deve ser exercido não apenas no momento da autorização da medida investigativa, mas também na fase de admissão da prova em juízo, com análise substantiva da proporcionalidade e da regularidade procedimental.

Ademais, mostra-se indispensável a garantia efetiva do contraditório sobre a prova digital, assegurando à defesa acesso aos dados originais e aos métodos técnicos empregados na sua análise, como condição de legitimidade do processo penal democrático.

A legitimidade da prova digital no processo penal contemporâneo depende, assim, da harmonização entre eficiência investigativa e garantismo, de modo que o avanço tecnológico não se converta em instrumento de flexibilização indevida de direitos fundamentais, mas se consolide como ferramenta compatível com os valores do Estado Democrático de Direito. Nesse sentido, mostra-se pertinente a observação de Provasi Vaz (2012, p. 4), ao afirmar que "as provas digitais [...] apresentam características peculiares, que demandam regulamentação específica de seu procedimento probatório".

Tal compreensão reforça que a construção de um modelo normativo adequado não constitui mera opção legislativa, mas uma exigência necessária para a preservação da legitimidade do processo penal em um cenário marcado pela crescente centralidade das tecnologias digitais.

Por fim, conclui-se que o desafio do processo penal contemporâneo não reside apenas na incorporação de tecnologias à atividade investigativa, mas na capacidade de estabelecer limites jurídicos capazes de impedir que a busca por eficiência comprometa a proteção da privacidade e das garantias fundamentais. Nesse contexto, a cadeia de custódia digital revela-se instrumento necessário, porém estruturalmente insuficiente, cuja eficácia depende de sua articulação com garantias

constitucionais, controle judicial rigoroso e parâmetros claros de atuação estatal, de modo que o avanço tecnológico se consolide como ferramenta compatível com os valores do Estado Democrático de Direito.

REFERÊNCIAS

BITTAR, Eduardo Carlos Bianca. *Metodologia da pesquisa jurídica: teoria e prática da monografia para os cursos de direito*. 18. ed. São Paulo: Saraiva, 2024.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 24 nov. 2025.

BRASIL. Decreto-Lei n.º 3.689, de 3 de outubro de 1941. *Código de Processo Penal*. Rio de Janeiro, 13 out. 1941. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 24 nov. 2025.

BRASIL. *Lei n.º 9.296, de 24 de julho de 1996*. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Brasília, DF, 25 jul. 1996. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9296.htm.> Acesso em: 24 nov. 2025.

BRASIL. Lei n.º 12.965, de 23 de abril de 2014. *Marco Civil da Internet*. Brasília, DF, 24 abr. 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 24 nov. 2025.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Brasília, DF, 15 ago. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 24 nov. 2025.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade n.º 6.393/DF*. Relatora: Ministra Rosa Weber. Brasília, 7 maio 2020.

BRASIL. Supremo Tribunal Federal. *Habeas Corpus n.º 80.949/RJ*. Relator: Ministro Sepúlveda Pertence. Segunda Turma. Julgado em 30 out. 2001. *Diário da Justiça*, Brasília, 14 dez. 2001.

BRASIL. Supremo Tribunal Federal. *Habeas Corpus n.º 91.867/PA*. Relator: Ministro Gilmar Mendes. Tribunal Pleno. Julgado em 24 abr. 2012. *Diário da Justiça Eletrônico*, Brasília, 20 ago. 2012.

BRASIL. Supremo Tribunal Federal. *Habeas Corpus n.º 126.851/PR*. Relator: Ministro Dias Toffoli. Segunda Turma. Julgado em 2 fev. 2016. *Diário da Justiça Eletrônico*, Brasília, 1 mar. 2016.

BRASIL. Superior Tribunal de Justiça. *Habeas Corpus n.º 598.886/SC*. Relator: Ministro Ribeiro Dantas. Quinta Turma. Julgado em 17 set. 2020. Diário da Justiça Eletrônico, Brasília, 23 set. 2020.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário n.º 926.883/MG. Relator: Ministro Edson Fachin. Tribunal Pleno. Julgado em 10 maio 2024. *Diário da Justiça Eletrônico*, Brasília, 14 maio 2024. Tema 990. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=RE926883>. Acesso em: 24 nov. 2025.

BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário n.º 1.055.941/SP.* Relator: Ministro Dias Toffoli. Tribunal Pleno. Julgado em 4 dez. 2019. *Diário da Justiça Eletrônico*, Brasília, 4 maio 2020. Tema 977.

BRASIL. Superior Tribunal de Justiça. *Habeas Corpus n.º 372.411/PR*. Relator: Ministro Reynaldo Soares da Fonseca. Quinta Turma. Julgado em 25 abr. 2017. *Diário da Justiça Eletrônico*, Brasília, 5 maio 2017.

BRASIL. Superior Tribunal de Justiça. *Recurso em Habeas Corpus n.º 90.376/MG*. Relatora: Ministra Maria Thereza de Assis Moura. Sexta Turma. Julgado em 6 dez. 2018. *Diário da Justiça Eletrônico*, Brasília, 14 dez. 2018.

ECO, Umberto. *Como se faz uma tese.* 23. ed. Tradução de Gilson Cesar Cardoso de Souza. São Paulo: Perspectiva, 2010.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. São Paulo: Thomson Reuters, 2020.

KIST, Dario José. *Prova digital no processo penal*. 2. ed. Leme: Mizuno, 2024.

LINARES FILHO, Sergio. *Prova eletrônica em matéria penal: requisitos e formalidades*. São Paulo: Editora Dialética, 2025.

LOPES JR., Aury. *Direito processual penal*. 19. ed. São Paulo: Saraiva, 2022.

LOPES JR., Aury. *Direito processual penal*. 21. ed. São Paulo: Saraiva Educação, 2024.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional*. 16. ed. São Paulo: Saraiva Educação, 2021.

MENEZES, Isabela Aparecida de; BORRI, Luiz Antonio; SOARES, Rafael Junior. *A quebra da cadeia de custódia da prova e seus desdobramentos no processo penal brasileiro.* Revista Brasileira de Direito Processual Penal, Porto Alegre, v. 4, n. 1, p. 277–310, jan./abr. 2018.

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, Porto Alegre, v. 10, n. 3, set./dez. 2024.

SOUZA, Bernardo de Azevedo e; MUNHOZ, Alexandre; CARVALHO, Romullo. Manual prático de provas digitais. 3. ed. rev. atual. e ampl. São Paulo: Thomson Reuters Brasil, 2025.

SILVA, José Afonso da. *Curso de direito constitucional positivo*. 39. ed. rev. e atual. São Paulo: Malheiros, 2016.

VAZ, Denise Provasi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório*. 2012. Tese (Doutorado em Direito) — Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012.

WANDERLEY, Gisela Aguiar. *Privacidade e cidadania: os limites jurídicos da atividade investigativa e a legalidade do acesso policial a aparelhos celulares.* In: ANTONIALLI, Dennys; FRAGOSO, Nathalie (eds.). *Direitos fundamentais e processo penal na era digital: doutrina e prática em debate*. São Paulo: InternetLab, v. 2, 2019.