OS *STANDARDS* METODOLÓGICOS DE PRODUÇÃO NA PROVA DIGITAL E A IMPORTÂNCIA DA CADEIA DE CUSTÓDIA

THE METHODOLOGICAL STANDARDS ON THE PRODUCTION OF DIGITAL EVIDENCE PRODUCTION AND THE IMPORTANCE OF THE CHAIN OF CUSTODY

Gustavo Badaró
Professor Titular de Direito Processual Penal da USP. Advogado Criminalista e Consultor Jurídico.
ORCID: 0000-0002-4526-9316
gustavobadaro@usp.br

RESUMO: O presente artigo analisa a prova digital e os problemas decorrentes de suas diferença com as provas tradicionais. Diante do caráter não material e da congênita mutabilidade da prova digital, defende-se que sua validade epistêmica depende da observância dos *standards* metodológicos próprios para *computer forensics*, para individualizar o suporte informático que contém o dado digital útil à investigação, sua obtenção, conservação, análise e apresentação judicial dos resultados, mediante prova pericial, bem como da completa e integral documentação da cadeia de custódia.

Palavras-chave: Prova Digital, Cadeia de Custódia, Computação Forense.

ABSTRACT: This article analyzes digital evidence and the problems arising from its differences with traditional evidence. Due to the non-material character and the "congenital mutability" of digital evidence, it is argued that its epistemic validity depends on the compliance with specifics methodological standards of computer forensics, which are required to individualize the computer system that stored the digital data useful to the investigation, its collection, conservation, analysis and results presentation in Court, through digital evidence expert opinion, as well as the complete chain of custody documentation.

Keywords: Digital Evidence, Chain Of Custody, Computer Forensics.

Na chamada prova digital ou, como se costuma denominar, *digital evidence*, 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 os diversos temas novos e difíceis da prova digital, destacam-se duas diferenças relevantíssimas, comparadas com os meios de 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 relatório:

> 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.[4]

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

Por todas essas diferenças, quando comparadas com as tradicionais provas utilizadas no processo penal, em especial as chamadas fontes reais de provas, notadamente os documentos, a *digital evidence*, 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 pudesse estabelecer uma técnica específica a ser empregada para a individualização e apreensão da prova digital, sob pena de inutizabilidade da prova. Todavia, considerando, de um lado, que a informática é uma ciência relativamente jovem e ainda não há meios e técnicas uniformemente aceitos e, de outro, que tem havido rapidíssima mutação e evolução das técnicas computacionais, tal solução se mostra inviável.

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 impalpabilidade que decorre 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] 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.[13]

Justamente por isso, a prova digital é tema central da chamada *computer forensics*, que deve se valer de instrumentos técnicos ou *tools* adequados para os trabalhos de investigação de dados digitais que poderão constituir uma prova utilizável em processo judicial. Para tanto, é necessário: (*i*) individualizar o suporte informático que contém 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.[14]

É imprescindível que o método empregado garanta a integridade do dado digital e, com isso, a força *probandi* do conteúdo probatório por ele representado.[15] Normalmente, é necessário fazer 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.

Evidente que todo esse processo técnico precisa 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 sujeito à mutação.[16] Exatamente pela diferença ontológica da prova digital com relação à prova tradicional, bem como devido àquela não se valer de uma linguagem natural, mas digital, é que uma cadeia de custódia detalhada se faz ainda mais necessária.[17]

Realmente, a documentação da cadeia de custódia é essencial no caso de análise de dados digitais,[18] porque permitirá assegurar a autenticidade e integralidade dos elementos de prova e submeter tal atividade investigativa à posterior crítica judiciária das partes, e excluirá que tenha havido alterações indevidas do material digital.[19]

Quanto ao laudo técnico, no qual se consubstanciará a prova digital, deve conter uma completa e exaustiva descrição dos sistemas informáticos utilizados, um elenco dos instrumentos (*tolls*) utilizados e um detalhado relatório dos resultados obtidos.[20] 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 encontrados; (*vi*) conclusão.[21]

No campo internacional, destacam-se na matéria 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; ISO/IEC 27042/2015, consistente 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 podem ser citados, do ponto de vista operacional, e no que se refere a *mobile forensics*, 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.

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*.

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 no processo penal 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 do Código de Processo Penal traz uma 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.

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 precisam ser registrados, isto é, documentados, para que se saiba, exatamente, quem teve contado com a coisa e quando isso ocorreu.

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.[22]

No que toca às 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.

Se não há nenhum registro das pessoas que tiveram contato, p. ex., um *pen-drive* coletado 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 possível 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 à valoração do meio de prova dela correspondente.

Na doutrina, uma corrente defende que, não documentada integralmente a cadeia de custódia, a prova se torna ilegítima, não podendo ser admitida no processo. Outro posicionamento supera o problema de admissão da prova, resolvendo o vício da falha na documentação 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. Filio-me à segunda corrente: 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.[23]

No caso da *digital evidence*, contudo, a solução deve ser diversa ante a desmaterialização dos elementos de prova, que impede a constatação diretamente pelos sentidos, e a facilidade de mutação dos elementos de prova, se sua obtenção e produção não respeitarem as *best practices*. Se forem utilizados métodos não fiáveis, os elementos de prova digitais não terão o mínimo potencial epistêmico, e a prova eletrônica não será apta a provar qualquer fato. Em regra, portanto, é necessário o emprego de um método adequado, de acordo com as melhores práticas, e que haja a documentação completa da cadeia de custódia. Se o método for inadequado ou se, embora adequado, não houver comprovação de seu emprego por ausência de registro da cadeia de custódia, não há como garantir a tutela da genuinidade e não alteração do dado informático devido a sua natureza frágil e volátil. Assim, "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".[24]

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.

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'.[25]

Em suma, no caso das provas digitais, para que seja minimamente atestada a sua autenticidade e integridade, devem ser seguidos os métodos informáticos de obtenção, registro, armazenamento, análise e apresentação dos elementos de prova digitais que registrem as *best practices* nacionais e internacionais. Sua apresentação judicial, para que tenha potencial epistêmico adequado, deve se dar por meio de prova pericial, sendo essencial a completa documentação da cadeia de custódia.

NOTAS

1 DANIELE, 2011, p. 283.
2 KERR, 2005, p. 284.
3 A ausência de materialidade da prova digital, como destaca Daniele, não significa que a mesma 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". (DANIELE, 2011, 284.)
4 KENT, 2006.
5 Nesse sentido: ZICARDI, 2007, p. 120; VACIAGO, 2012, p. 7; PITTIRUTI, 2017, p. 4. Com pequena variação, Caria divide a análise forense nas seguintes fases: identificação, aquisição, análise e relatório. (CARIA, 2020, p. 3)
6 Kerr sustenta a necessidade de repensar todas as regras probatórias comuns, originariamente concebidas para as provas tradicionais (KERR, 2005, 290 e segs.). De modo semelhante, DANIELE, 2011, p. 284.
7 LUPÁRIO, 2007, p. 133.
8 Nesse sentido: DANIELE, 2011, p. 284; PITTIRUTI, 2017, p. 6.
9 DANIELE, 2011, p. 284.
10 Nesse sentido: PITTIRUTI, op. cit., p. 11.
11 PITTIRUTI, 2017, p. 25; ZICARDI, 2007, p. 117.
12 DANIELE, 2011, p. 292.
13 ZICARDI, 2007, p. 51.
14 VACIAGO, 2012, p. 23. De modo semelhante; ZICARDI, 2007, p. 57.
15 LORENZETTO, 2009, p. 149.
16 PITTIRUTI, 2017, p. 114.
17 PITTIRUTI, 2017, p. 115.
18 Nesse sentido: DANIELE, 2011, p. 292; LORENZETTO, 2009, p. 150. No mesmo sentido: CASEY, 2011, p. 60.
19 PITTIRUTI, 2017, p. 114-115.
20 VACIAGO, 2012, p. 100.
21 CASEY, 2011, p. 76-77.
22 BADARÓ, 2020, p. 511.
23 BADARÓ, 2020, p. 511-515, item 10.2.9.3.
24 PITTIRUTI, 2017, p. 159.
25 LUPÁRIA, 2007, p. 197.

Referências

CARIA, Giovanni. Le quattro fasi dell'analise forense: identificazione, acquisizione, analisi, *reporting*. In: IASELLI, Michele (Org.) *Invesytigazione ditigali*. Milano: Giuffrè Francies Lefebvre, 2020, p. 3

CASEY, E. *Digital evidence and computer crime*. 3. ed., London: Elsevier, 2011, p. 60.

DANIELE, Marcello. La prova digitale nel processo penale. *Rivista di Diritto Processuale*, v. 66, n. 2, p. 283-298, 2011, p. 283.

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. Gaithersburg: NIST, 2006. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf. Acesso em: 12 mai. 2021.

KERR, O.S. Digital evidence and the new criminal procedure. *Columbia law review*, v. 105, p. 279-318, 2005, p. 284.

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

LUPÁRIO, 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.

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

VACIAGO, Giuseppe. *Digital Evidence*. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato. Torino: Giappichelli, 2012.

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

Autor convidado