Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

OPEN ACCESS

doi.org/10.51891/rease.v12i2.24021

OS DESAFIOS DA INVESTIGAÇÃO POLICIAL ORIENTADA POR DADOS

Ana Maria de Araújo Padilha[1]

RESUMO: A intensificação dos processos de digitalização da vida social e a consolidação da sociedade em rede provocaram profundas transformações no modelo contemporâneo de investigação criminal, deslocando parcela significativa dos vestígios penalmente relevantes para o plano imaterial dos dados digitais. Nesse contexto, a atividade de Polícia Judiciária, especialmente a exercida pelo Delegado de Polícia, passa a lidar com evidências caracterizadas pela volatilidade, fragmentação, dependência de terceiros e mediação por sistemas tecnológicos complexos. O presente estudo analisa os impactos da chamada datificação das relações sociais sobre a lógica investigativa e probatória da persecução penal, com especial atenção aos desafios dogmáticos e práticos relacionados à obtenção, preservação e valoração da prova digital no processo penal brasileiro. A partir de abordagem qualitativa e método dedutivo, com base em pesquisa bibliográfica, análise normativa e exame crítico da prática investigativa, investiga-se o papel da cadeia de custódia digital como instrumento de garantia da autenticidade, integridade e confiabilidade das evidências digitais. Conclui-se que a prova digital demanda tratamento dogmático específico e rigor procedimental reforçado, sob pena de comprometimento da eficácia da persecução penal e da legitimidade do exercício do poder punitivo estatal.

Palavras-chave: Investigação criminal. Prova digital. Cadeia de custódia. Datificação. Processo penal.

ABSTRACT: The intensification of social digitalization processes and the consolidation of the network society have profoundly transformed contemporary criminal investigation models, shifting a significant portion of legally relevant traces to the immaterial domain of digital data. In this context, Judicial Police activity—particularly that performed by Police Chiefs—must increasingly deal with evidence characterized by volatility, fragmentation, third-party dependence, and mediation by complex technological systems. This study analyzes the impacts of the so-called datafication of social relations on investigative and evidentiary logic within criminal prosecution, with special emphasis on the doctrinal and practical challenges related to the collection, preservation, and assessment of digital evidence in Brazilian criminal procedure. Adopting a qualitative approach and a deductive method, grounded in bibliographic research, normative analysis, and critical examination of investigative practice, the research examines the role of digital chain of custody as a procedural safeguard for ensuring the authenticity, integrity, and reliability of digital evidence. The study concludes that digital evidence requires specific doctrinal treatment and enhanced procedural rigor, under penalty of undermining both the effectiveness of criminal prosecution and the legitimacy of state punitive power.

Keywords: Criminal investigation. Digital evidence. Chain of custody. Datafication. Criminal procedure.

[1]Delegada de Polícia Civil do Estado do Ceará, Orientadora da Célula de Inteligência Cibernética e Análise de Dados de Extração do Departamento de Inteligência Policial. Especialização em Gestão de Organizações de Inteligência pela Escola de Inteligência Militar do Exército Brasileiro. Professora e conteudista da Academia Estadual de Segurança Pública. Orcid https://orcid.org/0009-0007-5752-7662.

1. A SOCIEDADE EM REDE E O NOVO PARADIGMA DA INVESTIGAÇÃO POLICIAL

A atividade de Polícia Judiciária exercida pelo Delegado de Polícia tem sido profundamente impactada pela transformação da vida social, cada dia mais interconectada com elementos intangíveis virtuais, na medida em que parcela significativa dos vestígios relevantes para a investigação criminal passou a se manifestar sob a forma de dados digitais. Registros de geolocalização, comunicações eletrônicas, interações em plataformas digitais e informações armazenadas em nuvem tornaram-se elementos centrais na reconstrução dos fatos penalmente relevantes, sendo produzidos, armazenados e controlados por sistemas tecnológicos complexos e, muitas vezes, por terceiros.

É muito percuciente a lição de SOUZA (2025), ao ponderar que

> O desafio não é mais coletar dados—algo relativamente fácil nos dias atuais—mas sim dar sentido e extrair informações úteis dessa imensidão digital. É aí que entram as técnicas avançadas de visualização de dados, que prometem transformar grandes massas de dados aparentemente desconexas em insights claros e decisivos para o combate ao crime.

Nesse cenário, a condução da investigação criminal pelo Delegado de Polícia exige não apenas a adaptação da forma de investigar, cada vez mais orientada por dados e por análises digitais, mas também a observância rigorosa de procedimentos capazes de assegurar que a prova digital obtida seja tecnicamente íntegra, juridicamente válida e processualmente confiável. A experiência prática da investigação revela, contudo, dificuldades recorrentes na obtenção de evidências digitais, seja em razão de sua volatilidade, da dependência de provedores e plataformas tecnológicas, da criptografia ou da fragmentação do armazenamento dos dados.

A prática investigativa revela, contudo, a existência de lacunas procedimentais, dificuldades técnicas e incertezas dogmáticas relacionadas à coleta, preservação, documentação e valoração da prova digital, o que pode comprometer a eficácia da persecução penal e a credibilidade do trabalho policial no momento de sua submissão ao controle judicial.

Diante desse contexto, o problema de pesquisa pode ser formulado nos seguintes termos: De que modo a influência da chamada datificação das coisas impactou na investigação criminal e quais são os principais desafios dogmáticos e práticos relacionados à obtenção, preservação e valoração da prova digital, especialmente no que se refere à cadeia de custódia digital no processo penal?

O objetivo do presente estudo consiste em analisar criticamente esses desafios, à luz do papel constitucional da Polícia Judiciária e das garantias processuais penais, buscando

identificar pontos de tensão entre a prática investigativa e o arcabouço normativo vigente. Para tanto, adota-se o método dedutivo, com abordagem qualitativa, valendo-se de pesquisa bibliográfica, análise normativa e exame crítico da experiência prática da investigação criminal, de modo a contribuir para o aprimoramento dogmático e procedimental da prova digital no processo penal brasileiro.

2. A TRANSFORMAÇÃO DO MODELO DE INVESTIGAÇÃO POLICIAL

A investigação criminal contemporânea é fortemente impactada pela intensificação dos processos de digitalização da vida social e pela consolidação da chamada *Era da Datificação*. Conforme aponta Mayer-Schönberger e Cukier (2013), a datificação consiste na conversão sistemática de comportamentos, interações e eventos sociais em dados passíveis de armazenamento, processamento e análise, fenômeno que altera de maneira estrutural a forma como o conhecimento é produzido e utilizado. De acordo com os autores, "As big-data predictions improve, using them will only become more appealing, fueling an obsession over data since it can do so much" (Mayer-Schönberger e Cukier, 2013, p. 167).[2]

No campo da persecução penal, esse processo repercute diretamente sobre a forma de identificação, coleta e interpretação dos vestígios relevantes à reconstrução dos fatos penalmente relevantes.

Tradicionalmente, o modelo de investigação policial esteve orientado à apuração de fatos delimitados no tempo e no espaço, a partir de vestígios predominantemente materiais e de relatos pessoais, organizados segundo uma lógica indiciária essencialmente narrativa. A literatura processual penal clássica descreve, de forma geral, a investigação como uma atividade retrospectiva, voltada à reconstrução de acontecimentos pretéritos mediante a reunião progressiva de indícios que permitam a formação de uma hipótese sobre autoria e materialidade delitivas. Nesse sentido, MIRABETE (2004, p. 78) afirma que o procedimento investigativo tem por objeto "a apuração de fato que configure infração penal e respectiva autoria, para servir de base à ação penal ou às providências cautelares".

Esse modelo, contudo, passou a ser tensionado pela centralidade assumida pelos dados digitais no contexto investigativo atual. Isso porque a sociedade em rede produz um ambiente informacional caracterizado pela circulação contínua de fluxos de dados, nos quais ações

[2] Em tradução livre: À medida que as previsões baseadas em big data melhoram, usá-las tende a se tornar cada vez mais atraente, alimentando uma obsessão pelos dados, já que eles podem fazer tanto.

humanas deixam rastros digitais persistentes, ainda que frequentemente dispersos, fragmentados e controlados por infraestruturas tecnológicas complexas.

Esses rastros não decorrem, necessariamente, de uma conduta criminosa específica, mas são gerados de forma contínua por sistemas tecnológicos que registram, armazenam e processam informações para finalidades diversas, como comunicação, logística, consumo e segurança, e podem se tornar elementos essenciais para a elucidação de condutas delitivas. No âmbito da investigação criminal, esses rastros passam a constituir elementos centrais da atividade investigativa, podendo ser citados como exemplos registros de geolocalização, comunicações eletrônicas, metadados e logs de sistemas.

Nesse contexto, a investigação criminal passa a lidar com um volume expressivo de dados pré-existentes ao fato investigado, os quais podem ser posteriormente mobilizados para fins probatórios. A atividade investigativa deixa, assim, de se iniciar exclusivamente a partir do fato conhecido para, em muitos casos, partir da análise e correlação de dados disponíveis, em busca de padrões, vínculos ou incongruências que permitam a identificação de eventos penalmente relevantes. De acordo com Mayer-Schönberger e Cukier (2013),

> In the spirit of Google or Facebook, the new thinking is that people are the sum of their social relationships, online interactions, and connections with content. In order to fully investigate an individual, analysts need to look at the widest possible penumbra of data that surrounds the person — not just whom they know, but whom those people know too, and so on. This was technically very hard to do in the past. Today it's easier than ever.[3] (p. 155)

Nesse cenário, a literatura contemporânea, especialmente nos campos da criminologia empírica e dos estudos sobre policiamento, passou a empregar a expressão *data-driven investigation* para designar modelos investigativos orientados prioritariamente pela análise e correlação de dados, e não pela reconstrução linear de fatos isolados. Ao observar a relação entre tecnologia e persecução penal, conclui-se que o trabalho investigativo passa a envolver não apenas a coleta de vestígios, mas a gestão, correlação e interpretação de grandes volumes de informações, frequentemente mediadas por ferramentas automatizadas e técnicas de análise preditiva, em contraste com a investigação clássica, que se baseia na reconstrução direta de eventos isolados.

[3] Em tradução livre: No espírito do Google ou do Facebook, o novo pensamento é que as pessoas são a soma de suas relações sociais, interações online e conexões com conteúdos. Para investigar plenamente um indivíduo, os analistas precisam examinar a mais ampla penumbra possível de dados que o cerca — não apenas quem ele conhece, mas também quem essas pessoas conhecem, e assim por diante. Isso era tecnicamente muito difícil de fazer no passado. Hoje, é mais fácil do que nunca.

Essa transformação não se limita à introdução de novas ferramentas tecnológicas, mas implica uma alteração qualitativa na racionalidade investigativa. A investigação orientada por dados desloca o foco da causalidade linear entre fato e vestígio para uma lógica probabilística e correlacional, na qual padrões informacionais assumem papel relevante na formulação de hipóteses investigativas. Tal deslocamento impacta diretamente a lógica probatória da persecução penal, na medida em que o dado digital não constitui o fato em si, mas uma representação técnica mediada por sistemas informacionais complexos. Nessa esteira, VIEIRA e SANTOS (2025) afirmam:

> O convencimento da ocorrência de fatos através das provas deve considerar as necessidades provenientes da ambientação virtual na qual ela se extrai. Ou seja, deve-se ter em mente as especificidades linguísticas do ecossistema digital, além do fato de que elas são aptas a cadenciar contextos diversos e maleáveis. A produção nativa digital se destaca fundamentalmente pelo seu potencial de relacionalidade. Isso porque as relações baseadas em algoritmos, ao mesmo tempo em que integram as produções, também garantem seu funcionamento e sua circulação, pela característica linguisticamente inéditas da clicabilidade.

Ainda assim, isso amplia a distância epistemológica entre o acontecimento investigado e o elemento probatório que o representa, tornando indispensável a verificação dos procedimentos técnicos e institucionais que asseguram sua autenticidade, integridade e confiabilidade.

Do ponto de vista dogmático, esse fenômeno impõe desafios relevantes à teoria da prova, visto que a confiabilidade da prova não depende apenas de seu conteúdo informativo, mas também dos procedimentos de obtenção, preservação e documentação que permitem aferir sua autenticidade e integridade. No caso da evidência digital, esses procedimentos tornam-se ainda mais relevantes, diante da volatilidade, da facilidade de manipulação e da replicabilidade dos dados.

Além disso, a crescente dependência de dados produzidos e armazenados por pessoas jurídicas classificadas como *bigtechs* ou *fintechs*, tais como provedores de aplicações, plataformas digitais e empresas de tecnologia, introduz novos riscos à transparência e ao controle da atividade investigativa. A formulação de hipóteses passa a depender de correlações e padrões identificados por ferramentas analíticas, o que aumenta a eficiência investigativa, mas também potencializa riscos de vieses, opacidade e erros sistêmicos.

Nessa perspectiva, a atuação da Polícia Judiciária, especialmente do Delegado de Polícia, exige não apenas competência técnica, mas também capacidade de aplicar normas e procedimentos institucionais que assegurem a confiabilidade e a admissibilidade da prova

digital, reforçando a importância da cadeia de custódia como instrumento de garantia processual.

Dessa forma, a transformação do modelo de investigação policial não pode ser compreendida apenas como um fenômeno de modernização tecnológica, mas como um processo que exige a revisão crítica das categorias tradicionais da investigação criminal e da prova penal. É a partir dessa perspectiva que se justifica a análise do deslocamento de uma investigação centrada em fatos para uma investigação estruturada em dados, bem como de seus reflexos sobre a validade, a confiabilidade e a valoração da prova no processo penal contemporâneo.

2.1. O papel da análise preditiva, do cruzamento massivo de dados e da Inteligência policial

A investigação criminal contemporânea não se limita mais à coleta de vestígios isolados: ela se apoia cada vez mais na integração e análise de grandes volumes de dados, que permitem antecipar padrões de comportamento e mapear relações potencialmente relevantes à persecução penal. Ferramentas de análise preditiva, basicamente oriundas da ciência de dados e do *machine learning* (técnica de aprendizagem de máquina), possibilitam identificar vínculos e tendências antes mesmo da ocorrência de certos eventos, direcionando a investigação de forma mais estratégica e eficiente. Nesse viés, fala-se em policiamento preditivo, que diz respeito a "sistemas computadorizados cujo processamento de informações por algoritmos se utilizam tanto de bancos de dados robustos quanto de análises estatísticas para fins de predição de um acontecimento criminoso futuro" (MORAES, 2022, p. 35).

Essas ferramentas preditivas compreendem o homem a partir de uma perspectiva meramente estatística, por meio de uma relação entre a base de dados e os padrões de regularidades comportamentais de uma população (Garland, 1997, p. 182).

O cruzamento massivo de dados, técnica bastante utilizada com o fito de tornar mais célere e eficientes os trabalhos de análise, consiste na interligação de diferentes bases informacionais, sejam públicas ou privadas, com o objetivo de revelar padrões que não seriam perceptíveis em análises fragmentadas. Na prática investigativa, isso inclui a correlação entre registros telefônicos, logs de aplicativos, sistemas de vigilância e informações geoespaciais, criando um arcabouço de evidências que permite reconstruir contextos complexos e identificar relações entre suspeitos, vítimas e eventos.

A Inteligência policial, por sua vez, emerge como o elo entre a análise técnica dos dados e a decisão investigativa, mediando informações provenientes de fontes diversas e garantindo

que a interpretação de padrões e probabilidades seja convertida em estratégias concretas de atuação. Ao mesmo tempo, essa abordagem exige cautela: a dependência de dados produzidos por terceiros e a complexidade dos algoritmos utilizados podem introduzir vieses, opacidade e erros sistemáticos, exigindo fiscalização rigorosa e validação contínua das inferências utilizadas na investigação (BADARÓ, 2020).

Dessa forma, o modelo contemporâneo de investigação policial transita de uma lógica centrada exclusivamente na reconstrução de fatos para uma lógica que integra análise preditiva, correlação massiva de dados e inteligência estratégica, ainda que permeada por desafios técnicos, institucionais e dogmáticos relacionados à confiabilidade da prova.

2.3. Impactos da datificação na lógica probatória da persecução penal

A incorporação crescente de dados digitais à investigação criminal vem alterando, assim, a lógica tradicional da prova penal, provocando um deslocamento epistemológico que afeta tanto a coleta quanto a valoração de evidências. Diferentemente da prova clássica, que se estruturava a partir de vestígios materiais e testemunhos diretos, a prova digital consiste, em sua ampla maioria, em representações mediadas por sistemas tecnológicos, cuja interpretação requer não apenas conhecimento jurídico, mas também competências técnicas e metodológicas para aferir sua autenticidade, integridade e confiabilidade, além de ferramentas tecnológicas adequadas.

Isso porque, em linhas gerais, a prova digital não é apenas uma representação do fato, mas um produto técnico que exige validação meticulosa dos seus métodos de obtenção. Deste modo, para ser confiável, deve ser analisada à luz dos parâmetros técnicos que garantem sua veracidade.

Entre os impactos mais significativos da datificação, destaca-se a necessidade de repensar a relação entre fato e evidência. Os dados digitais não reproduzem diretamente o acontecimento investigado, mas registram vestígios de ações em ambientes virtuais ou em sistemas informatizados. Essa mediação tecnológica aumenta a distância epistemológica entre o evento e a prova, exigindo que o Delegado de Polícia e demais atores do processo penal considerem não apenas o conteúdo do dado, mas também seu contexto de produção, as condições de armazenamento e os procedimentos utilizados para sua extração e preservação.

Não se pode descurar de que a distância entre o evento original e sua evidência digital exige uma nova abordagem epistemológica para garantir a fidedignidade da prova no processo

penal, sendo, portanto, imprescindível a observância de critérios metodológicos rigorosos que permitam indicar que o dado digital é autêntico, e capaz de demonstrar um fato ou uma fração significativa que permitirá a compreensão do contexto fático em torno de um crime.

Isto é ainda mais relevante quando se consideram as características da volatilidade e replicabilidade dos dados digitais, bem como a dependência de terceiros (tais como provedores de serviços, plataformas digitais e sistemas de armazenamento em nuvem) para acesso e controle das informações. Essa realidade impõe desafios inéditos à integridade da prova, uma vez que qualquer manipulação, falha técnica ou inadequação no procedimento de coleta pode comprometer sua confiabilidade e admissibilidade perante o Judiciário. Segundo Prado (2019, p. 118), "a manipulação de dados digitais por terceiros, sem a devida cadeia de custódia, coloca em risco a legitimidade da prova no processo".

A datificação também provoca transformações na lógica investigativa e probatória. A análise de grandes volumes de dados permite identificar padrões, relacionamentos e indícios que seriam imperceptíveis por métodos tradicionais, ou que demandariam maior tempo para serem percebidos. Contudo, esse mesmo potencial analítico exige mecanismos institucionais robustos, como auditoria técnica, documentação rigorosa e validação de procedimentos, para assegurar que as inferências derivadas da informação digital possam ser sustentadas em juízo (BADARÓ, 2020).

Por fim, esses impactos da datificação na prova penal estabelecem a necessidade de um olhar específico sobre a prova digital, seus critérios de validade e confiabilidade, e sobre os procedimentos de cadeia de custódia digital que garantam a preservação e integridade das evidências. É nesse contexto que se insere o próximo capítulo, que abordará de forma sistemática o conceito, a classificação e as especificidades epistemológicas da prova digital no processo penal contemporâneo.

3. PROVA DIGITAL NO PROCESSO PENAL CONTEMPORÂNEO

A prova digital é definida como qualquer vestígio de um fato produzido, armazenado ou transmitido através de sistemas tecnológicos, como computadores, celulares, servidores e redes sociais. Segundo PRADO (2021), a prova digital, também chamada eletrônica, tecnológica ou e-evidence, pode ser definida como "qualquer classe de informação (dados) que tenha sido produzida, armazenada ou transmitida por meios eletrônicos". Sua caracterização envolve uma

interpretação mais complexa, que vai além da simples análise de dados numéricos ou textos, exigindo, portanto, competência técnica para ser validada.

Dessa maneira, a prova digital não se limita a ser um reflexo direto do fato ocorrido, mas uma representação do acontecimento, com particularidades que exigem um estudo aprofundado de sua origem e contexto de criação. Tais provas, de acordo com CAPANEMA (2024, p.192),

> Constituem o denominado 'direito probatório de 3ª geração', que abarca as tecnologias extremamente invasivas, as quais permitem que as autoridades investigativas obtenham muito mais informações do que pelos meios tradicionais normalmente utilizados. Há a possibilidade de obtenção de provas em maior quantidade e melhor qualidade.

As provas digitais possuem especificidades epistemológicas, que envolvem uma distância entre o evento original e o registro digital, já que os dados digitais não representam o evento de forma direta. Nesse sentido, a análise desses vestígios exige não só conhecimento jurídico, mas também métodos e ferramentas adequados, além de um entendimento técnico sobre os sistemas que geram e armazenam essas informações, uma vez que o dado digital é, muitas vezes, apenas uma representação ou intermediação do acontecimento real. Para BADARÓ (2021),

> A prova digital é tema central da chamada computer forensics, que deve se valer de instrumentos técnicos ou tools adequados para os trabalhos de investigação de dados digitais que poderão constituir uma prova utilizável em processo judicial. (...) É imprescindível que o método empregado garanta a integridade do dado digital e, com isso, a força probandi do conteúdo probatório por ele representado.

No contexto da prova digital, os critérios de autenticidade e integridade são essenciais para garantir que os dados coletados possam ser utilizados efetivamente no processo penal, pois "é fundamental avaliar o grau de segurança e de certeza que se pode ter, sobretudo quanto à sua *autenticidade*, que permite identificar a sua autoria, e à sua *integridade*, que permite garantir a inalterabilidade do seu conteúdo" (DIDIER JÚNIOR; BRAGA; OLIVEIRA, 2016, p. 221-222).

A autenticidade da prova digital constitui requisito essencial para sua admissibilidade e valoração no processo, e diz respeito à "qualidade da prova digital que permite a certeza com relação ao autor ou autores do fato digital". É, portanto, "a qualidade que assegura que o autor aparente do fato é, com efeito, seu autor real" (THAMAY; TAMER, 2020, p. 40).

A integridade da prova digital consiste na garantia de que o conteúdo informacional do dado permaneceu inalterado desde o momento de sua geração, coleta ou apreensão até sua apresentação em juízo, assegurando a correspondência exata entre o estado atual da prova e sua forma originária. Trata-se de requisito de natureza predominantemente técnica, cuja comprovação se dá mediante a adoção de procedimentos forenses padronizados, como a

preservação da cadeia de custódia e o emprego de mecanismos de verificação criptográfica, notadamente funções hash e registros de auditoria, capazes de evidenciar qualquer modificação, ainda que mínima, no conteúdo do arquivo.

A integridade deve ser compreendida, assim, como "a qualidade da prova digital que permite a certeza com relação à sua completude e não adulteração", sendo considerada íntegra quando "isenta de qualquer modificação em seu estado ou adulteração desde o momento da realização do fato até a apresentação do resultado prova", mostrando-se, assim, idônea "a demonstrar a reprodução do fato em sua completude e integridade" (THAMAY; TAMER, 2020, p. 45).

Cumpre salientar que os parâmetros da autenticidade e da integridade encontram previsão expressa na legislação processual no tocante ao registro dos atos processuais eletrônicos, nos termos do art. 195 do Código de Processo Civil, os quais, embora formulados para disciplinar a prática de atos no ambiente digital do processo, revelam standards normativos de confiabilidade da informação eletrônica. Tais standards são passíveis de extensão, seja por aplicação analógica, seja em razão da teleologia da atividade probatória, a todo e qualquer registro eletrônico cuja admissão se pretenda com eficácia probatória, na medida em que a função epistêmica da prova exige a observância de requisitos mínimos de fidedignidade, rastreabilidade e preservação do conteúdo informacional.

Segundo Marinoni e Arenhart (2019, p. 660), "(...) vê-se a carência efetiva de dispositivos para tratar da força probante do documento eletrônico, especificamente em razão da dificuldade em se ter por autêntica a informação transmitida por via digital".

É sabido, contudo, que a evidência digital pode ser facilmente corrompida ou manipulada, o que torna o procedimento de cadeia de custódia fundamental. Qualquer falha nos procedimentos de coleta pode comprometer a confiabilidade da prova digital, resultando em sua inadmissibilidade no processo. A admissibilidade, portanto, depende não só da conformidade com os requisitos legais, mas também da verificação da integridade do dado.

A análise dos dados digitais deve levar em conta o contexto em que foram gerados, além dos meios utilizados para sua obtenção. Isso implica que, para que a prova digital seja admissível no processo penal, ela deve ser acompanhada de documentação detalhada que demonstre que os procedimentos de coleta foram seguidos adequadamente e que o dado não foi adulterado ou manipulado.

4. DESAFIOS NA OBTENÇÃO DA PROVA DIGITAL

Diferentemente das provas tradicionais, a prova digital caracteriza-se por sua natureza imaterial, alta volatilidade e suscetibilidade a alterações imperceptíveis, o que exige métodos específicos de coleta, preservação e análise, sob pena de comprometimento de sua confiabilidade e de violação aos direitos fundamentais do investigado ou acusado.

A obtenção desses elementos probatórios frequentemente envolve intervenções invasivas, dependência de terceiros e tecnologias complexas, tornando imprescindível a atuação técnica especializada e o controle jurisdicional efetivo. Assim, a prova digital não pode ser compreendida apenas como uma extensão das provas documentais clássicas, mas como uma categoria probatória autônoma, que exige maior atenção e cuidados por parte da Polícia Judiciária, mas aplicados analogicamente os marcos regulatórios já existentes, como defende BADARÓ (2021, p. 7) observadas duas características que destaca como mais relevantes: "a desmaterialização e a dispersão dos elementos de prova".

Acerca da desmaterialização, BADARÓ pondera que

> Não se trata de provas pensáveis como objetos físicos, dotados de uma evidente corporeidade. E é exatamente dessa impalpabilidade que decorre os caráteres de volatilidade e fragilidade da própria prova digital, razão pela qual há necessidade de uma maior preocupação com a possibilidade de falsificação ou destruição. Há, na prova digital, uma "congênita mutabilidade". Em suma, trata-se de fonte de prova que pode ser facilmente contaminada, sendo sua gestão muito delicada, por apresentar um alto grau de vulnerabilidade a erros" (2021, p. 7-8).

A volatilidade e a mutabilidade dos dados digitais representam um dos maiores desafios na investigação criminal. Ao contrário das provas físicas, que são tangíveis e podem ser preservadas de maneira mais estática, os dados digitais podem ser alterados ou perdidos com facilidade, seja por falhas técnicas, atualizações de sistema ou até mesmo por ação humana.

Além disso, a mutabilidade dos dados digitais implica que os vestígios de um crime podem ser alterados, apagados ou modificados, especialmente em dispositivos de fácil acesso, como smartphones e computadores pessoais. Em um ambiente digital dinâmico, onde alterações podem ser feitas a qualquer momento, a integridade da prova pode ser comprometida sem deixar rastros visíveis.

A dependência de terceiros é outro fator crítico na obtenção da prova digital. Cada vez mais, os dados são armazenados em servidores de plataformas terceirizadas, como provedores de serviços em nuvem, redes sociais e outras empresas de tecnologia, que exercem um controle significativo sobre o acesso e a integridade desses dados. Nesse sentido, a dependência de plataformas privadas e empresas de tecnologia para armazenamento e processamento de dados

implica em desafios legais e práticos, dado o controle limitado dos investigadores sobre essas informações, que são recebidas, na maioria dos casos, mediante determinação para o fornecimento.

Esses desafios exigem que os investigadores possuam não apenas ferramentas adequadas, mas também uma compreensão profunda das tecnologias em questão e das normas jurídicas que regulam o acesso a essas plataformas externas. A ausência de legislação específica sobre o tema é um dos problemas mais abordados por diversos autores que se debruçam sobre o tema. Com efeito,

> Considerando a mutabilidade e a volatilidade como características dos dados eletrônicos, isto é, a possibilidade de que aconteçam modificações e, inclusive, mudanças no conteúdo probatório que levantem questões sobre a confiabilidade da evidência, a falta de legislação específica que aborde a cadeia de custódia para provas digitais causa grande instabilidade e insegurança em relação aos dados eletrônicos utilizados como prova no processo penal, uma vez que não há garantia da existência de documentação que registre todas as etapas percorridas pela evidência". (MAIA; PEREIRA. 2024, p. 45)

Retratando as nuances em torno desse vácuo legislativo, preceitua BADARÓ (2021, p.7)

> Para garantir a autenticidade, evitando a contaminação da prova digital, o ideal seria que o legislador pudesse estabelecer uma técnica específica a ser empregada para a individualização e apreensão da prova digital, sob pena de inutizabilidade da prova. Todavia, considerando, de um lado, que a informática é uma ciência relativamente jovem e ainda não há meios e técnicas uniformemente aceitos e, de outro, que tem havido rapidíssima mutação e evolução das técnicas computacionais, tal solução se mostra inviável.

Nesse cenário de desafios e ausência de marcos regulatórios claros sobre a coleta e manuseio da prova digital, faz-se imprescindível que a investigação policial obedeça rigorosamente as leis processuais já vigentes, com a especial observância da cadeia de custódia.

5. CADEIA DE CUSTÓDIA DIGITAL COMO GARANTIA DA PROVA

5.1. A cadeia de custódia aplicada à prova digital

A cadeia de custódia digital é essencial para garantir que os dados coletados durante uma investigação não sejam adulterados ou corrompidos. Ela compreende uma série de procedimentos técnicos e administrativos que asseguram que a evidência digital seja tratada, preservada e documentada corretamente, desde sua coleta até sua apresentação no processo judicial.

O art. 158-A do Código de Processo Penal traz a definição de cadeia de custódia, apresentando-a como "o conjunto de todos os procedimentos utilizados para manter e

documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte".

Como destaca Badaró (2017, p. 561), "a cadeia de custódia é a história cronológica escrita, ininterrupta e testemunhada, de quem teve a evidência desde o momento da coleta até que ela seja apresentada como prova no tribunal". Renato Brasileiro de Lima (2020, p. 250-251) conceitua-a como

> Um mecanismo garantidor da autenticidade das evidências coletadas e examinadas, assegurando que correspondem ao caso investigado, sem que haja lugar para qualquer tipo de adulteração. Funciona, pois, como a documentação formal de um procedimento destinado a manter e documentar a história cronológica de uma evidência, evitando-se, assim, eventuais interferências internas e externas capazes de colocar em dúvida o resultado da atividade probatória, assegurando, assim, o rastreamento da evidência desde o local do crime até o Tribunal.

É a adoção desse conjunto de procedimentos que garantirá a utilização da evidência digital no processo penal. Nesse sentido, julgado da Quinta Turma do STJ, pondera que

> Mostra-se indispensável que todas as fases do processo de obtenção das provas digitais sejam documentadas, cabendo à polícia, além da adequação de metodologias tecnológicas que garantam a integridade dos elementos extraídos, o devido registro das etapas da cadeia de custódia, de modo que sejam asseguradas a autenticidade e a integralidade dos dados.[4]

Nessa mesma esteira, no âmbito doutrinário, Gustavo Badaró pontua que

> [n]ão havendo documentação da cadeia de custódia, e não sendo possível sequer ligar o dado probatório à ocorrência do delito, o mesmo não deverá ser admitido no processo. A parte que pretende a produção de uma prova digital tem o ônus de demonstrar previamente a sua integridade e autenticidade, por meio da documentação da cadeia de custódia. Sem isso, sequer é possível constatar sua relevância probatória (2023, p. 183).

Também defendendo a aplicação da cadeia de custódia nas provas imateriais, BADARÓ (2017, p. 522) defende ser necessária a documentação da cadeia de custódia de todos os elementos obtidos eletronicamente. MATILDA (2021, p. 19), corroborando, entende que a cadeia de custódia se aplica às provas imateriais, devendo a acepção da palavra "vestígios" ser ampliada para abarcar vestígios digitais como troca de e-mails, interceptação telefônica, mensagens por aplicativo etc.

No entanto, a aplicação da cadeia de custódia na prova digital é particularmente desafiadora devido à natureza volátil dos dados, que podem ser facilmente alterados. Em resposta a essa questão, Prado (2019) argumenta que "a custódia deve ser aplicada de maneira

[4] BRASIL. Superior Tribunal de Justiça (STJ). Habeas Corpus n. 828054/RN. Relator: Min. Joel Ilan Paciornik. Brasília, DF, 24 de abril de 2024. Disponível em: <https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=integra&documento_sequencial=242041837&registro_numero=202301896150&peticao_numero=202300906480&publicacao_data=20240429&formato=PDF>. Acesso em: 10 jan. 2026

minuciosa, com documentação rigorosa de cada passo do processo de coleta e armazenamento" (PRADO, 2019, p. 125).

5.2. Procedimentos técnicos de preservação, coleta e documentação

A preservação e a coleta de dados digitais requerem procedimentos específicos, a fim de evitar que a prova digital seja corrompida durante o processo de obtenção. É fundamental que os investigadores utilizem ferramentas forenses digitais adequadas para preservar a integridade dos dados. Como menciona Badaró (2020), "a coleta de dados digitais exige o uso de softwares forenses que garantam a obtenção da evidência sem modificar seu conteúdo original" (BADARÓ, 2020, p. 100).

Ensina Aury Lopes (2023, p. 196):

> A preservação da cadeia de custódia exige grande cautela por parte dos agentes do estado, da coleta à análise, de modo que se exige o menor número de custódios possível e a menor manipulação do material. O menor número de pessoas manipulando o material faz com que seja menos manipulado e a menor manipulação conduz a menor exposição. Expor menos é proteção e defesa da credibilidade do material probatório.

Além disso, a documentação detalhada de cada etapa do processo é essencial para garantir a transparência e a credibilidade da prova. Cada acesso aos dados, seja para coleta, extração ou análise, deve ser devidamente registrado, conforme ressaltado por Prado (2019), que argumenta: "a documentação minuciosa de cada passo no processo de coleta e análise é vital para garantir a admissibilidade da prova digital no processo judicial" (PRADO, 2019, p. 134).

Ao tratar da cadeia de custódia, "a expressão deve ser entendida como a elipse de documentação da cadeia de custódia". (BADARÓ, 2021, p. 8). Isso implica no registro documental de cada etapa e de todas as pessoas que tiveram contato com a evidência, sendo certo que já há softwares e ferramentas que permitem a redução do tráfego da evidência, através do imediato armazenamento em nuvem.

Gustavo Badaró (2023, p. 179), neste sentido, leciona que:

> Evidente que independentemente de qual procedimento técnico empregado, além de adequado segundo as melhores práticas, ele também precisará ser documentado e registrado em todas as suas etapas. Tal exigência é uma garantia de um correto emprego das operating procedures, especialmente por envolver um dado probatório volátil e facilmente sujeito à mutação. Além disso, exatamente pela diferença ontológica da prova digital com relação à prova tradicional, devido àquela não se valer de uma linguagem natural, mas digital, é que, como diz Pittiruti, uma cadeia de custódia detalhada se faz ainda mais necessária

Assim, em que pese não haver ainda um regramento próprio acerca da cadeia de custódia da evidência digital, é certo que, no bojo da investigação policial, é dever do presidente da investigação adotar todas as providências necessárias para que a prova digital requisitada seja

íntegra, idônea e confiável, mediante a documentação de todos os atos praticados, bem como dos policiais que tiveram acesso a evidência, e em qual fase. Com a adoção desses cuidados, a Polícia Judiciária torna-se mais técnica, mitigando erros e permitindo que, ao final do processo, o trabalho realizado desde a origem esteja incólume.

6. CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo deste trabalho evidenciou que a consolidação da sociedade em rede e o avanço dos processos de datificação das relações sociais impuseram uma reconfiguração estrutural da investigação criminal contemporânea. A crescente centralidade assumida pelos dados digitais desloca o modelo investigativo tradicional, fundado na reconstrução linear de fatos a partir de vestígios predominantemente materiais, para um paradigma de investigação policial orientada por dados, no qual a identificação, a correlação e a interpretação de grandes volumes de informações assumem papel determinante na formulação de hipóteses investigativas e na reconstrução dos fatos penalmente relevantes.

Esse novo paradigma, a investigação policial orientada por dados exige não apenas o domínio de ferramentas tecnológicas e analíticas, mas, sobretudo, a adoção de critérios metodológicos rigorosos capazes de assegurar a confiabilidade das inferências produzidas a partir dessas informações. A eficiência proporcionada pelo uso intensivo de dados, análise preditiva e cruzamento massivo de bases informacionais, embora relevante para a persecução penal, não pode prescindir de mecanismos institucionais de controle, sob pena de comprometimento da legitimidade do exercício do poder punitivo estatal.

Diante desse cenário, restou demonstrado que a prova digital não pode ser compreendida como simples prolongamento da prova documental clássica, mas como categoria probatória autônoma, dotada de especificidades técnicas e jurídicas que impõem um reforço procedimental na sua obtenção, preservação e valoração. A volatilidade, a mutabilidade e a dispersão dos dados digitais, aliadas à crescente dependência de plataformas tecnológicas e terceiros privados, tornam imprescindível a observância rigorosa da cadeia de custódia digital como garantia da autenticidade, integridade e rastreabilidade das evidências.

Reforça-se, portanto, que a investigação policial orientada por dados deve ser acompanhada de maior rigor técnico na obtenção, análise e armazenamento dos dados, a fim de atender ao robusto arcabouço de garantias processuais, no qual a cadeia de custódia desempenha função central de contenção de riscos epistêmicos, técnicos e jurídicos inerentes à prova digital.

Ainda que o ordenamento jurídico brasileiro não disponha de regulamentação específica para todas as etapas do tratamento da evidência digital, a aplicação criteriosa dos marcos normativos já existentes, aliada à adoção de boas práticas técnicas e à atuação responsável da Polícia Judiciária, revela-se essencial para compatibilizar eficiência investigativa, segurança jurídica e respeito aos direitos fundamentais no processo penal contemporâneo.

REFERÊNCIAS

BADARÓ, Gustavo Henrique. Ônus da prova no processo penal. 2. ed. São Paulo: Revista dos Tribunais, 2020.

BADARÓ, G. H. R. I. A Cadeia de Custódia e sua Relevância para a Prova Penal. In: Temas Atuais da Investigação Preliminar no Processo Penal. SIDI, R.; LOPES, A. B. (Orgs.). Belo Horizonte: Editora D'Plácido, 2017.

BADARÓ, Gustavo Henrique Righi Ivahy. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia . Boletim IBCCRIM, São Paulo, v. 29, n. 343, p. 7–9, 2021. Disponível em: https://www.publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1325. Acesso em: 4 jan. 2026.

BADARÓ, Gustavo. A Cadeia de Custódia da Prova Digital. In: OSNA, Gustavo et. al. Direito Probatório. Londrina: Thoth, 2023

CASTELLS, Manuel. A sociedade em rede. 13. ed. São Paulo: Paz e Terra, 2010.

DELGADO MARTÍN apud PRADO, G. L. M. Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital, 2021. Disponível em: <https://geraldoprado.com.br/artigos/breves-notas-sobre-o-fundamento-constitucional-da-cadeia-de-custo-dia-da-prova-digital/>. Acesso em: 15 jan 2026.

DIDIER JÚNIOR, Fredie; BRAGA, Paula Sarno; OLIVEIRA, Rafael Alexandria de. Curso de direito processual civil. 11. ed. Salvador: Jus Podivm, 2016. v. 2.

LIMA, Renato Brasileiro de. Manual de Processo Penal. 8. ed. Salvador: Jus Podivm, 2020.

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

LUIS FERNANDES, André; MONTES, Rodrigo Henrique de Oliveira. Meta-evidência digital: A dualidade na cadeia de custódia envolvendo dispositivos eletrônicos e evidências digitais. Direito & TI, [S. l.], v. 1, n. 14, p. 59–73, 2023. DOI: 10.63451/ti.v1i14.115. Disponível em: https://direitoeti.com.br/direitoeti/article/view/115. Acesso em: 21 dez. 2025.

MAIA, Juliana Kryssia Lopes.; PEREIRA, Romulo Lopes Maia S. Cadeia de Custódia das Provas Digitais no Processo Penal: Normas Aplicáveis. Cadeia de Custódia, Metodologias e Prova Digital: conhecimento prático e interdisciplinar. Org. Juliana Kryssia Lopes Maia, Sergio Hernandez. 1a ed. Rio de Janeiro: Lumen Juris, 2024.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. Prova e convicção. 5. ed. São Paulo: Thomson Reuters, 2019.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. Big data: a revolution that will transform how we live, work, and think. Boston: Houghton Mifflin Harcourt, 2013.

MIRABETE, Julio Fabbrini. Processo Penal. ed. 16. São Paulo: Altas, 2004.

MORAES, F. de. Policiamento preditivo e aspectos constitucionais. Belo Horizonte: Dialética, 2022.

PRADO, Geraldo. Sistema acusatório: a conformidade constitucional das leis processuais penais. 6. ed. Rio de Janeiro: Lumen Juris, 2019.

PRADO, Geraldo. Parecer: investigação criminal digital e processo penal. Revista Brasileira de Ciências Criminais , São Paulo, v. 199, n. 199, p. 315–350, 2023. DOI: 10.5281/zenodo.8381070. Disponível em: https://publicacoes.ibccrim.org.br/index.php/RBCCRIM/article/view/707. Acesso em: 12 dez. 2025.

SOUZA, Bruno. Visualização de Dados na Investigação Criminal: Solucionando Crimes com Análise Visual. Modal – Ciência, Tecnologia & Inovação, 14 mar. 2025. Disponível em: https://modal.org.br/2025/03/14/visualizacao-dados-investigacao-criminal/. Acesso em: 04 jan 2026.

THAMAY, Rennan; TAMER, Mauricio. Provas no direito digital: conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020.

VIEIRA, Andrey B. C.; SANTOS, Hugo L. R. Investigação criminal e tecnologias digitais: algumas reflexões sobre o policiamento preditivo e a admissibilidade de provas digitais. Revista Brasileira de Direito Processual Penal, v. 11, n. 1, e1072, jan./abr. 2025. https://doi.org/10.22197/rbdpp.v11i1.1072