A cadeia de custódia da prova digital[*]

Gustavo Badaró [**]

1 A prova digital: características e seus *standards* metodológicos

O presente artigo pretende analisar a cadeia de custódia da chamada prova digital ou, como se costuma denominar, *digital evidence*. Nesse caso, o adjetivo "digital" decorre exatamente de a prova se originar de uma manipulação eletrônica de número,[1] ou nas palavras de Kerr, "*zeros and ones of eletricity*".[2]

Entre tantos temas novos e difíceis da prova digital, destacam-se duas diferenças relevantíssimas com as provas tradicionais: uma ontológica e outra metodológica.

Os elementos de prova relevantes, no caso da *computer forensics*, são conservados e transmitidos em linguagem não natural, mas digital. Assim, ainda que os dados digitais, em seu conteúdo informativo, possam ser diretamente percebidos por quem está em contato com eles, eles não possuem uma materialidade[3] imediatamente constatável.

Justamente por isso, para que produzam informação jurídica útil para a reconstrução histórica dos fatos, devem seguir os princípios informáticos. O *National Institute for Standard and Technology* (NIST) distingue quatro fases da *computer forensics*: em suas fases de *coleta* dos dados, *exame*, *análise* e *relatóri*o: "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,

---

[*] Artigo elaborado para apresentação de palestra, como mesmo tema, no Congresso Internacional de Direito Probatório, realizado nos dias 18 e 19 de novembro de 2021, em Porto Alegre-RS, pela Pontifícia Universidade Católica do Rio Grande do Sul e pela Universidade Alberto Hurtado, com apoio do IBDP e da Procnet.

[**] Professor Titular de Direito Processual Penal da Universidade de São Paulo. Advogado Criminalista e Consulto Jurídico

1. Marcello Daniele, La prova digitale nel processo penale, *Rivista di Diritto Processuale*, 2011, p. 283.
2. O.S. Kerr, Digital evidence and the new criminal procedure, In: *105 Columbia law review,* 2005, p. 284.
3. A ausência de materialidade da prova digital, como destaca Daniele (La prova digitale nel processo penale…, p. 284) não significa que ela seja privada de "fisicidade": trata-se de "impulsi elettrici che rispondono ad una sequenza numerica prestabilita e che, convogliati in un supporto informatico dotato di una memoria, originano informazioni intelligibili".

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".[4]

A doutrina processual penal tem aderido a tal sistemática, sugerindo sua aplicação nos casos de produção de *digital evidence*.[5]

Por essas diferenças, quando comparadas com as tradicionais provas utilizadas no processo penal, em especial as chamadas fontes reais de provas, notadamente os documentos cartáceos, a produção da prova informática exigiria uma intervenção legislativa, com regras legais próprias para sua produção, admissão e valoração, sendo muitas vezes inadequadas as regras tradicionais sobre as provas clássicas do processo penal.[6]

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

---

4 Karen Kent; Suzanne Chevalier; Tim Grance; Hug Dang, *Guide to Integrating Forensic Techniques into Incident Response*. Recommendations of the National Institute of Standards and Technology, NIST publication, 2006. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

5. Nesse sentido: Giovanni Zicardi, Le linee guida della Association of Chief Police Officers Inglese, In. Luca Lupária; Giovanni Ziccardi, *Investigazione penale e tecnologia informatica*. L'accertamento del reato tra progresso scientifico e garanzie fondamentale, Milano: Giuffrè, 2007, p. 120; Giuseppe Vaciago, *Digital Evidence*. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato. Torino: Giappichelli, 2012, p. 7; Marco Pittiruti, Digital evidence *e procedimento penale*. Torino: Giappichelli, 2017, p. 4. Diversamente, Stefano Aterno Digital Forensics (Investigazioni informatiche). *Digesto delle Discipline Penalistiche*. Torino: Utet, aggiornamento, 2014. t. II, p. 220) assim descreve o ciclo do processo de *computer forensics*: "a) riconoscimento e identificazione della fonte di prova; b) acquisizione del dato (o del sistema); c) conservazione e protezione del dato (do del sistema), trasversale rispetto a tutte le successive fasi; d) analisi forense; e) valutazione dei risultati estratti dell'analisi (sotto il profilo tecnico, giuridico ed investigativo); f) presentazione dei risultati (al titolare delle indagini, al Giudice o al committente in caso di attività difensiva o stragiudiziale)".

6. Kerr (Digital evidence and the new criminal procedure..., p. 290 e segs.) sustenta a necessidade de repensar todas as regras probatórias comuns, originariamente concebidas para as provas tradicionais. De modo semelhante, Daniele, La prova digitale nel processo penale…, p. 284.

Assim sendo, diante do desarmador silêncio por parte do legislador, o aplicador do direito se vê constrito a adaptar os tradicionais meios de prova e meios de obtenção de prova às específicas dinâmicas de obtenção dos dados digitais.[7] Para essa aplicação analógica das regras probatórias dos códigos, para a prova digital, duas características são destacadas como mais relevantes: a **desmaterialização** e a **dispersão** dos elementos de prova.[8]

No que toca à sua "desmaterialização", não se trata de provas pensáveis como objetos físicos, dotados de uma evidente corporeidade.[9] E é exatamente dessa não materialidade que decorrem os caráteres de volatilidade e fragilidade da própria prova digital,[10] razão pela qual há necessidade de uma maior preocupação com a possibilidade de falsificação ou destruição.[11] Há, na prova digital, uma "congênita mutabilidade"[12] ou "fácil alterabilidade". [13] Em suma, trata-se de fonte de prova que pode ser facilmente contaminada, sendo sua gestão muito delicada, por apresentar um alto grau de vulnerabilidade a erros.[14]

Por certo, não se trata de um problema que somente se coloca no caso de má-fé ou, no limite, de prática criminosa.[15] O comprometimento da genuinidade da prova pode se dar acidentalmente, por falta de conhecimento ou por mal emprego da técnica do particular ou mesmo o perito, que realiza a atividade no suporte informático no qual está armazenado o dado.

Justamente por isso, a prova digital é tema central da chamada *computer forensics*, que se preocupa em desenvolver e definir instrumentos técnicos ou *tools* adequados para os trabalhos de investigação de dados digitais que poderão constituir uma prova utilizável em processo judicial. Para tanto, é necessário: (*i*) individualizar o suporte

---

7. Luca Lupária, Processo penale e scienza informatica: anatomia de una transformazione epocale, In. Luca Lupária; Giovanni Ziccardi, *Investigazione penale e tecnologia informatica*. L'accertamento del reato tra progresso scientifico e garanzie fondamentale, Milano: Giuffrè, 2007, p. 133.
8. Nesse sentido: Daniele, La prova digitale nel processo penale…, p. 284; Pittiruti, Digital evidence *e procedimento penale*..., p. 6.
9. Daniele, La prova digitale nel processo penale…, p. 284.
10. Nesse sentido: Pittiruti, Digital evidence *e procedimento penale*..., p. 11; Aterno, Digital Forensics…, p. 219.
11. Pittiruti, Digital evidence *e procedimento penale*..., p. 25; Zicardi, Le linee guida della Association of Chief Police Officers Inglese…, p. 117.
12. Daniele, La prova digitale nel processo penale…, p. 292.
13. Aterno, Digital Forensics…, p. 219.
14. Giovanni Ziccardi, Aspetti informatico-giuridico della fonte di prova digitale, In. Luca Lupária; Giovanni Ziccardi, *Investigazione penale e tecnologia informatica*. L'accertamento del reato tra progresso scientifico e garanzie fondamentale, Milano: Giuffrè, 2007, p. 51.
15. O Código Penal, no art. 347 tipifica o crime de fraude processual: "Art. 347 - Inovar artificiosamente, na pendência de processo civil ou administrativo, o estado de lugar, de coisa ou de pessoa, com o fim de induzir a erro o juiz ou o perito".

informático que contem o dado digital útil à investigação; (*ii*) obter o dado digital através de técnica de interceptação, no caso de fluxo de comunicação, ou mediante o sequestro e cópia ou espelhamento do suporte em que está registrado o arquivo de dados; (*iii*) conservar os dados digitais obtidos e copiados em local seguro e adequado; (*iv*) realizar a análise dos dados obtidos – examinando exclusivamente a cópia do suporte informático – que sejam relevantes para o objeto da investigação; (*v*) apresentar os resultados da investigação em juízo, mediante a produção de prova pericial e eventuais esclarecimentos verbais dos peritos em audiência.[16]

É imprescindível que o método empregado garanta a integridade do dado digital e, com isso, a força *probandi* do conteúdo probatório por ele representado.[17] Normalmente, faz-se uma cópia ou "espelhamento", obtendo o *bitstream* da imagem do disco rígido ou suporte de memória em que o dado digital está registrado. Além disso, por meio de um cálculo de algoritmo de *hash*, é possível verificar a perfeita identidade da cópia com o arquivo original. Com isso, de um lado, se preserva o material original, e, de outro, se garante a autenticidade e integridade do material que foi examinado pelos peritos.

Não existe um *standard* ou uma metodologia para o tratamento da prova digital forense, mas apenas um conjunto de procedimentos mais ou menos consolidados e testados através da experiência.[18] De qualquer modo, na comunidade técnico-científica de referência, há um conjunto de *best practicies* nacional e internacionalmente reconhecido. No campo internacional, destacam-se os *standards* técnicos da sério ISO/IEC 27000, publicados pela ISO (*International Organization for Standardization*) e pela IEC (*International Electrotechnical Commission*), com destaque para: ISO/IEC 27035:2011, com indicações sobre a gestão dos incidentes informáticos; ISO/IEC 27037:2012, que contém uma série de indicações concernentes à identificação, recolhimento, aquisição e conservação da prova digital; ISO/IEC 2741:2015, que fornece indicações destinadas a garantir a idoneidade e a adequação dos métodos investigativos;

---

16. Nesse sentido, no direito italiano: Vaciago, *Digital evidence*…, p. 23. De modo semelhante, Giovanni Zicardi (Aspetti informatico-giuridico della fonte di prova digitale…, p. 57) refere-se aos seguintes aspectos: (*i*) a coleta ou recolhimento da fonte de prova sem alterá-la; (*ii*) a cadeia de custódia da prova; (*iii*) a autenticidade da fonte de prova, que não foi alterada em comparação com o estado em que se encontrava no computador originário; (*iv*) o *recovery* dos arquivos deletados, dos fragmentos de *file* e dos arquivos temporários; (*v*) verificabilidade das conclusões expostas por uma terceira parte ou mesmo por uma juiz, de acordo com padrões reconhecidos pela comunidade científica de referência.
17. Elisa Lorenzetto, Le attività urgente di investigazione informatica e telematica, In. Luca Lupária (Coord.). *Sistema penale e criminalità informatica*. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime. Milano: Giuffrè, 2009, p. 149.
18. Aterno, Digital Forensics…, p. 219.

ISO/IEC 27042/2015, que consiste num guia de análise e interpretação das provas digitais, com o objetivo de enfrentar as questões de continuidade, validade, reproduzibilidade e repetibilidade dos resultados obtidos. Também cabe elencar a RFCC3227 – *Guidelines for Evidence Collection and Archiving*, publicada em fevereiro de 2002, considerada o guia de referência para a certificação do iter operativo que deve ser adotado no desenvolvimento de atividades de aquisição de informações digitais.

Do ponto de vista operacional, e no que se refere a *mobile forensics*, podem ser citados: o NIST *Guidelines on Mobile Forensics*, de 2014, sob responsabilidade do *National Institute for Standards and Technology* (NIST), o SWGDE *Best Practices for Mobile Devices Evidence Collection and Preservation, Handling, and Acquisition*, de 2019, sob responsabilidade do *Scientific Working Group on Digital Evidence*, e o INTERPOL *Global Guidelines for Digital Forensics Laboratory,* da INTERPOL, que, de uma maneira geral, são guias com indicação das melhores práticas para recolhimento, conservação, aquisição, análise e apresentação de relatório em dispositivos móveis.

No Brasil, merece destaque a norma técnica da ABNT - NBR ISO/IEC 27037:2013, que estabelece diretrizes para identificação, coleta, aquisição e preservação de evidência digital - família ISO 27000 – Gestão da Segurança da Informação.

Destaque-se, também, que o artigo 4º da Lei nº 12.735, de 30 de novembro de 2021 estabelece que: "Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado"

2. A prova digital como prova atípica no processo penal e os seus requisitos de admissibilidade

A prova digital caracteriza-se como prova atípica no processo penal.[19] No processo penal, embora não haja regra expressa, não vigora o princípio de taxatividade dos meios de prova, sendo permitida a produção de provas atípicas. Aplicação analógica,

[19]. Mesmo em relação ao processo civil, em que o Código de Processo Civil de 2105 apresenta uma disciplina dos chamados documentos digitais, em apenas três artigos. E, mesmo diante das disposições dos artigos 439 a 441, que tratam do documento eletrônico, Luiz Guilherme Marinoni e Sérgio Cruz Arenhart (*Comentários ao Código de Processo Civil.* São Paulo: RT, v. VII, 2016, p. 416) afirmam que "seria extremamente necessário que a lei processual brasileira desse tratamento a esse tipo de prova. Dificilmente será possível assimilar, *simpliciter*, a prova eletrônica à prova documental. A variação da qualidade do suporte e as características acima apontadas não o recomendam. Por outro lado, também não há elementos para qualificar essa prova na forma de nenhuma outra prova típica conhecida"

como permitido pelo art. 3º do Código de Processo Penal, da regra do art. 369 do Código de Civil que a admite a produção de provas atípicas, "para provar a verdade dos fatos".[20]

Nos diplomas processuais penais mais modernos há regra equivalente. Por exemplo, o *Codice di Procedura Penale* italiano, de 1989, em seu art. 189, disciplina a produção de *prove non disciplinate dalla legge*, exigindo para sua admissibilidade que seja "idônea a assegurar o acertamento dos fatos".[21]

Nos casos de meios de prova típicos, o legislador, se valendo da evolução das leis de seu país, do exemplo do direito comparado, dos ensinamentos da doutrina e da jurisprudência de seus tribunais, procura estabelecer uma disciplina de admissão e produção dos meios de prova que gere um experimento probatório com aptidão epistêmica. Em outras palavras, o rito probatório tem por um de seus escopos produzir experimentos cujo resultado seja confiável do ponto de vista epistêmico e, portanto, cognitivamente útil para a reconstrução histórica dos fatos.

Já nas provas atípicas, por não haver um rito probatório preestabelecido pelo legislador, a sua admissão deve ser submetida a um controle mais rigoroso de admissibilidade. É possível a produção de provas atípicas, mas isso não significa que possa ser introduzido no material provatório a ser valorado pelo juiz todo e qualquer tipo de experimento.

Em geral exige o legislador que as provas atípicas atendam a duas ordens de requisitos: serem epistemicamente uteis para a reconstrução histórica dos fatos e respeitarem na sua produção as garantias constitucionais, notadamente, a dignidade humana e as liberdades fundamentais das partes. Em outras palavras, se o meio de prova atípico que se pretende produzir for moralmente inidôneo, ou se não tiver potencial cognitivo, a prova não será admitida. Por exemplo, não se admite como prova atípica, realizar um depoimento o interrogatório mediante hipnose ou subministrando os

---

[20]. O CPC, no art. 369, estabelece que: "As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, *para provar a verdade dos fatos* em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz". (destaquei)

[21]. Prevê o citado dispositivo legal: "Art.189.1 Quando è richiesta una prova non disciplinata dalla legge, il giudice *può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti* e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova" (destaquei). Em sentido inverso ao do ordenamento jurídico brasileiro, a doutrina italiana defende a aplicação da regra geral de admissibilidade das provas atípicas, do Código de Processo Penal italiano, no âmbito processual civil, cf.: Luigi Paolo Comoglio, *Le prove civile*, Torino: Utet, 1998, p. 41; Gian Franco Ricci, *Le prove atipiche*, Milano: Giuffrè, 1999, p. 223; Id., Atipicità della prova, processo ordinario e rito camerale, *Rivista trimestrale di diritto e procedura civile*, 2020, p. 422; Michele Taruffo, *La prova nel processo civile*. Milano: Guiffrè, 2012, p. 73.

chamados "soros da verdade".[22] Também não se admite, a produção como prova atípica, da leitura de borras de café ou do emprego da cartomancia.[23]

Tal situação, no que toca ao tema do presente artigo, merece ser analisada sob o enfoque do segundo requisito de validade da prova. Isto é, o que os italianos tratam como "idoneidade" da prova para assegurar o acertamento dos fatos", ou o que o legislador pátrio prescreve como sendo um meio apto "para provar a verdade dos fatos".

No sistema italiano, em que há regra expressa sobre as provas atípicas, a admissibilidade da prova informática se dá sob regência do art. 189 do *Codice di Procedura Penale* italiano, que tem por um dos requisitos, sua idoneidade para o acertamento dos fatos. E a doutrina tem considerado que, se sua obtenção das informações memorizadas em suporte informático não seja efetuada por meio de atividade pericial de análise, se estará diante de uma anomalia inidônea a incidir sobre a validade do ato.[24]

A mesma conclusão pode ser aplicada ao processo penal brasileiro. A prova digital, por aplicação analógica do art. 369 do Código de Processo Civil, somente deve admitir, e na condição de prova atípica, se for produzida seguindo os *standards* metodológicos adequados e, consequentemente, for apta "para provar a verdade dos fatos".

3. A cadeia de custódia da prova digital

Evidente que independentemente de qual procedimento técnico empregado, além de adequado segundo as melhores práticas, ele também precisará ser documentado e registrado em todas as suas etapas. Tal exigência é uma garantia de um correto emprego das *operating procedures*, especialmente por envolver um dado probatório volátil e facilmente sujeito à mutação.[25] Além disso, exatamente pela diferença ontológica da prova digital com relação à prova tradicional, devido àquela não se valer de uma linguagem natural, mas digital, é que, como diz Pittiruti, uma cadeia de custódia detalhada se faz ainda mais necessária.[26]

---

[22]. José Frederico Marque, A narcoanálise e a investigação criminal. In. *Estudos de Direito Processual Penal*. Rio de Janeiro: Forense, 1960, p. 292.

[23]. Os exemplos são de Michele Taruffo, Conoscenza scientifica e decisione giudiziaria: profili generali, *Decisione Giudiziaria e verità scientifica*, Milano: Giuffrè, 2005, p. 7.

[24]. Il tratamento della prova digitale..., p. 40.

[25]. Pittiruti, Digital evidence *e procedimento penale*..., p. 114.

[26]. Digital evidence *e procedimento penale*..., p. 115.

Realmente, **a documentação da cadeia de custódia é essencial no caso de análise de dados digitais**,[27] porque permite assegurar a autenticidade e integralidade dos elementos de prova e submeter tal atividade investigativa à posterior crítica judiciária das partes, excluindo que tenha havido alterações indevidas do material digital.[28]

Quanto ao laudo técnico, ele deve conter uma completa e exaustiva descrição dos sistemas informáticos utilizados, um elenco dos instrumentos (*tolls*) utilizados e um detalhado relatório dos resultados obtidos.[29] Segundo Casey, o laudo pericial deve conter: (*i*) introdução; (*ii*) descrição da fonte de prova; (*iii*) resumo do exame; (*iv*) o sistema de arquivos examinados; (*v*) análise pericial e os resultados encontrado; (*vi*) conclusão.[30]

Enunciados as características, os métodos técnicos e o regime legal da chamada prova digital, resta analisar quais as consequências da violação da cadeia de custódia da prova digital, de um lado, e da violação dos *standards* metodológicos próprios da *computer forensics*, de outro,

A necessidade de documentação da cadeia de custódia é fundamental para assegurar o potencial epistêmico das fontes de prova reais. As coisas, por existirem independente e extraprocessualmente, deverão ser coletadas e levadas ao processo por algum meio de prova correspondente, como a juntada de documentos, o laudo pericial ou mesmo a inspeção judicial. Para tanto, será necessário manter um registro rigoroso de todas as pessoas que tiveram sob seu poder físico os elementos de prova, desde sua coleta até a sua apresentação em juízo.

A cadeia de custódia da prova penal passou a ter disciplina legal, entre nós, com a Lei nº 13.964/2019, que inseriu os art. 158-A a 158-F no Código de Processo Penal. O art. 158-A traz a definição de cadeia de custódia: "Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte". Como facilmente se percebe, não se trata de definição da cadeia de custódia em si, mas sim da documentação da cadeia de custódia.

---

27. Nesse sentido: Daniele, La prova digitale nel processo penale…, p. 292; Lorenzetto, Le attività urgente di investigazione informatica…, p. 150. No mesmo sentido: E. Casey, *Digital evidence and computer crime*, 3 ed., London: Elsevier, 2011, p. 60.
28. Pittiruti, Digital evidence *e procedimento penale*..., p. 114-115.
29. Vaciago, *Digital evidence*…, p. 100.
30. *Digital evidence and computer crime*…, p. 76-77.

Importante destacar que, quando se fala em "cadeia de custódia" a expressão deve ser entendida como a elipse de "documentação da cadeia de custódia". A cadeia de custódia, em si, deve ser entendia com a sucessão encadeada de pessoas que tiveram contato com a fonte de prova real, desde que foi colhida, até que seja apresentada em juízo. É o conjunto de pessoas, uma após a outra, (p. ex.: o investigador, o delegado de polícia, o perito, o escrivão do cartório etc.) que teve contato com tal coisa (p. ex.: uma arma, um líquido, um tufo de fios de cabelo).

Esse conjunto de pessoas, e os momentos específicos em que cada uma delas teve contato com a evidência, precisa ser registrado, isto é, documentado, para que se saiba, exatamente, quem teve contado com a coisa e quando isso ocorreu.

De outro lado, o art. 158-B do CPP disciplina detalhadamente as etapas da cadeia de custódia, fazendo-o em dez diferentes fases, descrevendo, de modo didático, no que consiste cada uma das etapas de rastreamento do vestígio, que são: (1) reconhecimento; (2) isolamento; (3) fixação; (4) coleta; (5) acondicionamento; (6) transporte; (7) recebimento; (8) processamento; (9) armazenamento; (10) descarte.

Sobre o sujeito que tem o dever de registrar a cadeia de custódia, como já destacamos, "A documentação da cadeia de custódia é de responsabilidade das pessoas que têm contato com a fonte de prova custodiada. Assim, na investigação criminal, conduzida por órgãos oficiais, como é o caso do inquérito policial, o dever de registro e documentação da cadeia de custódia é dos funcionários públicos que tiverem contato com os elementos materiais que servem de prova".[31]

4. Da violação da cadeia de custódia da prova digital

No que toca as consequências da chamada "violação da cadeia de custódia", é importante ressaltar que, do ponto de vista terminológico, não é possível violar a cadeia de custódia em si. Uma pessoa ou tem ou não tem contato com a fonte de prova. Por sua vez, essa fonte de prova – ou vestígio, como se refere o § 3º do art. 158-A do CPP – pode se manter integra ou ser adulterada. Falsificar a fonte de prova real não é violar a cadeia de custódia (isto é, a documentação da cadeia de custódia), é fraudar ou adulterar a própria fonte de prova. Não se viola a sucessão de pessoas que teve contato com a coisa, mas a documentação que atesta essa realidade.

[31] *Processo penal*..., p. 511.

Se não há nenhum registro das pessoas que tiveram contato, p. ex., com uma mostra sanguínea coletada na cena do crime, inexiste "cadeia de custódia", entendida como "documentação da cadeia de custódia", por ausência do procedimento de integral registro das pessoas que tiveram contato com tal fonte de prova. Mas é evidente que houve uma cadeia de custódia, isto é, um conjunto maior ou menor de pessoas que tiveram contato com a prova. Por outro lado, se houve o registro somente de algumas das pessoas que tiveram contato com a fonte de prova, há uma documentação parcial da cadeia de custódia. Nesse caso, pode-se dizer que a cadeia de custódia, no sentido de documentação da cadeia de custódia, foi violada, porque essa não foi registrada em sua integralidade.

De qualquer modo, sem a documentação da cadeia de custódia, será impossível questionar a autenticidade e integridade de tal fonte de prova e, consequentemente, dos elementos de prova dela extraídos. O legislador, contudo, não estabelece quais as consequências processuais de seu desrespeito, sejam em termos de admissibilidade, seja quanto a valoração do meio de prova dela correspondente.

Há divergência na doutrina. Uma corrente defende que, não documentada integralmente a cadeia de custódia, a prova se torna ilegítima, não podendo ser admitida no processo.[32] Outros, contudo, superam o problema de admissão da prova e resolvem o problema do vício da cadeia de custódia dando menor valor ao meio de prova produzido a partir de fontes de prova cuja cadeia de custódia tenha sido violada. Ou seja, para os primeiros, a prova é inadmissível; para os segundos, é lícita, mas terá o seu valor probatório reduzido.

Temos defendido que, a constatação de vícios na cadeia de custódia, não leva, necessariamente, à ilicitude ou ilegitimidade da prova, que seria inadmissível no processo. Isso porque, é possível que haja apenas omissões ou irregularidade leves, sem que haja indicativos concretos de que a fonte de prova possa ter sido modificada, adulterada ou substituída. Em tais casos, a questão deve ser resolvida no momento da valoração.[33] Essa posição acabou sendo acolhida pelo STJ, que decidiu recentemente: "Mostra-se mais adequada a posição que sustenta que as irregularidades constantes da cadeia de custódia devem ser sopesadas pelo magistrado com todos os elementos

---

[32]. Nesse sentido, na doutrina nacional, com relação às provas em geral: Geraldo Prado, *Prova penal e Sistema de controles epistêmicos*. A quebra da cadeia de custódia das provas obtidas por mios ocultos. São Paulo: Marcial Pons, 2014, p. 92; Marcos Eberhardt, *Provas no Processo Penal*. Porto Alegre: Livraria do Advogado, 2015, p. 223; Yuri Azevedo e Caroline Regina Oliveira Vasconcelos, *Ensaios sobre a cadeia de custódia das provas no processo penal brasileiro.* Florianópolis: Empório do Direito, 2017, p. 109.

[33]. Gustavo Badaró, *Processo penal*. 9 ed. São Paulo: RT, 2021, p. 511-515.

produzidos na instrução, a fim de aferir se a prova é confiável. Assim, à míngua de outras provas capazes de dar sustentação à acusação, deve a pretensão ser julgada improcedente, por insuficiência probatória, e o réu ser absolvido". [34]

A solução, contudo, é diversa em dois casos: o primeira, quando não há qualquer documentação da cadeia de custódia; o segundo, quando não seja possível, minimamente, assegurar que o vestígio tenha potencial para o acertamento do fato.

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

Nesse sentido, p. ex., é a Section 31.1 do *Canada Evidence Act*: "Any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purposed to be".

Mesmo não havendo dispositivo legal equivalente no direito brasileiro, tal regra deve ser observada, por ser inerente a *digital evidence*. Como explica Lupária, "a tutela da genuinidade da *eletronic evidence* constitui um valor absoluto, ao qual deve se conformar os órgãos de investigação, sob pena de inutilizabilidade do material obtido por *unreliability*. Isto é, por inidoneidade da prova para assegurar um acertamento atendível dos fatos criminosos. Ao imputado cumpre somente demonstrar que a modalidade utilizada para a apreensão, para a manutenção da cadeia de custódia e para a sucessiva elaboração não respeitaram os cânones geralmente reconhecidos como aceitáveis. Onde isso ocorre, grava sobre a acusação o peso de demonstrar que o método, ainda que em desconformidade com a melhor prática técnica, não alterou, no caso concreto, os dados e salvaguardou a chamada 'integridade digital'". [35]

No mesmo sentido manifesta-se Manfredi Bontemplelli: "O tema de fundo é a natureza mutável do dado digital, que é suscetível de alterar pelo simples fato do acesso ao sistema informático, ainda mais se do tipo virtual, devendo antes de tudo, ser verificado o eventual emprego de técnica nova ou controversa. Em tal caso, deve ser verificada positivamente, no momento de decisão de admissibilidade, e não de modo

---

34. No caso, a substância havia chegado para perícia em um saco de supermercado, fechado por nó e desprovido de lacre. (STJ, HC 653.515/RJ, Rel. Min. Rogério Schietti Cruz, j. 23.11.2021, m.v.)
35. Luca Lupária, Processo penale e scienza informatica…, p. 197.

presumido, a idoneidade do procedimento empregado para a duplicação dos dados para assegurar a conformidade da cópia ao original a sua não modificabilidade, com exclusão dos dados obtidos através de procedimentos que não estejam de acordo com esse requisito".[36]

Em suma, elementos de prova que consistam, originariamente, em dados digitais, para serem admitido em juízo como prova, devem ter atestada a sua autenticidade e integridade, com a documentação da cadeia de custódia que demonstre os métodos informáticos de obtenção, registro, armazenamento, análise e apresentação.

Por outro lado, a *digital evidence* não terá o mínimo potencial epistêmico, não sendo apta a provar qualquer fato, quando a sua obtenção e produção não respeite as *best pratices*, por utilizar métodos não fiáveis.

A fase de aquisição do dado digital deve se desenvolver em condições que assegurem totalmente a "integridade e a não alterabilidade dos traços, na perspectiva de uma eventual e sucessiva repetibilidade da operação".[37] Ou, como diz Carlota Conti: "na hipótese em exame, o *modus procedendi* delineia uma verdadeira e própria 'forma essencial' para a utilização do dado coletado". [38]

Diversamente, se o método empregado não garante a tutela da genuinidade e não alteração do dado informático, devido à natureza frágil e volátil do material informático, "o emprego de métodos de aquisição incorretos muda a própria natureza da prova, a qual perde, de uma vez por todas, a idoneidade para prova qualquer coisa, porque irremediavelmente contaminada". [39] Itens que podem ser facilmente alterados e cujas características não são visualmente evidentes exigirão autenticação adicional que descreva o processo usado para chegar à conclusão a que se chega sobre as informações. Como destaca Heilik, "deve haver documentação que mostre claramente como esses processos são realizados, afetando a proveniência e autenticação da prova".[40]

---

[36]. Manfredi Bomtempelli, Acquisizione di dati custoditi in ambiente *cloud*. In: Scalfati, Adolfo (ed). *Le indagini atipiche*. Torino: G. Giappichelli Editore, 2019, p. 597.

[37]. Digital Forensics…, p. 219.

[38]. Carlota Conti, La prova informatica e il mancato rispetto della *best practice*: lineamenti sistematici sulle conseguenze processuali, in *Cybercrime*, Alberto Cadoppi, Stefano Canestrati, Adelmo Manna, Michele Papa, (Coord), *Trattato di diritto penale*, Torino: UTET, 2019, p. 1335. Acolhendo expressamente tal posicionamento: Enrico Maria. L'acquisizione di contenuti *e-mail*. In: SCALFATI, Adolfo (ed). *Le indagini atipiche*. Torino: G. Giappichelli Editore, 2019, p. 533.

[39]. Pittiruti, Digital evidence *e procedimento penale*..., p. 159.

[40]. Jacob Heilik, *Chain of custody for digital data*. A Practioner's Guide. 2019, p. 17. No original: "items that can be easily altered do whose characteristics are not visually evident will require additional authentication that describes the process used to come to the conclusion reached about the information. More importantly, there must be documentation that clearly shows how these processes are carried out with affecting the provenance and authentication of the exhibit"

Nesse caso, num sistema que respeite a presunção de inocência, não se poderá exigir do acusado a demonstração do prejuízo pela não utilização das melhores práticas segundo a *computer forensics*, devendo a prova ser destituída de valor probatório.

Por fim, além da completa documentação da cadeia de custódia, e do emprego das melhores práticas no processo de coleta, análise e exame do dado digital, a sua apresentação judicial, para que tenha potencial epistêmico adequado, deve se dar por meio de prova pericial.

Importante lembrar que o Projeto de Código de Processo Penal, atualmente tramitando na Câmara dos Deputados – PL nº 8045/10 - em sua última versão, correspondente ao substitutivo apresentado pelo Deputado João Campos, além da disciplina da prova digital,[41] também traz normas sobre a cadeia de custódia da prova digital relativamente aos meios de obtenção de provas digitais, definindo o seu conteúdo (art. 313)[42] e a sua finalidade (art. 314).[43] Além disso, exige a documentação da cadeia de custódia da prova digital como requisito para a sua admissibilidade. A cabeça do art. 300 projetado dispõe: "Art. 300. **A admissibilidade da prova nato-digital o**u digitalizada na investigação e no processo exigirá a **disponibilidade dos metadados** e a **descrição dos procedimentos de custódia** e tratamento suficientes para a verificação da sua **autenticidade** e **integridade**". (destaquei)

Mesmo que, de *lege lata* não exista regra semelhante, considerando que a prova digital tem por característica a ausência de materialidade, bem como não é elaborada em linguagem natural, ela é altamente volátil, estando sujeita a constante alterabilidade. Consequentemente, para sua admissão no processo deve haver prévia comprovação de sua integridade[44] e autenticidade, sendo essencial a documentação completa da cadeia de custódia, conforme exposto no presente tópico.

---

41. O art. 298 do Projeto de CPP traz definições de dispositivo eletrônico, sistema informático, protocolos de rede, rede de dados, pacotes de dados, dados em transmissão, dados em repouso, prova nato-digital e prova digitalizada. E o art. 299 traz o conceito de provas digitais: "Art. 299. Considera-se prova digital toda informação armazenada ou transmitida em meio eletrônico hábil ao esclarecimento de determinado fato".

42. "Art. 313. Além do auto circunstanciado, *será elaborado o registro da custódia do que foi apreendido na diligência*, indicando os custodiantes e as transferências havidas, bem como as demais operações realizadas em cada momento da cadeia" (destaquei)

43. "Art. 314. 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 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*". (destaquei)

44. A prova digital integra é aquela em relação à qual há certeza sobre a sua completude e não adulteração, não tendo sofrido qualquer modificação em seu conteúdo, desde o momento de sua criação até sua apresentação em juízo. Nesse sentido: Rennan Thamay e Maurício Tamer, *Provas no direito digital*. São Paulo: RT, 2020, p. 45.

Ou, o que seria o reverso da moeda, sem dados técnicos prévios, que permitam demonstrar a integridade e autenticidade do dado digital, a prova digital não deve ser admitida e, se o for, deverá ser desentranhada. Trata-se, pois, de tema prévio, que se resolve no exame de admissibilidade da prova digital e não uma questão sucessiva, relativa ao seu valor probatório.

5. Conclusões

Por fim, cabe sumariar cinco conclusões parciais:

1. A desmaterialização das provas digitais e a dispersão dos elementos digitais implicam sua congênita mutabilidade e fácil alterabilidade.

2. As provas digitais não possuem uma materialidade imediatamente constatável e são conservadas e transmitidas em linguagem não natural, o que torna mais difícil constatar modificações involuntárias ou adulterações voluntárias, quando comparadas com as tradicionais fontes reais de provas, notadamente os documentos cartáceos.

3. Embora não exista exigência legal, a produção da prova digital deve seguir os *standards* metodológicos da chamada *computer forensics*, adotando as melhores práticas do conjunto de procedimentos mais ou menos consolidados e testados através da experiência na área.

4. A prova digital caracteriza-se como prova atípica no processo penal, cuja admissibilidade deve se dar com fundamento no artigo 369 do Código de Processo Civil, sendo necessário demonstrar previamente a sua aptidão "para provar a verdade dos fatos".

5. Se não houve a documentação completa da cadeia de custódia da prova digital, restará impossibilita qualquer análise sobre sua integridade e a autenticidade, torna os arquivos digitais, inadmissíveis como prova atípica no processo penal, porque destituídos de qualquer potencial epistêmico.

Bibliografia

ATERNO, Stefano. Digital Forensics (Investigazioni informatiche). *Digesto delle Discipline Penalistiche*. Torino: Utet, aggiornamento, 2014. t. II.

AZEVEDO, Yuri; VASCONCELOS, Caroline Regina Oliveira. *Ensaios sobre a cadeia de custódia das provas no processo penal brasileiro.* Florianópolis: Empório do Direito, 2017.

BADARÓ, Gustavo *Processo penal*. 9 ed. São Paulo: RT, 2021.

BOMTEMPELLI, Manfredi. Acquisizione di dati custoditi in ambiente *cloud*. In: Scalfati, Adolfo (ed). *Le indagini atipiche*. Torino: G. Giappichelli Editore, 2019.

CASEY, E. *Digital evidence and computer crime*, 3 ed., London: Elsevier, 2011.

COMOGLIO, Luigi Paolo. *Le prove civile*, Torino: Utet, 1998.

CONTI, Carlota. La prova informatica e il mancato rispetto della *best practice*: lineamenti sistematici sulle conseguenze processuali, in *Cybercrime*, Alberto Cadoppi, Stefano Canestrati, Adelmo Manna, Michele Papa, (Coord), *Trattato di diritto penale*, Torino: UTET, 2019.

DANIELE, Marcello. La prova digitale nel processo penale, *Rivista di Diritto Processuale*, 2011.

EBERHARDT, Marcos. *Provas no Processo Penal*. Porto Alegre: Livraria do Advogado, 2015.

HEILIK, Jacob. *Chain of custody for digital data*. A Practioner's Guide, 2019.

KENT, Karen; CHEVALIER, Suzanne; GRANCE, Tim; DANG, Hug. *Guide to Integrating Forensic Techniques into Incident Response*. Recommendations of the National Institute of Standards and Technology, NIST publication, 2006. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

KERR, O.S.. Digital evidence and the new criminal procedure, In: *105 Columbia law review,* 2005.

LORENZETTO, Elisa. Le attività urgente di investigazione informatica e telematica, In. Luca Lupária (Coord.). *Sistema penale e criminalità informatica*. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime. Milano: Giuffrè, 2009.

LUPÁRIA, Luca. Processo penale e scienza informatica: anatomia de una trasformazione epocale, In. Luca Lupária; Giovanni Ziccardi, *Investigazione penale e tecnologia informatica*. L'accertamento del reato tra progresso scientifico e garanzie fondamentale, Milano: Giuffrè, 2007.

MARIA, Enrico. L'acquisizione di contenuti *e-mail*. In: Adolfo Scalfati, (ed). *Le indagini atipiche*. Torino: G. Giappichelli Editore, 2019.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. *Comentários ao Código de Processo Civil.* São Paulo: RT, v. VII, 2016.

MARQUES, José Frederico. A narcoanálise e a investigação criminal. In. *Estudos de Direito Processual Penal*. Rio de Janeiro: Forense, 1960, p. 292.

PITTIRUTI, Marco. Digital evidence *e procedimento penale*. Torino: Giappichelli, 2017.

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

RICCI, Gian Franco. Atipicità della prova, processo ordinario e rito camerale, *Rivista trimestrale di diritto e procedura civile*, 2020.

_____. *Le prove atipiche*, Milano: Giuffrè, 1999.

TARUFFO, Michele. Conoscenza scientifica e decisione giudiziaria: profili generali, *Decisione Giudiziaria e verità scientifica*, Milano: Giuffrè, 2005.

_____. *La prova nel processo civile*. Milano: Guiffrè, 2012.

THAMAY, Rennan; TAMER, Maurício. *Provas no direito digital*. São Paulo: RT, 2020, VACIAGO, Giuseppe. *Digital Evidence*. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato. Torino: Giappichelli, 2012.

ZICCARDI, Giovanni. Aspetti informatico-giuridico della fonte di prova digitale, In. Luca Lupária; Giovanni Ziccardi, *Investigazione penale e tecnologia informatica*. L'accertamento del reato tra progresso scientifico e garanzie fondamentale, Milano: Giuffrè, 2007.

_____. Le linee guida della Association of Chief Police Officers Inglese, In. Luca Lupária; Giovanni Ziccardi, *Investigazione penale e tecnologia informatica*. L'accertamento del reato tra progresso scientifico e garanzie fondamentale, Milano: Giuffrè, 2007.