Felipe Segura Guimarães Rocha

INSTRUMENTOS OCULTOS

de investigação criminal tecnológica

Emprego de *software* espião estatal

2025

EDITORA JusPODIVM

www.editorajuspodivm.com.br

II

PROVA DIGITAL NA INVESTIGAÇÃO: (IN)ADMISSIBILIDADE NO PROCESSO PENAL CONTEMPORÂNEO

A investigação conduzida pelas autoridades policiais deve sempre se manter atualizada, *pari passu* com o desenvolvimento tecnológico. Da mesma forma, os métodos de obtenção de provas, bem como os meios à disposição para realizá-lo, devem evoluir, em resposta às novas tecnologias. Portanto, a criminalidade informática revisitou a questão da prova de forma renovada e inserida no âmbito de uma nova realidade social.

A tradicional definição de prova referia-se a todos os meios disponibilizados às partes na tentativa de persuadir o magistrado acerca da veracidade dos fatos alegados na causa de pedir, em suas defesas e/ou em manifestações. As partes possuiriam, dessa forma, o direito de utilizar os meios de prova típicos ou atípicos para comprovar o direito em que se funda sua tese, trazendo a ideia de reconstrução (pesquisa) de um fato, demonstrado ao Juízo, capacitando-o a ter certeza sobre os eventos ocorridos e permitindo-lhe exercer a sua função[1].

Contemporaneamente, a sociedade está experimentando transformações profundas e abrangentes, tanto nas relações humanas quanto nas jurídicas, iniciadas no final do século passado. Essas mudanças são impulsionadas, sobretudo, pelo desenvolvimento

1. MARINONI, L. G.; ARENHART, S. C. **Prova**. São Paulo: Ed. Revista dos Tribunais, 2010. p. 55.

exponencial das tecnologias, especialmente daquelas relacionadas às Tecnologias da Informação e da Comunicação. Observa-se uma transição acelerada do domínio físico para o digital, um fenômeno evidenciado não só pela comercialização de bens, mas também de imóveis, no metaverso[2]. Essa realidade atesta a amplitude e a velocidade sem precedentes dessas transformações, superando qualquer outro fenômeno visto nos milênios anteriores.

Natural que, com a crescente digitalização, as evidências de atos e fatos jurídicos, assim como a execução ou descumprimento de cláusulas contratuais, estejam cada vez mais inseridas no ambiente virtual. Atualmente, a maioria dos dados é armazenada em arquivos eletrônicos, mídias sociais e serviços de armazenamento em nuvem, o que tem nos levado a uma redução significativa na impressão de documentos; práticas como revelar fotografias ou imprimir contratos são cada vez menos frequentes.

Diante dessa realidade, a doutrina jurídica foi também desafiada a desenvolver novas categorias para classificar e compreender os crimes informáticos, organizando-os e tipologias principais: próprios/impróprios, puros/impuros e mistos. Os crimes informáticos próprios e puros são foram descritos como aqueles que só poderiam ser cometidos por meio de sistemas informáticos ou redes de computadores, com a tecnologia atuando como o elemento central do delito. Exemplos incluiriam a invasão de dispositivos informáticos e a disseminação de vírus. Em contrapartida, os crimes informáticos impróprios e impuros se utilizariam da tecnologia como meio para a prática de delitos tradicionais, como fraudes eletrônicas ou difamação em plataformas online[3].

2. RAMALHO, D. S. **Métodos Ocultos de Investigação Criminal em Ambiente Digital**. Coimbra: Almedina, 2017.
3. ALBUQUERQUE, R. C. **A Criminalidade Informática**. São Paulo: Editora Juarez de Oliveira, 2006.

Os crimes mistos, por sua vez, acabam, por combinar práticas criminosas tanto no ambiente virtual, quanto no físico[4]. Um exemplo claro é o tráfico de drogas facilitado por plataformas digitais, onde as negociações ocorrem *online,* mas a entrega da substância ilícita é realizada presencialmente.

Esse cenário, no qual foi necessário categorizar e classificar os ilícitos na esfera digital, reflete uma mudança significativa na maneira como interagimos e conduzimos nossas transações no mundo contemporâneo. Todo esse espaço-tempo digital tem dado origem ao que se tem convencionado denominar de metadados. Surge, aqui, o grande problema jurídico referente à construção de uma teoria acerca das provas digitais, buscando respostas para várias questões, dentre elas: (1) o que é uma prova digital; (2) qual sua natureza jurídica; (3) como atender aos requisitos da (3a) autenticidade, (3b) integridade e (3c) preservação da cadeia de custódia; e, inclusive; (4) de quem será o ônus da prova quando se tratar de prova digital[5].

A prova é o meio utilizado pelas partes envolvidas no processo para comprovar os eventos relacionados à causa, ou seja, conferir credibilidade às afirmações apresentadas por cada uma das partes, como base para pleitear a tutela jurisdicional[6].

Ao abordar juridicamente o tema, é pertinente referenciar a taxonomia proposta por Gustavo Badaró. O autor estrutura o conceito de prova em três dimensões distintas: a atividade probatória, que engloba os atos praticados para a averiguação de um fato; o meio de prova, que se refere aos instrumentos utilizados para introduzir evidências no processo; e o resultado probatório, que é a convicção que tais meios geram no julgador sobre os fatos investigados. Ademais, como atividade comprobatória, há o

4. *Ibidem*, p. 40-41.
5. SILVA, J. A. R. de O. A prova digital: um breve estudo sobre seu conceito, natureza jurídica, requisitos e regras de ônus da prova. **Revista do Tribunal Superior do Trabalho**, São Paulo, v. 88, n. 2, abr./jun. 2022.
6. MOUGENOT, E. **Curso de processo penal**. 13 ed. São Paulo: Saraiva. Educação, 2019.

conjunto de atos para verificar um fato, "já como meio de provas, está ligado ao instrumento por meio do qual a prova é produzida". Finalmente, resultado probatório está ligado ao convencimento que geram no julgador e nas partes[7].

Aury Lopes Jr., por sua vez, define prova, dentro do contexto processual, como os instrumentos empregados para a reconstrução de um evento histórico, mais especificamente, um delito: "[…] a prova possui a função de convencimento do magistrado, através de elementos de reconstrução do fato criminoso que criam condições para 'a atividade recognitiva do juiz acerca de um fato passado'"[8].

No que se refere à prova digital, esta decorreria de fatos praticados por meio de dispositivos eletrônicos e a respeito dos quais a certificação de fiabilidade pudesse ser realizada. Muito embora os dados digitais possam ser diretamente percebidos em seu conteúdo informativo por aqueles que têm acesso a eles, tais dados não possuem uma materialidade imediatamente constatável[9].

Cita-se como exemplos: o envio de um *e-mail* ou de uma mensagem por aplicativo (*WhatsApp*, *Telegram*, entre outros); cópia ou desvio da base de dados; cópia de *software*; disponibilização de um vídeo na internet (conteúdo íntimo ou difamador); dentre outros. Também é possível que o meio digital sirva como instrumento para demonstrar a existência de um fato ocorrido em meio não digital. Basta pensar em uma ata notarial lavrada a partir da constatação pelo tabelião de foto em mídia social em que constam juntos um colaborador e um diretor de uma empresa concorrente, a fim de demonstrar o conluio fático entre eles.

7. BADARÓ, G. H. **Processo Penal**. 9. ed. São Paulo: Revista dos Tribunais, Thomson Reuters Brasil, 2021, p. 438-439.
8. LOPES, A. Jr. **Direito Processual Penal**. 16ª ed. São Paulo: Saraiva Educação, 2016, p. 383.
9. MARCELLO, D. La prova digitale nel processo penale. **Rivista di Diritto Processuale**, 2011.

Na seara criminal, é factível que, por meio de monitoramento de conta autorizado judicialmente, de conversas de *WhatsApp*, seja possível provar a prática de tráfico de drogas, ou mesmo de crimes de alta complexidade investigativa. Os fatos não são digitais em si, mas os suportes digitais servem de mecanismo para sua demonstração[10]. Rennan Thamay e Mauricio Tamer, a seu turno, conceituam a prova digital como sendo um instrumento jurídico voltado à demonstração da ocorrência (ou não) de um fato e as suas circunstâncias, tendo ele ocorrido total ou particularmente. Ainda, a prova digital "é o meio de demonstrar a ocorrência de um fato ocorrido em meio digital, ou que tem no meio digital um instrumento de demonstração de determinado fato (e) de seu conteúdo"[11].

A prova digital poderia, então, ser sinteticamente definida como sendo "os dados em forma digital (no sistema binário) constantes de um suporte eletrônico ou transmitidos em rede de comunicação, os quais contêm a representação de fatos ou mesmo, ideias"[12]. A legislação processual penal em vigor, por sua vez, não aborda explicitamente o conceito desta denominada "prova digital". No entanto, o projeto do novo Código de Processo Penal busca regular esses elementos, evitando detalhes excessivos ao propor uma definição clara e abrangente, estipulando que se considera "prova digital toda informação armazenada ou transmitida em meio eletrônico hábil ao esclarecimento de determinado fato"[13].

10. THAMAY, R.; TAMER, M. **Provas no direito digital**: conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020.
11. *Ibidem*, p. 33.
12. VAZ, D. P. **Provas digitais no Processo Penal**. Tese (Doutorado em Direito), Faculdade de Direito da USP, Universidade de São Paulo, São Paulo, 2012, p. 147.
13. BRASIL. **Projeto de Lei n. 8.045/2010.** Brasília: Câmara dos Deputados, 2010. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1668776. Acesso em: 11 abr. 2024.

As provas digitais poderiam ser categorizadas conforme as disposições tradicionais do Código de Processo Civil (CPC): poder-se-ia argumentar que se enquadram no conceito *lato sensu* de prova documental, conforme estabelecido no artigo 422 e parágrafos do CPC, ou, até mesmo, seriam consideradas documentos eletrônicos, conforme os artigos 439 a 441 do mesmo código. No entanto, esta análise preliminar não captura plenamente a essência e a amplitude que as provas digitais têm adquirido no âmbito processual brasileiro[14].

O cenário atual demanda um olhar mais acurado e uma abordagem que reconheça as provas digitais não apenas como uma extensão das categorias tradicionais, mas como uma categoria própria, dotada de peculiaridades e desafios específicos. Essa nova perspectiva não é meramente acadêmica, mas uma exigência prática que reflete as transformações trazidas pela era digital ao Direito Processual.

Argumenta-se, portanto, com base em uma análise detalhada, além de uma compreensão profunda das dinâmicas processuais contemporâneas, pela necessidade de se reconhecer as provas digitais como sendo um meio atípico de prova: tal reconhecimento implica não apenas em uma expansão conceitual, mas também em toda uma adaptação legislativa e operacionalização procedimental que considere suas especificidades. Isso significa ir além da mera classificação, alcançando a elaboração de diretrizes que assegurem sua correta admissibilidade, avaliação e valoração dentro do processo judicial.

A adoção dessa postura não é um capricho teórico, mas uma resposta necessária às exigências de uma sociedade cada vez mais digitalizada; afinal, reconhecer as provas digitais como um meio próprio de prova é reconhecer também a evolução do Direito e da prática jurídica em face das novas realidades. Tal abordagem reforça o compromisso do sistema jurídico com a busca pela

14. SILVA, J. A. R. de O. A prova digital: um breve estudo sobre seu conceito, natureza jurídica, requisitos e regras de ônus da prova. *op. cit.*

verdade factual, a justiça efetiva e a adequação aos novos desafios impostos pela tecnologia.

Reconhecidas tais premissas, é fundamental que a comunidade jurídica e as autoridades policiais estejam preparadas para lidar com as complexidades dessas ditas provas digitais. A definição e compreensão do que constitui uma prova digital são desafios que devem ser abordados com clareza e precisão, garantindo a autenticidade, integridade e preservação da cadeia de custódia dessas evidências.

Na articulação dessas idiossincrasias, é imprescindível a consideração da teoria geral da prova, um edifício teórico erigido ao longo de séculos, cujas reflexões e princípios fornecem substrato valioso para a compreensão da essência da prova digital e para o delineamento de como esta deve ser adequadamente tratada, no âmbito jurisdicional.

Desdobra-se, assim, uma análise bifurcada sobre as provas digitais: por um lado, a vertente concernente aos fatos ou atos jurídicos perpetrados em ambientes digitais, sustentados por meios digitais – que se qualificam como provas digitais de primeiro grau; por outro lado, a análise se estende aos fatos ou atos jurídicos consumados em meios tradicionais, em suporte físico, mas cuja demonstração se viabiliza por intermédio de meios digitais disponíveis – configurando o que se denomina como provas digitais de segundo grau.

A comunidade acadêmica, diante desse panorama, tem atribuído à prova digital a qualificação de prova documental, reconhecendo sua natureza jurídica. O documento, seja em suporte físico ou eletrônico, constitui o registro fidedigno do fato e suas circunstâncias, consagrando-se a prova documental como o corolário do processo, sob a égide do procedimento legalmente estabelecido para sua produção. A distinção premente, desse modo, advém do tipo de suporte de origem da prova documental. Originada de suporte físico, tem-se uma prova documental *stricto sensu*; emanada de suporte digital ou eletrônico – como computadores,

CDs, HDs, internet –, caracteriza-se um documento eletrônico ou digital, ergo, uma prova documental *lato sensu*[15].

Para que a prova digital ascenda à mesma estatura de credibilidade atribuída à prova documental tradicional, é imperativo que ela esteja imbuída da mesma segurança jurídica, condição que somente se satisfaz mediante a rigorosa observância de três pilares fundamentais: (1) autenticidade – a origem do fato digital deve ser inquestionável, sendo a autenticidade a garantia de que o autor presumido é efetivamente o autor real; (2) integridade – é vital assegurar a imutabilidade do conteúdo da prova digital, que se consagra íntegra ao resistir incólume a quaisquer modificações ou adulterações; e (3) preservação da cadeia de custódia – é essencial salvaguardar a autenticidade e a integridade ao longo de todo o itinerário de produção da prova digital, desde sua identificação até sua inserção nos autos, diligenciando para documentar (a) datas e horários de acesso e extração da prova, assim como o local de tal ocorrência; (b) eventual acesso de terceiros à prova; e (c) a ocorrência de modificações inevitáveis durante a extração dos dados[16].

A evidência digital exige a aplicação das normativas clássicas sobre o ônus da prova, conforme previsto para a apresentação e impugnação de documentos. Impera, portanto, a adesão às diretrizes do artigo 429 do Código de Processo Civil, que delineiam o marco inicial para a definição desse encargo probatório. Resumidamente, impõem-se duas normas basilares: (1) caso a parte oposta a uma prova digital não conteste sua assinatura ou autoria, mas apenas seu conteúdo, recai sobre ela o ônus da prova; (2) se a parte contrária negar sua assinatura ou desmentir a autoria do fato digital, incumbirá ao proponente do fato o ônus de

15. SILVA, J. A. R. de O. A prova digital: um breve estudo sobre seu conceito, natureza jurídica, requisitos e regras de ônus da prova. *op. cit.*

16. THAMAY, R.; TAMER, M. **Provas no direito digital**: conceito da prova digital, procedimentos e provas digitais em espécie. *op. cit.*

comprovar sua ocorrência, pois, nesta circunstância, materializa-se uma negativa absoluta[17].

Para que então produza informação jurídica útil para a reconstrução histórica dos fatos, a manipulação da prova digital deve seguir princípios informáticos: o *National Institute for Standard and Technology* (NIST), por sua vez, distingue quatro fases da perícia computacional: captura de dados, exame, análise e elaboração de relatórios; fazendo ainda a seguinte consideração:

> Durante a coleta, os dados relacionados a um evento específico são identificados, rotulados, registrados e coletados, e sua integridade é preservada. Na segunda fase, de exame, ferramentas e técnicas forenses adequadas aos tipos de dados que foram coletados são executados para identificar e extrair as informações relevantes dos dados coletados, protegendo sua integridade. O exame pode usar uma combinação de ferramentas automatizadas e processos manuais. A próxima fase, a análise, envolve a análise dos resultados do exame para obter informações úteis que abordem as questões que foram o ímpeto para a realização da coleta e do exame. A fase final envolve relatar os resultados da análise, que podem incluir a descrição das ações executadas e recomendar melhorias para políticas, diretrizes, procedimentos, ferramentas e outros aspectos do processo forense[18].

Importante salientar que, cada elemento guardará suas próprias especificidades de acordo com sua natureza e, deve ser administrado de maneira individualizada de forma resguardar a cadeia de custódia e evitar o reconhecimento de futuras nulidades

17. SILVA, J. A. R. de O. A prova digital: um breve estudo sobre seu conceito, natureza jurídica, requisitos e regras de ônus da prova. **Revista do Tribunal Superior do Trabalho**, São Paulo, v. 88, n. 2, abr./jun. 2022, p. 218.

18. KENT, K. CHEVALIER, Suzanne, GRANCE Tim, DANG Hung. **Guide to integrating forensic techniques into incident response**: recomendations of the National Institute of Standards and Technology. Specialpublication. Gaithersburg: NIST, 2006. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf. Acesso em: 8 maio 2024.

procedimentais. Nesse âmbito, observa-se que no Brasil, a elaboração da norma técnica ABNT – NBR ISO/IEC 27037:2013 foi de grande relevância – uma vez que fornece orientações para a identificação, captura, aquisição e preservação de evidências digitais, integrando-se à família ISO 27000, a qual trata da Gestão da Segurança da Informação.

A normativa aborda, entre outros aspectos, a necessidade em se observar criteriosamente a cadeia de custódia, documentando rigorosamente todas as ações e assegurar que a evidência não seja alterada, intencionalmente ou não, durante sua manipulação. A norma é parte da família ISO 27000, que trata da Segurança da Informação, e busca harmonizar práticas internacionalmente para facilitar o uso e a troca de evidências digitais entre diferentes jurisdições, e busca estabelecer uma cronologia de movimentação e manuseio da evidência digital.

Dentre outras padronizações, ela dispõe que, durante a análise da evidência digital, deve-se incluir, no mínimo, uma identificação única para cada evidência (*hash)*, além de registros detalhados de quem lhe fora franqueado o manuseio, especificando o tempo e o local do acesso. Além disso, devem ser documentadas quaisquer alterações realizadas nas evidências, incluindo a identificação do usuário responsável por este manuseio.

1. AQUISIÇÃO DA FONTE DE PROVA DIGITAL: O ÔNUS DA PROVA A RESPEITO DA PROVA DIGITAL

Para que a prova digital seja utilizada sem contestações quanto à sua autenticidade e valor, é necessário que ela atenda, no mínimo, pressupostos de *confiabilidade*: a integridade, autenticidade e preservação da cadeia de custódia, os quais são expressamente previstos pela legislação para o registro de atos processuais eletrônicos no artigo 195 do Código de Processo Civil: "A falha em qualquer deles resultará na fragilidade da própria prova,

tornando-a fraca e até, por vezes, imprestável ou impotente de produzir efeitos no caso concreto"[19].

Por integridade, entende-se que a garantia de que o conteúdo da prova não foi adulterado ou manipulado, devendo ser auditável e periciável; a autenticidade depende da clareza da origem do documento digital, preservando-o desde sua identificação, captura e extração de resultados. Em outras palavras, a prova será íntegra quando "isenta de qualquer modificação em seu estado ou adulteração desde o momento da realização do fato até a apresentação do resultado prova", estando apta "a demonstrar a reprodução do fato em sua completude e integridade"[20].

A cadeia de custódia visa garantir o acompanhamento de toda a manipulação e deslocamento da prova colhida: "a ideia é construir verdadeiro registro histórico da evidência, de toda a vida da prova – caso alguém decida seguir os mesmos passos já percorridos durante a produção da prova, o resultado será o mesmo. Nesse ponto, é importante sinalizar datas, horários, quem teve acesso, onde o acesso foi feito e até quaisquer alterações inevitáveis relacionadas"[21].

As salvaguardas estipuladas pela legislação citada nos conduz a, pelo menos, duas conclusões relevantes para o tratamento de provas digitais: (1) que a validade probatória do conteúdo de um documento está intrinsecamente ligada à sua origem e, consequentemente, à credibilidade da fonte que o gerou; e (2) que a integridade das informações, quando não se tem acesso direto ao documento original, depende da confiabilidade de quem as converte em formato documental para ser inserido nos registros do processo.

19. THAMAY, R.; TAMER, M. **Provas no direito digital: conceito da prova digital, procedimentos e provas digitais em espécie**. São Paulo: Thomson Reuters Brasil, 2020, p. 39-40.
20. *Ibidem*, p. 45.
21. *Ibidem*, p. 114.

A autenticidade pode ser verificada por meio da utilização de outros métodos de verificação, como a tecnologia de certificação digital, que inclui o uso de chaves públicas e privadas (por meio da ICP-Brasil, por exemplo), e a validação por meio da função *hash*. A verificação por esta última função assegura que o documento digital não foi alterado, comparando-se o valor *hash* original com o gerado no momento da verificação, garantindo assim a integridade e autenticidade das informações originais.

A técnica, ou função de *hash*, é um método fundamental na extração de dados, especialmente no contexto de segurança da informação e integridade dos dados. *Hash* é um algoritmo que transforma uma entrada de dados de qualquer tamanho em uma saída de tamanho fixo, normalmente uma *string* de caracteres. Essa *string* é conhecida como valor *hash*, ou simplesmente *hash*. Essa técnica permite a verificação de "assinaturas digitais efetivamente exclusivas para qualquer parte dos dados digitais"[22].

David Ramalho discorre que a função *hash* é aplicada a certos documentos ou a um conjunto de dados informáticos, de modo a criar um código alfanumérico que funciona como uma impressão digital[23]. Uma das principais observações a serem feitas em relação à função de *hash* é que pequenas mudanças na entrada produzem saídas radicalmente diferentes, sendo que, tal circunstância torna essa função *o* mecanismo ideal para a verificação da integridade dos dados. Se o *hash* de um arquivo recebido corresponde ao *hash* do arquivo original, pode-se confiar que o arquivo não foi alterado durante o procedimento de captura.

Por sua vez, os algoritmos responsáveis pela criação da imagem devem ser exatamente iguais aos originais, considerando a "mesmidade" dos dados copiados. O princípio da "mesmidade" é de fácil comprovação pois a aplicação da função *hash* em um

22. MARSHALL, A. **Digital forensics: digital evidence in Criminal Investigation**. Chichester: John Wiley & Sons, 2008, p. 47.

23. RAMALHO, D. **Métodos ocultos de investigação criminal no ambiente digital**. *op. cit.*

conjunto idêntico de dados resulta sempre no mesmo valor[24], de maneira que "a alteração de apenas um único *bit* resulta em valores de *hash* completamente diferentes", tornando a integridade da prova penal questionável.

Ainda no que tange à aferição da integridade dos fatos, esta se refere à correta captura dos dados e à correspondente descrição em ata notarial, ou ainda, à realização de um exame pericial minucioso para atestar a sua devida certificação. A cadeia de custódia, por seu turno, garante o acompanhamento do deslocamento e tratamento da prova digital – o que será abordado adiante.

No que se refere aos métodos empregados no processo de captura de evidências digitais, ressalta-se a rápida preservação de dados, a retenção de informações de comunicação em trânsito e, por último, a realização de buscas e apreensões de dados informáticos[25].

O processo de captura de evidências digitais é geralmente dividido em dois estágios distintos. O primeiro é destinado à busca e apreensão de dispositivos eletrônicos e digitais de armazenamento de informações, ou seja, qualquer meio físico que contenha dados potencialmente relevantes para a investigação criminal. Já o segundo estágio concentra-se na busca das verdadeiras fontes de provas digitais, exigindo a criação de uma cópia completa e exata (imagem) do dispositivo. Somente após essa etapa é possível identificar as evidências pertinentes, conforme estabelecido pela ordem judicial[26].

Para materializar essas apreensões, é necessário abordar também algumas das formas de obtenção de fontes de prova digitais. A primeira delas envolve o acesso ao conteúdo do sistema, por meio da apreensão do dispositivo ou equipamento eletrônico.

24. *Ibidem*, p. 125.

25. SALT, M. **Tecnologia informática**: un nuevo desafio para el derecho procesal penal?, 2017.

26. MENDES, C. H. C. F. **Tecnoinvestigação criminal**: entre a proteção de dados e a infiltração por *software*. Salvador: Juspodivm, 2020.

Outra possibilidade é alcançar as informações desejadas em um sistema digital sem a necessidade de apreender o suporte físico, o que é denominado de "*remote search*". No entanto, apenas se configuram como fontes de evidência digital, quando for possível demonstrar a confiabilidade e a integridade das provas adquiridas por meio desses acessos remotos enumerados.

Em relação ao ônus da prova, é crucial reconhecer a novidade desse tema no âmbito das evidências digitais. Tanto a doutrina, quanto a jurisprudência, continuam delineando as bases para compreender a prova digital, sua natureza jurídica e os critérios essenciais para sua admissibilidade e eficácia em processos judiciais, temas que foram superficialmente abordados anteriormente.

Nesse processo de formulação teórica, a determinação das normas aplicáveis – seja de caráter estático ou dinâmico – ao ônus da prova, na apresentação de evidências digitais em processos judiciais, deve se fundamentar na teoria geral das provas. É nesse campo que juristas podem encontrar fundamentação teórica e normativa para orientar a definição de regras específicas relacionadas ao ônus probatório, no contexto de provas digitais.

Sob esse prisma e, considerando a prova digital como sendo uma prova documental *lato sensu*, conforme indicam as tendências atuais na doutrina e na jurisprudência, é prudente aplicar, inicialmente, as normativas tradicionais do ônus da prova, tal como são utilizadas para provas documentais convencionais. Essa abordagem mantém-se até que uma compreensão mais detalhada sobre as provas digitais seja desenvolvida.

Pela leitura do artigo 429 do Código de Processo Civil Brasileiro, verifica-se a delimitação de um marco inicial para definir a responsabilidade probatória em casos envolvendo fatos digitais. A questão central se torna a determinação de quem – autor ou réu – deve provar o fato digital alegado no processo. Se uma parte, seja autor ou réu, não contestar a assinatura em um documento digital, ou mesmo reconhecê-la, conforme o artigo 410, II, do CPC, ela assume um significativo ônus probatório, em linha com

o artigo 429, I, do mesmo Código de Processo Civil. Ademais, em seu artigo 412, resta estipulado que um documento particular, uma vez não contestado, autentica a declaração atribuída ao seu autor.

Consequentemente, a regra primária sobre o ônus probatório, ao menos em âmbito cível, em matéria de provas digitais, é a seguinte: se uma parte não contesta a autenticidade de uma prova digital, mas questiona seu conteúdo, o ônus da prova recai sobre ela. Nesse contexto, é comum a alegação de falta de integridade na prova digital, como adulteração ou incompletude, por exemplo, em capturas de tela de conversas no *WhatsApp*. Também pode haver alegações sobre violação da cadeia de custódia na extração de dados, atribuindo a essa parte o ônus da prova.

Sob esse raciocínio, se acaso alegada a adulteração de informações em uma prova digital, caberá à parte contrária provar tal fato, apresentando o documento original, a prova integral (como conversas completas), realizando perícia ou solicitando expedição de ofícios a empresas detentoras dos dados originais, como provedores de internet.

Se uma pessoa, física ou jurídica, argumentar em juízo o uso indevido de dispositivos, como cartão ou *pen drive* que contenham sua assinatura digital, ela tem o desafio probatório de demonstrar tal ocorrência. Nas relações jurídicas, impera a necessidade de se respeitar a boa-fé objetiva, pressupondo-se que a assinatura foi utilizada pela pessoa autorizada, até que se prove o contrário.

Quando a autenticidade de uma assinatura em um documento digital é questionada, ou a autoria do fato digital é negada, criando uma incerteza objetiva sobre quem de fato realizou a ação, a responsabilidade de provar, tanto a ocorrência quanto a autoria do fato digital, recai sobre a parte que o afirma (esta obrigação é estabelecida pelo artigo 429, II, do Código de Processo Civil). Nesse contexto, o fato digital pode ser considerado, com ainda mais razão, como um fato constitutivo do direito do demandante, similar ao que ocorre em ações de indenização por danos morais.

Em casos nos quais o autor de uma ação não consegue comprovar de forma contundente que um determinado fato digital ocorreu e que foi o réu quem o cometeu – como uma violação trabalhista manifestada por meio de mensagens ofensivas no *WhatsApp* ou publicações em redes sociais como *Facebook* e *Instagram* –, sua reivindicação é susceptível de ser julgada improcedente.

Quando a ocorrência de um ilícito ou de sua autoria for categoricamente negada, o ônus da prova recairá sobre a parte que alega a existência do fato digital. É necessário que essa parte demonstre não apenas o conteúdo da prova digital, mas também que a parte adversa cometeu realmente o ato ou fato jurídico em questão. Isso pode incluir situações diversas, como a assinatura de um documento digital, a realização de viagens ou mesmo um período de licença médica.

Assim sendo, verifica-se que, ao lidar com negações veementes de autoria ou da própria ocorrência do ilícito, a carga probatória passa a ser um fator decisivo. A comprovação não se limita à apresentação da prova digital, mas se estende à necessidade de demonstrar, de maneira inequívoca, a participação do oponente no ato jurídico questionado. Esse cenário requer um exame minucioso de todos os elementos apresentados, avaliando-se a consistência e a confiabilidade das evidências digitais, em consonância com os preceitos legais vigentes.

No contexto penal, no entanto, a aplicação de regras do Código de Processo Civil (aplicado subsidiariamente) deve ser realizada com um pouco mais de cautela: a presunção de inocência, que se extrai do artigo 5º, inciso LVII, da Constituição Federal, determina que "ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória". Isso significa que, em regra, é o Ministério Público (acusação) que carrega o ônus de provar a culpa do réu, e não o contrário; é responsabilidade da acusação, em princípio, provar que esses dados são relevantes e vinculados ao réu de maneira lícita e convincente. Eventuais desafios que surjam com a prova digital, como a volatilidade dos dados e a complexidade técnica, não alteram o princípio