doi.org/10.51891/rease.v12i11.33639

OS DESAFIOS TECNOLÓGICOS À OBTENÇÃO E À PRESERVAÇÃO DA PROVA DIGITAL NA PERSECUÇÃO PENAL BRASILEIRA

TECHNOLOGICAL CHALLENGES TO THE COLLECTION AND PRESERVATION OF DIGITAL EVIDENCE IN BRAZILIAN CRIMINAL PROSECUTION

Gustavo de Oliveira Nogueira[1]
Juliano Leonel[2]

RESUMO: Este artigo analisa os desafios técnicos e jurídicos que o avanço das tecnologias digitais impõe à obtenção, à preservação e à utilização da prova digital na persecução penal brasileira. O problema de pesquisa consiste em saber de que modo recursos como criptografia de ponta a ponta, redes privadas virtuais, mecanismos de anonimização, armazenamento em nuvem e a própria volatilidade dos dados dificultam a identificação da origem da informação, a preservação de metadados e a demonstração da autenticidade e da integridade do vestígio eletrônico, e quais limites constitucionais condicionam a resposta estatal a esses obstáculos. O objetivo geral é examinar tais questões à luz do Direito Processual Penal, em especial da cadeia de custódia prevista nos arts. 158-A a 158-F do Código de Processo Penal, e das garantias do art. 5º da Constituição Federal. Adotou-se pesquisa qualitativa, de natureza básica, com método hipotético-dedutivo e procedimentos de pesquisa bibliográfica, documental e jurisprudencial. Os resultados indicam que a validade da prova digital depende de dois filtros cumulativos: a licitude da obtenção, submetida à reserva de jurisdição e ao princípio da proporcionalidade, e a confiabilidade do resultado, assegurada pela preservação do suporte e dos metadados e pela documentação da cadeia de custódia. Conclui-se que a tecnologia amplia a capacidade investigativa, mas eleva o risco de perda, alteração ou contestação da evidência, o que exige protocolos verificáveis, controle judicial e respeito às garantias fundamentais.

Palavras-chave: Prova digital. Cadeia de custódia. Persecução penal. Direitos fundamentais. Prova ilícita.

ABSTRACT: This article analyzes the technical and legal challenges that the advancement of digital technologies poses to the collection, preservation and use of digital evidence in Brazilian criminal prosecution. The research problem concerns how end-to-end encryption, virtual private networks, anonymization tools, cloud storage and data volatility hinder source attribution, metadata preservation and the demonstration of the authenticity and integrity of electronic evidence, and which constitutional limits govern the State's response to these obstacles. The general objective is to examine these issues in light of the chain of custody rules of Articles 158-A to 158-F of the Code of Criminal Procedure and the guarantees of Article 5 of the Federal Constitution. The study is qualitative and basic, with a hypothetical-deductive method and bibliographic, documentary and case-law research. The results indicate that the validity of digital evidence depends on two cumulative filters: the lawfulness of its acquisition, subject to prior judicial authorization and to the principle of proportionality, and the reliability of the result, ensured by preserving the original source and metadata and by documenting the chain of custody. It is concluded that technology expands investigative capacity but increases the risk of loss, alteration and challenge of evidence, requiring verifiable protocols, judicial scrutiny and respect for fundamental rights.

[1] Graduando em Direito. Centro Universitário Santo Agostinho (UNIFSA).
[2] Doutor em Ciências Criminais pela PUCRS. Mestre em Direito pela UCB. Especialista em Direito Penal e Processual Penal (UFPI/ESA). Professor. Orientador. Centro Universitário Santo Agostinho (UNIFSA).

Keywords: Digital evidence. Chain of custody. Criminal prosecution. Fundamental rights. Unlawful evidence.

1 INTRODUÇÃO

O desenvolvimento acelerado das tecnologias da informação transformou as relações sociais, os meios de comunicação e as formas de armazenamento de dados. No campo criminal, essa mudança repercute diretamente sobre a investigação e sobre a formação do conjunto probatório, já que condutas penalmente relevantes deixam rastros em celulares, computadores, aplicativos de mensagens, serviços em nuvem, redes sociais e registros de conexão. A prova digital deixou, assim, de ocupar posição periférica e passou a integrar, com frequência cada vez maior, a reconstrução dos fatos submetidos à justiça criminal.

A multiplicação das fontes eletrônicas, contudo, não tornou a prova mais simples. O mesmo ambiente que registra enorme quantidade de dados oferece mecanismos capazes de dificultar sua localização, obtenção e preservação. Criptografia de ponta a ponta, redes privadas virtuais (VPNs), ferramentas de anonimização, exclusão remota e armazenamento descentralizado reduzem a visibilidade do investigador sobre a origem e o percurso da informação, que, além disso, pode ser copiada, editada ou apagada sem deixar sinais perceptíveis ao usuário comum.

Por essas razões, a prova digital não pode ser avaliada apenas pelo conteúdo que aparece na tela. Uma captura de conversa ou a fotografia de uma mensagem podem conter informação relevante sem preservar metadados, registros de criação, histórico de alterações ou a identificação do dispositivo de origem. A análise jurídica precisa considerar não só o que o dado informa, mas também como foi obtido, preservado, documentado e apresentado em juízo.

Há, ainda, uma dimensão anterior à da confiabilidade. Diante da sofisticação dos meios de ocultação, o Estado tem recorrido a técnicas investigativas igualmente sofisticadas, como o acesso ao conteúdo de celulares apreendidos, o espelhamento de aplicativos de mensagens, a requisição de dados mantidos em nuvem e, em alguns países, a instalação de programas espiões. Essas medidas tocam diretamente a intimidade, o sigilo das comunicações e a inviolabilidade do domicílio, garantidos pelo art. 5º da Constituição Federal.

O problema que orienta o estudo pode ser assim formulado: como o avanço das tecnologias digitais dificulta a obtenção, a preservação e a utilização da prova digital na persecução penal brasileira, e quais limites constitucionais devem balizar a resposta estatal a essas dificuldades? O objetivo geral consiste em analisar os principais desafios técnicos e

jurídicos impostos pela tecnologia à prova digital no processo penal. De modo específico, busca-se contextualizar a natureza jurídica da prova digital; identificar recursos tecnológicos que dificultam a produção probatória; discutir a volatilidade da informação diante das exigências de integridade e cadeia de custódia; e examinar os limites impostos pelo art. 5º da Constituição às novas técnicas de investigação, inclusive quanto às consequências da prova ilícita.

A relevância do tema decorre do fato de que a legitimidade do processo penal depende da possibilidade de submeter a prova a controle racional e contraditório. Quando a informação digital chega aos autos sem documentação de sua origem, ou quando é obtida mediante intervenção não autorizada na esfera privada, o problema deixa de ser apenas técnico e alcança direitos fundamentais.

Quanto à metodologia, a pesquisa é de abordagem qualitativa, pois busca compreender problemas ligados à licitude, à autenticidade e à integridade da prova digital, sem pretensão de mensuração estatística, e de natureza básica, voltada à sistematização de conhecimentos úteis ao debate jurídico. Adotou-se o método hipotético-dedutivo, a partir da hipótese de que a evolução tecnológica, embora amplie as fontes de informação, eleva os riscos de volatilidade e de fragilidade da cadeia de custódia e pressiona os limites constitucionais da investigação.

Foram empregados procedimentos de pesquisa bibliográfica, documental e jurisprudencial. A pesquisa bibliográfica concentrou-se em autores que tratam de prova digital, processo penal, cadeia de custódia e direitos fundamentais, como Badaró, Prado, Lopes Jr., Lima, Pinheiro, Ferraz Júnior e Alexy. A pesquisa documental abrangeu a Constituição Federal, o Código de Processo Penal, as alterações da Lei nº 13.964/2019, a legislação sobre interceptação, organizações criminosas e internet, bem como a norma ISO/IEC 27037:2012. A análise jurisprudencial considerou precedentes do Supremo Tribunal Federal e do Superior Tribunal de Justiça sobre acesso a dados de dispositivos, ingresso domiciliar, espelhamento de aplicativos, dados em nuvem, prova ilícita e cadeia de custódia. O estudo não realiza experimento de computação forense nem levantamento estatístico de julgados.

O trabalho está organizado em quatro seções, além desta introdução. Na seção 2, examinam-se a natureza jurídica da prova digital, o princípio da mesmidade, a cadeia de custódia prevista nos arts. 158-A a 158-F do Código de Processo Penal e o problema das capturas de tela. Na seção 3, analisam-se os obstáculos tecnológicos à obtenção e à preservação dos dados, como criptografia, VPNs, anonimização, armazenamento em nuvem e volatilidade, bem como os procedimentos técnico-forenses de preservação da integridade. Na seção 4, discutem-se os

limites impostos pelo art. 5º da Constituição Federal às novas técnicas de investigação, com destaque para a reserva de jurisdição, o Tema 977 do Supremo Tribunal Federal, o espelhamento de aplicativos, o *malware* estatal e a teoria dos frutos da árvore envenenada. Por fim, na seção 5, apresentam-se as considerações finais.

2 A PROVA DIGITAL NA PERSECUÇÃO PENAL BRASILEIRA

2.1 Natureza jurídica e especificidades da prova digital

A prova digital pode ser compreendida como a informação de natureza eletrônica apta a contribuir para a demonstração de um fato juridicamente relevante. Embora costume ser aproximada da prova documental, apresenta características que os documentos físicos não possuem com a mesma intensidade: é imaterial em sua representação lógica, depende de suporte tecnológico para ser armazenada e lida e pode ser reproduzida sem que a cópia exiba qualquer diferença visível em relação ao original. Por isso, a aferição de sua força probatória deve alcançar a integridade lógica do conteúdo e os elementos que permitam identificar sua proveniência (PINHEIRO, 2021).

O uso da prova digital no processo penal acompanhou a passagem da lógica do papel para a lógica do dado. Em um primeiro momento, era comum materializar o conteúdo eletrônico por meio de impressões e fotografias de tela, como se a transposição para o suporte físico bastasse para estabilizar a informação. Com o desenvolvimento do direito digital e da computação forense, ficou mais evidente a importância dos metadados, dos registros de acesso, dos arquivos originais e do contexto técnico em que o dado foi produzido (LIMA, 2023).

No ordenamento brasileiro, a Lei nº 12.737/2012 tipificou delitos informáticos, e o Marco Civil da Internet (Lei nº 12.965/2014) consolidou parâmetros sobre registros, dados e responsabilidades na rede (BRASIL, 2012, 2014). Não se criou, com isso, uma categoria probatória autônoma, mas ficou claro que a prova digital exige leitura funcional, capaz de conciliar as regras gerais do processo penal com requisitos técnicos próprios da informação eletrônica.

Dispositivos conectados registram horários, deslocamentos, comunicações e interações com precisão superior à memória humana. Esse potencial informacional, entretanto, não se confunde com confiabilidade automática. Para que o dado tenha valor probatório, é preciso demonstrar que aquilo que chegou ao processo corresponde, de forma verificável, ao vestígio

obtido na fonte e que não sofreu alteração relevante durante a coleta, o armazenamento, a análise ou a apresentação (LOPES JR., 2024).

2.2 O princípio da mesmidade e a identidade do vestígio

A discussão sobre autenticidade encontra fundamento no princípio da mesmidade, segundo o qual o elemento apresentado ao julgador deve ser o mesmo que foi originalmente coletado, com sua identidade preservada ao longo de todo o percurso probatório. Essa preocupação é particularmente relevante no ambiente digital, no qual alterações podem ocorrer de forma silenciosa e a duplicação de arquivos constitui operação corriqueira do próprio funcionamento dos sistemas.

Para Prado (2014, 2019), a cadeia de custódia tem função epistêmica, pois oferece as condições para controlar a identidade e a história da prova. Sem registro de quem coletou o dado, em qual dispositivo, por qual método, em que momento e com quais cuidados de preservação, torna-se inviável verificar se o conteúdo apresentado corresponde ao elemento originário. A mesmidade, nessa perspectiva, não constitui mera exigência formal: liga-se à confiabilidade da informação e ao exercício efetivo do contraditório.

No campo digital, a geração e a comparação de valores *hash*, a preservação de imagens forenses, a documentação das ferramentas utilizadas e a conservação dos metadados contribuem para demonstrar a integridade do vestígio. O *hash* funciona como identificador matemático do conjunto de dados e permite verificar se o arquivo permaneceu inalterado entre etapas distintas do procedimento. Nenhum instrumento técnico substitui a análise jurídica, mas esses mecanismos reduzem a margem de incerteza e oferecem parâmetros objetivos para que acusação, defesa e juízo examinem a prova.

A mesmidade também se relaciona com o contraditório. Se a parte não tem acesso ao arquivo original, ao método de extração ou à documentação da coleta, sua capacidade de questionar a autenticidade, a completude e o contexto do dado fica seriamente reduzida. Mais do que afirmar que determinado conteúdo foi encontrado, cabe ao Estado permitir que o percurso de obtenção e preservação seja compreendido e, quando pertinente, tecnicamente auditado.

2.3 Cadeia de custódia, integridade e documentação

A Lei nº 13.964/2019 introduziu no Código de Processo Penal disciplina expressa sobre a cadeia de custódia, estabelecendo, nos arts. 158-A a 158-F, as etapas de reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte do vestígio (BRASIL, 2019). A previsão reforçou que a prova não pode ser analisada apenas no momento em que ingressa nos autos; importa todo o caminho percorrido desde o primeiro contato com o vestígio.

No ambiente digital, essas etapas precisam ser adaptadas. A coleta de um dispositivo não se esgota na apreensão física do aparelho, cujo conteúdo pode estar protegido por senha, sincronizado com serviços externos, sujeito a atualizações automáticas ou vinculado a contas que permitem exclusão remota. A preservação adequada pode exigir isolamento de rede, aquisição forense, registro dos identificadores do dispositivo, documentação de data e hora, geração de *hash* e manutenção de cópias de trabalho separadas do material original.

Badaró (2021) destaca que a mutabilidade inerente à prova digital torna indispensável a observância de *standards* metodológicos próprios da computação forense e a documentação integral da cadeia de custódia. A validade epistêmica da evidência eletrônica depende de individualizar o suporte, registrar a forma de obtenção, conservar o dado, analisá-lo por método controlável e apresentar resultados verificáveis. A cadeia de custódia aproxima-se, assim, de uma garantia de qualidade do processo de produção da prova.

A ISO/IEC 27037:2012, referência técnica internacional sobre identificação, coleta, aquisição e preservação de evidências digitais, aponta na mesma direção ao associar a confiabilidade do dado a procedimentos documentados e tecnicamente orientados. A norma não substitui o Código de Processo Penal, mas pode servir de parâmetro auxiliar para avaliar a adequação dos métodos empregados (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2012). Em suma, quanto maior a mutabilidade do objeto probatório, maior a necessidade de documentação capaz de demonstrar sua continuidade, autenticidade e integridade.

2.4 Capturas de tela, metadados e controle de autenticidade

O uso de capturas de tela de aplicativos de mensagens e redes sociais constitui um problema recorrente na prática forense. O *print* preserva uma representação visual do conteúdo, mas normalmente não contém os metadados necessários à verificação de origem, cronologia e

integridade. Imagens podem ser recortadas, editadas ou retiradas de contexto, o que não as torna imprestáveis em qualquer situação, mas impede que sejam tratadas como prova autossuficiente, sem exame das circunstâncias de obtenção e de outros elementos de corroboração.

O Superior Tribunal de Justiça tem exigido metodologia adequada para a extração e a preservação de dados de aparelhos celulares. No AgRg no HC 828.054/RN, julgado pela Quinta Turma em 23 de abril de 2024, sob relatoria do Ministro Joel Ilan Paciornik, o Tribunal considerou inadmissíveis capturas de tela extraídas de celular apreendido sem procedimento capaz de assegurar a idoneidade e a integridade dos dados (BRASIL, 2024). O ponto central não está na forma gráfica da informação, mas na ausência de garantias técnicas sobre o processo de obtenção.

A discussão alcança também o ônus da acusação. Quando o órgão acusatório pretende utilizar determinado dado digital para sustentar a imputação, cabe a ele demonstrar a confiabilidade da fonte e do procedimento empregado, sobretudo diante de questionamento concreto da defesa. A fragilidade do método de coleta não pode ser compensada pela simples aparência de verossimilhança do conteúdo (BORGES, 2024; VITAL, 2025).

3 DESAFIOS TECNOLÓGICOS À OBTENÇÃO E À PRESERVAÇÃO DA PROVA DIGITAL

3.1 Criptografia, VPNs, anonimização e armazenamento descentralizado

A criptografia de ponta a ponta é, talvez, o exemplo mais evidente da ambivalência tecnológica. O recurso protege a confidencialidade das comunicações e desempenha papel relevante na tutela da privacidade e da segurança informacional. Sob o ângulo investigativo, porém, pode impedir o acesso ao conteúdo mesmo quando há autorização judicial, deslocando a investigação para outras fontes, como dispositivos apreendidos, *backups*, registros de conexão e dados cadastrais mantidos pelos provedores.

As redes privadas virtuais acrescentam outra camada de complexidade ao ocultar ou substituir, perante os serviços acessados, o endereço IP do usuário, o que dificulta associar uma atividade a um ponto de acesso específico. Ferramentas de anonimização vão além e fazem o tráfego passar por múltiplos servidores e jurisdições. O desafio jurídico consiste em impedir que a dificuldade técnica se converta em presunção de autoria ou em justificativa para medidas desproporcionais.

O armazenamento em nuvem, por sua vez, desafia a lógica tradicional da apreensão. Um arquivo exibido no aparelho pode não estar fisicamente armazenado nele; pode residir em servidor situado em outra jurisdição, ser compartilhado por várias contas ou ser atualizado simultaneamente em diferentes dispositivos. A investigação precisa distinguir o dispositivo usado para acessar a informação do local lógico em que o dado efetivamente se encontrava.

Nenhum desses recursos é ilícito em si, e todos possuem usos legítimos amplamente difundidos. A análise processual deve, portanto, separar a existência de uma ferramenta de privacidade de qualquer inferência automática sobre a prática de crime, concentrando-se na obtenção lícita dos dados, em sua pertinência com o fato investigado e na preservação das condições de autenticidade.

3.2 Volatilidade, exclusão remota e perda de contexto

A volatilidade é traço central da prova digital. Dados podem ser alterados por atualizações automáticas, apagados por políticas de retenção, sobrescritos pelo uso cotidiano do dispositivo ou eliminados remotamente. Em aplicativos de mensagens, conteúdos podem desaparecer por configuração do próprio usuário; em serviços de nuvem, versões podem ser substituídas. A demora na adoção de medidas de preservação pode significar a perda irreversível de informação relevante.

A urgência, contudo, não dispensa a legalidade. Ela reforça, ao contrário, a importância de protocolos prévios que permitam agir de forma célere, documentada e proporcional. Na apreensão de equipamentos, devem ser registradas as condições em que foram encontrados e as providências adotadas para impedir alterações. Quando a prova estiver sob guarda de terceiros, os pedidos de preservação e as ordens de fornecimento devem delimitar o objeto, o período e os dados pretendidos.

Outro risco é a perda de contexto. Mensagens isoladas podem adquirir sentido distinto quando analisadas sem os diálogos anteriores e posteriores, sem identificação dos participantes ou sem data e horário. Nesse ponto, os metadados assumem função probatória própria: informações sobre criação, modificação, localização, dispositivo e usuário auxiliam na verificação da autenticidade e na reconstrução dos fatos. Sua ausência não invalida automaticamente o conteúdo, mas reduz as possibilidades de controle quando a autenticidade é controvertida.

3.3 Integridade, hash e procedimentos técnico-forenses

A integridade da prova digital depende da possibilidade de demonstrar que o conjunto de dados permaneceu estável desde a aquisição. A geração de valores *hash* antes e depois de cada etapa relevante do processamento é um dos mecanismos mais utilizados para esse fim, já que qualquer alteração no arquivo tende a modificar o valor calculado. O *hash*, entretanto, só é útil quando integra um procedimento documentado, no qual se sabe sobre qual arquivo ou imagem forense foi calculado, em que momento e por quem.

A aquisição forense busca preservar o conteúdo de forma controlada, evitando que a própria análise modifique o material original. Trabalha-se, sempre que possível, com cópias destinadas ao exame, conservando-se o original para eventual verificação. Também é preciso registrar *softwares*, versões, parâmetros e etapas da extração, pois ferramentas distintas podem produzir resultados diferentes ou alcançar conjuntos de dados diversos.

Santoro, Tavares e Gomes (2017) ressaltam a importância da rastreabilidade dos sistemas tecnológicos de obtenção de prova, demonstrando que a confiabilidade não decorre apenas do produto final, mas da possibilidade de reconstruir o procedimento utilizado. A observação vale integralmente para a prova digital: quanto mais complexo o sistema de coleta, maior a necessidade de transparência metodológica para que o resultado possa ser submetido ao contraditório.

Padronizar procedimentos não significa engessar a atividade pericial, já que dispositivos, sistemas e formas de armazenamento mudam rapidamente. O essencial é a existência de princípios estáveis de preservação, como identificação do vestígio, registro da coleta, minimização de alterações, controle de acesso, integridade verificável e documentação suficiente, que permitem adaptar a técnica ao caso concreto sem abrir mão da confiabilidade.

3.4 Contraditório e ônus de demonstrar a confiabilidade

A jurisprudência tem papel decisivo na definição dos limites de admissibilidade da prova digital, porque muitos conflitos chegam ao Judiciário antes que exista regulamentação específica para cada tecnologia. O movimento recente revela uma mudança de enfoque: o conteúdo digital deixa de ser aceito pela aparência e passa a ser examinado a partir do procedimento que o produziu.

Esse controle é coerente com o sistema acusatório e com a presunção de inocência. Se a prova foi produzida ou apresentada pela acusação, incumbe a ela demonstrar sua procedência e

confiabilidade, sobretudo quando a defesa aponta falhas concretas de coleta ou preservação (VITAL, 2025). Ao mesmo tempo, o processo penal deve evitar soluções automáticas, pois nem toda deficiência documental tem a mesma gravidade. Cabe ao juiz verificar se houve perda efetiva de rastreabilidade, prejuízo ao contraditório ou risco concreto de alteração.

O avanço tecnológico desloca, assim, parte do debate probatório para a qualidade do método. A pergunta deixa de ser apenas se determinada mensagem existe e passa a incluir quem a obteve, de onde foi extraída, com quais ferramentas, como foi preservada e se o resultado pode ser conferido. Há, porém, uma pergunta anterior a todas essas: se o Estado podia, naquele caso, ter acesso ao dado. É dela que trata a seção seguinte.

4 A CONSTITUIÇÃO FEDERAL DE 1988 E OS LIMITES À OBTENÇÃO DA PROVA DIGITAL

4.1 As garantias do art. 5º e a reserva de jurisdição

Um arquivo perfeitamente preservado, com *hash* conferido e cadeia de custódia documentada, continua imprestável se foi obtido com violação de direito fundamental. A licitude da obtenção e a confiabilidade do resultado constituem filtros distintos e cumulativos, e o segundo só se coloca depois de superado o primeiro.

Esse primeiro filtro tem matriz constitucional. O art. 5º da Constituição Federal declara invioláveis a intimidade e a vida privada (inciso X) e a casa (inciso XI), assegura o sigilo das comunicações e dos dados (inciso XII), condiciona a privação da liberdade ou dos bens ao devido processo legal (inciso LIV) e veda, no processo, as provas obtidas por meios ilícitos (inciso LVI) (BRASIL, 1988). A Emenda Constitucional nº 115/2022 acrescentou o inciso LXXIX, que reconhece o direito à proteção dos dados pessoais, inclusive nos meios digitais (BRASIL, 2022). Como a Lei Geral de Proteção de Dados exclui de seu âmbito o tratamento realizado para investigação e repressão de infrações penais (art. 4º, III, "d") e a lei específica sobre o tema ainda não foi editada (BRASIL, 2018a), o controle da investigação tecnológica depende, em grande medida, da aplicação direta dessas garantias.

Nesse contexto, ganha relevo a reserva de jurisdição, isto é, a exigência de que certas restrições a direitos fundamentais sejam autorizadas exclusivamente pelo Poder Judiciário, por decisão prévia e fundamentada. A Constituição a prevê expressamente para o ingresso domiciliar sem consentimento fora das hipóteses de flagrante e para a interceptação telefônica. Para o acesso a dados armazenados em dispositivos e servidores, a exigência decorre da lei, como

o art. 7º, III, do Marco Civil da Internet, e da interpretação que os tribunais vêm conferindo ao art. 5º (BRASIL, 2014).

A garantia do domicílio continua especialmente relevante, pois computadores e celulares costumam ser apreendidos no interior de residências. No RE 603.616/RO (Tema 280), o Supremo Tribunal Federal firmou a tese de que a entrada forçada em domicílio sem mandado só é lícita quando amparada em fundadas razões, justificadas a posteriori, que indiquem situação de flagrante delito, sob pena de nulidade dos atos praticados (BRASIL, 2015). Se o ingresso for ilícito, os dispositivos ali apreendidos e todo o conteúdo deles extraído ficam comprometidos, por mais sofisticada que seja a perícia posterior.

4.2 Dados armazenados, celulares apreendidos e proporcionalidade

O inciso XII protege o sigilo "de dados", mas só ressalva expressamente as comunicações telefônicas. Ferraz Júnior (1993) sustentou que o objeto da proteção é a comunicação de dados, e não os dados em si, cuja tutela estaria no inciso X e admitiria restrições ponderadas. O Supremo acolheu essa leitura no RE 418.416/SC, relatado pelo Ministro Sepúlveda Pertence, ao afirmar que a garantia recai sobre a comunicação, e não sobre os dados armazenados em computador apreendido (BRASIL, 2006).

A distinção foi pensada para um tempo em que o telefone registrava chamadas e pouco mais. O *smartphone* atual reúne conversas, fotografias, localização, dados bancários e acesso a contas em nuvem, de modo que tratar seu conteúdo como simples dado armazenado franquearia à polícia um acesso mais amplo que o de uma busca domiciliar. Por isso, o Superior Tribunal de Justiça declarou ilícita, no RHC 51.531/RO, a leitura de mensagens de WhatsApp em celular apreendido em flagrante sem autorização judicial (BRASIL, 2016), na mesma linha adotada pela Suprema Corte norte-americana em *Riley v. California* (ESTADOS UNIDOS, 2014).

O Supremo enfrentou a questão no ARE 1.042.075/RJ (Tema 977), concluído em 25 de junho de 2025. Em síntese, a tese distingue o celular encontrado fortuitamente no local do crime, cujo acesso para identificar o autor ou o proprietário dispensa ordem prévia, desde que justificado depois, do celular apreendido com base no art. 6º do Código de Processo Penal ou em flagrante, cujo conteúdo só pode ser acessado com consentimento livre e expresso do titular ou com decisão judicial prévia, fundamentada e proporcional. A Corte admitiu, ainda, providências imediatas de preservação de dados e metadados enquanto se aguarda a autorização (BRASIL, 2025). Apreender o aparelho e acessar seu conteúdo passam a ser, portanto, atos

distintos, e a preservação cautelar só cumpre sua função se for documentada de modo a demonstrar que nada foi acessado ou alterado antes da decisão judicial.

A exigência de ordem judicial, por sua vez, não encerra o problema: transfere ao juiz a tarefa de decidir se a restrição é legítima. O instrumento para isso é a proporcionalidade, examinada sob as perspectivas da adequação, da necessidade e da proporcionalidade em sentido estrito (ALEXY, 2008). A Lei nº 9.296/1996 incorporou parte desse raciocínio ao vedar a interceptação quando não houver indícios razoáveis de autoria, quando a prova puder ser obtida por outros meios ou quando o crime for punido apenas com detenção (art. 2º), e estendeu seu regime ao fluxo de comunicações em sistemas de informática e telemática (art. 1º, parágrafo único) (BRASIL, 1996). O teste ganha nova importância diante das ordens genéricas de quebra de sigilo, dirigidas a todos os usuários que estiveram em certa área. No RMS 61.302/RJ, o Superior Tribunal de Justiça admitiu a medida, mas condicionou sua validade à delimitação espacial e temporal, à fundamentação concreta e à proteção dos dados de terceiros alheios aos fatos (BRASIL, 2020).

4.3 Espelhamento, malware estatal, nuvem e infiltração virtual

O espelhamento consiste em vincular a conta de mensagens do investigado a um dispositivo controlado pela autoridade, como ocorre com o WhatsApp Web. No RHC 99.735/SC, o Superior Tribunal de Justiça recusou-se a equipará-lo à interceptação telemática: enquanto o interceptador é observador passivo, quem espelha a conta pode enviar mensagens como se fosse o usuário e apagar conversas sem deixar vestígio. Sem previsão legal e sem possibilidade de garantir a integridade do material, a prova foi declarada nula (BRASIL, 2018b). Garantia constitucional e cadeia de custódia, nesse caso, apontam para a mesma solução.

Mais intrusiva ainda é a instalação de *software* espião no dispositivo do investigado para capturar mensagens antes da criptografia, registrar a digitação ou ativar câmera e microfone. Não há lei brasileira que autorize essa técnica. O art. 8º-A da Lei nº 9.296/1996, incluído pela Lei nº 13.964/2019, disciplina apenas a captação ambiental, e seu § 2º, restabelecido com a derrubada do veto em 2021, permite instalar o equipamento de captação por operação policial disfarçada ou à noite, ressalvada a casa (BRASIL, 2019). Um *malware*, ao contrário, alcança comunicações passadas e futuras, arquivos pessoais e dados de terceiros, e sua instalação altera o próprio dispositivo, o que dificulta demonstrar, posteriormente, quais dados já existiam ali. O Tribunal Constitucional Federal alemão, ao examinar a técnica em 2008, só a admitiu

mediante lei específica, ordem judicial e perigo concreto a bens jurídicos de máxima relevância (ALEMANHA, 2008). À luz da reserva legal do inciso XII e do devido processo legal, a infiltração remota não pode ser autorizada no Brasil por analogia.

Quanto aos dados em nuvem, o Marco Civil exige ordem judicial para o fornecimento do conteúdo de comunicações privadas (art. 10, § 2º) e submete à lei brasileira as operações de coleta e tratamento em que ao menos um ato ocorra no território nacional (art. 11) (BRASIL, 2014). Na ADC 51, o Supremo reconheceu a validade dos acordos de cooperação jurídica internacional, mas afirmou que eles não impedem a requisição direta de dados a provedores que atuam no Brasil, com base no art. 11 do Marco Civil e no art. 18 da Convenção de Budapeste (BRASIL, 2023).

Na *deep web*, a identificação de autores costuma depender da atuação de agentes que se inserem nas comunidades investigadas. A infiltração virtual está prevista no Estatuto da Criança e do Adolescente (arts. 190-A a 190-E) para crimes contra a dignidade sexual de crianças e adolescentes, e no art. 10-A da Lei nº 12.850/2013 para organizações criminosas (BRASIL, 2013, 2017). Em ambos os casos, exige-se autorização judicial, prazo determinado e demonstração de que a prova não pode ser produzida por outros meios. Toda interação do agente deve ser registrada de forma íntegra, inclusive as mensagens que ele próprio enviou, para que a defesa possa distinguir a conduta espontânea do investigado daquela eventualmente estimulada pelo Estado.

4.4 Ilicitude probatória e a teoria dos frutos da árvore envenenada

A violação desses limites conduz à inadmissibilidade prevista no art. 5º, LVI, da Constituição e no art. 157 do Código de Processo Penal, que determina o desentranhamento das provas obtidas em violação a normas constitucionais ou legais e estende a vedação às provas delas derivadas, salvo quando não houver nexo de causalidade ou quando puderem ser obtidas por fonte independente (BRASIL, 1941). A teoria dos frutos da árvore envenenada já havia sido acolhida pelo Supremo no HC 93.050/RJ, relatado pelo Ministro Celso de Mello, no qual se afirmou que a ilicitude originária se transmite às provas derivadas, salvo demonstração de fonte autônoma (BRASIL, 2008).

No ambiente digital, a teoria tem peso particular, porque uma única extração irregular pode orientar toda a investigação: mensagens lidas sem autorização revelam nomes, endereços e contas que fundamentam novas quebras de sigilo, buscas e prisões. Reconhecida a ilicitude

inicial, o juiz deve examinar o nexo causal de cada elemento subsequente. Lopes Jr. (2024) adverte que as exceções da fonte independente e da descoberta inevitável devem ser interpretadas restritivamente, exigindo-se a demonstração concreta de linha investigativa autônoma, e não a mera afirmação de que a polícia chegaria ao mesmo resultado por outros meios.

É preciso, por fim, distinguir a prova ilícita da prova com falha na cadeia de custódia. A primeira resulta da violação de norma protetiva de direito fundamental; a segunda, de falhas na preservação de vestígio licitamente obtido, em regra resolvidas no plano da valoração. Quando a falha metodológica inviabiliza qualquer controle sobre a integridade do material, como no caso julgado no AgRg no HC 828.054/RN, a consequência prática se aproxima da exclusão (BRASIL, 2024). Em ambos os casos, a reserva de jurisdição e a cadeia de custódia funcionam como garantias complementares: a primeira legitima a intervenção, a segunda assegura que o resultado dela seja confiável.

5 CONSIDERAÇÕES FINAIS

A análise permite responder ao problema de pesquisa no sentido de que o avanço das tecnologias digitais dificulta a obtenção e a preservação da prova penal não apenas porque cria barreiras de acesso, mas também porque torna mais complexa a demonstração de autenticidade, integridade e origem. Criptografia, VPNs, anonimização, armazenamento em nuvem e exclusão remota fragmentam o acesso aos dados, enquanto a volatilidade e a facilidade de reprodução exigem cautela para que a evidência apresentada em juízo corresponda ao vestígio efetivamente coletado.

A hipótese de que a tecnologia pode comprometer a cadeia de custódia na ausência de procedimentos técnicos uniformes mostrou-se compatível com a doutrina, a legislação e a jurisprudência examinadas. A prova digital necessita de documentação metodológica, preservação de metadados, controle de acesso, identificação do suporte e mecanismos de verificação de integridade, como valores *hash* e cópias forenses. Sem esses cuidados, a história do vestígio não pode ser reconstruída nem submetida ao contraditório.

Verificou-se, ainda, que a resposta a esses obstáculos não pode consistir na ampliação irrestrita dos poderes investigativos. A Constituição de 1988, embora anterior à revolução digital, oferece parâmetros suficientes para disciplinar a investigação tecnológica: a reserva de jurisdição, reforçada pelo Tema 977 do Supremo Tribunal Federal quanto ao conteúdo de

celulares apreendidos; a proporcionalidade, como critério de controle das ordens judiciais; e a vedação da prova ilícita, cujos efeitos se estendem às provas derivadas. Técnicas sem base legal específica, como o espelhamento de aplicativos e o *malware* estatal, não podem ser autorizadas por analogia, seja pela reserva legal do art. 5º, XII, seja pela impossibilidade de assegurar a integridade do material produzido.

O aprimoramento da prova digital depende, assim, de investimento em capacitação, padronização de protocolos, integração entre profissionais do Direito e especialistas em tecnologia e documentação detalhada dos procedimentos. Conclui-se que a tecnologia atua, ao mesmo tempo, como fonte de prova e como fator de risco probatório. O desafio da persecução penal brasileira é aproveitar a capacidade informacional do ambiente digital sem abandonar os critérios de licitude, autenticidade, rastreabilidade e contraditório que conferem legitimidade à prova, pois apenas a evidência obtida dentro dos limites constitucionais e preservada com integridade verificável pode sustentar uma condenação.

REFERÊNCIAS

ALEMANHA. Bundesverfassungsgericht (Erster Senat). **1 BvR 370/07, 1 BvR 595/07**. Urteil vom 27. Februar 2008. Karlsruhe: BVerfG, 2008. Disponível em: https://www.bundesverfassungsgericht.de. Acesso em: 28 out. 2026.

ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008.

BADARÓ, Gustavo Henrique. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim IBCCRIM**, São Paulo, ano 29, n. 343, p. 7-9, jun. 2021.

BORGES, Ademar. A prova digital e o STJ: a inadmissibilidade do print screen e a necessidade de preservação da cadeia de custódia. **Consultor Jurídico**, São Paulo, 2024.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 28 out. 2026.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. **Diário Oficial da União**: seção 1, Rio de Janeiro, RJ, 13 out. 1941.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. **Diário Oficial da União**: seção 1, Brasília, DF, 11 fev. 2022.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. **Diário Oficial da União**: seção 1, Brasília, DF, 25 jul. 1996.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. **Diário Oficial da União**: seção 1, Brasília, DF, 3 dez. 2012.

BRASIL. Lei nº 12.850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal. **Diário Oficial da União**: seção 1, Brasília, DF, 5 ago. 2013.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. **Diário Oficial da União**: seção 1, Brasília, DF, 24 abr. 2014.

BRASIL. Lei nº 13.441, de 8 de maio de 2017. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente. **Diário Oficial da União**: seção 1, Brasília, DF, 9 maio 2017.

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. 2018a.

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 (5. Turma). **Agravo Regimental no Habeas Corpus 828.054/RN**. Relator: Min. Joel Ilan Paciornik, 23 abr. 2024. Diário da Justiça Eletrônico, Brasília, DF, 29 abr. 2024.

BRASIL. Superior Tribunal de Justiça (3. Seção). **Recurso em Mandado de Segurança 61.302/RJ**. Relator: Min. Rogerio Schietti Cruz, 26 ago. 2020.

BRASIL. Superior Tribunal de Justiça (6. Turma). **Recurso Ordinário em Habeas Corpus 51.531/RO**. Relator: Min. Nefi Cordeiro, 19 abr. 2016.

BRASIL. Superior Tribunal de Justiça (6. Turma). **Recurso Ordinário em Habeas Corpus 99.735/SC**. Relatora: Min. Laurita Vaz, 27 nov. 2018. Diário da Justiça Eletrônico, Brasília, DF, 12 dez. 2018b.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Ação Declaratória de Constitucionalidade 51/DF**. Relator: Min. Gilmar Mendes, 23 fev. 2023.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário com Agravo 1.042.075/RJ** (Tema 977 da repercussão geral). Relator: Min. Dias Toffoli, 25 jun. 2025.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário 418.416/SC**. Relator: Min. Sepúlveda Pertence, 10 maio 2006.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário 603.616/RO** (Tema 280 da repercussão geral). Relator: Min. Gilmar Mendes, 5 nov. 2015.

BRASIL. Supremo Tribunal Federal (2. Turma). **Habeas Corpus 93.050/RJ**. Relator: Min. Celso de Mello, 10 jun. 2008.

ESTADOS UNIDOS. Supreme Court. **Riley v. California**, 573 U.S. 373. Washington, DC, 25 jun. 2014.

FERRAZ JÚNIOR, Tercio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, v. 88, p. 439-459, 1993.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27037:2012**: information technology: security techniques: guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO, 2012.

LIMA, Renato Brasileiro de. **Manual de processo penal**: volume único. 12. ed. São Paulo: JusPODIVM, 2023.

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

PINHEIRO, Patrícia Peck. **Direito digital**. 7. ed. São Paulo: Saraiva Jur, 2021.

PRADO, Geraldo. **A cadeia de custódia da prova no processo penal**. São Paulo: Marcial Pons, 2019.

PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos**: a quebra da cadeia de custódia das provas obtidas por métodos ocultos. São Paulo: Marcial Pons, 2014.

SANTORO, Antonio Eduardo Ramires; TAVARES, Natália Lucero Frias; GOMES, Jefferson de Carvalho. O protagonismo dos sistemas de tecnologia da informação na interceptação telefônica: a importância da cadeia de custódia. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 3, n. 2, p. 605-632, 2017. DOI: 10.22197/rbdpp.v3i2.76. Disponível em: https://rbdpp.emnuvens.com.br/RBDPP/article/view/76. Acesso em: 28 maio 2026.

VITAL, Danilo. Cabe à acusação comprovar confiabilidade do print de WhatsApp, diz ministro. **Consultor Jurídico**, São Paulo, 14 nov. 2025. Disponível em: https://oabguacui.org.br/cabe-a-acusacao-comprovar-confiabilidade-do-print-de-whatsapp-diz-ministro/. Acesso em: 28 maio 2026.