Sauvei LAI

POLICEWARE

Infecção de Software em Sistema Informático do Investigado para Fins de Vigilância Eletrônica

2024

EDITORA JusPODIVM

www.editorajuspodivm.com.br

2

PROVA DIGITAL

2.1. DIREITO FUNDAMENTAL À PROVA

A etimologia da palavra "prova" remonta ao latim *probatio*, derivado do verbo *probare*[1], cujo significado abrange a ideia de demonstração e reconhecimento de algum fato. *Probare* emana de *probus*[2], refletindo a noção de probo, integridade, confiança e correção nas operações intelectuais voltadas à busca do conhecimento da verdade.

A adequada verificação dos fatos, sobre os quais se estruturam as pretensões das partes no processo, constitui premissa indeclinável para se alcançar uma decisão justa, compreendendo-se a prova a partir de "um contraditório em sentido forte ou caracterizado como substancial", que reclama "a presença das partes como instrumento de formação e produção da prova e coprodução da atividade"[3]. É dentro dessa moldura que se poderá discutir apropriadamente acerca de um verdadeiro e legítimo direito à prova.

---

1. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_publicacao_divulgacao/doc_gra_dout_crim/crime%2038.pdf. Acesso em: 22/01/2024.
2. Disponível em: https://origemdapalavra.com.br/palavras/prova/. Acesso em: 22/01/2024.
3. SAMPAIO, Dênis. Valoração da prova penal. Florianópolis: Emais, 2022, p. 435.

Somente a prova, preponderante e convincente da autoria e do crime, de acordo com o standard probatório[4], exigido pelo Estatuto de Roma do Tribunal Penal Internacional (promulgado pelo Decreto nº 4.388 de 25 de setembro de 2002[5]), possui força suficiente para afastar o princípio constitucional da não culpabilidade (art. 5°, LVII), além da dúvida razoável[6][7], o "que representa a maior garantia do cidadão contra o uso arbitrário do poder punitivo"[8].

Ao mesmo tempo em se aprimora os critérios probatórios para a condenação, torna-se imperativo dotar as autoridades de investigação de poderes legais, eficazes e apropriados para a persecução criminal e a obtenção de evidências, especialmente de natureza digital. Caso contrário, os desafios se transformarão em obstáculos praticamente intransponíveis, fomentando a impunidade e a violação dos direitos humanos, sobretudo do ponto de vista da vítima.

2.2. CONCEITO DE PROVA DIGITAL

A prova digital, diante da crescente expansão dos crimes cibernéticos (próprios ou impróprios), assume cada vez mais importância no processo penal contemporâneo e pode ser conceituada como toda "informação armazenada ou transmitida em meio eletrônico", em consonância com o art. 4º[9] do Projeto de Lei n° 4.939/2020.

---

4. "Um modelo de constatação de prova". *Ibid.*, p. 385.
5. Artigo 66.3. Para proferir sentença condenatória, o Tribunal deve estar convencido de que o acusado é culpado, além de qualquer dúvida razoável.
6. "[...] jamais basear-se em termos de grau de confiança subjetiva certeza pessoal de quem deve proferir uma decisão". SAMPAIO, Dênis. Valoração da prova penal. Florianópolis: Emais, 2022, p. 438.
7. "[...] essa prova deve resultar da coexistência de inferências suficientemente fortes, claras e concordantes ou de presunções de fato similares não refutadas. [...] Não é uma mera dúvida possível, é aquele estado de processo que, depois da comparação e da consideração completa por todas as provas, deixa a mente dos jurados em tal condição que não podem dizer que sentem uma convicção perturbável acerca da verdade da imputação". *Ibid.*, p. 453-454.
8. GOMES Filho, Antônio Magalhães. YARSHELL, Flávio Luiz. (org). Estudo em homenagem à professora Ada Pellegrini Grinover. São Paulo: DPJ, 2005, p. 303.
9. Art. 4º Considera-se prova digital toda informação armazenada ou transmitida em meio eletrônico que tenha valor probatório.

Outros a definem como o "instrumento jurídico vocacionado a demonstrar a ocorrência ou não de determinado fato e suas circunstâncias, tendo ele ocorrido ou não em meios digitais"[10]. As conceituações se referem aos "dados produzidos e processados a partir da 'lógica binária', que tem potencial para serem utilizados como fonte de prova"[11], independente do suporte físico em que se acham armazenados.

Os dados digitais são coletados, através dos meios de obtenção de prova digital, como a busca e apreensão de um computador e a sua extração. Posteriormente, são introduzidos no processo por um meio de prova, a exemplo do laudo pericial dos dados eletrônicos adquiridos do computador e devidamente analisados.

O art. 1º, "c", da Convenção de Budapeste, descreve os dados informáticos como "qualquer representação de fatos, de informações ou de conceitos sob uma forma suscetível de processamento num sistema de computadores, incluindo um programa, apto a fazer um sistema informático executar uma função".

Um ponto relevante é entender que a prova digital se constitui, na verdade, do produto de um contexto. É um erro objetificar a prova digital e achar que ela se traduz no suporte físico que a armazena (pendrive, computador, dispositivo móvel, tablet etc.), pois "o que importa é o dado ou arquivo digital em si, que pode ser obtido quando está armazenado em um dispositivo ou quando está sendo transmitido"[12]. Para sua plena existência e utilidade, o exame da prova digital deve ser contextual e de acordo com o caso concreto, até porque "outras pessoas podem ter utilizado o dispositivo praticante

10. THAMAY. Rennan e Tamer, Maurício. Provas no direito digital: conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: RT, 2020. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/2-provas-em-especie-provas-no-direito-digital-conceito-da-prova-digital-procedimentos-e-provas-digitais-em-especie/1147564673?unlock-feature-code=abnt_quote_doctrine&unlock-from-component=AbntModal. Acesso em: 22/11/2023.

11. MINTO, Andressa Olmedo. A prova digital no processo penal. São Paulo: LiberArs, 2021, p. 15.

12. *Ibid*., p. 32.

da conduta, bem como esse dispositivo pode ter sofrido uma contaminação ou controle remoto"[13]: quem produziu os dados ou os armazenou, como, quando e onde? Qual foi o suporte físico de armazenamento? Como foi a extração, aquisição, coleta e análise?

Por conseguinte, não está a se falar de um mero conjunto de zeros e uns, organizado em uma pré-estabelecida ordem para ser interpretado como informação legível pelo ser humano, mas, sim, de uma realidade multivariada, cuja manifestação deverá ser perseguida pelos meios idôneos para a real e completa formação do chamado "princípio do mosaico"[14] da prova digital.

2.3. NATUREZA JURÍDICA DA PROVA DIGITAL

A prova digital, segundo a doutrina especializada[15], não é, na realidade, um novo meio de prova[16], porém uma fonte de prova *sui generis*[17], cujo suporte físico (como um pendrive) armazena uma informação de pertinência e relevância processual e, ao ser levada ao conhecimento do juízo competente (através, por exemplo, do laudo pericial dos dados eletrônicos extraídos e analisados), é, só então, classificada como meio de prova.

---

13. SYDOW, Spencer Toth. Curso de direito penal informático. Salvador: Juspodivm, 2022, p. 125.
14. "A valoração, pois, é feita através da reunião de diversas peças de informação que, consideradas como um todo, fazem com que se atinja materialmente uma conclusão segura". *Ibid*., p. 124.
15. "En conclusión, la prueba tecnología no está considerada como un nuevo medio de prueba en sí, sino como una de tantas fuentes de prueba, donde "la fuente de prueba electrónica, es el soporte (material) en el cual ha quedado grabado el hecho histórico que vamos a introducir en el proceso y el medio probatorio será la reproducción realizada ante el órgano jurisdiccional"108. Por lo tanto, toda prueba electrónica debe ser aportada al proceso a través de cualquiera de los medios de prueba enunciados en el artículo 299.1 de la LEC". ILLÁN FERNÁNDEZ, José María. La prueba electrónica, eficacia y valoración en el proceso civil. Navarra: Aranzadi, 2009, p. 264. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.pensamientopenal.com.ar/system/files/2017/04/doctrina45110.pdf. Acesso em: 22/11/2023.
16. "[...] instrumento ou a atividade por meio dos quais os dados probatórios (elementos de prova) são introduzidos e fixados no processo (produção da prova)". GOMES Filho, Antônio Magalhães. YARSHELL, Flávio Luiz. (org). Estudo em homenagem à professora Ada Pellegrini Grinover. São Paulo: DPJ, 2005, p. 308.
17. Fala-se em fonte de prova para designar as coisas ou as pessoas das quais pode-se conseguir os elementos de prova. *Ibid*., p. 30.

Portanto, conclui-se que os meios, que introduzem os elementos de prova[18] no processo, não mudaram substancialmente, mas as fontes de prova, sim[19].

Mais distintivamente, cuida-se de uma fonte real de prova (e não pessoal), porém pertencente a uma "categoria jurídica própria"[20], se forem considerados "os suportes físicos, em que se encontram armazenados os dados – computadores, pendrives, CDs, DVDs, telefones celulares, aparelho de MP3, as urnas eletrônicas, câmeras de vídeo ou fotografias etc. Do mesmo modo, com relação aos arquivos neles contidos – imagens, vídeos, músicas, documentos de texto, correspondências eletrônicas, página de sites, dentre outros"[21].

Os meios de obtenção de prova digital se traduzem na forma, no procedimento e no protocolo para a aquisição dessa fonte, empregando-se diversos tipos de pesquisa, como a busca e apreensão física de dispositivos eletrônicos[22] e a infiltração virtual em redes sociais, estruturada no art. 10-A da Lei nº 12.850/2013 com redação dada pela Lei nº 13.964/2019[23].

2.4. CLASSIFICAÇÃO

A prova digital pode relacionar-se com os fatos praticados nos próprios meios eletrônicos, a exemplo (1) do envio

18. "É tudo aquilo que, uma vez inserido no processo, pode vir a ser utilizado como fundamento pelo juiz". MINTO, Andressa Olmedo. A prova digital no processo penal. São Paulo: LiberArs, 2021, p. 28.
19. *Ibid.*, p. 21.
20. *Ibid.*, p. 32.
21. VAZ, Denise Provasi. Provas digitais no processo penal: Formulação do conceito definição das características e sistematização do procedimento probatório. Tese (doutorado). Faculdade de Direito da Universidade São Paulo. São Paulo, 2012. Disponível em: https://teses.usp.br/teses/disponiveis/2/2137/tde-28052013-153123/pt-br.php. Acesso em: 22/11/2023.
22. VAZ, Denise Provasi. Provas digitais no processo penal: Formulação do conceito definição das características e sistematização do procedimento probatório. Tese (doutorado). Faculdade de Direito da Universidade São Paulo. São Paulo, 2012. Disponível em: https://teses.usp.br/teses/disponiveis/2/2137/tde-28052013-153123/pt-br.php. Acesso em: 22/11/2023.
23. Art. 10-A. Será admitida a ação de agentes de polícia infiltrados virtuais, obedecidos os requisitos do caput do art. 10, na internet, com o fim de investigar os crimes previstos nesta Lei e a eles conexos, praticados por organizações criminosas, desde que demonstrada sua necessidade e indicados o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas.

de e-mails ou de mensagens por aplicativos de mensageria com teor racista, (2) da publicação de vídeos na internet com informação da qual deveria se manter sigilo profissional ou (3) da cópia ilícita de software ou da base de dados de um computador. Por outro lado, a prova digital também pode se referir a um fato desenvolvido em ambiente físico, mas que pode ser demonstrado, através de meios digitais disponíveis, que servem como instrumento da sua comprovação, como as fotografias divulgadas em redes sociais, que atestam encontros e viagens entre a vítima do estupro e o criminoso, que nega tê-la encontrado no dia do abuso sexual.

Naquela situação, a doutrina[24] classifica a prova digital como de primeiro grau. Nesta, de segundo grau, porque o fato principal não é cometido, propriamente, no ambiente digital, no entanto, a prova do fato em si ocorre a partir de meio ou suporte eletrônico.

2.5. CARACTERÍSTICAS DA PROVA DIGITAL

2.5.1. Imaterialidade ou intangibilidade

Imaterialidade ou intangibilidade é a qualidade relacionada à natureza incorpórea da prova digital. Mesmo considerando a prova digital como o produto extraído de um dispositivo eletrônico, os arquivos de log, por exemplo, constituem uma mera sequência do código binário[25], cuja existência independe "do suporte físico do qual é incorporada"[26] e que serve apenas para armazená-la, além de possibilitar sua leitura, análise e apresentação no processo. Vale dizer, a prova digital não se

24. SILVA, José Antônio Ribeiro de Oliveira. A prova digital: um breve estudo sobre seu conceito, natureza jurídica, requisitos e regras de ônus da prova. Revista TST. São Paulo, v. 88, n. 2, abril 2022.

25. "O sistema binário é usado pelos computadores é e constituído de dois dígitos o 0 e o 1. A combinação desses dígitos leva o computador a criar várias informações: letras, palavras, textos, cálculos". Disponível em: https://brasilescola.uol.com.br/matematica/sistema-numeracao-binaria.htm#:~:text=O%20sistema%20bin%C3%A1rio%20%C3%A9%20usado,%2C%20palavras%2C%20textos%2C%20c%C3%A1lculos. Acesso em: 22/11/2023.

26. MINTO, Andressa Olmedo. A prova digital no processo penal. São Paulo: LiberArs, 2021, p. 35.

confunde com o suporte físico. Trata-se do conjunto, do contexto ou mosaico intangível de informações, que auxiliarão na reconstrução histórica de fatos, para fins de convencimento em sede de cognição judicial.

2.5.2. Volatilidade ou fragilidade

O dado eletrônico é passível de fácil edição ou eliminação (intencional ou por descuido), muitas vezes sem deixar vestígios patentes, seja pelo usuário do sistema informático, seja por terceiro, através de acesso remoto, sem a necessidade de qualquer de contato físico com ele. Destarte, é vital a preservação do contexto da sua existência, isto é, dos metadados, que servirão para atestar qualquer modificação ou não do dado principal.

Se um dispositivo eletrônico móvel apreendido estiver ainda conectado à internet, um "terceiro interessado na sua alteração ou eliminação poderia fazer inclusive à distância"[27]. Logo, para evitar tal operação, o perito deve desativar imediatamente a sua conexão *on-line*, deixando-o no "modo avião".

A volatilidade da informação eletrônica também se manifesta na natureza do armazenamento ou da transmissão.

O alto custo de armazenamento da informação eletrônica, especialmente na computação em nuvem, faz com que os provedores de aplicação e de conexão guardem apenas os dados essenciais para o seu modelo de negócio ou para o cumprimento de obrigação legal, como estabelecem os arts. 13[28] e 15[29] do MCI, que estipulam os prazos mandamentais de guarda de registros de conexão e de aplicação de, respectivamente, um ano e seis meses. Ultrapassado o prazo legal, as empresas de

27. *Ibid*., p. 36.

28. Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

29. Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

tecnologia descartam as informações, abrindo espaço para o armazenamento de novos dados.

Em outra conjuntura, os dados – armazenados em dispositivo eletrônico de modo temporário e de curto prazo, na denominada memória RAM (*Random Access Memory*), onde o processador salva apenas as informações necessárias para funcionar durante o uso do sistema computacional – podem ser automaticamente apagados[30], se o computador apreendido for desligado, apesar de eventual pertinência e relevância probatória.

2.5.3. Dispersão

A difusão e espalhamento da prova digital decorre do fato de que ela pode estar situada em diversos locais, seja no próprio sistema informático (quando o mesmo arquivo é salvo em pastas diferentes), seja em um ponto geográfico longínquo, como na hipótese de dados armazenados na computação em nuvem[31], isto é, em servidores de empresas privadas, sediadas, na maioria das vezes, no estrangeiro.

Por causa das características peculiares da prova digital, os meios de obtenção dessa evidência – assim compreendidos como a forma, procedimento e protocolo para a aquisição da prova –, devem ter mais preocupação ainda em aderir ao devido processo legal e a todos os seus corolários dele decorrentes[32].

2.6. ARMAZENAMENTO E TRANSMISSÃO EM MEIO ELETRÔNICO

Os dados informáticos existem, em regra, armazenados ("repousando" num dispositivo eletrônico) ou em transmissão, fluindo por intermédio de protocolos de rede. A distinção é relevante em termos de limitação da obtenção da prova. A interceptação dos dados telemáticos em transmissão se sujeita às restrições do art.

30. Disponível em: https://edu.gcfglobal.org/pt/informatica-basica/memoria-ram-e-disco-rigido/1/. Acesso em: 22/11/2023.
31. MINTO, Andressa Olmedo. A prova digital no processo penal. São Paulo: LiberArs, 2021, p. 36.
32. MINTO, *op. cit.*, p. 28.

5º, XII[33], da CF/88 c/c do art. 2º[34] da Lei nº 9.296/1996, admitindo-se apenas para crimes punidos com reclusão, por exemplo.

Os dados que foram transmitidos anteriormente e que, agora, se encontram armazenados em um dispositivo eletrônico podem ser extraídos, mediante busca e apreensão física do sistema ou por intermédio de ordem judicial dirigida à empresa que os guarda, na forma do art. 22, parágrafo único[35], da Lei nº 12.965/2014 (MCI).

A intervenção estatal na primeira hipótese relativiza o direito constitucional ao sigilo das comunicações (art. 5º, XII), enquanto, na segunda, à privacidade (art. 5º, X). Diante dessa diferença, a extensão do amparo jurídico não pode ser idêntica, como decidiu o STJ (RMS 62.143/RJ[36], Terceira Seção, Min. Rogério Schietti, DJe 08/09/2020), porquanto a quebra do sigilo de dados armazenados corresponde ao acesso de

33. XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

34. Art. 2º Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:
I – não houver indícios razoáveis da autoria ou participação em infração penal;
II – a prova puder ser feita por outros meios disponíveis;
III – o fato investigado constituir infração penal punida, no máximo, com pena de detenção.

35. Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.
Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:
I – fundados indícios da ocorrência do ilícito;
II – justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
III – período ao qual se referem os registros.

36. "4. A determinação do Magistrado de primeiro grau, de quebra de dados informáticos estáticos, relativos a arquivos digitais de registros de conexão ou acesso a aplicações de internet e eventuais dados pessoais a eles vinculados, é absolutamente distinta daquela que ocorre com as interceptações das comunicações, as quais dão acesso ao fluxo de comunicações de dados, isto é, ao conhecimento do conteúdo da comunicação travada com o seu destinatário. Há uma distinção conceitual entre a quebra de sigilo de dados armazenados e a interceptação do fluxo de comunicações. Decerto que o art. 5º, X, da CF/88 garante a inviolabilidade da intimidade e da privacidade, inclusive quando os dados informáticos constarem de banco de dados ou de arquivos virtuais mais sensíveis. Entretanto, o acesso a esses dados registrados ou arquivos virtuais não se confunde com a interceptação das comunicações e, por isso mesmo, a amplitude de proteção não pode ser a mesma".

dados retrógrados, já produzidos, transmitidos, coletados e/ou salvos, realidade bem diversa da captação de comunicações em tráfego e em tempo real pelos investigadores, cujo exame de admissibilidade é mais rigorosa.

Em ambos os cenários, a decisão judicial deve apontar os fundados indícios da ocorrência do ilícito, a justificativa motivada da utilidade dos registros solicitados e o período ao qual se referem os dados, incumbindo ao juiz tomar as providências necessárias à garantia do sigilo das informações para a preservação da intimidade, vida privada, honra e imagem do usuário, como prescreve o art. 22, *caput* e § 1º, do MCI.

O art. 13 do Projeto de Lei 4.939/2020[37] avança e estipula outros requisitos da decisão judicial autorizadora, que indicará, outrossim, "os motivos, a necessidade e os fins da diligência, estabelecendo os limites da atividade a ser empreendida", evitando-se, ao máximo, o deferimento de medidas descabidas e abusivas, ensejadoras de aventuras jurídicas de captura genérica e indiscriminada de dados massivos, conhecidas como "*fishing expedition*", "pescaria probatória" ou "efeito hidra". Nas palavras de ROSA (2021), seria "a procura especulativa, no ambiente físico ou digital, sem ´causa provável', alvo definido, finalidade tangível ou para além dos limites autorizados (desvio de finalidade), de elementos capazes de atribuir responsabilidade penal a alguém"[38]. Vale dizer, evita-se o emprego das provas digitais como meio de encalços investigativos "especulativos, indiscriminados, abrangentes, genéricos e vagos de informações sem a indispensável delimitação e sem a 'particularização razoável'[41] do conteúdo, correndo-se, assim, o risco de se violar ilegitimamente a privacidade da parte contrária ou de terceiros, pois, nas palavras de Alexandre Morais da Rosa, o 'termo se refere à incerteza própria das expedições de pesca, em que não se sabe, antecipadamente, se haverá peixe, nem os espécimes que podem ser fisgados, muito

37. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2264367. Acesso em: 11/10/2022.

38. Disponível em: https://www.conjur.com.br/2021-jul-02/limite-penal-pratica-fishing-expedition-processo-penal. Acesso em: 19/07/2023.

menos a quantidade, mas se tem ´convicção (o agente não tem provas, mas tem convicção)´[42]"[39].

2.7. CADEIA DE CUSTÓDIA ESPECÍFICA

2.7.1. Introdução

O art. 158-A do CPP, incluído pelo Pacote Anticrime (Lei nº 13.964/2019), define a cadeia de custódia 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"[40]. BRASILEIRO (2020) explica que se trata de um "mecanismo garantidor da autenticidade das evidências coletadas e examinadas"[41], buscando prevenir qualquer tipo de adulteração (intencional ou acidental) delas.

Ao registrar todos os passos percorridos pela prova, da sua identificação até a valoração judicial, consagra-se o "direito à prova lícita"[42], titularizado pela defesa, no qual a persecução criminal se compromete a respeitar todos os protocolos probatórios, apresentando em juízo tão somente as evidências produzidas em consonância com os parâmetros constitucionais e legais.

O objeto da cadeia de custódia é o vestígio, conceituado pelo art. 158-A, § 3º, do CPP, como "todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal", características distintas das da prova digital (imaterialidade, volatilidade e dispersão), que é sujeita

39. Disponível em: https://www.conamp.org.br/publicacoes/artigos-juridicos/8706-despejo-de-provas-excessivas-e-inuteis-no-processo-penal.html. Aceso em: 22/01/2024.

40. "Todo esse cuidado é necessário e justificado: quer-se impedir a manipulação indevida da prova com o propósito de incriminar (ou isentar) alguém de responsabilidade, com vistas a obter a melhor qualidade da decisão judicial e impedir uma decisão injusta. Mas o fundamento vai além: não se limita a perquirir a boa ou má-fé dos agentes policiais/estatais que manusearam a prova. Não se trata nem de presumir a boa-fé, nem a má-fé, mas sim de objetivamente definir um procedimento que garanta e acredite a prova independente da problemática em torno do elemento subjetivo do agente. A discussão acerca da subjetividade deve dar lugar a critérios objetivos, empiricamente comprováveis, que independam da prova de má-fé ou 'bondade e lisura' do agente estatal". LOPES Jr., Aury, Direito Processual Penal. 17ª ed. São Paulo: Saraiva, 2020, p. 666.

41. LIMA, Renato Brasileiro de. Manual de Processo Penal. Salvador: Juspodivm, 2020, p. 716.

42. STJ, RHC 77.836-PA, Quinta Turma, Min. Ribeiro Dantas, DJe 12/02/2019.

às influências externas, seja pelo autor do crime, seja pela vítima ou seja pelo próprio investigador, que podem alterá-las, realocá-las ou eliminá-las, fisicamente ou à distância.

Por isso, parte da doutrina defende um regime jurídico autônomo[43], incorporando normas relativas à apreensão das variadas tipologias de prova digital e à garantia da qualidade da preservação da cadeia de custódia, elaboradas em atenção às particularidades do ambiente digital, porquanto "[...] a ausência de princípios generalizáveis nesse campo poderá repercutir na utilização de instrumentos tecnológicos [...] na persecução penal"[44].

A título de ilustração, em outubro de 2022, o STJ[45] julgou inadmissíveis as provas digitais sem registro documental dos procedimentos adotados pela polícia para a preservação da integridade, autenticidade e confiabilidade dos elementos informáticos, como "o modo de coleta e preservação dos equipamentos, quem teve contato com eles, quando tais contatos aconteceram e qual o trajeto administrativo interno percorrido pelos aparelhos, uma vez apreendidos pela polícia. Nem se precisa questionar se a polícia espelhou o conteúdo dos computadores e calculou a *hash*[46] da imagem resultante, porque até mesmo providências muito mais básicas do que essa – como documentar o que foi feito – foram ignoradas pela autoridade policial".

A vulnerabilidade da prova digital é enorme, haja vista a po-tencial contaminação dos dados, tanto pelo mau uso dos instrumen-tos, quanto pelo conhecimento inadequado do sistema e das suas ferramentas, que poderá acarretar a invalidação daquela em juízo.

O art. 19 do Projeto de Lei 4.939/2020[47] organizou os protocolos de uma cadeia de custódia específica das provas

43. MINTO, Andressa Olmedo. A prova digital no processo penal. São Paulo: LiberArs, 2021, p. 56.

44. QUINTIERE, Victor Minervino. O direito penal nas sociedades digitais. Belo Horizonte, São Paulo: D´Plácido, 2023, p. 59.

45. AgRg no RHC 143.169-RJ, Quinta Turma, Min. Jesuíno Rissato, j. 25/10/2022.

46. "O código hash o resultado de um algoritmo matemático [...] com base no conteúdo de um determinado arquivo. Caso seja feita qualquer alteração deste conteúdo, a sequência de caracteres sofre uma mudança drástica em seu conteúdo". SOUZA, Bernardo de Azevedo e et al. Manual prático de provas digitais. São Paulo: RT, 2023, p. 61.

47. Art. 19 Os meios de obtenção da prova digital serão implementados por perito oficial ou assistente técnico da área de informática, que deverão proceder conforme as boas práticas aplicáveis

digitais, prescrevendo como princípios reitores a autenticidade, integridade, completude, auditabilidade e reprodutibilidade delas, que serão exploradas adiante.

A diretriz ABNT/ISO nº 27.037/2013, redigida pela Associação Brasileira de Normas Técnicas, órgão responsável pela regulação técnica no país, se alicerçou nos métodos estrangeiros organizados pela *International Organization for Standardization* (ISO)[48], "aceitos mundialmente para padronizar os passos à evidência digital"[49].

A diretriz conceitua e estabelece que o processo de manuseio é composto por quatro etapas de identificação[50], coleta[51], aquisição[52] e preservação[53] da evidência digital, estruturando os quatro principais eixos da sua cadeia de custódia: auditabilidade[54], justificabilidade[55], repetibilidade[56] e reprodutividade[57].

---

aos procedimentos a serem desenvolvidos, cuidando para que se preserve a integridade, a completude, a autenticidade, a auditabilidade e a reprodutibilidade dos métodos de análise.

48. Disponível em: https://academiadeforensedigital.com.br/iso-27037-identificacao-coleta-aquisicao-e-preservacao-de-evidencia/. Acesso em: 22/11/2023.

49. SOUZA, *op. cit.*, p. 57.

50. 3.12 Identificação: processo envolvendo a busca, reconhecimento e documentação da potencial evidência digital.

51. 3.3 Coleta: processo de recolhimento de itens físicos que contêm potencial evidência digital.

52. 3.1 Aquisição: processo de criação de cópia de dados em um conjunto definido.

53. 3.15 Preservação: processo para manter e proteger a integridade e/ou a condição original da potencial evidência digital.

54. 5.3.2 Convém que seja possível para um assistente independente ou outra parte autorizada interessada avaliar as atividades realizadas por um DEFR e DES. Isto se torna possível por meio de adequada documentação de todas as ações realizadas. Recomenda-se que os DEFR e DES sejam capazes de justificar o processo de tomada de decisão para escolha de um determinado curso de ação. É recomendado que os processos realizados pelos DEFR e DES estejam disponíveis para avaliação independente com o intuito de determinar se o método científico, a técnica ou o procedimento foi adequadamente seguido.

55. 5.3.5 É recomendado que o DEFR seja capaz de justificar todas as ações e métodos utilizados para o manuseio da potencial evidência digital. A justificativa pode ser alcançada demonstrando que a decisão foi a melhor escolha para obter toda a potencial evidência digital. Qualquer DEFR ou DES poderia, também, demonstrar isto, reproduzindo com sucesso ou validando as ações ou métodos utilizados.

56. 5.3.3 A repetibilidade é estabelecida quando os mesmos resultados de testes são produzidos sob as seguintes condições: — Utilizando os mesmos procedimentos e métodos de medição; — Utilizando os mesmos instrumentos e sob as mesmas condições; e — Pode ser repetido a qualquer tempo depois do teste original.

57. 5.3.4 A reprodutibilidade é estabelecida quando os mesmos resultados de testes são produzidos sob as seguintes condições: — Utilizando os mesmos métodos de medição; — Utilizando diferentes instrumentos e sob diferentes condições; e — Pode ser reproduzido a qualquer tempo depois do teste original.

Por sua vez, o modelo proposto pela *National Institute for Standards and Technology* (NIST) recomenda quatro etapas na investigação digital: a coleta, exame, análise e relatório[58]. A primeira etapa do procedimento forense da evidência digital é a coleta, identificando-a, buscando tanto os arquivos visíveis quanto os excluídos, porém recuperáveis, arrecadando-a, rotulando-a e praticando atos complementares, a fim de garantir a integridade dos dados. O exame consiste no processamento dos dados coletados, filtrando, selecionando e indexando aqueles que possuem relevância probatória no conjunto extraído. Na análise, organiza-se os dados pertinentes (por exemplo, em uma linha cronológica e correlacionando pessoas, locais, eventos e padrões), possibilitando a avaliação do seu verdadeiro valor probatório. A última etapa do modelo do NIST envolve a elaboração do relatório, no qual o perito registra as conclusões obtidas a partir da análise dos dados eletrônicos coletados, examinados e analisados, não se contentando com as descobertas alcançadas, mas abordando também as dúvidas remanescentes e os resultados inconclusivos.

2.7.2. Autenticidade

Certificar-se da autenticidade da prova digital é demonstrar o vínculo entre os dados obtidos e o respectivo usuário (proveniência), afastando qualquer dúvida quanto à "identificação da origem e autoria"[59] das informações.

Suscitada dúvida razoável pela defesa quanto à fiabilidade da fonte, caberá à acusação esclarecê-la (art. 156[60] do CPP) e novas provas serão produzidas com a análise dos metadados da evidência principal.

---

58. Disponível em: https://csrc.nist.gov/glossary/term/digital_forensics#:~:text=NIST%20SP%20800%2D86%20under,be%20used%20in%20judicial%20proceedings chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf. Acesso em: 22/11/2023.

59. SOUZA, Bernardo de Azevedo e et al. Manual prático de provas digitais. São Paulo: RT, 2023, p. 53.

60. Art. 156. A prova da alegação incumbirá a quem a fizer, sendo, porém, facultado ao juiz de ofício:

No plano legislativo, o art. 3º, XI, do Projeto de Lei nº 4.939/2020, a define como a "certeza da sua origem [...] ou autoria", enquanto o art. 411, III, do CPP considera autêntico o documento quando "a autoria estiver identificada por qualquer outro meio legal de certificação, inclusive eletrônico, nos termos da lei".

2.7.3. Integridade

A prova digital há de ser íntegra e isso diz respeito à não modificação do seu conteúdo, conhecida também no direito latino-americano como a "*ley de la mismidad*"[61], um "preceito universal da autenticidade da prova"[62], assegurando que os dados coletados e tratados sejam os mesmos, sem qualquer alteração informacional, "imutável e confiável"[63], quando da valoração pelo juiz, ao proferir a decisão.

A relevância do debate adquiriu vulto no México, onde foi apresentada iniciativa legislativa "que adiciona el articulo 241 bis. al Código Nacional de Procedimientos Penales, a cargo de la Diputada Martha Patricia Ramírez Lucero, del grupo parlamentario de Morena"[64], com o objetivo de normatizar a

61. "[...] con una cita expresa de la doctrina de Juan Carlos Urazán Bautista (2005), "la autenticidad del elemento [probatorio] constituye seguridad para la administración de justicia, fundamentando-se la exigencia de la preservación de la cadena de custodia en el principio universal de autenticidad de la prueba, definido como 'ley de mismidad', esto es, el principio por el cual se determina que 'el mismo' que se encontró en la escena [del crimen] es 'el mismo' que se está utilizando para tomar la decisión judicial".

"[...] com uma citação explícita da doutrina de Juan Carlos Urazán Bautista (2005), "a autenticidade do elemento [probatório] constitui segurança para a administração da justiça, fundamentando a exigência da preservação da cadeia de custódia no princípio universal de autenticidade da prova, definido como 'lei de mesmidade', isto é, o princípio pelo qual se determina que 'o mesmo' que foi encontrado na cena [do crime] é o 'mesmo' que está sendo usado para tomar a decisão judicial". (tradução livre) Disponível em https://revistas.uns.edu.ar/disc/article/view/2388/1503. Acesso em: 11/10/2022.

62. JUNIOR, Ivan Jezler. Prova penal digital. Tempo, risco e busca telemática. Florianópolis: Tirant, 2019, p. 183.

63. SOUZA, Bernardo de Azevedo e et al. Manual prático de provas digitais. São Paulo: RT, 2023, p. 53.

64. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://infosen.senado.gob.mx/sgsp/gaceta/64/2/2020-08-12-1/assets/documentos/Inic_ini_32_adiciona_art_241_bis_cnpp_dip._martha_patricia_ramrez_lucero.pdf. Acesso em: 22/01/2024.

preservação da evidência eletrônica dentro da cadeia de custódia devido à sua natureza especial de intangibilidade e de suscetibilidade de manipulação e alteração, atestando, destarte, a certeza do estado original, no qual o dado foi coletado, em conformidade com o princípio da mesmidade[65].

O art. 3º, X, do Projeto de Lei nº 4.939/2020, a apresenta como "a certeza de que a informação que a constitui se mantém inalterada após o seu tratamento" e, entenda-se, como tratamento do dado, "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração", nos termos do art. 5º, X, da Lei nº 13.709/2018.

Na prática, como visto anteriormente, cabe ao perito gerar o código *hash*[66], logo ao extrair os dados e enviá-lo ao juízo. Na hipótese de questionamento defensivo quanto à modificação do material, basta produzir novo algoritmo e comparar se os resultados são os mesmos ou não, a fim de atestar a (in) alteração. Cuida-se de providência simples, à qual os tribunais

65. "El propósito de legislar el aseguramiento de la evidencia electrónica dentro de la cadena de custodia es resolver el problema y complicaciones que tienen este tipo de pruebas por su misma naturaleza, ya que como son intangibles hasta en tanto son reproducidos en una pantalla o impresos, son susceptibles de manipulación y alteración, por lo tanto es necesario prever los mecanismos que constaten la veracidad de su origen y contenido durante su recolección, pues así se tendrá la certeza del estado original en el cual la prueba fue recabada, procurando el principio de mismidad, además de tener la seguridad de conocer el medio electrónico que le dio origen a la prueba y que si el documento fue impreso, su contenido es el mismo que el plasmado en medio digital de origen".

"O propósito de legislar sobre a garantia de provas eletrônicas na cadeia de custódia é solucionar o problema e as complicações que esse tipo de prova apresenta pela sua própria natureza, pois por serem intangíveis até serem reproduzidas em tela ou impressas, são suscetível de manipulação e alteração, portanto é necessário prever mecanismos que verifiquem a veracidade de sua origem e conteúdo durante sua coleta, pois isso garantirá a certeza do estado original em que a prova foi coletada, buscando o princípio da mesmidade, além disso, ter a segurança de conhecer o meio eletrônico que deu origem à prova e que, se o documento foi impresso, seu conteúdo é o mesmo captado no meio digital original". (tradução livre)

66. "O código hash o resultado de um algoritmo matemático [...] com base no conteúdo de um determinado arquivo. Caso seja feita qualquer alteração deste conteúdo, a sequência de caracteres sofre uma mudança drástica em seu conteúdo". SOUZA, Bernardo de Azevedo e et al. Manual prático de provas digitais. São Paulo: RT, 2023, p. 61.