UNIFAMA – UNIÃO DAS FACULDADES DO MATO GROSSO

LÍNIQUER GABRIEL MARCOMINI OLIVEIRA

DIREITO DIGITAL – A PROVA DIGITAL NO PROCESSO PENAL: VALIDADE E MEIOS DE OBTENÇÃO

Nova Mutum – MT

2026

LÍNIQUER GABRIEL MARCOMINI OLIVEIRA

DIREITO DIGITAL – A PROVA DIGITAL NO PROCESSO PENAL: VALIDADE E MEIOS DE OBTENÇÃO

Trabalho de Conclusão de Curso apresentado no curso de graduação em Direito da UNIFAMA – União das Faculdades do Mato Grosso como requisito parcial à obtenção do grau de bacharel em Direito.

Orientador: Esp. Christiano Garbin Guimarães**.**

Nova Mutum – MT

2026

LÍNIQUER GABRIEL MARCOMINI OLIVEIRA

DIREITO DIGITAL – A PROVA DIGITAL NO PROCESSO PENAL: VALIDADE E MEIOS DE OBTENÇÃO

Orientador

Nova Mutum – MT, _____/____/_____

Nota: _____

BANCA EXAMINADORA

_____

Prof. Christiano Garbin Guimarães

_____

Prof. Membro

_____

Prof. Membro

Dedico esta conquista, primeiramente, à minha mãe, por todo amor, dedicação e apoio incondicional ao longo da minha trajetória. Sua força, seus ensinamentos e suas orações foram fundamentais para que eu pudesse superar os desafios encontrados durante essa caminhada acadêmica. Em cada momento de dificuldade, encontrei em sua presença o incentivo necessário para continuar seguindo em frente.

Dedico também às pessoas próximas de mim, que de alguma forma contribuíram para esta jornada, oferecendo apoio, compreensão, palavras de incentivo e companhia nos momentos mais difíceis. Cada gesto de carinho, confiança e motivação teve importância significativa na construção deste trabalho e na realização deste sonho.

A todos vocês, que fizeram parte da minha caminhada e permaneceram ao meu lado durante esse processo, deixo minha mais sincera gratidão. Esta conquista também pertence a vocês.

AGRADECIMENTOS

À Deus, por me conceder saúde, força e perseverança para continuar sonhando e conquistando novos desafios, mesmo quando o caminho parecia difícil.

À minha mãe, expresso minha mais profunda gratidão por todo amor, apoio, dedicação e incentivo incondicional. Sua presença constante, suas palavras de conforto e sua confiança em mim foram fundamentais para que eu chegasse até aqui. Muito mais do que apoio material, encontrei nela um exemplo diário de força, caráter e determinação.

Agradeço também às pessoas próximas de mim, que estiveram ao meu lado durante essa trajetória, oferecendo apoio, compreensão, incentivo e amizade nos momentos de maior dificuldade. Cada palavra de motivação e cada gesto de carinho tiveram importância significativa nesta conquista.

Ao meu orientador, agradeço pelas orientações, contribuições acadêmicas e pelo acompanhamento durante o desenvolvimento desta pesquisa, fundamentais para o amadurecimento deste trabalho.

Por fim, agradeço a todos aqueles que, direta ou indiretamente, contribuíram para minha formação acadêmica e pessoal, tornando possível a realização deste sonho e a conclusão desta importante etapa da minha vida.

“No ambiente digital, a fragilidade da prova exige rigor técnico e respeito absoluto às garantias fundamentais, pois a integridade da evidência tornou-se condição indispensável da própria legitimidade do processo penal.” Adaptado da obra de Eoghan Casey e da doutrina processual penal contemporânea.

RESUMO

O presente Trabalho de Conclusão de Curso analisa a validade da prova digital no processo penal brasileiro e os meios juridicamente legítimos de sua obtenção, diante dos desafios impostos pela sociedade da informação e pela crescente digitalização das relações sociais. A pesquisa parte da compreensão de que a expansão tecnológica transformou profundamente os mecanismos de produção probatória, exigindo releitura dos institutos processuais tradicionais à luz das garantias constitucionais e das especificidades técnicas da evidência digital. O estudo aborda a volatilidade e a fragilidade da prova digital, destacando a necessidade de observância rigorosa da cadeia de custódia e da preservação da integridade dos dados eletrônicos. Examina-se o arcabouço normativo brasileiro aplicável ao tema, com destaque para a Constituição Federal, o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais, a Lei Carolina Dieckmann e o Pacote Anticrime. Também são analisadas decisões do Supremo Tribunal Federal e do Superior Tribunal de Justiça relacionadas à reserva de jurisdição, extração de dados de aparelhos celulares, validade de capturas de tela de aplicativos de mensagens e preservação da autenticidade probatória. A pesquisa possui natureza bibliográfica, abordagem qualitativa e caráter descritivo, desenvolvida mediante análise doutrinária, legislativa e jurisprudencial. Conclui-se que a admissibilidade da prova digital depende da conjugação entre rigor técnico e respeito às garantias fundamentais, sendo indispensável a observância dos limites constitucionais e dos procedimentos técnico-científicos destinados à preservação da autenticidade da evidência digital.

Palavras-chave: prova digital; processo penal; cadeia de custódia; Direito Digital; evidência digital; garantias fundamentais.

ABSTRACT

This Course Completion Paper analyzes the validity of digital evidence in Brazilian criminal procedure and the legally legitimate means of obtaining it, considering the challenges imposed by the information society and the increasing digitalization of social relations. The research is based on the understanding that technological expansion has profoundly transformed evidentiary mechanisms, requiring a reinterpretation of traditional procedural institutes in light of constitutional guarantees and the technical specificities of digital evidence. The study addresses the volatility and fragility of digital evidence, emphasizing the need for strict observance of the chain of custody and preservation of the integrity of electronic data. The Brazilian legal framework applicable to the subject is examined, with emphasis on the Federal Constitution, the Brazilian Civil Rights Framework for the Internet, the General Data Protection Law, the Carolina Dieckmann Law and the Anti-Crime Package. Decisions issued by the Federal Supreme Court and the Superior Court of Justice regarding judicial authorization, extraction of data from mobile devices, validity of screenshots from messaging applications and preservation of evidentiary authenticity are also analyzed. The research is bibliographic in nature, with a qualitative and descriptive approach, developed through doctrinal, legislative and jurisprudential analysis. It is concluded that the admissibility of digital evidence depends on the combination of technical rigor and respect for fundamental rights, making it essential to observe constitutional limits and technical-scientific procedures aimed at preserving the authenticity of digital evidence.

Keywords: digital evidence; criminal procedure; chain of custody; Digital Law; digital forensics; fundamental rights.

SUMÁRIO

1 INTRODUÇÃO

A tradição do processo penal historicamente se estruturou sobre a ideia de busca da denominada “verdade real”, concebida como finalidade última da atividade jurisdicional e frequentemente utilizada como fundamento legitimador da atuação estatal no âmbito investigativo e probatório. Durante décadas, esse paradigma sustentou a compreensão de que o Estado, no exercício do poder punitivo, deveria alcançar a reconstrução mais próxima possível dos fatos ocorridos, permitindo, para tanto, a utilização de mecanismos investigativos amplos destinados à descoberta da verdade material. Contudo, o desenvolvimento constitucional contemporâneo, especialmente após a promulgação da Constituição Federal de 1988, passou a questionar a própria concepção absoluta dessa pretensão estatal.

A denominada “verdade real”, em sua acepção clássica, passou a ser alvo de severas críticas doutrinárias por representar, em muitos casos, resquício de modelos processuais marcadamente inquisitórios. Sob essa perspectiva, a busca irrestrita pela verdade pode converter-se em justificativa para práticas invasivas, flexibilizações indevidas de garantias fundamentais e ampliação excessiva dos poderes estatais. Nesse contexto, parcela significativa da doutrina contemporânea sustenta que o processo penal democrático não deve orientar-se pela busca ilimitada de uma verdade absoluta, mas por uma reconstrução dos fatos condicionada aos limites constitucionais e processuais impostos pelo Estado Democrático de Direito.

Aury Lopes Jr. (2021) observa que a noção tradicional de verdade real frequentemente opera como instrumento retórico capaz de legitimar práticas autoritárias incompatíveis com o modelo constitucional garantista. Para o autor, o processo penal contemporâneo não deve admitir uma busca ilimitada da verdade a qualquer custo, mas reconhecer que a atividade probatória encontra barreiras intransponíveis nos direitos fundamentais, especialmente nos princípios do devido processo legal, contraditório, ampla defesa, proporcionalidade e dignidade da pessoa humana.

Esse debate adquire contornos ainda mais complexos diante da consolidação da sociedade digital. Se anteriormente o processo penal se estruturava predominantemente sobre provas físicas, documentos escritos, perícias materiais, objetos apreendidos, testemunhos e confissões, atualmente a realidade tecnológica deslocou parte significativa da atividade humana para ambientes virtuais,

produzindo novos mecanismos de interação social e, simultaneamente, novas modalidades de ilícitos.

A digitalização das relações humanas transformou profundamente a forma pela qual indivíduos se comunicam, trabalham, realizam operações financeiras e armazenam informações pessoais. Atividades anteriormente restritas ao espaço físico passaram a ocorrer em plataformas digitais, aplicativos de mensagens instantâneas, redes sociais, sistemas bancários eletrônicos e ambientes virtuais diversos. Consequentemente, a prática criminosa acompanhou essa transformação estrutural, passando igualmente a produzir rastros digitais capazes de servir como elementos probatórios relevantes em investigações criminais.

Nesse cenário, a prova digital deixou de ocupar posição secundária para assumir papel central dentro da persecução penal contemporânea. Dados divulgados pelo Fórum Brasileiro de Segurança Cibernética (2024) indicam crescimento superior a 30% dos crimes digitais registrados no Brasil nos últimos cinco anos. O aumento expressivo de delitos como estelionatos eletrônicos, invasões de dispositivos informáticos, fraudes bancárias virtuais, crimes patrimoniais digitais, crimes contra a honra em redes sociais, divulgação ilícita de dados pessoais e utilização criminosa de mecanismos de inteligência artificial demonstra que a realidade processual brasileira atravessa profunda transformação.

Tal crescimento evidencia que a prova digital não representa mera categoria acessória ou complementar dentro do processo penal contemporâneo. Ao contrário, em diversos procedimentos investigativos ela constitui elemento central da persecução criminal, sendo frequentemente determinante para a identificação de autoria, materialidade e circunstâncias relacionadas ao delito investigado.

Todavia, justamente em razão dessa crescente importância, surgem novos desafios jurídicos, técnicos e epistemológicos. Diferentemente das provas tradicionalmente concebidas pelo direito processual penal, a evidência digital apresenta características particulares que desafiam estruturas clássicas de obtenção, preservação e valoração probatória.

Enquanto uma prova física sofre deterioração gradual, desgaste natural ou desaparecimento material perceptível, a prova digital apresenta natureza substancialmente distinta. Sua fragilidade não decorre da degradação física visível, mas de sua extrema volatilidade tecnológica.

Segundo Casey (2011), um dos principais referenciais da informática forense contemporânea, os vestígios digitais possuem característica essencial denominada volatilidade. Dados eletrônicos podem ser alterados, sobrescritos, modificados, corrompidos ou eliminados em frações mínimas de tempo, muitas vezes sem produzir sinais perceptíveis ao observador comum. Um simples desligamento de equipamento, alteração automática de sistema operacional, atualização de software ou acesso inadequado a determinado dispositivo pode modificar informações relevantes para a reconstrução dos fatos investigados.

Essa fragilidade estrutural diferencia substancialmente a prova digital da prova tradicional. Enquanto uma impressão digital deixada em objeto físico tende a permanecer estável até sua coleta, informações presentes em memória RAM, logs temporários[1], registros de navegação, dados de geolocalização ou metadados[2] eletrônicos podem desaparecer em questão de segundos.

Casey (2011) sustenta que a volatilidade impõe necessidade de observância rigorosa de protocolos específicos destinados à preservação da integridade da informação digital. A obtenção da prova eletrônica exige técnicas científicas capazes de garantir autenticidade, rastreabilidade e manutenção da cadeia de custódia[3], evitando alterações indevidas que comprometam sua confiabilidade processual.

A discussão ultrapassa aspectos meramente tecnológicos e alcança questão essencialmente jurídica: como garantir validade constitucional a elementos probatórios cuja existência, preservação e autenticidade dependem de procedimentos altamente especializados?

O problema assume relevância ainda maior quando se observa que a coleta de provas digitais frequentemente exige acesso a conteúdos profundamente relacionados à esfera privada dos indivíduos. Dispositivos eletrônicos modernos concentram dados sensíveis relativos à vida pessoal, profissional e social de seus usuários, incluindo mensagens privadas, fotografias, registros de localização, movimentações financeiras, arquivos pessoais, históricos de navegação e comunicações diversas.

[1] Registros eletrônicos automáticos relacionados a acessos, conexões, atividades ou operações realizadas em sistemas informáticos e ambientes digitais.
[2] Dados estruturados que descrevem características técnicas relacionadas a arquivos digitais, como data de criação, modificação, autoria, localização e histórico de acesso.
[3] Conjunto de procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou vítimas de crimes, visando preservar sua autenticidade e integridade probatória.

Nesse sentido, a Constituição Federal de 1988 estabelece limites claros à atividade investigativa estatal. O artigo 5º, inciso X, assegura proteção à intimidade, vida privada, honra e imagem das pessoas, enquanto o inciso XII protege o sigilo das comunicações telefônicas, telemáticas e de dados. Paralelamente, o inciso LVI dispõe expressamente serem inadmissíveis, no processo, provas obtidas por meios ilícitos.

A conjugação desses dispositivos demonstra que o acesso estatal a dados digitais não pode ocorrer de maneira indiscriminada. A busca pela eficiência investigativa encontra limites constitucionais intransponíveis, especialmente quando confrontada com direitos fundamentais relacionados à privacidade e proteção de dados pessoais.

Nesse ponto emerge uma das principais tensões do processo penal contemporâneo: de um lado, a necessidade de aprimoramento dos mecanismos de investigação criminal diante da crescente sofisticação dos delitos digitais; de outro, a preservação das garantias fundamentais que estruturam o modelo constitucional democrático.

A legislação brasileira buscou responder parcialmente a esses desafios. A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, promoveu importante alteração legislativa ao criminalizar a invasão de dispositivos informáticos. Posteriormente, a Lei nº 12.965/2014, denominada Marco Civil da Internet, estabeleceu regras relativas à guarda e disponibilização de registros eletrônicos, disciplinando hipóteses de fornecimento mediante autorização judicial.

Em seguida, a Lei Geral de Proteção de Dados — Lei nº 13.709/2018 — introduziu novos parâmetros relacionados ao tratamento de informações pessoais, fortalecendo princípios de finalidade, necessidade e proporcionalidade. Mais recentemente, a Lei nº 13.964/2019, denominada Pacote Anticrime, incorporou disciplina detalhada acerca da cadeia de custódia, reconhecendo expressamente a necessidade de preservação da integridade probatória.

Apesar desses avanços normativos, persistem importantes lacunas interpretativas relacionadas à admissibilidade, obtenção, autenticidade e valoração da prova digital no processo penal brasileiro.

A jurisprudência dos tribunais superiores revela crescente preocupação com a temática. O Supremo Tribunal Federal e o Superior Tribunal de Justiça passaram a enfrentar controvérsias relacionadas à licitude de provas extraídas de aparelhos celulares, aplicativos de mensagens, dados

telemáticos e registros digitais, buscando estabelecer parâmetros para compatibilização entre eficiência investigativa e proteção constitucional.

Entretanto, a ausência de critérios uniformes e a constante evolução tecnológica produzem ambiente de insegurança jurídica, exigindo análise doutrinária e jurisprudencial mais aprofundada.

Diante desse panorama, a presente pesquisa parte da seguinte problemática: diante das particularidades técnicas e jurídicas inerentes à prova digital, quais critérios devem ser observados para assegurar sua validade no processo penal brasileiro sem comprometer direitos fundamentais constitucionalmente protegidos?

O objetivo geral da presente pesquisa consiste em analisar os critérios jurídicos e técnicos necessários à validade da prova digital no processo penal brasileiro, examinando os limites constitucionais relacionados aos meios de obtenção da evidência eletrônica e os mecanismos destinados à preservação de sua autenticidade probatória.

Como objetivos específicos, busca-se compreender a natureza jurídica da prova digital e suas particularidades técnicas; analisar o arcabouço normativo aplicável à obtenção de dados eletrônicos no ordenamento jurídico brasileiro; examinar os procedimentos relacionados à cadeia de custódia e à preservação da integridade da evidência digital; bem como investigar criticamente o posicionamento jurisprudencial adotado pelo Supremo Tribunal Federal e pelo Superior Tribunal de Justiça acerca da admissibilidade da prova digital no processo penal.

A relevância científica da pesquisa decorre da crescente centralidade assumida pela prova digital na persecução penal contemporânea, associada às dificuldades interpretativas existentes acerca de seus meios de obtenção, preservação e admissibilidade jurídica.

Sob perspectiva social, o estudo justifica-se pela expansão dos crimes praticados em ambiente virtual e pela necessidade de construção de parâmetros jurídicos capazes de assegurar equilíbrio entre eficiência investigativa e proteção das garantias individuais constitucionalmente asseguradas.

Quanto aos aspectos metodológicos, a presente pesquisa caracteriza-se como bibliográfica, qualitativa e descritiva. O desenvolvimento do estudo ocorrerá mediante levantamento doutrinário nacional e estrangeiro, análise legislativa e exame jurisprudencial.

A pesquisa bibliográfica utilizará obras especializadas em processo penal, direito digital, informática forense e proteção de dados, além de artigos científicos disponíveis em bases

acadêmicas reconhecidas, especialmente SciELO, Google Scholar, Portal de Periódicos CAPES e repositórios institucionais especializados.

A análise jurisprudencial concentrar-se-á especialmente na *ratio decidendi*[4] das decisões proferidas pelo Supremo Tribunal Federal e pelo Superior Tribunal de Justiça, buscando identificar os fundamentos determinantes utilizados pelos tribunais superiores na resolução de controvérsias envolvendo obtenção de dados digitais, cadeia de custódia, reserva de jurisdição e admissibilidade da prova eletrônica.

Quanto à estrutura, o trabalho será dividido em capítulos destinados ao exame dos fundamentos conceituais da prova digital, análise do arcabouço normativo relacionado à proteção de dados e aos limites constitucionais da investigação criminal, estudo da cadeia de custódia e investigação dos parâmetros jurisprudenciais relacionados à validade da prova digital no processo penal brasileiro.

Assim, mais do que examinar novos instrumentos tecnológicos, a presente pesquisa busca discutir a própria transformação epistemológica enfrentada pelo processo penal na sociedade digital. A passagem do paradigma físico ao paradigma eletrônico exige releitura constitucional capaz de compatibilizar eficiência investigativa, inovação tecnológica e preservação das garantias fundamentais inerentes ao Estado Democrático de Direito.

2 CAPÍTULO I – NATUREZA JURÍDICA E CONCEITOS DA PROVA DIGITAL

2.1 O conceito de rastro digital e a transformação da prova no processo penal contemporâneo

As profundas transformações tecnológicas ocorridas nas últimas décadas alteraram significativamente a dinâmica das relações sociais, econômicas e comunicacionais, produzindo reflexos diretos sobre a atividade jurisdicional e, especialmente, sobre os mecanismos de produção probatória no processo penal. A progressiva digitalização das interações humanas fez surgir nova realidade em que atividades cotidianas, anteriormente restritas ao espaço físico, passaram a ser desenvolvidas em ambientes virtuais. Operações bancárias, comunicações pessoais, relações de

[4] Expressão em latim utilizada para designar o fundamento jurídico central que sustenta determinada decisão judicial.

trabalho, práticas comerciais e interações sociais passaram a ocorrer em plataformas digitais, gerando registros eletrônicos permanentes capazes de constituir relevantes fontes de informação para fins investigativos.

Essa transformação produziu o fenômeno denominado rastro digital, expressão utilizada para designar o conjunto de vestígios eletrônicos gerados pelas atividades desempenhadas em sistemas informatizados. Tais registros podem manifestar-se sob múltiplas formas, incluindo mensagens eletrônicas, arquivos digitais, registros de acesso, metadados, dados de geolocalização, históricos de navegação e informações produzidas automaticamente pelos sistemas tecnológicos.

A existência desses vestígios altera substancialmente a compreensão tradicional da prova processual. Historicamente, o direito processual penal desenvolveu-se tendo como referência mecanismos probatórios de natureza física e materialmente perceptível, como documentos escritos, objetos apreendidos, perícias materiais, testemunhos e confissões. O ambiente digital, entretanto, rompe essa estrutura clássica ao introduzir elementos cuja existência depende de linguagem binária e sistemas computacionais capazes de interpretar e armazenar dados.

Sob essa perspectiva, a prova digital não consiste propriamente em objeto físico, mas em representação informacional de determinado acontecimento. Trata-se de manifestação tecnológica de fatos juridicamente relevantes cuja interpretação depende da utilização de instrumentos técnicos especializados. A prova deixa de possuir materialidade imediatamente perceptível e passa a exigir processos específicos de reconstrução e interpretação.

Nesse ponto, Eoghan Casey destaca que a principal singularidade da evidência digital reside em sua natureza extremamente volátil, uma vez que informações eletrônicas podem sofrer alterações sem manifestações perceptíveis externamente (CASEY, 2011). Diferentemente das provas tradicionais, cuja alteração frequentemente produz sinais físicos identificáveis, modificações em dados digitais podem ocorrer em frações mínimas de tempo e sem qualquer evidência aparente.

A volatilidade mencionada por Casey representa uma das principais rupturas epistemológicas introduzidas pela tecnologia no âmbito processual. Enquanto documentos físicos sofrem deterioração gradual, os dados digitais podem ser alterados, sobrescritos ou eliminados instantaneamente por simples interações sistêmicas. Atualizações automáticas, acessos indevidos,

desligamento de equipamentos e modificações em sistemas operacionais podem comprometer informações relevantes para a investigação criminal.

Essa característica impõe desafios inéditos ao processo penal contemporâneo. A preocupação tradicional relacionada à autenticidade documental passa a coexistir com nova exigência: a necessidade de preservação da integridade lógica da informação digital.

Nesse contexto, surgem mecanismos técnicos destinados a assegurar a confiabilidade probatória dos vestígios eletrônicos. Entre eles destacam-se a imagem forense (*forensic Imaging*[5]) e os sistemas de verificação mediante função hash[6].

A imagem forense consiste na realização de cópia integral e tecnicamente fiel de dispositivos eletrônicos, permitindo reprodução completa do conteúdo lógico do equipamento investigado. Diferentemente de simples cópia de arquivos visíveis, o procedimento busca preservar integralmente o ambiente digital, incluindo registros temporários, arquivos excluídos, espaços vazios e metadados invisíveis ao usuário comum.

A utilização desse procedimento busca impedir alterações decorrentes da manipulação direta do dispositivo original, preservando a integridade do material analisado.

Complementando essa proteção, os sistemas hash desempenham função essencial na validação da autenticidade da prova. O hash pode ser compreendido como sequência alfanumérica gerada mediante operação matemática aplicada sobre determinado conjunto de dados. Pequenas alterações no conteúdo original geram resultados completamente distintos, permitindo verificação precisa da integridade da informação.

Patrícia Peck observa que a confiabilidade da evidência digital depende da manutenção de mecanismos técnicos capazes de assegurar que o material apresentado em juízo corresponda exatamente ao elemento originalmente coletado (PECK PINHEIRO, 2018). Sob essa perspectiva, a tecnologia deixa de representar mero instrumento auxiliar da atividade investigativa e passa a integrar o próprio conceito de validade probatória.

[5] Expressão da informática forense utilizada para designar técnica de criação de cópia integral de dispositivos eletrônicos com preservação absoluta do conteúdo original.
[6] Mecanismo matemático utilizado para gerar sequência única de caracteres capaz de identificar determinado arquivo digital, permitindo verificação de autenticidade e integridade da evidência eletrônica.

Percebe-se, portanto, que a prova digital não pode ser analisada exclusivamente sob categorias tradicionais do direito processual. Sua compreensão exige aproximação interdisciplinar entre Direito, informática forense e ciência da computação, inaugurando nova lógica probatória fundada não apenas na legalidade formal, mas também na preservação científica dos dados investigados.

2.2 Dialética doutrinária: Nucci e Casey entre a perspectiva jurídica e a perspectiva forense

O surgimento da prova digital no processo penal produziu desafios interpretativos que ultrapassam questões meramente tecnológicas. O desenvolvimento de novas formas de produção probatória exige redefinição de categorias jurídicas tradicionais, especialmente no que se refere aos critérios de admissibilidade, classificação e proteção constitucional das evidências eletrônicas.

Nesse cenário, diferentes autores passaram a construir modelos teóricos destinados a explicar a natureza jurídica da prova digital. Entre eles, destacam-se as contribuições de Guilherme de Souza Nucci e Eoghan Casey, cujas formulações, embora desenvolvidas sob perspectivas distintas, apresentam relevante potencial de diálogo.

A abordagem proposta por Nucci estrutura-se predominantemente sobre critérios jurídicos relacionados à expectativa de privacidade existente no ambiente em que a informação se encontra inserida. Segundo essa perspectiva, a classificação da prova digital depende da distinção entre espaços virtuais abertos e ambientes protegidos por mecanismos de privacidade.

Nucci sustenta que conteúdos disponibilizados voluntariamente em ambientes públicos possuem regime jurídico distinto daquele aplicável a informações armazenadas em espaços privados, especialmente quando protegidos por senhas ou restrições de acesso (NUCCI, 2020).

Essa diferenciação produz relevantes consequências processuais. Informações disponíveis em perfis públicos de redes sociais, por exemplo, não recebem o mesmo nível de proteção constitucional atribuído a conteúdos armazenados em aplicativos privados de mensagens instantâneas ou dispositivos pessoais protegidos.

A perspectiva jurídica desenvolvida por Nucci concentra-se, portanto, na ideia de domicílio digital e na proteção constitucional das expectativas legítimas de privacidade.

Em direção distinta, Eoghan Casey desenvolve abordagem fundamentada predominantemente em pressupostos técnico-forenses. Seu interesse não se concentra prioritariamente no ambiente em que a informação está inserida, mas na própria estrutura e natureza dos dados eletrônicos.

Para Casey (2011), a questão central relacionada à validade probatória não se encontra na localização do dado, mas em sua volatilidade e na necessidade de procedimentos técnicos capazes de preservar autenticidade e integridade.

Enquanto Nucci dirige atenção à proteção jurídica do espaço digital, Casey concentra sua análise nos mecanismos científicos de preservação da informação.

Num primeiro momento, as abordagens parecem antagônicas. De um lado, encontra-se perspectiva jurídica voltada à proteção de direitos fundamentais; de outro, visão predominantemente técnica relacionada à preservação científica do dado eletrônico.

Todavia, a realidade contemporânea demonstra que tais modelos não se excluem.

Ao contrário, a complexidade das provas digitais exige construção interpretativa híbrida. O processo penal contemporâneo demanda simultaneamente respeito aos limites constitucionais relacionados à privacidade e observância rigorosa dos protocolos técnicos destinados à preservação da integridade informacional.

Essa necessidade de diálogo interdisciplinar aproxima-se da análise desenvolvida por Pierpaolo Bottini, para quem o processo penal contemporâneo não pode ignorar conhecimentos produzidos pela ciência da computação, sob pena de enfraquecimento da legitimidade jurisdicional (BOTTINI, 2021).

Sob essa perspectiva, a admissibilidade da prova digital passa a depender de dupla exigência: legitimidade jurídica e confiabilidade técnica.

2.3 Garantismo digital e a crítica ao expansionismo tecnológico no processo penal

A crescente incorporação de recursos tecnológicos ao processo penal produziu profundas alterações na forma pela qual a atividade investigativa estatal passou a se desenvolver. Ferramentas de extração de dados, mecanismos automatizados de rastreamento, softwares especializados em recuperação de informações e sistemas capazes de processar grandes quantidades de dados

passaram a integrar a rotina investigativa contemporânea. Todavia, embora tais instrumentos representem significativo avanço operacional, sua utilização também inaugura novas preocupações relacionadas à expansão dos poderes investigatórios estatais.

A modernização tecnológica, frequentemente apresentada sob discurso de eficiência, rapidez e aprimoramento da persecução penal, nem sempre é acompanhada de igual desenvolvimento dos mecanismos de controle jurídico destinados à proteção dos direitos fundamentais. Surge, assim, importante tensão entre eficiência investigativa e garantias constitucionais.

Historicamente, a ampliação do poder punitivo estatal foi frequentemente justificada por discursos relacionados à necessidade de enfrentamento de novas formas de criminalidade. A criminalidade organizada, o terrorismo, os crimes financeiros e, mais recentemente, os delitos praticados em ambientes digitais passaram a ser utilizados como argumentos legitimadores de medidas investigativas progressivamente invasivas.

Entretanto, Alexandre Moraes da Rosa adverte que o processo penal contemporâneo deve resistir ao expansionismo punitivo, fenômeno marcado pela flexibilização progressiva das garantias constitucionais em nome da eficiência investigativa estatal (ROSA, 2019). Para o autor, o processo penal não pode transformar-se em instrumento de maximização irrestrita da capacidade investigativa, sob pena de reprodução de práticas incompatíveis com a ordem constitucional democrática.

Sob essa perspectiva, a eficiência não constitui valor absoluto. Ao contrário, deve permanecer submetida aos limites estruturais estabelecidos pelo Estado Democrático de Direito.

A crítica formulada por Alexandre Moraes da Rosa ganha relevância especial diante da realidade digital contemporânea. Diferentemente dos mecanismos tradicionais de investigação, dispositivos eletrônicos modernos concentram quantidades massivas de informações relativas à esfera privada dos indivíduos. Um único aparelho celular pode armazenar registros capazes de revelar padrões comportamentais, preferências pessoais, deslocamentos geográficos, comunicações privadas, hábitos cotidianos e informações profissionais.

Tal realidade altera substancialmente a dimensão do problema investigativo. Em investigações tradicionais, a apreensão de determinado objeto geralmente produzia acesso limitado

a informações específicas. No ambiente digital, entretanto, o acesso a um único dispositivo frequentemente permite verdadeira reconstrução integral da vida privada do indivíduo.

Laura Schertel Mendes observa que o desenvolvimento tecnológico produziu novas formas de vulnerabilidade relacionadas ao tratamento massivo de informações pessoais, exigindo fortalecimento dos mecanismos de proteção jurídica (MENDES, 2019). Sob essa perspectiva, o avanço tecnológico amplia a necessidade de tutela constitucional, e não sua relativização.

Em semelhante direção, Danilo Doneda destaca que a proteção contemporânea da privacidade deixou de limitar-se à simples proibição de interferências estatais indevidas, passando a abranger mecanismos destinados ao controle do fluxo informacional relacionado ao indivíduo (DONEDA, 2020). A proteção de dados pessoais assume, assim, papel central dentro da estrutura constitucional contemporânea.

Esse debate torna-se especialmente relevante diante da utilização de mecanismos tecnológicos capazes de atuar de forma invisível ou silenciosa. Softwares espiões, programas de monitoramento remoto, sistemas automatizados de vigilância e tecnologias invasivas de rastreamento ampliam significativamente a assimetria informacional existente entre Estado e indivíduo.

A utilização indiscriminada desses instrumentos produz risco de naturalização da vigilância permanente. O problema deixa de limitar-se à obtenção de determinada prova e passa a envolver a própria redefinição dos limites constitucionais da atuação estatal.

Nessa mesma linha, Aury Lopes Jr. sustenta que o processo penal democrático encontra limites intransponíveis nos direitos fundamentais, não sendo admissível a flexibilização das garantias processuais em nome de uma suposta eficiência investigativa (LOPES JR., 2021).

Enquanto Alexandre Moraes da Rosa direciona sua crítica à expansão estrutural do poder punitivo, Aury Lopes Jr. concentra sua análise nos limites constitucionais da atividade jurisdicional. Apesar das diferenças metodológicas, ambos convergem em ponto fundamental: a busca pela eficiência não pode transformar-se em justificativa para mitigação do devido processo legal.

Essa aproximação evidencia verdadeira costura doutrinária. Enquanto Alexandre Moraes da Rosa adverte sobre os riscos políticos do expansionismo investigativo, Aury Lopes Jr. reforça a necessidade de preservação das garantias processuais clássicas. Juntos, os autores demonstram que

o problema central não reside na tecnologia em si, mas em sua utilização desprovida de controle constitucional.

A discussão torna-se ainda mais relevante diante do fenômeno conhecido como “eficiência a qualquer custo”, expressão utilizada para descrever a tendência contemporânea de justificar práticas invasivas mediante promessas de maior capacidade investigativa.

Sob essa lógica, mecanismos potencialmente lesivos à privacidade passam a ser tolerados em razão de sua utilidade prática. O risco, entretanto, consiste na transformação gradual da exceção em regra.

O processo penal democrático não pode admitir estruturas investigativas fundadas em critérios exclusivamente utilitaristas. A Constituição Federal de 1988 estabeleceu modelo processual comprometido com limites claros ao exercício do poder estatal. A proteção da intimidade, da vida privada e do sigilo das comunicações não constitui obstáculo à investigação; representa condição necessária para sua legitimidade.

Assim, a construção de um verdadeiro garantismo digital exige equilíbrio permanente entre inovação tecnológica e proteção das liberdades individuais. O avanço tecnológico não elimina a necessidade de garantias processuais; ao contrário, amplia sua importância.

Conclui-se, portanto, que a admissibilidade da prova digital não depende exclusivamente de sua capacidade técnica de demonstrar determinado fato investigado. Sua legitimidade decorre também da observância rigorosa dos limites constitucionais que estruturam o processo penal contemporâneo.

3 CAPÍTULO II — O MARCO REGULATÓRIO BRASILEIRO E DIREITOS FUNDAMENTAIS

3.1 A Lei Carolina Dieckmann (Lei nº 12.737/2012) e a redefinição da ilicitude no ambiente digital

O desenvolvimento tecnológico e a crescente inserção de dispositivos eletrônicos na rotina social produziram novas formas de interação humana, mas também inauguraram modalidades inéditas de práticas ilícitas. A evolução da criminalidade digital demonstrou a insuficiência dos instrumentos normativos tradicionais para responder a condutas realizadas em ambientes virtuais,

sobretudo diante da expansão de ataques a sistemas informáticos, invasões de dispositivos eletrônicos e divulgação indevida de informações privadas.

Durante longo período, o ordenamento jurídico brasileiro enfrentou dificuldades relacionadas à tipificação de condutas praticadas em ambiente digital. A ausência de previsão normativa específica produzia debates acerca da adequação típica de determinadas práticas, criando lacunas interpretativas relevantes para a atividade jurisdicional.

Nesse cenário, a promulgação da Lei nº 12.737/2012, conhecida popularmente como Lei Carolina Dieckmann, representou importante marco legislativo no tratamento jurídico dos delitos informáticos no Brasil. A norma recebeu tal denominação em razão do episódio envolvendo a divulgação não autorizada de conteúdos privados pertencentes à atriz Carolina Dieckmann, caso que produziu ampla repercussão social e impulsionou o debate acerca da necessidade de proteção jurídica mais específica para dispositivos informáticos.

A referida legislação introduziu o artigo 154-A ao Código Penal, tipificando a conduta de invasão de dispositivo informático mediante violação indevida de mecanismo de segurança, especialmente quando praticada com finalidade de obtenção, adulteração ou destruição de dados sem autorização do titular.

Embora a inovação legislativa tenha sido inicialmente analisada sob perspectiva exclusivamente criminal, seus efeitos ultrapassam a simples criação de novo tipo penal. A Lei Carolina Dieckmann produziu repercussões relevantes também no âmbito processual, especialmente quanto aos critérios relacionados à obtenção de elementos probatórios digitais.

Isso ocorre porque a criminalização da invasão indevida de dispositivos informáticos produz consequência lógica fundamental: o Estado não pode utilizar, como método investigativo, comportamento substancialmente semelhante àquela cuja prática a própria legislação criminaliza.

Sob perspectiva constitucional, admitir que agentes estatais realizem acessos arbitrários a dispositivos eletrônicos equivaleria a legitimar comportamento incompatível com a estrutura protetiva construída pelo próprio ordenamento jurídico.

A discussão assume especial relevância diante da crescente utilização de dispositivos móveis como instrumentos centrais de armazenamento de informações pessoais. Telefones celulares contemporâneos deixaram de desempenhar função meramente comunicacional, passando a operar como verdadeiros repositórios de informações privadas.

Laura Schertel Mendes observa que a expansão tecnológica produziu significativa alteração na forma pela qual dados pessoais passaram a ser produzidos, armazenados e compartilhados, criando novos riscos relacionados à proteção da esfera privada dos indivíduos (MENDES, 2019).

Nessa mesma direção, Danilo Doneda sustenta que a proteção contemporânea da privacidade não pode limitar-se à defesa do espaço físico individual, devendo abranger também mecanismos destinados à proteção do fluxo informacional relacionado à pessoa humana (DONEDA, 2020).

A aproximação entre os autores revela mudança importante na própria compreensão jurídica da intimidade. Se anteriormente a proteção constitucional dirigia-se predominantemente ao espaço físico, a realidade digital exige reconhecimento de novas formas de tutela relacionadas ao ambiente eletrônico.

Essa transformação permite compreender que o acesso indevido a dispositivos eletrônicos ultrapassa simples violação patrimonial ou invasão tecnológica. Em muitos casos, representa verdadeira interferência indevida em esfera constitucionalmente protegida.

A partir dessa perspectiva, a Lei Carolina Dieckmann produz relevante consequência interpretativa: a obtenção da prova digital não pode ocorrer mediante mecanismos incompatíveis com os direitos fundamentais cuja proteção a própria legislação busca assegurar.

A validade da prova digital não depende exclusivamente de sua capacidade demonstrativa, mas também da licitude dos meios empregados para sua obtenção.

Tal compreensão encontra fundamento direto na Constituição Federal de 1988, cujo artigo 5º, inciso LVI, estabelece a inadmissibilidade das provas obtidas por meios ilícitos.

A ilicitude probatória, nesse contexto, deixa de constituir mero vício procedimental e passa a representar importante instrumento de contenção do poder estatal. A vedação constitucional impede que a eficiência investigativa seja utilizada como justificativa para práticas invasivas incompatíveis com a ordem constitucional.

Aury Lopes Jr. observa que a atividade probatória desenvolvida no processo penal deve permanecer integralmente subordinada às garantias constitucionais, não sendo admissível flexibilização do devido processo legal sob pretexto de ampliação da capacidade investigativa estatal (LOPES JR., 2021).

Percebe-se, portanto, aproximação entre a proteção legislativa promovida pela Lei nº 12.737/2012 e a construção garantista desenvolvida pela doutrina processual contemporânea.

Não se trata apenas de impedir invasões ilegítimas praticadas por particulares, mas também de estabelecer limites claros ao exercício do poder investigatório estatal.

Assim, a Lei Carolina Dieckmann representa marco normativo relevante não apenas pela criação de figura típica específica, mas também por reforçar compreensão segundo a qual a obtenção da prova digital deve ocorrer mediante procedimentos juridicamente legítimos e constitucionalmente compatíveis.

3.2 O Marco Civil da Internet (Lei nº 12.965/2014): limites jurídicos da obtenção da prova digital

A expansão da internet e a crescente dependência social das plataformas digitais produziram novas preocupações relacionadas ao tratamento jurídico das informações geradas no ambiente virtual. O aumento exponencial da circulação de dados pessoais, associado à ampliação dos mecanismos de armazenamento e compartilhamento de informações, revelou a necessidade de construção de marco normativo capaz de disciplinar direitos, deveres e responsabilidades decorrentes do uso da rede mundial de computadores.

Nesse contexto, foi promulgada a Lei nº 12.965/2014, denominada Marco Civil da Internet, considerada importante instrumento legislativo destinado à consolidação de princípios estruturantes da utilização da internet no Brasil. Diferentemente de legislações voltadas exclusivamente à repressão de ilícitos informáticos, o Marco Civil foi concebido como verdadeiro estatuto jurídico do ambiente digital, estabelecendo parâmetros relacionados à liberdade de expressão, proteção da privacidade, tratamento de dados e fornecimento de registros eletrônicos.

Embora a norma possua abrangência ampla, seus impactos tornam-se especialmente relevantes no âmbito processual penal, uma vez que grande parte das investigações contemporâneas depende do acesso a informações armazenadas por provedores de aplicações e serviços digitais.

Sob essa perspectiva, o Marco Civil representa instrumento normativo fundamental para compreensão dos limites jurídicos da obtenção da prova digital.

Segundo Patrícia Peck Pinheiro, a crescente digitalização das relações humanas tornou indispensável a criação de mecanismos normativos destinados à proteção da identidade e das informações produzidas em ambientes virtuais (PECK PINHEIRO, 2018). Para a autora, a internet deixou de representar simples espaço tecnológico para assumir papel central na própria dinâmica social contemporânea.

Essa transformação produz relevantes consequências jurídicas, especialmente quando se considera a crescente centralidade dos dados digitais nas investigações criminais.

3.3 O artigo 11 e os limites da jurisdição brasileira sobre dados armazenados no exterior

Entre os dispositivos de maior relevância processual presentes no Marco Civil destaca-se o artigo 11, responsável por disciplinar a aplicação da legislação brasileira aos dados coletados, armazenados ou tratados por provedores de internet.

O referido dispositivo estabelece que empresas responsáveis pela coleta ou tratamento de informações deverão observar a legislação nacional sempre que qualquer operação envolvendo dados ocorrer em território brasileiro.

Aparentemente simples, a norma produziu profundas repercussões relacionadas ao alcance da jurisdição nacional sobre empresas transnacionais de tecnologia.

O desenvolvimento da economia digital permitiu que grande parte das informações pessoais produzidas por usuários brasileiros passasse a ser armazenada em servidores localizados fora do território nacional. Empresas responsáveis por redes sociais, aplicativos de mensagens instantâneas e plataformas digitais frequentemente utilizam sistemas distribuídos internacionalmente, dificultando a definição precisa acerca da competência jurisdicional aplicável.

Esse cenário inaugurou importante problema processual: poderia o Estado brasileiro exigir fornecimento de dados armazenados em servidores estrangeiros?

A interpretação do artigo 11 buscou responder justamente essa dificuldade.

Danilo Doneda observa que a circulação internacional de dados representa uma das principais características estruturantes da sociedade informacional contemporânea, exigindo novas formas de construção normativa relacionadas à proteção da privacidade (DONEDA, 2020).

Sob essa perspectiva, a localização física do servidor deixa de representar elemento exclusivo para definição da incidência normativa.

A regra prevista no artigo 11 busca impedir que empresas utilizem a estrutura internacional de armazenamento como mecanismo de afastamento da incidência da legislação brasileira.

Contudo, a aplicação prática dessa previsão não ocorre sem dificuldades.

A crescente internacionalização dos fluxos informacionais frequentemente produz conflitos envolvendo soberania estatal, cooperação internacional e limites jurisdicionais.

Tal realidade explica a relevância progressiva de instrumentos internacionais destinados à cooperação em matéria de crimes cibernéticos, tema que será posteriormente aprofundado ao tratar da Convenção de Budapeste.

3.4 Artigos 13 e 15: registros de conexão e registros de acesso a aplicações

Outro aspecto de extrema relevância processual encontra-se nos artigos 13 e 15 do Marco Civil da Internet, responsáveis por disciplinar hipóteses de guarda obrigatória de registros eletrônicos.

Apesar de frequentemente tratados como expressões equivalentes, registros de conexão e registros de acesso a aplicações possuem natureza técnica distinta.

Os registros de conexão correspondem ao conjunto de informações relacionadas ao momento em que determinado usuário estabelece vínculo com a rede de internet, abrangendo dados como endereço IP, data, horário de início e término da conexão.

Por outro lado, os registros de acesso a aplicações referem-se às atividades desenvolvidas em plataformas específicas, incluindo utilização de redes sociais, aplicativos, serviços digitais e demais ambientes eletrônicos.

A distinção não possui relevância meramente terminológica. Produz consequências diretas para a atividade investigativa estatal.

Enquanto os registros de conexão permitem identificar a presença de determinado usuário na rede, os registros de aplicação possibilitam reconstrução significativamente mais ampla das atividades desempenhadas no ambiente virtual.

Laura Schertel Mendes sustenta que a utilização massiva de dados digitais exige observância rigorosa dos princípios da necessidade e proporcionalidade, especialmente quando o tratamento dessas informações ocorre em contextos potencialmente invasivos (MENDES, 2019).

Nesse sentido, a obtenção indiscriminada de registros eletrônicos pode representar risco relevante à proteção constitucional da privacidade.

Essa preocupação torna-se ainda mais evidente diante da possibilidade de utilização excessiva de ordens genéricas de fornecimento de dados.

3.5 A vedação às ordens genéricas e o problema da "pesca probatória"

A obtenção de provas digitais mediante ordens judiciais excessivamente amplas constitui tema de crescente preocupação doutrinária e jurisprudencial.

No âmbito investigativo, tornou-se relativamente comum a formulação de pedidos destinados ao fornecimento abrangente de informações relacionadas ao investigado, muitas vezes sem delimitação precisa quanto ao objeto da investigação.

Essa prática aproxima-se do fenômeno denominado *fishing expedition*[7] ou "pesca probatória", expressão utilizada para designar investigações indiscriminadas realizadas sem objeto probatório previamente definido.

Sob essa lógica, o Estado não busca elemento específico relacionado ao fato investigado, mas realiza verdadeiro rastreamento amplo de informações na expectativa de encontrar eventuais ilícitos.

A doutrina contemporânea tem dirigido severas críticas a essa prática.

Aury Lopes Jr. observa que a atividade investigativa não pode converter-se em mecanismo ilimitado de exploração da vida privada do investigado, sendo indispensável delimitação clara entre objeto investigado e medida probatória requerida (LOPES JR., 2021).

Essa preocupação torna-se ainda mais relevante no ambiente digital, onde o acesso irrestrito a determinado dispositivo ou conta eletrônica frequentemente permite acesso a informações completamente desvinculadas do objeto investigativo.

[7] Expressão utilizada no Direito para designar investigações genéricas, indiscriminadas ou exploratórias, realizadas sem delimitação concreta de objeto investigativo ou justa causa específica.

O problema ultrapassa mera discussão procedimental.

Permitir ordens genéricas significaria admitir que a tecnologia fosse utilizada como instrumento de ampliação ilimitada da atividade estatal, produzindo risco de enfraquecimento das garantias constitucionais relacionadas à intimidade, privacidade e proteção de dados.

Assim, o Marco Civil da Internet não apenas disciplina aspectos técnicos relacionados ao armazenamento e fornecimento de registros digitais. Sua função também consiste em estabelecer limites jurídicos destinados a impedir que a atividade investigativa ultrapasse os parâmetros constitucionais do Estado Democrático de Direito.

Percebe-se, portanto, que a obtenção da prova digital exige não apenas autorização judicial formal, mas também fundamentação específica, delimitação adequada e observância rigorosa dos princípios constitucionais que orientam a atividade jurisdicional.

3.6 A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) no contexto criminal e a vedação à fishing expedition

A intensificação da produção e circulação de dados pessoais no ambiente digital produziu profundas alterações na forma pela qual informações passaram a ser coletadas, armazenadas e utilizadas por instituições públicas e privadas. A sociedade contemporânea passou a operar por meio de estruturas informacionais cada vez mais complexas, nas quais atividades cotidianas deixam rastros permanentes capazes de revelar aspectos extremamente sensíveis da vida dos indivíduos.

Nesse contexto, a proteção jurídica da privacidade deixou de limitar-se à tutela tradicional da intimidade e passou a incorporar preocupações relacionadas ao controle da circulação de informações pessoais. A simples garantia de inviolabilidade física do espaço privado mostrou-se insuficiente diante da capacidade tecnológica de coleta, cruzamento e processamento massivo de dados.

Foi nesse cenário que surgiu a Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), considerada importante marco normativo voltado à disciplina do tratamento de informações pessoais no ordenamento jurídico brasileiro.

Embora a legislação possua finalidade predominantemente voltada às relações civis e empresariais, seus princípios apresentam impacto significativo sobre a discussão relacionada à obtenção da prova digital no processo penal.

Isso ocorre porque a atividade investigativa contemporânea depende, cada vez mais, do acesso a informações digitais capazes de revelar comportamentos, deslocamentos, comunicações e padrões de interação social.

Laura Schertel Mendes sustenta que a proteção de dados pessoais representa desdobramento contemporâneo do próprio direito fundamental à privacidade, exigindo mecanismos normativos destinados a assegurar maior controle do indivíduo sobre suas informações pessoais (MENDES, 2019).

Sob essa perspectiva, a tutela jurídica deixa de limitar-se à proteção contra invasões físicas indevidas e passa a abranger a própria dinâmica relacionada ao fluxo informacional.

Em semelhante direção, Danilo Doneda observa que a proteção de dados pessoais não possui natureza meramente patrimonial ou tecnológica, constituindo instrumento destinado à preservação da autonomia individual em sociedades marcadas pelo processamento massivo de informações (DONEDA, 2020).

A aproximação entre ambos os autores revela importante mudança paradigmática.

Enquanto modelos tradicionais de proteção jurídica concentravam-se na defesa do espaço físico individual, a realidade digital exige proteção direcionada também às informações produzidas pela atividade humana.

Essa transformação produz importantes repercussões no âmbito processual penal.

A utilização crescente de provas digitais faz surgir questionamento essencial: até que ponto o Estado pode acessar dados pessoais armazenados em dispositivos eletrônicos sem ultrapassar limites constitucionalmente estabelecidos?

A resposta exige análise dos princípios estruturantes introduzidos pela Lei Geral de Proteção de Dados.

Entre esses princípios destacam-se a finalidade, necessidade e minimização.

O princípio da finalidade determina que o tratamento de dados deve ocorrer para objetivos legítimos, específicos e previamente delimitados.

Por sua vez, o princípio da necessidade estabelece que a utilização das informações deve restringir-se ao mínimo necessário para atingir a finalidade pretendida.

Já o princípio da minimização busca impedir tratamento excessivo ou coleta indiscriminada de informações desvinculadas da finalidade inicialmente estabelecida.

Embora tais princípios tenham sido originalmente estruturados para relações envolvendo tratamento de dados em contextos administrativos e privados, sua lógica apresenta relevante potencial de aplicação no âmbito investigativo.

A atividade estatal desenvolvida durante a persecução penal não pode operar em ambiente de ausência de limites normativos.

Ao contrário, o exercício do poder investigativo deve permanecer submetido aos mesmos parâmetros constitucionais que condicionam qualquer atuação estatal.

É justamente nesse contexto que emerge o problema relacionado à denominada *fishing expedition*.

A expressão, frequentemente traduzida como “pesca probatória”, é utilizada para designar atividade investigativa ampla e indiscriminada, realizada sem delimitação precisa do objeto probatório pretendido.

Sob essa lógica, o objetivo da investigação deixa de consistir na busca de determinado elemento previamente identificado, passando a assumir caráter exploratório.

Em vez de procurar prova específica relacionada ao fato investigado, promove-se verdadeiro rastreamento integral da vida informacional do indivíduo.

No ambiente digital, a prática apresenta riscos ainda mais relevantes.

Dispositivos eletrônicos contemporâneos armazenam grande quantidade de informações desvinculadas do objeto investigativo. Um telefone celular, por exemplo, pode conter registros bancários, fotografias familiares, histórico médico, comunicações profissionais, localização geográfica e dados pessoais completamente alheios à investigação criminal.

Permitir acesso irrestrito a tais conteúdos equivaleria à criação de mecanismos investigativos potencialmente incompatíveis com a estrutura garantista do processo penal.

Aury Lopes Jr. adverte que a atividade probatória não pode converter-se em instrumento ilimitado de exploração da esfera privada do investigado, especialmente quando ausentes critérios objetivos relacionados ao objeto da investigação (LOPES JR., 2021).

A observação realizada pelo autor dialoga diretamente com os princípios estruturantes da Lei Geral de Proteção de Dados.

Enquanto Laura Schertel Mendes e Danilo Doneda enfatizam a necessidade de controle sobre o fluxo informacional, Aury Lopes Jr. direciona atenção aos limites processuais da atividade investigativa.

A aproximação desses referenciais demonstra que a vedação à *fishing expedition* não decorre exclusivamente de preocupação relacionada à proteção de dados pessoais, mas também da própria estrutura constitucional do processo penal.

Não se trata apenas de impedir excessos tecnológicos.

Busca-se evitar que a crescente capacidade investigativa estatal seja utilizada como fundamento para flexibilização progressiva das garantias fundamentais.

Nesse sentido, a prova digital exige critérios específicos de proporcionalidade, delimitação e necessidade, sob pena de transformar instrumentos tecnológicos em mecanismos incompatíveis com o Estado Democrático de Direito.

Percebe-se, portanto, que a LGPD, ainda que não tenha sido originalmente concebida para regular a atividade probatória criminal, produz impactos relevantes sobre a discussão relacionada à obtenção da prova digital, especialmente ao reforçar a necessidade de limitação, finalidade específica e proteção contra intervenções excessivamente invasivas.

3.7 O benchmark internacional: a Convenção de Budapeste, o GDPR europeu e a influência internacional na proteção da prova digital

A crescente transnacionalização das relações digitais produziu impactos significativos sobre a investigação criminal contemporânea. Diferentemente dos delitos tradicionais, cuja execução geralmente se encontrava vinculada a limites territoriais relativamente identificáveis, os crimes praticados em ambiente virtual frequentemente ultrapassam fronteiras estatais, envolvendo múltiplas jurisdições, servidores estrangeiros e circulação internacional de dados.

A própria estrutura da internet contribui para essa complexidade. Informações produzidas em território nacional podem ser armazenadas em servidores localizados em outros países, administradas por empresas transnacionais e acessadas simultaneamente em diferentes partes do

mundo. Em consequência, a obtenção da prova digital passou a depender, cada vez mais, de mecanismos internacionais de cooperação jurídica e harmonização normativa.

Nesse cenário, instrumentos internacionais relacionados à proteção de dados e ao enfrentamento da criminalidade cibernética passaram a exercer influência crescente sobre os ordenamentos jurídicos nacionais, inclusive sobre a interpretação desenvolvida pelos tribunais brasileiros.

Entre esses instrumentos destaca-se a Convenção de Budapeste sobre Crimes Cibernéticos, elaborada pelo Conselho da Europa em 2001.

A Convenção de Budapeste representa um dos principais referenciais internacionais relacionados ao combate à criminalidade informática e à cooperação transnacional para obtenção de provas digitais. O tratado surgiu diante da percepção de que os mecanismos tradicionais de investigação criminal se mostravam insuficientes para enfrentar delitos praticados em ambientes virtuais.

Embora inicialmente concebida no contexto europeu, a Convenção passou gradualmente a influenciar diversos sistemas jurídicos internacionais, especialmente em razão da necessidade de construção de parâmetros comuns para investigação de crimes digitais.

Entre os aspectos mais relevantes do tratado encontram-se as previsões relacionadas à preservação rápida de dados, cooperação internacional entre autoridades investigativas e criação de mecanismos destinados à obtenção célere de informações eletrônicas.

A preocupação central da Convenção consiste justamente na volatilidade da prova digital.

Como observa Casey (2011), dados eletrônicos podem ser rapidamente alterados ou eliminados, exigindo mecanismos investigativos capazes de preservar informações antes de sua destruição. A Convenção de Budapeste incorpora essa preocupação ao estabelecer instrumentos voltados à preservação urgente de registros digitais.

Mesmo não sendo originalmente signatário da Convenção, o Brasil passou progressivamente a aproximar-se de seus parâmetros interpretativos, especialmente diante da crescente necessidade de cooperação internacional em investigações envolvendo crimes cibernéticos.

Esse movimento demonstra que a proteção e obtenção da prova digital deixaram de constituir problema exclusivamente interno, assumindo dimensão global.

Todavia, a incorporação de mecanismos internacionais de cooperação não elimina a necessidade de observância dos limites constitucionais estabelecidos pelo ordenamento jurídico brasileiro.

A cooperação internacional não pode servir como instrumento de flexibilização das garantias fundamentais relacionadas à privacidade, intimidade e devido processo legal.

Sob essa perspectiva, percebe-se aproximação entre a lógica protetiva da Constituição Federal de 1988 e os parâmetros internacionais relacionados à proteção de dados pessoais.

Nesse ponto, ganha especial relevância o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), considerado um dos principais referenciais normativos contemporâneos em matéria de proteção informacional.

O GDPR foi elaborado em contexto marcado pela crescente preocupação com o processamento massivo de informações pessoais por empresas e instituições públicas. Seu objetivo central consiste em fortalecer o controle do indivíduo sobre seus próprios dados, impondo limites rigorosos ao tratamento informacional.

Laura Schertel Mendes sustenta que o modelo europeu de proteção de dados influenciou diretamente a construção da Lei Geral de Proteção de Dados brasileira, especialmente quanto à incorporação dos princípios da finalidade, necessidade e proporcionalidade (MENDES, 2019).

Da mesma forma, Danilo Doneda observa que a proteção contemporânea dos dados pessoais deve ser compreendida como instrumento essencial de preservação da liberdade individual em sociedades orientadas pelo processamento massivo de informações (DONEDA, 2020).

O diálogo entre os autores evidencia que a proteção de dados não pode ser compreendida como simples limitação burocrática ao exercício da atividade estatal. Trata-se de mecanismo voltado à preservação da autonomia individual diante da crescente capacidade tecnológica de monitoramento e vigilância.

Essa discussão assume importância ainda maior no âmbito processual penal.

A crescente utilização de provas digitais faz surgir risco permanente de expansão excessiva dos mecanismos investigativos estatais, especialmente diante da facilidade tecnológica de acesso, armazenamento e cruzamento de informações pessoais.

Nesse contexto, os parâmetros internacionais relacionados à proteção de dados passam a atuar como importantes referenciais interpretativos para limitação da atividade investigativa.

A influência desses instrumentos pode ser observada progressivamente na própria jurisprudência brasileira.

O Superior Tribunal de Justiça passou a desenvolver entendimento mais rigoroso quanto à necessidade de preservação da cadeia de custódia, fundamentação específica das ordens judiciais e observância da proporcionalidade na obtenção de provas digitais.

Da mesma forma, o Supremo Tribunal Federal tem reforçado a necessidade de compatibilização entre eficiência investigativa e proteção constitucional da privacidade.

Embora nem sempre façam referência expressa à Convenção de Budapeste ou ao GDPR, diversos julgados recentes incorporam lógica interpretativa compatível com os parâmetros internacionais relacionados à proteção informacional e limitação da vigilância estatal.

Esse movimento demonstra que o direito processual penal brasileiro passou a integrar debate global relacionado à proteção da prova digital.

A admissibilidade da evidência eletrônica deixou de depender exclusivamente da legislação interna e passou a sofrer influência de princípios internacionais relacionados à cooperação jurídica, proteção de dados e preservação das garantias fundamentais.

Percebe-se, portanto, que a construção contemporânea da prova digital no processo penal brasileiro ocorre mediante constante diálogo entre normas nacionais e referenciais internacionais.

A proteção constitucional da privacidade, a necessidade de preservação da integridade da prova e os limites relacionados à obtenção de dados digitais não constituem preocupações exclusivamente brasileiras, mas desafios compartilhados por sistemas jurídicos em escala global.

4 CAPÍTULO III — CADEIA DE CUSTÓDIA E INTEGRIDADE TÉCNICA DA PROVA DIGITAL

4.1 A cadeia de custódia como requisito de validade da prova digital

O crescente protagonismo da prova digital nas investigações criminais contemporâneas trouxe consigo preocupações relacionadas não apenas à obtenção dos dados eletrônicos, mas também à preservação de sua autenticidade, integridade e confiabilidade. Diferentemente das provas tradicionais, os vestígios digitais apresentam características próprias decorrentes de sua

natureza informacional, especialmente sua elevada volatilidade e suscetibilidade a alterações invisíveis ao observador comum.

Essa particularidade fez surgir a necessidade de construção de mecanismos destinados a assegurar que os elementos coletados durante a investigação permaneçam íntegros até sua apresentação em juízo. Nesse contexto, ganha destaque o instituto da cadeia de custódia.

A cadeia de custódia pode ser compreendida como o conjunto de procedimentos técnicos e documentais voltados à preservação da história cronológica do vestígio probatório, desde seu reconhecimento até o encerramento da atividade pericial. Sua finalidade consiste em demonstrar que o elemento apresentado ao magistrado corresponde exatamente ao material originalmente identificado durante a investigação.

Embora a preocupação relacionada à integridade probatória não seja recente, sua relevância adquiriu novas proporções no ambiente digital. Enquanto determinados elementos físicos permitem percepção visual de alterações ou adulterações, os dados eletrônicos podem sofrer modificações sem deixar vestígios imediatamente identificáveis.

Nesse sentido, Eoghan Casey observa que a principal fragilidade da prova digital decorre de sua extrema volatilidade, característica que exige protocolos rigorosos de preservação desde os primeiros momentos da atividade investigativa (CASEY, 2011).

A observação realizada pelo autor possui repercussões diretas no âmbito processual. Se a integridade da prova depende da preservação adequada do material digital, eventual falha procedimental deixa de representar simples irregularidade técnica e passa a comprometer a própria confiabilidade da evidência.

A importância jurídica da cadeia de custódia recebeu reforço significativo com a promulgação da Lei nº 13.964/2019, denominada Pacote Anticrime, responsável por introduzir no Código de Processo Penal disciplina específica relacionada ao tratamento dos vestígios probatórios.

A reforma legislativa incorporou ao CPP os artigos 158-A a 158-F, estabelecendo parâmetros normativos voltados à preservação dos elementos probatórios e à documentação das etapas de manipulação do vestígio.

Renato Brasileiro de Lima sustenta que a validade da prova não depende exclusivamente de sua obtenção regular, mas também da preservação integral de sua autenticidade durante todas as fases da persecução penal (BRASILEIRO DE LIMA, 2020).

A análise proposta pelo autor amplia a compreensão tradicional da licitude probatória. A preocupação deixa de concentrar-se exclusivamente no momento inicial de obtenção e passa a abranger o percurso técnico-documental desenvolvido posteriormente.

Sob essa perspectiva, a admissibilidade da prova digital passa a depender não apenas da autorização judicial ou da licitude da coleta, mas também da manutenção de sua integridade ao longo de toda a atividade investigativa.

Essa lógica torna-se especialmente relevante diante da facilidade com que dados eletrônicos podem ser alterados.

Uma simples abertura inadequada de dispositivo eletrônico pode produzir modificações automáticas em registros internos do sistema. O acesso direto a aplicativos de mensagens, por exemplo, pode alterar horários de visualização, gerar sincronizações automáticas ou modificar metadados relevantes à reconstrução dos fatos.

Consequentemente, a ausência de protocolos rigorosos pode comprometer significativamente a confiabilidade da prova produzida.

Não se trata, portanto, de formalismo excessivo.

A cadeia de custódia desempenha função essencial de proteção contra adulterações, manipulações indevidas e incertezas relacionadas à autenticidade do material apresentado em juízo.

Nessa direção, Patrícia Peck Pinheiro observa que a confiabilidade da prova digital exige documentação detalhada de todas as etapas relacionadas à manipulação da evidência, permitindo reconstrução precisa do percurso realizado desde a coleta até a apresentação processual (PECK PINHEIRO, 2018).

Percebe-se importante aproximação entre Patrícia Peck e Renato Brasileiro.

Enquanto Patrícia Peck enfatiza a necessidade de documentação técnica contínua, Renato Brasileiro direciona atenção à preservação da autenticidade jurídica do material probatório.

Ambas as perspectivas convergem em ponto fundamental: a integridade da prova não constitui aspecto acessório, mas requisito indispensável à própria validade processual.

Assim, a cadeia de custódia deixa de representar simples procedimento administrativo destinado à organização da atividade investigativa e passa a assumir papel central na estrutura de admissibilidade da prova digital.

No contexto contemporâneo, a validade da evidência eletrônica encontra-se diretamente vinculada à capacidade de demonstrar que o material analisado permaneceu íntegro, autêntico e livre de interferências indevidas durante toda a persecução penal.

4.2 Anatomia da cadeia de custódia: reconhecimento, coleta, acondicionamento, transporte e processamento

A crescente utilização de provas digitais no processo penal tornou insuficiente a simples observância de formalidades jurídicas relacionadas à autorização e obtenção da evidência. A complexidade técnica dos vestígios eletrônicos exige procedimentos especializados capazes de preservar a integridade do material desde os primeiros contatos com o elemento investigado até sua apresentação em juízo.

Nesse contexto, a cadeia de custódia não pode ser compreendida como mecanismo abstrato ou mera exigência documental. Sua efetividade depende da observância rigorosa de etapas técnicas sucessivas, cada uma destinada a reduzir riscos relacionados à perda, adulteração ou comprometimento da confiabilidade probatória.

Com a entrada em vigor da Lei nº 13.964/2019, o Código de Processo Penal passou a prever disciplina específica relacionada ao tratamento dos vestígios, especialmente por meio dos artigos 158-A e seguintes. O legislador buscou estruturar procedimento capaz de garantir rastreabilidade integral do material probatório, estabelecendo sequência lógica de procedimentos destinados à preservação da autenticidade.

No âmbito da prova digital, essas etapas assumem relevância ainda maior em razão da volatilidade dos dados eletrônicos.

Segundo Casey (2011), a manipulação inadequada de equipamentos digitais pode alterar automaticamente informações essenciais ao processo investigativo. O simples acionamento de determinado dispositivo pode modificar registros internos, alterar metadados, iniciar sincronizações automáticas ou produzir mudanças invisíveis ao usuário comum.

Essa observação demonstra que o contato inicial com a prova digital constitui momento particularmente sensível.

4.3 Reconhecimento: a identificação do potencial vestígio digital

A primeira etapa da cadeia de custódia consiste no reconhecimento do vestígio.

O reconhecimento corresponde à identificação inicial de elementos potencialmente relevantes à investigação criminal. Trata-se do momento em que agentes responsáveis verificam a existência de informações capazes de contribuir para reconstrução dos fatos investigados.

Embora aparentemente simples, essa etapa apresenta elevada complexidade no ambiente digital.

Diferentemente de provas físicas tradicionais, os vestígios eletrônicos frequentemente não são imediatamente perceptíveis. Informações relevantes podem encontrar-se armazenadas em dispositivos móveis, computadores, serviços em nuvem, aplicativos de mensagens, mídias removíveis ou registros automáticos produzidos por sistemas informatizados.

Além disso, determinados elementos probatórios podem estar ocultos ao usuário comum, exigindo conhecimento técnico específico para sua identificação.

Pierpaolo Bottini observa que a crescente digitalização da atividade humana exige aproximação progressiva entre Direito e ciência da computação, sob pena de limitação da capacidade investigativa e comprometimento da própria legitimidade da atividade jurisdicional (BOTTINI, 2021).

A observação do autor demonstra que o reconhecimento adequado da prova digital pressupõe formação interdisciplinar, afastando a ideia de que conhecimentos exclusivamente jurídicos seriam suficientes.

4.4 Coleta: obtenção do material e preservação da integridade informacional

Após identificação do vestígio relevante, inicia-se a etapa de coleta.

A coleta corresponde ao procedimento destinado à obtenção física ou lógica do elemento digital investigado. Diferentemente de simples apreensão de objetos materiais, a coleta digital exige adoção de protocolos específicos destinados à preservação integral dos dados.

Nesse contexto, Eoghan Casey destaca a importância da utilização de procedimentos de imagem forense, técnica destinada à criação de cópia integral do conteúdo armazenado em determinado dispositivo (CASEY, 2011).

A imagem forense busca reproduzir integralmente a estrutura lógica do equipamento investigado, incluindo elementos invisíveis ao usuário comum, como arquivos excluídos, espaços não alocados e metadados.

Sua finalidade consiste em evitar manipulação direta do dispositivo original, preservando a integridade da fonte primária de informação.

Associado ao procedimento de imagem forense, utiliza-se frequentemente o mecanismo hash, responsável pela criação de sequência matemática única destinada à verificação de autenticidade dos dados coletados.

Caso o valor hash obtido no momento da coleta permaneça idêntico ao longo da investigação, presume-se a manutenção da integridade do material.

A utilização conjunta desses procedimentos demonstra que a coleta da prova digital não constitui simples ato mecânico de obtenção de dados, mas procedimento técnico-científico complexo.

4.5 Acondicionamento: proteção física e lógica da evidência digital

Encerrada a coleta, surge necessidade de preservação do material obtido.

No ambiente digital, o acondicionamento possui finalidade mais ampla que a simples proteção física do objeto apreendido. Busca-se impedir interferências externas capazes de alterar o conteúdo eletrônico armazenado.

Dispositivos digitais permanecem constantemente sujeitos a riscos relacionados à conexão remota, sincronizações automáticas, atualizações sistêmicas e interferências eletromagnéticas.

Em razão disso, procedimentos especializados passaram a integrar a rotina pericial contemporânea.

Entre eles destacam-se os denominados sacos de Faraday.

Os sacos de Faraday constituem invólucros desenvolvidos com materiais capazes de bloquear sinais eletromagnéticos externos. Sua utilização impede conexões remotas capazes de alterar ou apagar informações armazenadas em dispositivos eletrônicos apreendidos.

A importância desses mecanismos tornou-se ainda mais evidente diante do desenvolvimento de ferramentas capazes de realizar exclusão remota de informações.

A ausência de proteção adequada pode permitir alterações automáticas ou intencionais antes mesmo do início da análise pericial.

Sob essa perspectiva, o acondicionamento deixa de representar simples atividade logística e passa a constituir instrumento relevante para preservação da autenticidade probatória.

4.6 Transporte e processamento: documentação contínua e rastreabilidade integral

As etapas posteriores relacionadas ao transporte e processamento possuem finalidade semelhante: assegurar rastreabilidade integral da manipulação realizada sobre a prova.

Renato Brasileiro de Lima sustenta que a validade da prova digital se encontra diretamente relacionada à capacidade de demonstrar quem teve contato com o material, quando ocorreu a manipulação e quais procedimentos foram empregados durante a investigação (BRASILEIRO DE LIMA, 2020).

Essa preocupação busca impedir situações de incerteza relacionadas à autenticidade do material produzido.

No ambiente digital, pequenas intervenções podem gerar consequências significativas.

Por essa razão, toda movimentação realizada sobre a prova deve ser adequadamente documentada.

Identificação dos responsáveis, horários, instrumentos utilizados, softwares empregados e procedimentos executados passam a integrar registros indispensáveis à manutenção da confiabilidade probatória.

Patrícia Peck observa que a integridade da evidência digital exige documentação contínua de todas as etapas de manipulação, permitindo reconstrução detalhada do histórico relacionado ao material apresentado em juízo (PECK PINHEIRO, 2018).

Percebe-se importante aproximação entre Patrícia Peck e Renato Brasileiro.

Enquanto Renato Brasileiro concentra sua análise na autenticidade jurídica do material probatório, Patrícia Peck enfatiza a necessidade de controle técnico-documental permanente.

Ambas as perspectivas convergem para conclusão comum: a quebra da cadeia de custódia não representa simples irregularidade formal.

Trata-se de circunstância capaz de comprometer a própria confiabilidade da prova.

Dessa forma, a anatomia da cadeia de custódia demonstra que a validade da prova digital não depende apenas de autorização judicial ou licitude inicial da coleta. Sua admissibilidade exige observância rigorosa de procedimentos técnicos destinados à preservação integral da evidência ao longo de toda a persecução penal.

4.7 O diálogo interdisciplinar entre Direito e informática forense: a contribuição de Patrícia Peck, Renato Brasileiro e Pierpaolo Bottini

A crescente utilização da prova digital no processo penal tornou insuficiente a adoção de perspectivas exclusivamente jurídicas para compreensão dos problemas relacionados à admissibilidade probatória. As particularidades técnicas dos vestígios eletrônicos impuseram aproximação cada vez maior entre o Direito e áreas tradicionalmente externas à formação jurídica, especialmente a informática forense, a ciência da computação e a tecnologia da informação.

A complexidade dos dados digitais evidencia que a validade da prova não pode ser analisada apenas sob critérios tradicionais relacionados à licitude, pertinência e relevância processual. A preservação da autenticidade informacional exige domínio de procedimentos técnicos específicos destinados a impedir alterações indevidas dos elementos coletados.

Sob essa perspectiva, a interdisciplinaridade deixa de representar característica acessória da prova digital e passa a constituir requisito necessário à própria estrutura de admissibilidade probatória.

Pierpaolo Bottini sustenta que o processo penal contemporâneo não pode ignorar conhecimentos produzidos pela ciência da computação, sob pena de enfraquecimento da legitimidade jurisdicional e comprometimento da própria confiabilidade das decisões judiciais (BOTTINI, 2021).

A análise proposta pelo autor demonstra importante ruptura com modelos tradicionais de compreensão processual. O magistrado, o membro do Ministério Público, a autoridade policial e os demais operadores jurídicos passam a atuar em contexto no qual conhecimentos exclusivamente normativos tornam-se insuficientes.

Isso não significa exigir formação técnica aprofundada em ciência da computação dos profissionais do Direito, mas reconhecer que a compreensão dos mecanismos básicos relacionados à produção e preservação da prova digital tornou-se condição relevante para adequada valoração processual.

Essa necessidade de diálogo interdisciplinar aproxima-se da perspectiva desenvolvida por Patrícia Peck Pinheiro.

Segundo a autora, a confiabilidade da evidência digital depende da existência de mecanismos documentais e técnicos capazes de assegurar rastreabilidade integral dos procedimentos realizados sobre o material investigado (PECK PINHEIRO, 2018).

A preocupação desenvolvida por Patrícia Peck concentra-se especialmente na documentação das etapas relacionadas à manipulação da evidência.

Sob sua perspectiva, a validade da prova não decorre exclusivamente do resultado final produzido pela perícia, mas também da capacidade de reconstrução precisa do caminho percorrido pelo material durante a investigação.

Essa abordagem aproxima-se da análise desenvolvida por Renato Brasileiro de Lima.

O autor sustenta que a autenticidade da prova encontra-se diretamente vinculada à manutenção da integridade do vestígio durante toda a cadeia de custódia, exigindo preservação contínua do material desde sua coleta até apresentação em juízo (BRASILEIRO DE LIMA, 2020).

Percebe-se importante diálogo doutrinário entre os autores.

Enquanto Patrícia Peck enfatiza a necessidade de documentação técnica contínua, Renato Brasileiro direciona sua atenção à preservação jurídica da autenticidade probatória. Bottini, por sua vez, amplia a discussão ao demonstrar que a compreensão da prova digital exige aproximação estrutural entre Direito e tecnologia.

Em conjunto, as perspectivas apresentadas revelam que a prova digital exige dupla proteção: jurídica e técnico-científica.

Essa discussão assume especial relevância diante de determinadas práticas observadas no cotidiano investigativo brasileiro.

Não raramente, dispositivos eletrônicos apreendidos são submetidos a acessos diretos realizados sem utilização de ferramentas forenses especializadas, permitindo manipulação inadequada do material probatório.

Em diversas situações, agentes responsáveis pela investigação acessam aplicativos de mensagens, galerias de arquivos ou conteúdos armazenados diretamente no dispositivo apreendido, sem realização prévia de imagem forense ou utilização de software extrator apropriado.

Embora aparentemente simples, essa prática produz riscos significativos relacionados à preservação da integridade probatória.

Isso ocorre porque a interação direta com o dispositivo pode gerar modificações automáticas nos próprios dados analisados.

Aplicativos de mensagens instantâneas frequentemente registram alterações relacionadas a horários de acesso, status de leitura, sincronizações automáticas e modificações em metadados internos. O simples ato de abrir determinada conversa pode alterar informações relevantes para reconstrução cronológica dos fatos investigados.

Casey observa que a manipulação inadequada de dispositivos eletrônicos pode comprometer dados relevantes de maneira praticamente imperceptível, reduzindo significativamente a confiabilidade do material posteriormente apresentado em juízo (CASEY, 2011).

Tal observação revela que o problema ultrapassa mera questão operacional.

Não se trata apenas da utilização de método investigativo tecnicamente inadequado, mas da possibilidade de comprometimento da própria autenticidade da prova.

Essa preocupação passou a receber crescente atenção da jurisprudência brasileira, especialmente por parte do Superior Tribunal de Justiça.

Decisões recentes passaram a reconhecer que a ausência de protocolos técnicos adequados pode gerar inadmissibilidade da prova digital, especialmente quando inexistentes registros claros relacionados aos procedimentos empregados durante a coleta e análise do material.

Verifica-se, portanto, progressiva aproximação entre produção doutrinária e orientação jurisprudencial.

A exigência de softwares extratores, documentação detalhada e protocolos especializados deixa de representar recomendação técnica facultativa para assumir relevância processual concreta.

Assim, a evolução contemporânea da prova digital demonstra que a validade da evidência eletrônica não depende apenas da existência de autorização judicial ou da observância formal das normas processuais. Sua admissibilidade exige diálogo permanente entre Direito e tecnologia, garantindo que a inovação investigativa permaneça compatível com os parâmetros constitucionais relacionados à proteção das garantias fundamentais.

5 CAPÍTULO IV — ANÁLISE CRÍTICA DA JURISPRUDÊNCIA DO STF E STJ

5.1 A reserva de jurisdição e os limites constitucionais de acesso aos dados digitais: análise do HC 91.867/SP

A crescente utilização de meios eletrônicos na comunicação contemporânea ampliou significativamente a relevância das informações digitais no contexto investigativo. Paralelamente, intensificou-se a necessidade de definição dos limites constitucionais relacionados ao acesso estatal a esses dados.

Nesse contexto, o Supremo Tribunal Federal enfrentou questão relevante no julgamento do Habeas Corpus nº 91.867/SP, de relatoria do Ministro Cezar Peluso, consolidando entendimento acerca da excepcionalidade das medidas invasivas relacionadas à obtenção de comunicações privadas. “A cláusula constitucional de proteção ao sigilo das comunicações representa garantia fundamental que somente pode sofrer mitigação mediante autorização judicial fundamentada, observadas as hipóteses legais excepcionais” (STF, HC 91.867/SP, Rel. Min. Cezar Peluso).

O julgamento possui especial relevância por reafirmar a incidência do princípio da reserva de jurisdição no âmbito das comunicações eletrônicas. Embora o caso tenha surgido em contexto relacionado à interceptação, sua fundamentação ultrapassa a discussão específica e produz impactos relevantes para o tratamento contemporâneo da prova digital.

A tese central desenvolvida pelo Supremo Tribunal Federal consiste na compreensão de que medidas investigativas potencialmente invasivas exigem controle judicial rigoroso e fundamentação específica. A Corte reconheceu que o acesso estatal a comunicações privadas não

pode ocorrer mediante justificativas genéricas ou argumentos abstratos relacionados à eficiência investigativa.

O fundamento adotado pelo Ministro Cezar Peluso encontra respaldo direto no artigo 5º, inciso XII, da Constituição Federal, dispositivo responsável pela proteção do sigilo das comunicações. A relevância da decisão decorre justamente do reconhecimento de que o avanço tecnológico não elimina a necessidade de observância das garantias constitucionais clássicas. Ao contrário, a ampliação tecnológica dos mecanismos de comunicação intensifica a necessidade de proteção dessas garantias constitucionais.

Aury Lopes Jr. sustenta que a expansão dos instrumentos investigativos não autoriza flexibilização das garantias processuais, especialmente quando a busca pela verdade passa a justificar restrições excessivas aos direitos fundamentais (LOPES JR., 2021). A observação do autor aproxima-se diretamente do entendimento firmado pelo STF. Enquanto o Supremo reforça a necessidade de controle judicial prévio, Aury Lopes Jr. enfatiza que a atividade probatória deve permanecer submetida aos limites constitucionais do processo penal democrático. Essa aproximação demonstra importante convergência entre doutrina e jurisprudência.

A decisão proferida pelo STF não se limita à proteção formal do sigilo das comunicações. Seu verdadeiro impacto consiste na construção de limite material ao exercício da atividade investigativa estatal. Sob essa perspectiva, a autorização judicial deixa de representar simples formalidade procedimental, constituindo instrumento destinado a impedir que a ampliação tecnológica dos mecanismos investigativos produza enfraquecimento progressivo das garantias fundamentais.

Percebe-se, portanto, que a ratio decidendi do HC 91.867/SP não está restrita à interceptação de comunicações. Sua lógica interpretativa alcança discussão mais ampla relacionada à obtenção da prova digital: quanto maior a capacidade tecnológica de acesso à esfera privada do indivíduo, maior deve ser a intensidade do controle jurisdicional.

Essa conclusão possui relevância direta para o objeto desta pesquisa. A validade da prova digital não depende exclusivamente de sua autenticidade técnica ou de sua utilidade investigativa. Exige, igualmente, observância rigorosa dos mecanismos constitucionais destinados à limitação do poder estatal e à preservação das garantias fundamentais inerentes ao processo penal democrático.

5.2 HC 51.531/DF e a proteção constitucional da intimidade

Em continuidade à construção jurisprudencial relacionada aos limites constitucionais da atividade investigativa, o Superior Tribunal de Justiça enfrentou questão igualmente relevante no julgamento do Habeas Corpus nº 51.531/DF. A controvérsia analisada pela Corte envolvia a utilização de elementos probatórios obtidos sem observância rigorosa dos requisitos legais relacionados à autorização judicial e à proteção da esfera privada do investigado.

Ao examinar a matéria, o STJ consolidou entendimento no sentido de que a proteção constitucional da intimidade não constitui garantia meramente formal, mas verdadeiro limite material ao exercício da atividade investigativa estatal. Nesse contexto, a Corte reconheceu que a legitimidade da prova não decorre exclusivamente de sua utilidade para a persecução penal, exigindo também compatibilidade dos meios empregados com os parâmetros constitucionais estabelecidos pelo ordenamento jurídico brasileiro.

> A proteção constitucional da intimidade e da vida privada impede que a atividade investigativa estatal se desenvolva mediante utilização de mecanismos incompatíveis com os direitos fundamentais assegurados pela Constituição Federal. A obtenção da prova deve observar os limites materiais impostos pelo devido processo legal e pelas garantias constitucionais relacionadas à esfera privada do indivíduo. (STJ, HC 51.531/DF)

A decisão reafirma entendimento já consagrado pelo artigo 5º, inciso LVI, da Constituição Federal, segundo o qual são inadmissíveis, no processo, provas obtidas por meios ilícitos. Todavia, a relevância do precedente ultrapassa a simples reafirmação textual da norma constitucional. Seu verdadeiro impacto consiste na ampliação da discussão relacionada aos limites da atividade investigativa no contexto das comunicações e dados digitais.

Danilo Doneda observa que a proteção contemporânea da privacidade deixou de restringir-se à tutela do espaço físico individual, passando a abranger mecanismos relacionados ao controle informacional e à circulação de dados pessoais (DONEDA, 2020). A análise desenvolvida pelo autor permite releitura contemporânea do entendimento firmado pelo Superior Tribunal de Justiça.

Sob essa perspectiva, a violação da esfera privada não ocorre apenas mediante ingresso físico indevido em determinado ambiente. No contexto digital, o acesso inadequado a dispositivos eletrônicos, registros telemáticos, aplicativos de mensagens e bancos de dados pessoais pode produzir restrições igualmente intensas aos direitos fundamentais do indivíduo.

Essa interpretação aproxima a construção jurisprudencial do STJ da evolução doutrinária relacionada à proteção de dados pessoais e à autodeterminação informacional. Enquanto a jurisprudência reforça os limites constitucionais da atividade investigativa, a doutrina contemporânea evidencia que o avanço tecnológico ampliou significativamente a capacidade estatal de acesso à intimidade dos indivíduos, exigindo mecanismos de contenção compatíveis com o modelo constitucional democrático.

A decisão proferida no HC 51.531/DF reforça, portanto, que a utilização de instrumentos tecnológicos no âmbito investigativo não autoriza flexibilização automática das garantias fundamentais. Ao contrário, a crescente sofisticação dos mecanismos digitais intensifica a necessidade de controle jurisdicional e observância rigorosa dos limites constitucionais relacionados à obtenção da prova.

Assim, a *ratio decidendi* do HC 51.531/DF demonstra que a proteção constitucional da intimidade permanece plenamente aplicável ao ambiente digital. A validade da prova eletrônica exige não apenas relevância investigativa ou autenticidade técnica, mas também conformidade material com os direitos fundamentais assegurados pela Constituição Federal.

5.3 A volatilidade dos prints de conversas eletrônicas: análise crítica do REsp 1.548.086/DF

A crescente utilização de aplicativos de mensagens instantâneas transformou profundamente a dinâmica comunicacional contemporânea. Plataformas como WhatsApp, Telegram e sistemas semelhantes passaram a desempenhar papel central nas interações pessoais, profissionais e comerciais, tornando-se fontes recorrentes de elementos probatórios em investigações criminais.

Nesse contexto, tornou-se cada vez mais comum a apresentação de capturas de tela (*screenshots* ou prints) como mecanismo destinado à comprovação de diálogos supostamente relevantes à persecução penal. A aparente simplicidade desse instrumento, entretanto, passou a gerar importantes questionamentos relacionados à autenticidade, integridade e confiabilidade do conteúdo digital apresentado em juízo.

O Superior Tribunal de Justiça enfrentou essa discussão no julgamento do Recurso Especial nº 1.548.086/DF, de relatoria da Ministra Maria Thereza de Assis Moura, firmando entendimento relevante acerca da insuficiência dos prints como elemento probatório autônomo.

Ao examinar a controvérsia, a Corte reconheceu que a simples reprodução visual de mensagens eletrônicas não assegura, por si só, a autenticidade do conteúdo apresentado, especialmente diante da facilidade contemporânea de manipulação dos registros digitais.

> A reprodução de mensagens eletrônicas por meio de capturas de tela não possui mecanismos próprios capazes de assegurar autenticidade, integridade e confiabilidade suficientes para utilização isolada como elemento probatório em persecução penal. A fragilidade estrutural desse tipo de registro exige confirmação mediante outros elementos capazes de demonstrar preservação adequada do conteúdo digital apresentado.
> (STJ, REsp 1.548.086/DF, Rel. Min. Maria Thereza de Assis Moura)

A Corte reconheceu, portanto, que capturas de tela, isoladamente consideradas, não apresentam grau de confiabilidade suficiente para sustentar condenação criminal quando desacompanhadas de perícia técnica ou de outros elementos probatórios destinados à verificação de autenticidade.

A relevância do precedente ultrapassa a simples discussão relacionada a imagens de conversas eletrônicas. A *ratio decidendi* do julgamento encontra fundamento na própria natureza tecnológica dos aplicativos contemporâneos e na fragilidade estrutural da evidência digital.

Eoghan Casey observa que a prova digital possui natureza intrinsecamente mutável, sendo passível de modificações praticamente imperceptíveis ao observador comum (CASEY, 2011). Sob essa perspectiva, a aparência visual do documento eletrônico não constitui garantia suficiente de autenticidade ou integridade probatória.

A preocupação torna-se ainda mais relevante diante das funcionalidades atualmente existentes nos aplicativos de mensagens. Sistemas contemporâneos permitem exclusão seletiva de conteúdos, sincronizações automáticas, edições de registros e manipulações realizadas simultaneamente em múltiplos dispositivos conectados.

O WhatsApp Web, por exemplo, possibilita determinadas alterações capazes de produzir inconsistências relacionadas ao histórico das comunicações. Mensagens podem ser apagadas, removidas ou modificadas em situações específicas, dificultando verificação posterior acerca da integridade do conteúdo originalmente produzido.

A simples captura de tela, portanto, não assegura que a informação apresentada corresponda integralmente ao diálogo efetivamente realizado entre os interlocutores. O problema deixa de envolver apenas existência material do conteúdo e passa a alcançar a própria confiabilidade do mecanismo utilizado para sua preservação.

Nesse ponto, a construção desenvolvida pelo STJ aproxima-se diretamente da perspectiva apresentada por Patrícia Peck Pinheiro. Segundo a autora, a confiabilidade da prova digital exige mecanismos técnicos capazes de assegurar rastreabilidade, preservação e integridade dos dados apresentados judicialmente (PECK PINHEIRO, 2018).

Enquanto o Superior Tribunal de Justiça evidencia a fragilidade dos prints isolados, Patrícia Peck Pinheiro demonstra que a validade da prova eletrônica depende da existência de procedimentos técnicos destinados à preservação da autenticidade do conteúdo digital. As abordagens convergem para conclusão comum: aparência visual não se confunde com confiabilidade probatória.

A decisão do STJ revela mudança significativa na compreensão contemporânea da prova digital. O debate deixa de concentrar-se exclusivamente na existência da informação eletrônica e passa a envolver análise crítica acerca da forma pela qual o conteúdo foi produzido, armazenado, preservado e apresentado em juízo.

Sob essa perspectiva, o REsp nº 1.548.086/DF estabelece parâmetro jurisprudencial relevante ao reconhecer que a validade da prova digital exige mais do que mera apresentação visual do conteúdo eletrônico. Exige demonstração efetiva de autenticidade, integridade e preservação técnica compatíveis com as garantias constitucionais do processo penal democrático.

> A confiabilidade da prova digital depende da possibilidade de verificação técnica de sua integridade e rastreabilidade, sendo insuficiente a mera aparência visual do conteúdo eletrônico quando ausentes mecanismos destinados à preservação da autenticidade do registro apresentado. A fragilidade estrutural das comunicações digitais exige observância de procedimentos capazes de assegurar que o material produzido em juízo corresponda efetivamente às informações originalmente geradas no ambiente eletrônico.
> (STJ, REsp 1.548.086/DF)

A construção jurisprudencial desenvolvida pelo Superior Tribunal de Justiça evidencia mudança significativa na compreensão contemporânea da prova digital. O debate deixa de concentrar-se exclusivamente na existência formal da informação eletrônica e passa a envolver

análise crítica acerca da forma pela qual o conteúdo foi produzido, preservado e apresentado em juízo.

Sob essa perspectiva, o REsp nº 1.548.086/DF consolida entendimento segundo o qual a validade da prova digital não pode fundamentar-se apenas na aparência visual do conteúdo eletrônico. A admissibilidade probatória exige observância de mecanismos técnicos destinados à preservação da autenticidade, integridade e rastreabilidade da evidência digital.

Percebe-se, portanto, que o precedente estabelece importante limitação à utilização indiscriminada de prints de conversas eletrônicas no processo penal. A decisão demonstra que a crescente utilização de tecnologias digitais na atividade investigativa não afasta a necessidade de rigor técnico e observância das garantias constitucionais inerentes ao devido processo legal.

5.4 A consulta direta ao aparelho celular e a inadmissibilidade da prova: análise do HC 828.054/RN

A discussão relacionada à integridade da prova digital ganhou novos contornos com o julgamento do Habeas Corpus nº 828.054/RN pelo Superior Tribunal de Justiça. A controvérsia examinada pela Quinta Turma envolvia situação em que dados extraídos de aparelho celular foram utilizados na persecução penal sem observância de procedimentos técnicos especializados destinados à preservação da autenticidade do material.

No caso analisado, a obtenção das informações ocorreu mediante acesso direto ao dispositivo eletrônico, sem utilização de softwares extratores, mecanismos de duplicação forense ou técnicas especializadas de preservação digital. Embora aparentemente operacional, a questão produziu debate relevante acerca da confiabilidade da prova eletrônica e dos riscos decorrentes da manipulação inadequada do aparelho investigado.

Ao examinar a controvérsia, o Ministro Joel Ilan Paciornik destacou que evidências digitais exigem cuidados específicos em razão de sua suscetibilidade a alterações automáticas e modificações tecnicamente imperceptíveis.

> A obtenção de dados digitais extraídos diretamente de aparelhos eletrônicos exige observância de procedimentos técnicos aptos à preservação da integridade do conteúdo investigado. A ausência de mecanismos especializados destinados à coleta e documentação da prova eletrônica compromete a confiabilidade do material produzido e impede verificação segura acerca da autenticidade das informações posteriormente apresentadas em juízo. (STJ, HC 828.054/RN, Rel. Min. Joel Ilan Paciornik)

A Corte reconheceu, portanto, que a inexistência de protocolos técnicos claros relacionados à coleta, armazenamento e análise do conteúdo eletrônico compromete significativamente a confiabilidade do material probatório produzido. A *ratio decidendi* desenvolvida no julgamento possui relevância especial porque desloca a discussão do campo exclusivamente jurídico da licitude para o campo técnico da preservação da integridade digital.

Não se tratava apenas de verificar existência de autorização judicial para acesso ao aparelho celular. O problema central consistia em avaliar se os procedimentos empregados eram suficientemente adequados para assegurar preservação autêntica das informações obtidas durante a investigação criminal.

Eoghan Casey observa que simples interações com dispositivos eletrônicos podem produzir alterações automáticas em metadados internos, registros sistêmicos e informações digitais invisíveis ao usuário comum (CASEY, 2011). A análise desenvolvida pelo autor dialoga diretamente com os fundamentos apresentados pelo Superior Tribunal de Justiça.

Aplicativos de mensagens instantâneas frequentemente alteram informações relativas a horários de acesso, sincronizações automáticas, status de leitura e registros internos simplesmente em razão do manuseio do aparelho. Assim, a consulta direta ao dispositivo eletrônico cria risco concreto de modificação involuntária do conteúdo posteriormente utilizado como elemento probatório.

Nesse contexto, a construção jurisprudencial desenvolvida pelo STJ aproxima-se da perspectiva apresentada por Pierpaolo Bottini, segundo a qual a utilização de mecanismos tecnológicos na persecução penal exige aproximação efetiva entre Direito e informática forense, sob pena de comprometimento da legitimidade jurisdicional (BOTTINI, 2021).

A convergência entre doutrina e jurisprudência evidencia compreensão contemporânea segundo a qual a validade da prova digital não depende exclusivamente de autorização judicial ou relevância investigativa. Exige, igualmente, observância de protocolos técnico-científicos destinados à preservação da autenticidade, rastreabilidade e integridade da evidência eletrônica.

> A simples manipulação direta de dispositivos eletrônicos pode produzir alterações relevantes em registros internos, metadados e informações sistêmicas, circunstância que exige adoção de procedimentos especializados destinados à preservação técnica da evidência digital e à manutenção de sua confiabilidade probatória.
> (STJ, HC 828.054/RN)

Dessa forma, o HC nº 828.054/RN consolidou entendimento relevante ao reconhecer que a ausência de protocolos especializados de preservação pode comprometer admissibilidade da prova eletrônica. O precedente demonstra que a crescente sofisticação tecnológica da atividade investigativa impõe necessidade de rigor técnico compatível com as garantias constitucionais inerentes ao processo penal democrático.

5.5 O registro documental e a quebra da cadeia de custódia: análise do RHC 143.169/RJ

A crescente preocupação jurisprudencial relacionada à integridade da prova digital alcançou novo estágio no julgamento do Recurso em Habeas Corpus nº 143.169/RJ pelo Superior Tribunal de Justiça. No caso analisado, discutiu-se a ausência de documentação adequada acerca dos procedimentos empregados durante coleta, armazenamento, manipulação e preservação dos dados digitais utilizados na persecução penal.

A controvérsia deslocou o debate para aspecto frequentemente negligenciado na atividade investigativa contemporânea: a necessidade de registro integral do percurso percorrido pela prova eletrônica desde sua obtenção até apresentação em juízo. A Quinta Turma reconheceu que a inexistência de documentação clara relacionada às etapas de manipulação do vestígio digital compromete diretamente a autenticidade e a confiabilidade do material produzido.

Ao examinar a matéria, o Superior Tribunal de Justiça consolidou entendimento segundo o qual a cadeia de custódia não constitui mera formalidade procedimental, mas mecanismo indispensável à preservação da integridade probatória.

> A ausência de registros claros relacionados ao percurso da prova compromete a verificação de sua autenticidade e reduz a confiabilidade processual do material apresentado. A preservação da cadeia de custódia exige documentação contínua acerca dos procedimentos empregados durante coleta, armazenamento, manipulação e análise da evidência digital, permitindo controle efetivo sobre integridade e rastreabilidade do vestígio probatório. (STJ, RHC 143.169/RJ)

A compreensão adotada pelo Superior Tribunal de Justiça evidencia que a cadeia de custódia deixou de representar simples formalidade procedimental para assumir função central na preservação da confiabilidade probatória. A ausência de documentação adequada impede verificação segura acerca da forma pela qual o vestígio digital foi coletado, armazenado e manipulado ao longo da investigação criminal.

Nesse contexto, a validade da prova eletrônica passa a depender não apenas do conteúdo apresentado em juízo, mas também da possibilidade de reconstrução integral do percurso técnico percorrido pela evidência digital. Sem registros contínuos relacionados aos procedimentos empregados, torna-se impossível identificar quem teve acesso ao material, quais instrumentos foram utilizados e se houve efetiva preservação da integridade do conteúdo produzido.

Renato Brasileiro de Lima sustenta que a preservação da autenticidade probatória exige documentação contínua de todas as etapas relacionadas ao vestígio investigativo, permitindo controle efetivo sobre integridade e rastreabilidade da prova (BRASILEIRO DE LIMA, 2020). Em perspectiva semelhante, Patrícia Peck Pinheiro afirma que a confiabilidade da evidência digital depende da possibilidade de reconstrução integral do histórico relacionado ao material analisado (PECK PINHEIRO, 2018).

Percebe-se, portanto, importante convergência entre doutrina e jurisprudência. A quebra da cadeia de custódia deixa de representar mera irregularidade burocrática e passa a comprometer diretamente a admissibilidade e a confiabilidade da prova digital no processo penal.

A decisão proferida no RHC nº 143.169/RJ demonstra amadurecimento jurisprudencial relevante ao reconhecer que a autenticidade probatória exige simultaneamente validade jurídica, preservação técnico-científica e rastreabilidade contínua da evidência eletrônica.

6 CONSIDERAÇÕES FINAIS

A presente pesquisa buscou analisar a validade da prova digital no processo penal brasileiro e os meios juridicamente legítimos de sua obtenção, considerando os desafios impostos pela crescente digitalização das relações sociais e pela transformação tecnológica da atividade investigativa contemporânea.

Ao longo do estudo, verificou-se que a expansão dos ambientes digitais produziu profundas alterações na dinâmica probatória do processo penal. A migração significativa das interações humanas para plataformas eletrônicas, redes sociais, aplicativos de mensagens e dispositivos informáticos fez com que os vestígios digitais passassem a ocupar posição central na persecução penal contemporânea.

Entretanto, constatou-se que a prova digital possui características próprias que a diferenciam substancialmente das provas tradicionalmente concebidas pelo direito processual penal. Sua volatilidade, fragilidade estrutural e suscetibilidade a alterações imperceptíveis exigem observância rigorosa de procedimentos técnicos destinados à preservação da autenticidade, integridade e rastreabilidade das informações eletrônicas.

Nesse contexto, verificou-se que a validade da evidência digital não depende exclusivamente de sua utilidade investigativa ou de sua capacidade de demonstrar determinado fato juridicamente relevante. A admissibilidade probatória exige simultaneamente legitimidade jurídica e confiabilidade técnico-científica, impondo respeito às garantias fundamentais previstas pela Constituição Federal e aos mecanismos técnicos relacionados à cadeia de custódia.

A análise do arcabouço normativo brasileiro demonstrou que a legislação nacional passou progressivamente a incorporar instrumentos destinados à proteção da privacidade e à regulamentação da obtenção de dados eletrônicos. A Lei Carolina Dieckmann, o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais e o Pacote Anticrime representam importantes avanços normativos voltados à construção de parâmetros jurídicos aplicáveis à investigação digital e à preservação da integridade probatória.

Todavia, verificou-se que a evolução legislativa não eliminou as dificuldades interpretativas relacionadas à obtenção e utilização da prova digital no processo penal. A constante evolução tecnológica produz novas modalidades de obtenção de dados, exigindo releitura permanente das

garantias constitucionais relacionadas à intimidade, privacidade, sigilo das comunicações e devido processo legal.

A pesquisa também evidenciou importante amadurecimento jurisprudencial por parte do Supremo Tribunal Federal e do Superior Tribunal de Justiça. Os precedentes analisados demonstram crescente preocupação dos tribunais superiores com a preservação da cadeia de custódia, a necessidade de autorização judicial fundamentada, a proteção da intimidade e a confiabilidade técnica da evidência digital.

Observou-se que a jurisprudência contemporânea passou a reconhecer que a simples existência material do conteúdo eletrônico não é suficiente para assegurar validade probatória. A autenticidade da prova digital depende da observância de procedimentos especializados de coleta, armazenamento, preservação e documentação capazes de impedir alterações indevidas e garantir rastreabilidade integral do vestígio eletrônico.

Nesse cenário, confirmou-se a hipótese inicialmente levantada pela pesquisa: a admissibilidade da prova digital no processo penal brasileiro exige equilíbrio permanente entre eficiência investigativa e proteção das garantias fundamentais. O avanço tecnológico não autoriza flexibilização indiscriminada dos limites constitucionais da atividade investigativa estatal.

Conclui-se, portanto, que a construção de um processo penal compatível com a realidade digital contemporânea depende da conjugação entre rigor técnico, controle jurisdicional e respeito absoluto aos direitos fundamentais. A preservação da legitimidade democrática da persecução penal exige que a inovação tecnológica permaneça permanentemente subordinada aos limites constitucionais estabelecidos pelo Estado Democrático de Direito.

Assim, mais do que simples instrumento de modernização investigativa, a prova digital representa verdadeiro desafio epistemológico ao processo penal contemporâneo, impondo releitura constitucional capaz de compatibilizar desenvolvimento tecnológico, eficiência investigativa e proteção da dignidade humana.

REFERÊNCIAS

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 3 dez. 2012.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Diário Oficial da União: seção 1, Brasília, DF, 24 dez. 2019.

BRASIL. Superior Tribunal de Justiça. Habeas Corpus nº 51.531/DF. Relator: Ministro Arnaldo Esteves Lima. Brasília, DF. Diário da Justiça Eletrônico.

BRASIL. Superior Tribunal de Justiça. Habeas Corpus nº 828.054/RN. Relator: Ministro Joel Ilan Paciornik. Brasília, DF. Diário da Justiça Eletrônico.

BRASIL. Superior Tribunal de Justiça. Recurso em Habeas Corpus nº 143.169/RJ. Relator: Ministro Ribeiro Dantas. Brasília, DF. Diário da Justiça Eletrônico.

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1.548.086/DF. Relatora: Ministra Maria Thereza de Assis Moura. Brasília, DF. Diário da Justiça Eletrônico.

BRASIL. Supremo Tribunal Federal. Habeas Corpus nº 91.867/SP. Relator: Ministro Cezar Peluso. Brasília, DF. Diário da Justiça Eletrônico.

BRASILEIRO DE LIMA, Renato. Manual de processo penal. 8. ed. Salvador: JusPodivm, 2020.
BOTTINI, Pierpaolo Cruz. Crimes informáticos e investigação digital. São Paulo: Revista dos Tribunais, 2021.

CASEY, Eoghan. Digital evidence and computer crime. 3. ed. Burlington: Academic Press, 2011.
DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

LOPES JR., Aury. Direito processual penal. 18. ed. São Paulo: Saraiva Educação, 2021.
MORAES DA ROSA, Alexandre. Guia do processo penal conforme a teoria dos jogos. 6. ed. Florianópolis: EMais, 2019.

NUCCI, Guilherme de Souza. Código de processo penal comentado. 19. ed. Rio de Janeiro: Forense, 2020.

PECK PINHEIRO, Patrícia. Direito digital. 6. ed. São Paulo: Saraiva, 2018.