

OS DESAFIOS DA PERSECUÇÃO PENAL FRENTE AOS CRIMES CIBERNÉTICOS: LIMITES DA PROVA DIGITAL E A NECESSIDADE DE ADAPTAÇÃO DO PROCESSO PENAL BRASILEIRO

THE CHALLENGES OF CRIMINAL PROSECUTION REGARDING CYBERCRIMES: LIMITS OF DIGITAL EVIDENCE AND THE NEED TO ADAPT BRAZILIAN CRIMINAL PROCEDURE

LOS DESAFÍOS DEL ENJUICIAMIENTO PENAL EN MATERIA DE CIBERDELITOS: LÍMITES DE LA PRUEBA DIGITAL Y NECESIDAD DE ADAPTAR EL PROCEDIMIENTO PENAL BRASILEÑO

Sara Eduarda Ferreira Batista¹

Maria Eduarda Vieira da Silva²

Letícia Vivianne Miranda Cury³

RESUMO: Este artigo analisa os desafios impostos pelos crimes cibernéticos à persecução penal brasileira, com ênfase nos limites jurídicos e epistemológicos da prova digital e na necessidade de adaptação do processo penal. Parte-se da constatação de que a digitalização ampliou a capacidade investigativa, mas também introduziu vestígios imateriais, voláteis, dispersos, clonáveis e sujeitos a alteração, o que exige procedimentos técnicos capazes de assegurar autenticidade, integridade e rastreabilidade. O estudo examina a tensão entre eficiência investigativa e proteção da intimidade, da vida privada, do sigilo das comunicações, da autodeterminação informativa e do devido processo legal, além de analisar a cadeia de custódia prevista no Código de Processo Penal e o uso da função *hash* como mecanismo de verificação da integridade, sem tratá-la como garantia absoluta de autenticidade. A jurisprudência do Superior Tribunal de Justiça, sobretudo em casos envolvendo WhatsApp e extração de dados de dispositivos eletrônicos, evidencia dificuldade de uniformização dos critérios de admissibilidade e valoração. Sustenta-se que adaptar o processo penal não significa flexibilizar garantias, mas construir parâmetros específicos para coleta, preservação, documentação, perícia, acesso e contraditório sobre dados digitais. Conclui-se pela necessidade de disciplina normativa mais detalhada, capacitação técnica dos agentes públicos, padronização forense e fortalecimento do controle judicial, preservando ao mesmo tempo a efetividade da persecução penal e os direitos fundamentais. Nesse cenário, a modernização processual deve incorporar criptografia e ciência de dados, com controles verificáveis desde a descoberta do vestígio até sua apreciação judicial segura.

Palavras-chave: Crimes cibernéticos. Prova digital. Cadeia de custódia.

¹ Graduanda do curso Direito pelo Centro Universitário São Lucas - Afya.

² Graduanda do curso Direito pelo Centro Universitário São Lucas - Afya.

³ Mestre em Corrupção e Estado de Direito e Mestre em Direito Penal. Ambos pela Universidade de Salamanca.

ABSTRACT: This article analyzes the challenges posed by cybercrimes to Brazilian criminal prosecution, emphasizing the legal and epistemological limits of digital evidence and the need to adapt criminal procedure. It begins with the premise that digitalization has expanded investigative capacity but also introduced traces that are intangible, volatile, dispersed, clonable, and susceptible to alteration, thereby requiring technical procedures capable of ensuring authenticity, integrity, and traceability. The study examines the tension between investigative efficiency and the protection of intimacy, private life, the confidentiality of communications, informational self-determination, and due process of law. It also analyzes the chain of custody provisions in the Code of Criminal Procedure and the use of hash functions as an integrity verification mechanism, without treating them as an absolute guarantee of authenticity. Case law from the Superior Court of Justice—particularly regarding cases involving WhatsApp and data extraction from electronic devices—highlights the difficulty of standardizing criteria for admissibility and evidentiary weight. The argument is made that adapting criminal procedure does not mean relaxing legal safeguards, but rather establishing specific parameters for the collection, preservation, documentation, forensic analysis, access, and adversarial scrutiny of digital data. The article concludes by calling for more detailed regulatory frameworks, technical training for public officials, forensic standardization, and strengthened judicial oversight, all while balancing the effectiveness of criminal prosecution with the protection of fundamental rights. In this context, procedural modernization must incorporate encryption and data science, featuring verifiable controls spanning from the initial discovery of the evidence to its secure judicial assessment.

Keywords: Cybercrimes. Digital evidence. Chain of custody.

RESUMEN: Este artículo analiza los desafíos que plantean los ciberdelitos para la persecución penal en Brasil, haciendo hincapié en los límites jurídicos y epistemológicos de la prueba digital y en la necesidad de adaptar el procedimiento penal. Parte de la premisa de que la digitalización ha ampliado la capacidad investigativa, pero también ha introducido rastros intangibles, volátiles, dispersos, clonables y susceptibles de alteración, lo que exige procedimientos técnicos capaces de garantizar la autenticidad, la integridad y la trazabilidad. El estudio examina la tensión entre la eficacia de la investigación y la protección de la intimidad, la vida privada, la confidencialidad de las comunicaciones, la autodeterminación informativa y el debido proceso legal. Asimismo, analiza las disposiciones sobre la cadena de custodia en el Código de Procedimiento Penal y el uso de funciones *hash* como mecanismo de verificación de integridad, sin considerarlas una garantía absoluta de autenticidad. La jurisprudencia del Tribunal Superior de Justicia —especialmente en casos relacionados con WhatsApp y la extracción de datos de dispositivos electrónicos— pone de relieve la dificultad de estandarizar criterios de admisibilidad y valor probatorio. Se argumenta que adaptar el procedimiento penal no implica flexibilizar las garantías jurídicas, sino establecer parámetros específicos para la recolección, preservación, documentación, análisis forense, acceso y examen contradictorio de los datos digitales. El artículo concluye abogando por marcos normativos más detallados, capacitación técnica para los funcionarios públicos, estandarización forense y un control judicial reforzado, todo ello equilibrando la eficacia de la persecución penal con la protección de los derechos fundamentales. En este contexto, la modernización procesal debe incorporar el cifrado y la ciencia de datos, contando con controles verificables que abarquen desde el hallazgo inicial de la prueba hasta su valoración judicial segura.

Palabras clave: Ciberdelitos. Prueba digital. Cadena de custodia.

I. INTRODUÇÃO

A transformação tecnológica modificou profundamente as relações sociais, econômicas e comunicacionais, com efeitos relevantes sobre a criminalidade. A expansão da internet, dos dispositivos móveis, das redes sociais, dos aplicativos de mensagens e dos serviços digitais, criou espaços para a prática de ilícitos e, ao mesmo tempo, passou a gerar volume crescente de informações potencialmente relevantes para a investigação criminal.

Nesse sentido, a prova digital, portanto, deixou de ocupar posição periférica na persecução penal. Conversas eletrônicas, fotografias, vídeos, dados de localização, registros de acesso, arquivos armazenados em dispositivos, metadados e informações mantidas por provedores podem ser decisivos na reconstrução de fatos criminosos. Fisberg (2025, p. 3) destaca que a tecnologia atravessa praticamente toda espécie de delito, de modo que conversas, áudios, imagens, localizações, metadados, históricos de pesquisa e publicações em redes sociais podem constituir elementos de convicção.

Dessa forma, essa realidade produz uma contradição: quanto maior a capacidade tecnológica de coleta e processamento de informações, maior também a possibilidade de intervenção na intimidade e na vida privada dos indivíduos, já que informações extremamente pessoais podem estar reunidas em um único dispositivo eletrônico.

3

Nesse contexto, formula-se o problema de pesquisa: em que medida os atuais instrumentos do processo penal brasileiro são capazes de assegurar a efetividade da persecução penal diante dos crimes cibernéticos, sem comprometer os direitos fundamentais e a confiabilidade da prova digital?

O objetivo geral é analisar os principais desafios jurídicos e epistemológicos relacionados à obtenção, preservação e valoração da prova digital no processo penal brasileiro, verificando a necessidade de adaptação dos mecanismos tradicionais de investigação e produção probatória.

A hipótese sustentada é a de que o processo penal brasileiro já possui instrumentos importantes para disciplinar a prova digital, sobretudo a partir da regulamentação da cadeia de custódia, mas ainda não dispõe de disciplina suficientemente específica para as particularidades da coleta, preservação, extração, autenticação e interpretação dos vestígios digitais.

2. FUNDAMENTAÇÃO EPISTEMOLÓGICA

A análise da prova digital exige uma perspectiva epistemológica jurídica⁴ porque a questão central não está apenas em saber se determinado dado foi coletado, mas se é possível demonstrar racionalmente que ele corresponde ao vestígio originalmente encontrado e que não sofreu alteração indevida durante sua trajetória até o processo.

A prova penal possui, nesse sentido, uma dimensão cognitiva: sua função é fornecer elementos capazes de sustentar uma conclusão racional sobre a ocorrência de determinado fato. Por isso, a confiabilidade da prova depende não apenas de seu conteúdo, mas das condições de sua produção, preservação, transmissão e análise. O problema é particularmente sensível quando se trata de dados digitais. A prova física normalmente apresenta materialidade perceptível, enquanto a prova digital pode ser reproduzida, copiada, transferida e modificada sem alteração perceptível em sua aparência o próprio conceito de originalidade assume configuração diferente nesse ambiente. Fisberg (2025, p. 13) observa que a distinção tradicional entre original e cópia perde parte de sua pertinência no ambiente digital, justamente porque o dado pode ser reproduzido sem perda de sua essência.

Nesse cenário, o conhecimento produzido pelo processo penal não pode depender exclusivamente da aparência do arquivo ou da confiança subjetiva no agente que realizou a coleta: é necessário estabelecer mecanismos objetivos de controle. A função hash insere-se nesse contexto como algoritmo matemático capaz de produzir uma representação padronizada de determinado conjunto de dados, permitindo posterior comparação para verificar se houve alteração. Fisberg (2025, p. 35) destaca que a função *hash* pode contribuir para a verificação da integridade dos dados digitais, embora sua utilização deva estar associada à documentação rigorosa da cadeia de custódia.

Contudo, o *hash* não pode ser transformado em uma espécie de certificado absoluto de autenticidade. O cálculo realizado sobre um arquivo demonstra, essencialmente, a correspondência entre aquele arquivo e determinado código produzido pelo algoritmo, não demonstra, isoladamente, que o arquivo originalmente apresentado seja verdadeiro ou que corresponda ao vestígio efetivamente encontrado. Fisberg (2025, p. 27) registra, inclusive, que a

⁴JUSBRASIL. A importância da Epistemologia na pesquisa jurídica. Disponível em: <<https://www.jusbrasil.com.br/artigos/a-importancia-da-epistemologia-na-pesquisa-juridica/2791564839>>. Acesso em: 8 ago. 2026.

simples existência do *hash* não permite concluir automaticamente pela autenticidade e integridade do arquivo.

Da perspectiva epistemológica, portanto, a prova digital deve ser compreendida como resultado de uma cadeia de procedimentos técnicos e jurídicos. O valor probatório não decorre exclusivamente do dado, mas da possibilidade de reconstruir sua trajetória e controlar racionalmente as condições em que foi obtido.

3. DISCUSSÃO TEÓRICA

3.1. Crimes cibernéticos e transformação da persecução penal

Inicialmente, a expansão da tecnologia alterou tanto os instrumentos usados pelos criminosos quanto a forma como os órgãos estatais investigam os delitos. Crimes essencialmente digitais convivem hoje com crimes tradicionais, homicídio, organização criminosa, fraude, crimes sexuais, corrupção, que também costumam deixar vestígios digitais relevantes. Fisberg (2025, p. 3) observa que a tecnologia pode estar relacionada a praticamente qualquer modalidade delitiva, fornecendo elementos como conversas, áudios, imagens, geolocalização, metadados e publicações em redes sociais.

Nesse sentido, a prova digital soma a isso características próprias que a distinguem da prova física tradicional: imaterialidade, volatilidade, possibilidade de clonagem, desprendimento do suporte físico e necessidade de intermediação tecnológica para sua compreensão. Conforme explica Saad, Rossi e Partata (2024, p. 5) ressaltam que os dados digitais podem sofrer alterações intencionais ou involuntárias mediante simples modificação da sequência numérica que os constitui.

Portanto, a prova digital deixou, assim, de ser um instrumento excepcional para se tornar componente estrutural da persecução penal contemporânea, exigindo que a investigação criminal lide simultaneamente com o ambiente físico e o digital.

3.1.2. Crimes cibernéticos e a expansão da criminalidade no ambiente virtual

Considerando que nos últimos 10 anos, a expansão das tecnologias digitais modificou significativamente as formas de interação social e, paralelamente, criou oportunidades para a prática de delitos. A utilização cotidiana de smartphones, redes sociais, aplicativos de

mensagens, plataformas digitais e serviços financeiros eletrônicos ampliou não só a velocidade e o alcance das relações sociais e econômicas, mas também possibilitou a adaptação de práticas criminosas aos ambientes virtuais. Nesse contexto, a criminalidade digital passou a representar um desafio crescente para as instituições de segurança pública, especialmente diante da dificuldade de identificação dos autores, da circulação transnacional das informações e da necessidade de obtenção e preservação de evidências digitais.

Nessa perspectiva, entre os crimes relacionados ao ambiente digital, destaca-se o estelionato por meio eletrônico, que apresentou expressivo crescimento no Brasil. Segundo o Anuário Brasileiro de Segurança Pública 2026, foram registrados 346.753 casos de estelionato por meio eletrônico em 2025, contra 286.226 em 2024, representando aumento de 20,6%. A taxa nacional passou de 204,2 para 246,2 ocorrências por 100 mil habitantes no período (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2026, p. 120).

Ademais, é importante destacar que a dimensão desse fenômeno se torna ainda mais evidente quando analisada a evolução do estelionato em geral. Em 2025, foram registradas 2.261.055 ocorrências, enquanto em 2018 haviam sido contabilizadas 426.799. Segundo o Anuário, essa evolução corresponde a um crescimento de 429,8% ao longo do período, evidenciando a consolidação do estelionato como importante modalidade da criminalidade patrimonial brasileira. A publicação destaca que os chamados golpes passaram a ocupar posição central nas preocupações da população, sendo que 83,2% dos brasileiros afirmaram temer ser vítimas de fraude pela internet ou pelo celular (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2026, p. 121-122).

A distribuição territorial dos registros também demonstra diferenças importantes entre as unidades da Federação. Em 2025, São Paulo apresentou a maior taxa de estelionato do país, com 1.808,3 ocorrências por 100 mil habitantes, seguido pelo Distrito Federal, com 1.717,0. Entre os estados com taxas superiores a 1.000 ocorrências por 100 mil habitantes estavam Paraná, Rondônia, Santa Catarina, Espírito Santo e Goiás. O destaque de Rondônia é particularmente relevante, pois o Estado constitui a única unidade da Região Norte entre aquelas que apresentaram taxas superiores a esse patamar (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2026, p. 122).

No caso específico de Rondônia, foram registrados 13.985 estelionatos por meio eletrônico em 2025, contra 12.444 em 2024. A taxa estadual passou de 712,6 para 798,3 ocorrências

por 100 mil habitantes, representando crescimento de 12%. O número total de estelionatos no Estado também aumentou, passando de 21.363 registros em 2024 para 23.294 em 2025 (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2026, p. 120).

A criminalidade relacionada às tecnologias digitais, contudo, não se restringe às fraudes patrimoniais. O ambiente virtual também passou a desempenhar papel relevante na prática de diferentes formas de violência contra crianças e adolescentes. Em 2025, foram registrados 4.063 casos de produção, posse ou distribuição de material de abuso sexual infantil, além de 2.464 registros de aliciamento de crianças para fins libidinosos. Também foram contabilizados 1.281 casos de exploração sexual infantil. Esses números demonstram a presença das tecnologias digitais em diferentes manifestações da violência sexual contra crianças e adolescentes (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2026, p. 232).

A evolução histórica desses delitos merece atenção. De acordo com o Anuário, os crimes relacionados à produção, posse e distribuição de material de abuso sexual infantil apresentaram crescimento de 176,7% entre 2021 e 2025. A publicação relaciona essa transformação à intensificação das experiências digitais, à popularização de novas tecnologias e à crescente utilização de plataformas digitais e tecnologias de inteligência artificial generativa (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2026, p. 267).

7

Outro aspecto relevante diz respeito à diferença entre as denúncias realizadas no ambiente digital e os registros formalizados pelas instituições policiais. Em 2025, a Central Nacional de Denúncias da SaferNet recebeu 63.214 imagens de abuso e exploração sexual infantil para análise e tratamento, enquanto as secretarias estaduais de segurança pública contabilizaram 4.063 registros relacionados aos crimes previstos nos arts. 240 a 241-C do Estatuto da Criança e do Adolescente. Embora as duas bases não sejam diretamente comparáveis, o próprio Anuário destaca que essa diferença evidencia que os registros das polícias civis representam apenas uma parcela do sistema de identificação e enfrentamento desse tipo de violência (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2026, p. 269).

O cyberbullying constitui outra manifestação da violência mediada pelas tecnologias digitais. Com a criminalização da intimidação sistemática virtual pela Lei nº 14.811/2024, os registros policiais passaram a apresentar maior visibilidade dessa modalidade. Em 2025, foram contabilizados 677 registros de cyberbullying envolvendo crianças e adolescentes de 0 a 17 anos, correspondentes à taxa de 1,7 ocorrência por 100 mil habitantes dessa faixa etária. No mesmo

período, foram registrados 4.549 casos de bullying presencial. Quando consideradas conjuntamente as duas modalidades, foram contabilizadas 5.226 ocorrências, representando crescimento de 67,3% em relação a 2024 (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2026, p. 252).

A distribuição etária dos registros de cyberbullying também revela uma concentração entre adolescentes. Em 2025, as taxas foram de 3,1 ocorrências por 100 mil habitantes entre crianças de 10 a 13 anos e 4,2 entre adolescentes de 14 a 17 anos. O Anuário observa que o cyberbullying alcança sua maior frequência por volta dos 14 anos, evidenciando a aproximação entre as formas tradicionais e digitais de violência entre pares (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2026, p. 252-253).

Outro indicador que merece ser considerado na análise da criminalidade digital é o roubo e furto de aparelhos celulares. Embora essas condutas não constituam, por si mesmas, crimes cibernéticos, os dispositivos móveis concentram informações pessoais, bancárias e de comunicação que podem ser utilizadas posteriormente para a prática de fraudes e outros delitos digitais. Em 2025, foram registrados 308.723 roubos e 483.561 furtos de celulares no Brasil (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2026, p. 14).

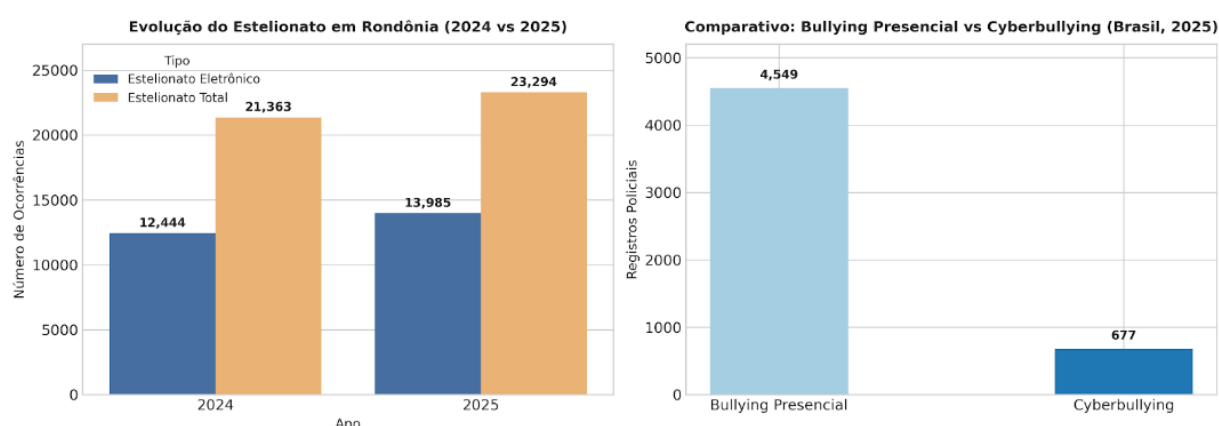
A realidade de Porto Velho merece especial atenção nesse contexto. Entre os municípios brasileiros com mais de 100 mil habitantes, a capital de Rondônia apresentou, em 2025, a sexta maior taxa de roubo e furto de celular, com 1.123,2 ocorrências por 100 mil habitantes. O município ficou atrás apenas de São Luís, Belém, São Paulo, Salvador e Lauro de Freitas (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2026, p. 112-113).

A análise conjunta desses indicadores demonstra que a transformação digital da sociedade também produz mudanças na dinâmica da criminalidade. Os dados do estelionato eletrônico revelam a expansão das fraudes praticadas mediante recursos tecnológicos; os registros de cyberbullying demonstram a transposição de formas tradicionais de violência para as redes digitais; enquanto os crimes relacionados ao material de abuso sexual infantil evidenciam a utilização das plataformas tecnológicas para produção, armazenamento, circulação e identificação de conteúdos relacionados à violência sexual. Portanto, não se trata de fenômeno restrito a uma única modalidade criminosa, mas de um processo de digitalização de diferentes formas de criminalidade.

Esse cenário impõe desafios específicos às instituições responsáveis pela segurança pública. A investigação de crimes digitais exige mecanismos capazes de acompanhar a velocidade das transformações tecnológicas e de lidar com informações produzidas em diferentes plataformas e localidades. No caso dos crimes relacionados ao abuso sexual infantil, por exemplo, o Anuário registra que denúncias podem ser identificadas inicialmente por plataformas digitais, organizações da sociedade civil, organismos internacionais e sistemas especializados, podendo envolver autores, vítimas e provedores situados em diferentes estados ou países.

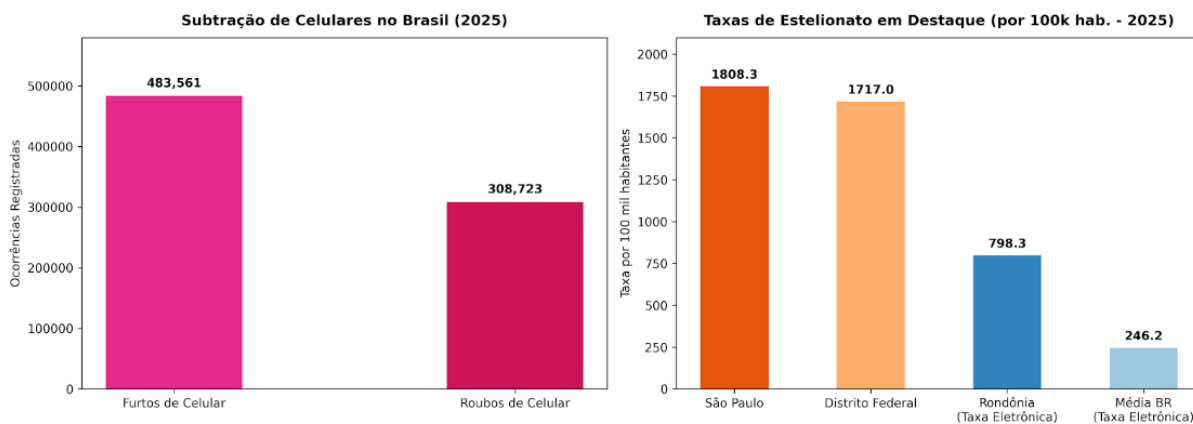
Por conseguinte, o crescimento da criminalidade digital exige que a atuação estatal seja analisada não apenas sob a perspectiva do número de ocorrências registradas, mas também a partir da capacidade institucional de prevenção, registro, investigação e responsabilização dos autores. A expansão dos estelionatos eletrônicos em Rondônia, associada à elevada incidência de roubo e furto de celulares em Porto Velho, demonstra que a temática possui relevância concreta para a segurança pública estadual. Nesse sentido, compreender como a Polícia Civil estrutura sua resposta aos crimes praticados ou mediados por tecnologias digitais constitui importante campo de investigação, sobretudo diante da necessidade de adequação dos recursos humanos, tecnológicos e institucionais às novas formas de criminalidade.

Figura 1: Evolução de crimes digitais 2024-2025



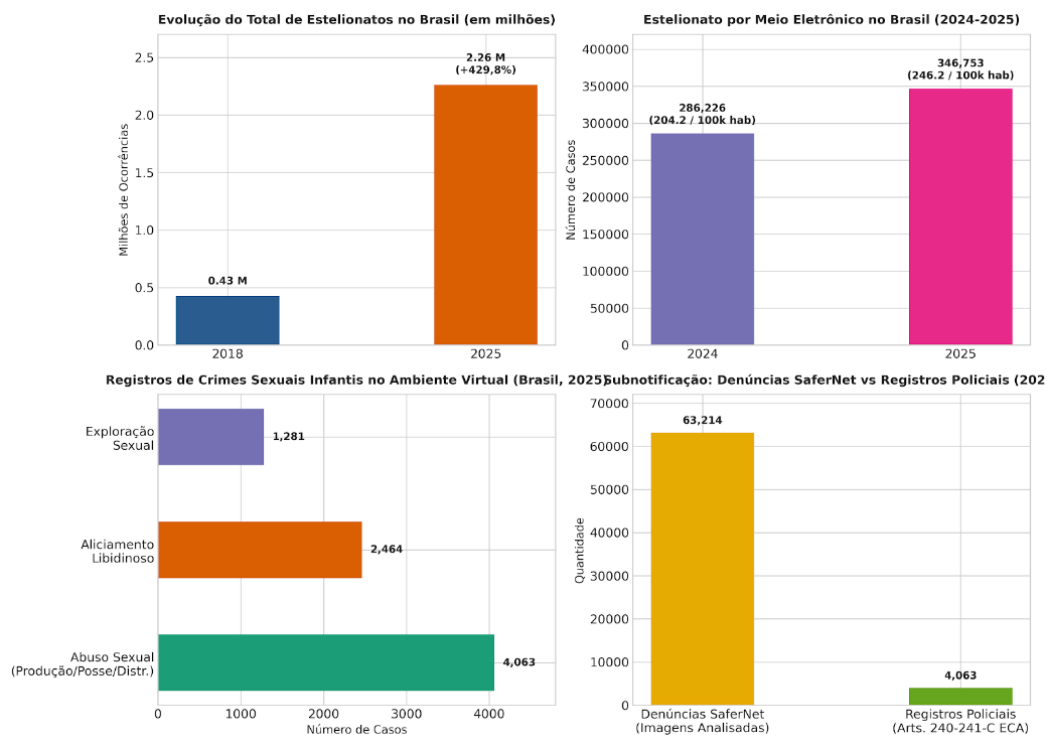
Fonte: Elaborado pelos Autores (2026)

Figura 2: Evolução de crimes digitais 2025



Fonte: Elaborado pelos Autores (2026)

Figura 3: Evolução de crimes digitais 2024-2025



Fonte: Elaborado pelos Autores (2026)

3.2. A natureza peculiar da prova digital

A primeira dificuldade está na própria natureza do objeto probatório. Saad, Rossi e Partata (2024, p. 4-5) definem, que:

A prova digital como dados em formato digital constantes de suporte eletrônico ou transmitidos por redes de comunicação, e identificam características que a diferenciam da prova tradicional: imaterialidade, volatilidade, desprendimento do suporte físico, possibilidade de clonagem e necessidade de intermediação tecnológica.

A volatilidade é a mais problemática dessas características: um dado pode ser excluído, sobrescrito ou automaticamente substituído por mecanismos próprios do sistema. Por isso, a investigação deve atuar com rapidez, mas sem renunciar à documentação, a urgência típica da prova digital não justifica a ausência de registro do procedimento.

3.3. Cadeia de custódia e confiabilidade normativa

A Lei nº 13.964/2019 (Pacote Anticrime) incluiu no Código de Processo Penal os arts. 158-A a 158-F, que disciplinam a cadeia de custódia como o conjunto de procedimentos destinados a documentar a trajetória do vestígio desde seu reconhecimento até o descarte, de modo a permitir o rastreamento de sua posse e manuseio (BRASIL, Lei nº 13.964/2019, art. 158-A do CPP). O objetivo do instituto é garantir a possibilidade de verificar a identidade e a preservação do vestígio ao longo de todo o processo.

11

No caso da prova digital, a cadeia de custódia ganha importância ainda maior porque o vestígio pode ser alterado sem sinais visíveis. Fisberg (2025, p. 27) sustenta que sua documentação constitui exigência fundamental para o controle epistêmico da prova, permitindo reconstruir a trajetória do vestígio e verificar sua correspondência com o que foi apresentado em juízo.

A legislação, contudo, estabelece apenas uma estrutura geral, enquanto as técnicas digitais variam conforme o dispositivo, o sistema operacional, o aplicativo, o serviço de armazenamento e o método de extração empregado. A tarefa do legislador é oferecer garantias mínimas sem tentar congelar tecnicamente procedimentos sujeitos a rápida evolução tecnológica, isso demonstra a relevância de normas técnicas complementares, como a ABNT NBR ISO/IEC 27037:2013, que trata da identificação, coleta, aquisição e preservação de evidências digitais e é hoje referência recorrente na jurisprudência sobre o tema.

3.4. A função *hash*: instrumento relevante, mas não absoluto

A função *hash* é uma das principais ferramentas associadas à integridade da prova digital. Seu funcionamento produz uma sequência de caracteres vinculada matematicamente ao conjunto de dados processado, usualmente por algoritmos como MD5, SHA-1 ou SHA-256, de modo que qualquer alteração no conteúdo tende a produzir um resultado diferente, permitindo verificar se um arquivo sofreu modificação.

O *hash*, todavia, não resolve todos os problemas da prova digital. Uma captura de tela de conversa, por exemplo, pode ter seu *hash* calculado, mas isso preserva apenas aquela imagem: não demonstra a origem da conversa, seus metadados, o contexto da comunicação, nem a inexistência de alterações anteriores à captura. Fisberg (2025, p. 13) chama atenção para essa limitação ao observar que o *hash* calculado sobre uma simples captura de tela tem utilidade restrita, pois não preserva necessariamente informações sobre a fonte, os metadados ou o conteúdo original da comunicação.

O próprio STJ já reconheceu esse limite: no julgamento do RHC 143.169/RJ (5ª Turma, rel. Min. Messod Azulay Neto, fev. 2023), a Corte considerou inadmissível a extração de dados sem o uso de ferramenta forense confiável e auditável, entendendo que o cálculo isolado do *hash*, sem metodologia adequada de extração, não basta para assegurar a integridade do vestígio. O debate, portanto, não deve se reduzir à pergunta sobre a existência do *hash*; a questão central é saber se todo o procedimento de coleta, preservação e análise foi tecnicamente adequado e suficientemente documentado.

12

3.5 A jurisprudência do STJ sobre prova digital e WhatsApp Web

A jurisprudência do Superior Tribunal de Justiça evidencia os desafios concretos da prova digital. Em precedente amplamente divulgado, a Sexta Turma reconheceu a nulidade de mensagens obtidas por print screen do WhatsApp Web, sob o fundamento de que a ferramenta permite o envio e a exclusão de mensagens sem deixar vestígio, o que compromete a verificação da autenticidade e da integridade do conteúdo (STJ, RHC 99.735, 6ª Turma, rel. Min. Nefi Cordeiro; notícia STJ de 9 mar. 2021). Cordeiro e Moraes (2024) analisam essa decisão e destacam que a Corte considerou tanto a ausência de regulamentação adequada do meio de

obtenção quanto a fragilidade da cadeia de custódia, diante da impossibilidade de aferir a autenticidade e a integridade das mensagens (CORDEIRO; MORAIS, 2024, p. 1-2).

Desa forma, o precedente demonstra que a simples apresentação de mensagens não resolve o problema probatório. O processo penal precisa responder a perguntas como: quem realizou a extração, de qual dispositivo, em que momento e por qual método; se houve preservação do conteúdo original; se o dispositivo foi previamente manipulado; se houve geração de cópia forense; quais ferramentas foram utilizadas; se o procedimento foi documentado; e se a defesa teve condições de verificar a metodologia empregada.

Fisberg (2025) mostra que a jurisprudência do STJ ainda apresenta divergências quanto ao tratamento de certas modalidades de extração. O próprio tribunal já registrou entendimentos distintos: enquanto a Sexta Turma fixou, no HC 653.515/RJ (rel. Min. Rogerio Schietti Cruz, j. 23 nov. 2021), que a quebra da cadeia de custódia não gera nulidade automática, devendo ser avaliada caso a caso, decisões posteriores, como a da Quinta Turma no HC 828.054/RN (mai. 2024), consideraram inadmissíveis provas extraídas sem metodologia técnica adequada. Consequentemente, essa oscilação confirma que a evolução jurisprudencial é importante, mas não substitui uma disciplina normativa clara.

3.6 Privacidade, intimidade e persecução penal

A prova digital frequentemente alcança uma quantidade de informação muito superior à necessária para a investigação. A apreensão de um smartphone pode dar acesso a fotografias, mensagens, documentos, localização, histórico de navegação, contatos, dados bancários e informações sobre terceiros, de modo que uma autorização judicial genérica para acessar um dispositivo pode se transformar em verdadeira devassa informacional.

Sousa Mendes (2021, p. 227) observa que a migração para o ciberespaço cria ameaças à privacidade, porque diferentes dimensões da vida humana permanecem armazenadas e potencialmente acessíveis em ambiente digital; o autor destaca que a proteção da privacidade alcança informações guardadas em computadores, servidores, arquivos digitais e e-mails (SOUSA MENDES, 2021, p. 227-228).

Diante desse cenário, a persecução penal precisa observar os critérios de necessidade, adequação e proporcionalidade. Isso não significa reconhecer proteção absoluta aos dados digitais o Estado pode restringir direitos fundamentais quando presentes os pressupostos

constitucionais e legais, mas exige limites claros para evitar que uma investigação específica se converta em acesso indiscriminado à vida privada.

3.7 Os conhecimentos fortuitos e o risco da investigação expansiva

Um problema correlato é a possibilidade de a investigação revelar informações estranhas ao fato que justificou a medida. Sousa Mendes (2021, p. 233) demonstra que o uso de palavras-chave ou mecanismos de filtragem não elimina os chamados conhecimentos fortuitos: informações irrelevantes para a investigação original podem ser identificadas e aproveitadas em outros procedimentos.

O risco cresce quando grandes volumes de dados são submetidos a ferramentas automatizadas de busca. Bachmaier Winter (2025, p. 4) alerta que o processo penal precisa seguir funcionando como marco de proteção do indivíduo diante da ampliação dos poderes estatais, sobretudo diante de tecnologias capazes de produzir vigilância e análise massiva de informações. A expansão tecnológica da investigação deve, portanto, ser acompanhada pela expansão proporcional dos mecanismos de controle.

3.8 A necessidade de uma disciplina jurídica própria

14

A discussão conduz a uma pergunta central: o processo penal brasileiro precisa de disciplina específica para a prova digital? Saad, Rossi e Partata (2024) respondem que sim. Para os autores, a legislação deve fixar requisitos mínimos para a obtenção de provas digitais, capazes de orientar as decisões judiciais que autorizam esses meios de investigação.

Adaptar a disciplina não significa abandonar as categorias tradicionais do processo penal, mas aplicar seus princípios às características próprias da tecnologia. Entre os aspectos que essa disciplina deveria contemplar estão: delimitação do objeto da busca digital; fundamentação específica da decisão judicial; preservação do dispositivo original; realização de cópia forense quando tecnicamente necessária; documentação completa da cadeia de custódia; identificação das ferramentas utilizadas; registro dos procedimentos de extração; preservação dos metadados relevantes; possibilidade de auditoria técnica; garantia de contraditório sobre a metodologia empregada; tratamento dos dados estranhos ao objeto da investigação; regras para conhecimentos fortuitos; proteção das informações de terceiros; critérios para uso de ferramentas automatizadas e técnicas de inteligência artificial.

Não é necessário que a lei detalhe cada ferramenta tecnológica. Basta que fixe garantias, procedimentos e critérios de controle claros o suficiente para que a evolução técnica ocorra sem comprometer direitos fundamentais.

3.9 O papel do devido processo legal na era digital

A adaptação tecnológica do processo penal precisa preservar sua dimensão garantista. Bachmaier Winter (2025, p. 2-4) sustenta que o processo penal liberal tem como eixo a dignidade humana, os direitos fundamentais, a presunção de inocência e a proteção do indivíduo diante do poder público, e alerta que a transformação digital pode alterar a estrutura do processo penal, sobretudo no plano probatório, tornando ainda mais necessário reforçar as garantias processuais. Ao analisar experiências estrangeiras, a autora demonstra que a complexidade técnica da prova eletrônica pode dificultar sua compreensão pelo julgador e limitar o exercício do contraditório: quando uma prova técnica tem peso determinante na condenação, a defesa precisa de condições efetivas para questionar sua origem, metodologia e confiabilidade (BACHMAIER WINTER, 2025, p. 25).

O contraditório contemporâneo, portanto, não pode se limitar ao conteúdo da prova; deve alcançar também o método utilizado para a produzir.

4. METODOLOGIA

A pesquisa possui natureza qualitativa, com caráter exploratório e descritivo, desenvolvida mediante pesquisa bibliográfica, documental e jurisprudencial. A abordagem qualitativa justifica-se pela necessidade de compreender os fundamentos jurídicos, técnicos da prova digital, especialmente quanto à sua confiabilidade, admissibilidade e compatibilidade com os direitos fundamentais.

O caráter exploratório decorre da necessidade de aprofundar a compreensão dos desafios provocados pela digitalização da persecução penal, sobretudo diante de mecanismos tecnológicos ainda sem disciplina específica ou suficientemente detalhada na legislação processual penal brasileira; já a dimensão descritiva concentra-se na identificação das características da prova digital, dos meios utilizados para sua obtenção, dos direitos fundamentais potencialmente afetados e dos mecanismos de preservação da cadeia de custódia.

As fontes principais foram cinco estudos científicos, Cordeiro e Morais (2024), Fisberg (2025), Bachmaier Winter (2025), Saad, Rossi e Partata (2024), Sousa Mendes (2021) e os dados dos crimes foram obtidos por meio do Fórum Brasileiro de Segurança Pública.

A análise documental concentrou-se na legislação processual penal relacionada à prova e à cadeia de custódia, bem como nos fundamentos jurisprudenciais.

5. CONSIDERAÇÕES FINAIS

A análise conduzida neste estudo mostra que os crimes cibernéticos provocaram uma transformação estrutural na persecução penal: o desafio contemporâneo não é apenas investigar novos delitos, mas investigar quase todos os delitos em uma realidade na qual os vestígios digitais ocupam papel cada vez maior.

A prova digital oferece vantagens investigativas significativas, mas exige cautela em razão de características próprias. Imaterialidade, volatilidade, dispersão, possibilidade de clonagem e de alteração tornam inadequada a aplicação automática dos mesmos procedimentos usados para provas físicas. A cadeia de custódia é instrumento importante de controle, mas sua eficácia depende de documentação adequada, conhecimento técnico e procedimentos padronizados. A função *hash*, por sua vez, é ferramenta relevante para verificar a integridade de um arquivo, mas não deve ser tratada como solução absoluta: integridade não se confunde com autenticidade, origem ou contexto.

O exame da jurisprudência do STJ revelou que a matéria ainda apresenta pontos de divergência. Há preocupação crescente com a confiabilidade da prova digital, mas decisões distintas sobre casos semelhantes mostram que critérios mais uniformes ainda são necessários. Por conseguinte, ficou evidente que a modernização da persecução penal não pode ocorrer à custa da privacidade, da intimidade, da autodeterminação informativa, do contraditório e do devido processo legal.

6. CONCLUSÃO

Os crimes cibernéticos desafiam o processo penal brasileiro porque exigem não apenas o domínio de novas tecnologias, mas uma revisão da própria estrutura da atividade probatória. A prova digital tornou-se elemento indispensável da persecução penal contemporânea; sua utilização legítima, porém, depende de demonstrar que o dado apresentado ao Poder Judiciário

é confiável, foi obtido por procedimento juridicamente válido e permaneceu preservado durante toda a sua trajetória.

A hipótese deste estudo confirma-se: o processo penal brasileiro já possui mecanismos relevantes para tratar a prova digital, mas ainda necessita de adaptação normativa, técnica e institucional para responder às particularidades desses vestígios. Essa adaptação não pode significar abandono das garantias fundamentais. O objetivo é tornar o processo penal tecnologicamente adequado e juridicamente controlável, não simplesmente mais invasivo.

A principal mudança necessária está em deixar de avaliar a investigação apenas pelo resultado obtido e passar a exigir também a auditabilidade do caminho percorrido pela prova. A cadeia de custódia, nesse contexto, deve funcionar como instrumento de controle, não como formalidade burocrática: a documentação precisa mostrar quem teve contato com o vestígio, que procedimentos foram realizados, que ferramentas foram usadas, quando ocorreram as intervenções e como os dados foram preservados.

A função *hash* contribui para esse controle, mas deve ser compreendida como parte de um conjunto mais amplo de medidas técnicas. Como se observa a documentação da cadeia de custódia continua essencial independentemente da tecnologia empregada.

A proteção da privacidade também precisa acompanhar a expansão dos poderes investigativos. Ser tecnicamente possível acessar grandes volumes de informação não equivale a estar juridicamente autorizado a fazê-lo de forma indiscriminada. A investigação digital deve ser delimitada pelo objeto da apuração, por decisão judicial fundamentada quando exigida, pela proporcionalidade e pela possibilidade de controle posterior pela defesa. Essa adaptação exige, por fim, atuação coordenada entre Poder Legislativo, Poder Judiciário, Ministério Público, polícia judiciária, Defensoria Pública e advocacia, além de investimento em formação especializada e em infraestrutura de informática forense.

A prova penal tende a se tornar cada vez mais digital. O desafio não é impedir essa transformação, mas garantir que o ganho de eficiência investigativa não sirva de justificativa para reduzir as garantias fundamentais.

REFERÊNCIAS

BACHMAIER WINTER, Lorena. A luta pelas garantias do devido processo e a mudança de paradigma na teoria da prova: do liberalismo à mass surveillance no processo penal europeu. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 11, n. 1, e1164, jan./abr. 2025. DOI: <https://doi.org/10.22197/rbdpp.viii.1164>.

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, ano 157, n. 249, p. 1-18, 24 dez. 2019.

BRASIL. Superior Tribunal de Justiça (5. Turma). Habeas Corpus nº 828.054/RN. Impetrante: Defensoria Pública do Estado do Rio Grande do Norte. Impetrado: Tribunal de Justiça do Estado do Rio Grande do Norte. Relator: Min. Joel Ilan Paciornik, 21 de maio de 2024. *Diário da Justiça Eletrônico*: Brasília, DF, 24 maio 2024.

BRASIL. Superior Tribunal de Justiça (5. Turma). Recurso em Habeas Corpus nº 143.169/RJ. Recorrente: M. V. S. de O. Recorrido: Ministério Público do Estado do Rio de Janeiro. Relator: Min. Messod Azulay Neto, 7 de fevereiro de 2023. *Diário da Justiça Eletrônico*: Brasília, DF, 14 fev. 2023.

BRASIL. Superior Tribunal de Justiça (6. Turma). Habeas Corpus nº 653.515/RJ. Impetrante: Defensoria Pública do Estado do Rio de Janeiro. Impetrado: Tribunal de Justiça do Estado do Rio de Janeiro. Relator: Min. Rogerio Schietti Cruz, 23 de novembro de 2021. *Diário da Justiça Eletrônico*: Brasília, DF, 1 fev. 2022.

BRASIL. Superior Tribunal de Justiça (6. Turma). Recurso em Habeas Corpus nº 99.735/SC. Recorrente: F. H. de S. Recorrido: Ministério Público do Estado de Santa Catarina. Relator: Min. Nefi Cordeiro, 9 de março de 2021. *Diário da Justiça Eletrônico*: Brasília, DF, 16 mar. 2021.

CORDEIRO, Flávio Vinícius Alves; MORAIS, Rafael Matos de Freitas. Prova digital: estudo sobre a decisão do Superior Tribunal de Justiça que reconheceu a nulidade de prova obtida do WhatsApp Web. *Revista Contemporânea*, v. 4, n. 4, p. 1-25, 2024. DOI: <https://doi.org/10.56083/RCV4N4-227>.

FISBERG, Yuri. Função "hash" e a integridade da prova digital. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 11, n. 3, e1227, set./dez. 2025. DOI: <https://doi.org/10.22197/rbdpp.viii.3.1227>.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. Anuário Brasileiro de Segurança Pública 2026. São Paulo: FBSP, 2026. Disponível em: <https://forumseguranca.org.br/wp-content/uploads/2026/07/anuario-2026.pdf>. Acesso em: 8 ago. 2026.

A IMPORTÂNCIA da Epistemologia na pesquisa jurídica. Jusbrasil, 2026. Disponível em: <https://www.jusbrasil.com.br/artigos/a-importancia-da-epistemologia-na-pesquisa-juridica/2791564839>. Acesso em: 15 ago. 2026.

SAAD GIMENES, Marta Cristina Cury; ROSSI, Helena Costa; PARTATA, Pedro Henrique. A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais. Revista Brasileira de Direito Processual Penal, Porto Alegre, v. 10, n. 3, e1071, set./dez. 2024. DOI: <https://doi.org/10.22197/rbdpp.v10i3.1071>.

SOUSA MENDES, Paulo de. A privacidade digital posta à prova no processo penal. Quaestio Facti: Revista Internacional sobre Razonamiento Probatorio, Madrid, n. 2, p. 225-250, 2021. DOI: https://doi.org/10.33115/udg_bib/qf.i2.22487.