Aquisição das fontes de prova penal digital: reflexões a partir do informativo de jurisprudência 763 do STJ

Acquisition of digital criminal evidence sources: reflections based on jurisprudence newsletter 763 of the STJ

Carlos Hélder Carvalho Furtado Mendes

Doutor e Mestre em Ciências Criminais pela PUC-RS. Especialista em Direito Penal Econômico pela Universidade de Coimbra/IBCCRIM (2017). Especialista em Ciências Penais pela Uniderp (2017). Bacharel em Direito pelo UNDB-Centro Universitário/MA (2015). Advogado.
Lattes: [http://lattes.cnpq.br/3034060693231004].
ORCID: [https://orcid.org/0000-0001-5256-1297].
helder@madeiraadvogados.com.br

Yuri Felix

Doutor e Mestre em Ciências Criminais pela PUC-RS. Professor, palestrante e parecerista com artigos publicados em revistas especializadas. Advogado.
Lattes: [http://lattes.cnpq.br/0866064520436785].
ORCID: [https://orcid.org/0000-0003-1494-9535].
advyuri@gmail.com

DOI: [https://doi.org/10.54415/rbccrim.v197i197.504].

Autores convidados

Áreas do Direito: Digital; Penal; Processual

Resumo: O presente artigo tem como objetivo de pesquisa o estudo acerca da aquisição de dados informáticos a partir da extração perpetrada na persecução penal, partindo da apreensão dos dispositivos informáticos. Trata-se de tema de contemporânea discussão nos Tribunais Superiores brasileiros. Assim, será analisado o julgamento do Superior Tribunal de Justiça no AgRg no Recurso em *Habeas Corpus* 143.169 – RJ (2021/0057395-6), e a partir deste precedente serão propostas outras discussões pertinentes ao tema, como a execução de mandados judiciais

Abstract: This article aims to study the acquisition of computer data from the extraction perpetrated in criminal prosecution, from the apprehension of computer devices. This is a subject of contemporary discussion in Brazilian Superior Courts. Thus, the judgment of the AgRg in the Appeal in *Habeas Corpus* 143,169 – RJ (2021/0057395-6) – STJ will be analyzed, and based on this precedent, other discussions pertinent to the subject will be proposed, such as the execution of concrete court orders, the guidelines established by Digital Forensic Science and

Mendes, Carlos Hélder Carvalho Furtado; Felix, Yuri. Aquisição das fontes de prova penal digital: reflexões a partir do informativo de jurisprudência 763 do STJ.
Revista Brasileira de Ciências Criminais. vol. 197. ano 31. p. 215-247. São Paulo: Ed. RT, jul./ago. 2023.
DOI: [https://doi.org/10.54415/rbccrim.v197i197.504].

concretos, as diretrizes estabelecidas pela Ciência Forense Digital e a observância da *Discovery* como instituto capaz de aportar maior confiabilidade na extração de dados por softwares de uso investigativo. O estudo do caso é, portanto, a metodologia empregada cuja análise também se complementa pela revisão bibliográfica e documental.

Palavras-chave: Prova Penal Digital – Extração de dados informáticos – Informativo de Jurisprudência 763 – STJ.

the observance of Discovery as an institute capable of providing greater reliability in the extraction of data by software for investigative use. The case study is, therefore, the methodology used whose analysis is also complemented by bibliographical and documentary review.

Keywords: Digital Criminal Evidence – Extraction of computer data – Jurisprudence Newsletter 763 – STJ.

Sumário: 1. Introdução. 2. Apreensão de dispositivos informáticos, pesquisa e recolha de fonte de prova digital: a execução de mandados judiciais. 3. *Best Practices* da ciência forense digital e o acertamento técnico informático para aquisição e recolha de fontes de prova digital. 4. A rastreabilidade da fonte de prova penal digital: *discovery* e *softwares*. 5. Considerações finais. 6. Referências. 7. Jurisprudência.

1. Introdução

A prova penal digital é tema cuja importância tem se destacado em diversos julgados proferidos pelos Tribunais Superiores Brasileiros. Embora ainda haja lacunas legislativas sobre tal instituto probatório, alguns avanços jurisprudenciais já são observados desde a perspectiva da confiabilidade probatória para a utilização de dados informáticos em processos penais. Assim, o presente artigo tem como objetivo estabelecer pressupostos que sirvam de diretrizes na atividade probatória em contexto digital.

Para tanto, propõe-se a análise do AgRg no Recurso em Habeas Corpus 143.169 – RJ (2021/0057395-6)[1], em que o Min. Ribeiro Dantas proferiu voto-vista responsável

1. BRASIL, Superior Tribunal de Justiça – STJ, AgRg no Recurso em Habeas Corpus 143.169 – RJ (2021/0057395-6), rel. Min. Jesuíno Rissato (Des. convocado do TJDFT); rel. p/acórdão Min. Ribeiro Dantas. "Ementa: penal e processual penal. Agravo regimental no recurso ordinário em habeas corpus. Operação open doors. Furto, organização criminosa e lavagem de dinheiro. Acesso a documentos de colaboração premiada. Falha na instrução do habeas corpus. Cadeia de custódia. Inobservância dos procedimentos técnicos necessários a garantir a integridade das fontes de prova arrecadadas pela polícia. Falta de documentação dos atos realizados no tratamento da prova. Confiabilidade comprometida. Provas inadmissíveis, em consequência. Agravo regimental parcialmente provido para prover também

pela fixação de entendimentos importantes quanto às cautelas necessárias para a aquisição e admissão de dados informáticos como fonte de prova penal extraídos de dispositivos digitais. A justificativa para a escolha metodológica desse precedente se pauta na fixação de entendimento registrado em Informativo Jurisprudencial 763 do Superior Tribunal de Justiça, cujo destaque aponta para a "inadmissibilidade de provas digitais sem registro documental acerca dos procedimentos adotados pela polícia para a preservação da integridade, autenticidade e confiabilidade dos elementos informáticos".

em parte o recurso ordinário. 1. O habeas corpus não foi adequadamente instruído para comprovar as alegações defensivas referentes ao acesso a documentos da colaboração premiada, o que impede o provimento do recurso no ponto. 2. A principal finalidade da cadeia de custódia é garantir que os vestígios deixados no mundo material por uma infração penal correspondem exatamente àqueles arrecadados pela polícia, examinados e apresentados em juízo. 3. Embora o específico regramento dos arts. 158-A a 158-F do CPP (introduzidos pela Lei 13.964/2019) não retroaja, a necessidade de preservar a cadeia de custódia não surgiu com eles. Afinal, a ideia de cadeia de custódia é logicamente indissociável do próprio conceito de corpo de delito, constante no CPP desde a redação original de seu art. 158. Por isso, mesmo para fatos anteriores a 2019, é necessário avaliar a preservação da cadeia de custódia. 4. A autoridade policial responsável pela apreensão de um computador (ou outro dispositivo de armazenamento de informações digitais) deve copiar integralmente (bit a bit) o conteúdo do dispositivo, gerando uma imagem dos dados: um arquivo que espelha e representa fielmente o conteúdo original. 5. Aplicando-se uma técnica de algoritmo *hash*, é possível obter uma assinatura única para cada arquivo, que teria um valor diferente caso um único *bit de* informação fosse alterado em alguma etapa da investigação, quando a fonte de prova já estivesse sob a custódia da polícia. Comparando as *hashes* calculadas nos momentos da coleta e da perícia (ou de sua repetição em juízo), é possível detectar se o conteúdo extraído do dispositivo foi modificado. 6. É ônus do Estado comprovar a integridade e confiabilidade das fontes de prova por ele apresentadas. É incabível, aqui, simplesmente presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia. No processo penal, a atividade do Estado é o objeto do controle de legalidade, e não o parâmetro do controle; isto é, cabe ao Judiciário controlar a atuação do Estado-acusação a partir do direito, e não a partir de uma autoproclamada confiança que o Estado-acusação deposita em si mesmo. 7. No caso dos autos, a polícia não documentou nenhum dos atos por ela praticados na arrecadação, armazenamento e análise dos computadores apreendidos durante o inquérito, nem se preocupou em apresentar garantias de que seu conteúdo permaneceu íntegro enquanto esteve sob a custódia policial. Como consequência, não há como assegurar que os dados informáticos periciados são íntegros e idênticos aos que existiam nos computadores do réu. 8. Pela quebra da cadeia de custódia, são inadmissíveis as provas extraídas dos computadores do acusado, bem como as provas delas derivadas, em aplicação analógica do art. 157, § 1º, do CPP. 9. Agravo regimental parcialmente provido, para prover também em parte o recurso ordinário em habeas corpus e declarar a inadmissibilidade das provas em questão."

Conforme consta no relatório do voto-vista proferido pelo Min. Ribeiro Dantas, a denúncia ministerial em desfavor de sete réus "relata que os acusados integravam o núcleo de *hackers* dirigentes da organização criminosa, tendo praticado 81 furtos e assim subtraído cerca de R$ 3.300.000,00". A investigação criminal que embasou o oferecimento da denúncia foi composta por diversas medidas cautelares probatórias e subsequentes quebras de sigilos de dados armazenados nos aparelhos eletrônicos apreendidos pela polícia. Tais dispositivos foram periciados primeiramente por uma as instituições financeiras vítima dos furtos e, após, pela autoridade policial.

No tocante ao tema da quebra da cadeira de custódia da prova digital, expõe o referido Ministro que a tese defensiva defendida era de que "a polícia não documentou nenhum de seus procedimentos no manuseio dos computadores apreendidos na casa do paciente".

Nesse sentido, conforme o Min. Ribeiro Dantas,

> "uma fonte de prova que armazena dados imateriais, se coletada de maneira profissional e técnica pela polícia, pode oferecer garantias de mesmidade superiores àquelas de uma fonte corpórea, dada a precisão e objetividade do algoritmo de *hash*."

Assim, no caso em apreço, constatou-se que não haveria nenhum tipo de registro documental sobre 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. Tais providências, entre outras, foram ignoradas pela autoridade policial. Em que pese haja menção de que a polícia extraiu arquivo de imagem, não há qualquer indicação de como ela fez isso, tampouco a indicação de *hash* respectiva.

De tal sorte, pelo entendimento do Ministro restaria comprometida a aferição da autenticidade entre a cópia periciada e o arquivo original. Como anota o voto-vista, não há explicação metodológica da extração dos arquivos de computadores. Assim, frisa o Min. Ribeiro Dantas que

> "no processo penal, a atividade do Estado é objeto do controle de legalidade, e não parâmetro do controle. Dito de outro modo, cabe ao Judiciário controlar a atuação do Estado-acusação a partir do direito, e não a partir de uma autoproclamada confiança que o Estado-acusação deposita em si mesmo."

Em contexto conclusivo, observa o Ministro que não se pode adjetivar de "desmedida formalidade", a documentação dos atos da cadeia de custódia, pois tal postura "equivale a dizer que a atuação estatal não é submetida a controle e que, se o Estado-acusação afirmar que atuou no manejo da prova, isso já bastaria para

encampar suas conclusões, dispensando-se a demonstração objetiva da regularidade de seus atos". Ou seja, uma patente incompatibilidade com o "processo penal democrático, racional e pautado em comprovações objetivas, para além das impressões pessoais dos agentes públicos que nele atuam".

Diante desse cenário, o presente artigo visa ao estudo acerca da aquisição de dados informáticos a partir da extração perpetrada na persecução penal, a partir da apreensão dos dispositivos informáticos. Portanto, partindo da análise do julgamento do Superior Tribunal de Justiça no AgRg no Recurso em Habeas Corpus 143.169 – RJ (2021/0057395-6), tem-se como objetivo a propositura de respostas às lacunas ainda presentes na Doutrina, Jurisprudência e Legislação que versem sobre a Prova Penal Digital.

Uma primeira pergunta problema que se destaca é: quais pressupostos devem ser obedecidos pela Autoridade Investigativa para que se garanta grau de confiabilidade adequado na produção de prova penal digital?

A resposta para tal pergunta, em termos metodológicos, será dividida em três partes organizadas em capítulos. No primeiro capítulo, elencar-se-á alguns critérios para a execução da extração de tais fontes de provas digitais, desde pressupostos necessários para evitar mandados judiciais genéricos que resultam em verdadeiras pescarias probatórias (*fishing expedition*). No segundo capítulo, apontar-se-á as boas práticas recomendadas pela Ciência Forense Digital, estabelecendo postulados próprios que devem ser observados pelas Autoridades Investigativas, em que são destacadas as peculiaridades da Prova Penal Digital e necessárias cautelas técnicas operacionais. Por fim, no terceiro capítulo, inaugurar-se-á uma discussão pautada no estabelecimento da *Discovery,* como instituto processual penal que garante o direito ao conhecimento de todo o procedimento desempenhado para a consagração daquilo denominado rastreabilidade da fonte de prova penal digital.

2. Apreensão de dispositivos informáticos, pesquisa e recolha de fonte de prova digital: a execução de mandados judiciais

A apreensão de dispositivos informáticos autorizada por determinação judicial motivada é efetivamente medida cautelar probatória legítima. Após a apreensão dos dispositivos informáticos visados, proceder-se-á com a cópia integral – ou aquisição[2] – dos dados, arquivos e programas pela técnica *bit stream* ou *image bit*

2. Falar em aquisição de fontes de prova digital, portanto, é diferente de se falar em apreensão, pois o que ocorre é a extração a partir da cópia do conteúdo dos dispositivos de armazenamento. COSTABILE, Gerado. Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008. *Ciberspazio e Diritto*, v. 11, n. 3, 2010. p. 478.

a bit[3]. Todavia, é preciso perceber que pela amplitude das informações[4] que podem ser armazenadas em tais dispositivos[5] devem existir critérios mais objetivos de pesquisa e recolha das fontes de prova digital contidas nos dispositivos informáticos

3. Como salienta Polansky, "esta copia no es una copia simple, sino una imagen forense (también definida como copia bit a bit o copia forense). […] La imagen forense es una réplica exacta del disco rígido. Es decir, es una copia idéntica de todos y cada uno de los bits del disco rígido, lo que incluye la totalidad de los archivos almacenados, el espacio libre y el no asignado, el 'Master file table', en el orden preciso en que se encuentran en el disco original. Esta puede ser obtenida en el lugar del allanamiento, o se puede secuestrar la unidad física de almacenamiento digital (el disco rígido) y obtenerla, en una etapa posterior, en un laboratorio de informática con personal especializado, lo que en general se recomienda. Una vez obtenida, las buenas prácticas de informática indican que, inmediatamente, se debe obtener su correspondiente código hash. Este código consiste en una compleja función matemática que sirve para determinar si dos archivos digitales son idénticos. […] Básicamente, cualquiera de los algoritmos que se utilicen transformará la totalidad de la información contenida en la imagen forense y arrojará como resultado un código único". POLANSKY, Jonathan A. *Garantías constitucionales del procedimiento penal en el entorno digital*. Buenos Aires: Hammurabi, 2020. p. 168-169.
4. KERR, Orin S. Executing warrants for digital evidence: the case for use restrictions on nonresponsive data. Texas *Tech Law Review*, v. 48:1, 2015. p. 3. "It is impossible to know if specific information is contained on a device without searching it. And behind the scenes, it turns out that electronic information can be stored anywhere on a device. Putting these facts together, a law enforcement search for digital evidence requires searching for a needle in an enormous electronic haystack. And because computers get better and better every year, storing more and more information, the haystack is becoming exponentially larger over time".
5. Exemplificativamente, como apontam Gloeckner e Eilberg, "o que deve ser imediatamente bem compreendido é que o aparelho celular configura-se, concomitantemente, como um objeto capaz de assegurar a portabilidade de registros e informações de conteúdo pessoal e receptáculo de tecnologias de informação (especialmente aplicativos), que faz o papel de conector entre o usuário e múltiplos veículos de informação e facilitadores. Dessa maneira, ao mesmo tempo que o celular integra aparatos tecnológicos – como câmeras digitais, agendas de contato, calculadoras, gravadores de voz e outros tantos instrumentais –, também acaba por servir como um verdadeiro computador, atuando, então, como uma plataforma tecnológica de integração entre múltiplos canais de comunicação, além de permitir, como dispositivo tecnológico, a utilização de aplicativos de trocas de mensagens (e.g. WhatsApp), de acesso e movimentação de contas bancárias, de aquisição e armazenamento de passagens aéreas, de verificação e utilização de e-mails registrados no dispositivo, de acesso às redes sociais como o Facebook". GLOECKNER, Ricardo; EILBERG, Daniela Dora. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. *Revista Brasileira de Ciências Criminais*, v. 156/2019, 2019. p. 353-393.

apreendidos. Tal preocupação, conforme Pitituri[6], decorre do perigo de que as metodologias de pesquisa e recolha possam se transformar em formas indevidas de *inquisitio generalis*.

Desse modo, o legislador processual penal deve descrever quais os requisitos, para além dos indícios de autoria e materialidade delitiva, e os limites da atuação estatal atrelados desde a aquisição até a recolha dos dados ou informações pretendidas, programas informáticos visados e a sua vinculação pertinente ao tipo penal ilícito em apuração. A restrição aos direitos fundamentais afetados deve, necessariamente, ser fator determinante para a disposição legislativa do método coativo. Na ausência legislativa para um procedimento de aquisição de fonte de prova digital, há algumas diretrizes que devem ser levadas em consideração.

Há, portanto, dois momentos distintos cujas autorizações judiciais devem ser particularizadas. O primeiro, efetivamente, refere-se à apreensão do dispositivo informático visado. O segundo, a seu turno, refere-se à pesquisa e à recolha das *fontes de prova digital* que possam ser encontradas nos dispositivos informáticos de armazenamento digital.

No tocante à apreensão dos dispositivos informáticos visados, para que se alcance uma determinação judicial favorável, a delimitação da representação investigativa pressupõe uma investigação preliminar cuja exaustividade seja capaz de apontar à autoridade judicial elementos plausíveis de que em determinado(s) dispositivo(s) informático(s), vinculado(s) a pessoas investigadas determinadas, possam ser encontradas *fontes de prova digital* capazes de sustentar a hipótese criminal em um processo judicial[7].

Nesse sentido, salienta Costabile[8] que a simples referência ao título do crime não pode substituir a indicação dos requisitos probatórios concretos, mas

6. PITTIRUTI, Marco. *Digital evidence e procedimento penale.* G. Giappichelli Editore: Torino, 2017. p. 143. "Il rischio di abusi appare particolarmente concreto con riguardo alle perquisizioni informatiche, giacché la res all'interno del quale si cercano i singoli file o programmi oggetto di attenzione investigativa è il sistema informatico o telematico nella sua interezza".

7. PITTIRUTI, Marco. *Digital evidence e procedimento penale*. Torino: G. Giappichelli Editore, 2017. p. 148. "allora il sequestro deve essere preceduto da un'attività mirata a verificare se siano presenti le informazioni ricercate, per poi acquisire unicamente queste ultime".

8. COSTABILE, Gerado. Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008. *Ciberspazio e Diritto*, v. 11, n. 3, 2010. p. 473. "In mancanza di tale individuazione non sarebbe possibile accertare né l'esistenza delle esigenze probatorie su cui si fonda il provvedimento, né la natura di corpo del reato o cosa ad esso pertinente, oggetto di

consubstancia-se apenas como referência ou pré-requisito para a atividade de aquisição probatória. É dizer, a hipótese criminal ou o *thema probandum* deve ser plenamente identificada, mesmo que de maneira hipotética, mas correspondente a uma infração que se amolda a uma descrição penal típica. Portanto, para que seja plausível a objetividade na determinação judicial autorizativa, deve-se observar como pressuposto necessário uma identificação prévia da hipótese criminal que se pretende comprovar[9], bem como fundamental a avaliação da "função" do dispositivo informático na empreitada delitiva[10].

É claro que, pela eficácia da medida cautelar probatória executada em fase de investigação preliminar, a decisão judicial autorizativa é tomada sem o estabelecimento do contraditório prévio, por isso é que se estabelece uma maior cautela para a restrição do direito fundamental do sujeito imputado. Exigindo-se assim apontamentos quanto à indicação dos dispositivos informáticos visados e sua relação com os investigados e com a investigação[11].

Após a apreensão do dispositivo informático, procedendo-se com a extração integral, ou cópia forense e sua autenticidade, a autoridade investigativa deverá executar as medidas de pesquisa e de recolha das *fontes de prova digital* identificadas no dispositivo de armazenamento. A pesquisa, cujo objetivo é a identificação das *fontes de prova digital* armazenadas nos dispositivos informáticos que foram copiadas,

---

ricerca ed acquisizione. In tal caso quindi la perquisizione non sarà più un mezzo di ricerca della prova, ma un criticato mezzo di acquisizione della notitia criminis".

9. PITTIRUTI, Marco. *Digital evidence e procedimento penale*. Torino: G. Giappichelli Editore, 2017. p. 147.

10. COSTABILE, Gerado. Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008. *Ciberspazio e Diritto*, v. 11, n. 3, 2010. p. 471. "Per questo motivo appare fondamentale valutare il "ruolo" del computer nell'attività illecita, per motivarne l'eventuale sequestro. La Cassazione, ad esempio ha ritenuto legittimo il sequestro, presso lo studio di un avvocato sottoposto ad indagini, di un intero server informatico completamente sigillato, al fine di verificare, con le garanzie del contraddittorio anticipato, la natura effettivamente pertinenziale al reato ipotizzato, di atti e documenti sequestrati, così escludendo indebite conseguenze sulle garanzie del difensore in violazione dell'art. 103 c.p.p. 18. Successivamente, invece, la Corte ha evidenziato 19 come sia inutile, ai fini probatori, il sequestro di materiale informatico 'neutro' rispetto alle indagini (es. stampante, scanner, ecc.); in particolare, nel caso di specie, non veniva indicata alcuna esigenza probatoria che avrebbe potuto rendere legittimo il permanere del vincolo sul medesimo materiale".

11. Sobre o tema MENDES, Carlos Hélder Carvalho Furtado. *Prova penal digital*: direito à não autoincriminação e contraditório na extração de dados armazenados em sistemas informáticos. Tese (Doutorado) – Programa de Pós-graduação em Ciências Criminais, PUCRS, 2023.

não deve se limitar, entretanto, à observação passiva, mas na detecção de arquivos que podem se encontrar ocultos ou deletados.

Não há consenso quanto à amplitude ou limitações do mandado judicial para a procura de *fontes de prova* em dispositivos de armazenamento digital. Kerr[12], por exemplo, aponta ter papel importante a não aplicação de uma restrição *ex ante,* posto que na execução de mandados de computador, muitas informações que não constam no mandado judicial ficam à vista do investigador. Assim, para que não haja uma permissão de mandado judicial genérico na identificação de *fontes de prova digital* armazenadas em dispositivos informáticos, a sugestão do autor é a eliminação, posterior, das informações que foram alcançadas sem vinculação prévia com a autorização judicial. Segundo o autor, as restrições *ex ante* em mandados judiciais,

12. "A valid warrant justifies the seizure and use of responsive files. On the other hand, nonresponsive files are seized at the physical search stage only out of investigative necessity to obtain the responsive files. Although the seizure of nonresponsive files is reasonable when needed to effectuate the search for responsive files, subsequent use of the seized nonresponsive files transforms the nature of the seizure and renders it constitutionally unreasonable. [...]Instead, it takes advantage of the overseizure and subsequent search necessary to carry out the warrant to transform the warrant for specific evidence into the equivalent of a general warrant. In effect, allowing use of nonresponsive data effectively treats that data as if it had been included in the warrant. This eliminates the role of the particularity requirement, making the warrant the equivalent of a general warrant.163 Subsequent use enables every computer warrant that is narrow in theory to become general in fact. Because subsequent use renders the ongoing seizure unreasonable, use of the nonresponsive files generally violates the Fourth Amendment. […] Agents can overseize, but they cannot receive a windfall from the overseizure. Courts should block the windfall by restoring the traditional limits on the seizure power to what was described in the warrant. They can do so by concluding that the overseizure is reasonable only when necessary to obtain the responsive data described in the warrant. Subsequent use of the nonresponsive data for reasons unrelated to carrying out the warrant renders the ongoing seizure of the nonresponsive data constitutionally unreasonable […] The reason goes back to the Fourth Amendment itself. On one hand, if agents can seize all of the suspect's digital property and use all that it contains, regardless of what the warrant says, the impact on the target's possessory interests is severe. The government can use and reveal the target's entire digital life, just as if the government had obtained a general warrant. On the other hand, the government's competing interest in the use of nonresponsive data is the usual interest in crime control. Although this can be a compelling interest in specific situations, in the ordinary case it is outweighed by the interest in avoiding general warrants. The Fourth Amendment itself proves the point. The Fourth Amendment leaves no ambiguity that general warrants are constitutionally unreasonable even if they may be useful to solve crimes". KERR, Orin S. Executing warrants for digital evidence: the case for use restrictions on nonresponsive data. *Texas Tech Law Review*, v. 48:1, 2015. p. 24-29.

mostram-se inócuas diante das buscas levadas a cabo pelas autoridades investigativas, que podem requerer mandados judiciais complementares a partir das informações que são identificadas por inspeção do material coletado sem observância dos limites estabelecidos no mandado judicial originário.

Acredita-se, porém, que a proposta de Kerr não serve para a proteção de direitos fundamentais implicados em investigações cujo objetivo é a recolha de *fontes de prova digital* armazenadas em dispositivos informáticos. Primeiramente, é preciso perceber-se que a proteção de direitos fundamentais que devem ser razoavelmente restringidos é sempre *ex ante* e em decorrência ao cumprimento das autorizações judiciais. Isso implica dizer que somente quando da usurpação da permissão, como desvio causal, por parte das autoridades estatais é que se torna passível de sanção processual que impõe a inadmissibilidade ou o desentranhamento probatório e, portanto, a eliminação do material coletado.

Dizer isso é afirmar que a determinação judicial autorizativa para o emprego da metodologia de pesquisa deve obedecer ao critério de especialidade da prova. É, portanto, afirmar, ainda segundo Kerr[13], que o objetivo da pesquisa ou busca eletrônica é identificar os dados correspondentes ao mandado judicial. É evidente que não se trata da delimitação concreta do que deve ser alcançado, mas as linhas essenciais e individualizadas do que pode ser alcançável como *fonte de prova digital* (dado, arquivo ou programa) e, efetivamente, demonstrar a justificativa razoável para a medida investigativa pretendida.

Nesse sentido, Gloeckner e Eilberg[14] salientam que o detalhamento deve ser característica da representação investigativa para a autoridade judicial, que por sua vez, após examiná-la, deve concretizar sua motivação autorizativa sob pena de, uma vez genérica – para além da inconstitucionalidade –, representar um "atalho" que facilitaria acesso a múltiplas dimensões violadoras dos direitos fundamentais afetados. O detalhamento que compõe a representação investigativa pode ser entendido como um "protocolo de pesquisa"[15], cujo objetivo é o estabelecimento de condições

13. KERR, Orin S. Executing warrants for digital evidence: the case for use restrictions on nonresponsive data. *Texas Tech Law Review*, v. 48:1, 2015. p. 7.

14. GLOECKNER, Ricardo; EILBERG, Daniela Dora. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. *Revista Brasileira de Ciências Criminais*, v. 156/2019, 2019. p. 353-393.

15. KERR, Orin S. Executing warrants for digital evidence: the case for use restrictions on nonresponsive data. *Texas Tech Law Review*, v. 48:1, 2015. p. 8. Como aponta o autor, nos Estados Unidos não está definido se a exigência de protocolo de buscas é determinante para que se adquira um mandado judicial, de mesmo modo, também não se tem consenso acerca das consequências de sua não obediência.

específicas e a demarcação de limites capazes de apontar à autoridade judicial determinados critérios que serão obedecidos[16] e que, assim, se perfaz de condição para a aquisição do mandado judicial de pesquisa e recolha da fonte de prova a partir da cópia forense. Portanto, requisito capaz de alcançar uma proteção substantiva que limita as ingerências de autoridades públicas na privacidade quando da execução das investigações, apontando uma "probabilidade razoável de descobertas de provas relacionadas com um crime"[17].

Para tanto, o que se propõe é uma nova autorização judicial para fins de pesquisa e, consequente, recolha das *fontes de prova digital* a partir da cópia forense. Todavia, dada a efetiva cautelaridade já observada na apreensão do dispositivo informático e o procedimento de cópia e autenticação, não há mais que se falar em frustração processual probatória decorrente de comportamento ativo do sujeito visado.

16. SOUSA MENDES, Paulo de. A privacidade digital posta à prova no processo penal. In: *Quaestio facti. Revista Internacional sobre Razonamiento Probatorio*, n. 2, 2021. p. 236. Como aponta o autor, "o mandado judicial não pode simplesmente autorizar uma pesquisa e apreensão de 'todos os registos' ('all records'), sob pena de ser um mandado genérico inconstitucional (unconstitutional general warrant). Em vez de os inspetores fazerem uma cópia eletrónica de todo o dispositivo de armazenamento, é, pois, admissível que façam uso de técnicas forenses (forensic techniques) que, por exemplo, lhes permitam restringir o universo da pesquisa e apreensão apenas aos ficheiros que contenham determinadas palavras-chave (keywords) relacionadas com os crimes investigados ao abrigo do mandado judicial, mas esta é uma possibilidade que não deverá ser imposta pela autoridade judicial, embora deva constar da promoção que lhe for dirigida".

17. Algo semelhante ao que dispõe a 4ª emenda Norte Americana, que como declara Sousa Mendes, expõe "o direito do povo à inviolabilidade de suas pessoas, casas, papéis e haveres contra busca e apreensão arbitrárias não poderá ser infringido; e nenhum Mandado será expedido a não ser mediante indícios de culpabilidade confirmados por Juramento ou declaração, e particularmente com a descrição do local da busca e a indicação das pessoas ou coisas a serem apreendidas". SOUSA MENDES, Paulo de. A privacidade digital posta à prova no processo penal. In: *Quaestio facti. Revista Internacional sobre Razonamiento Probatorio*, n. 2, 2021. p. 235. Nesse sentido, como também apontado pelo autor, nos Estados Unidos da América, "em 1994, o Departamento de Justiça publicou as Diretrizes Federais para Busca e Apreensão de Computadores (Federal Guidelines for Searching and Seizing Computers). As Diretrizes foram atualizadas através de Suplementos (Supplements), em 1997 e 1999, e foram sujeitas a uma ampla reformulação em forma de Manual de Busca e Apreensão de Computadores e Recolha de Prova Digital em Investigações Criminais (Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations), publicado em 2001 e amplamente revisto em 2009. De acordo com as Diretrizes de 2009, as pesquisas informáticas em disco rígido (hard-drive) ou em outros ambientes informáticos (computer media) carecem de autorização judicial que contemple, entre outros aspetos, o modo específico de realização dessa diligência de obtenção de provas".

Assim, não há razão para se manter a ausência de contraditório exercido pela parte afetada para que seja delimitada a atividade investigativa sob o material coletado. Ademais, deve ser a parte afetada sujeito processual oportunamente intimado para acompanhar a diligência investigativa de cumprimento ao mandado judicial de pesquisa e recolha da fonte de prova digital, exercendo um controle efetivo da observância dos limites impostos pelo mandado judicial. Nesse ponto, fazendo-se constar nos registros, eventuais desvios investigativos.

Mostrando-se necessária ampliação da diligência investigativa cujo pressuposto é a razoabilidade, o investigador especialista e a autoridade policial competente poderão demandar à autoridade judicial novamente para que seja determinada autorização complementar. Diante desse cenário investigativo complementar, também não há que se falar em impossibilidade de contraditório pela parte afetada. Logo, o conhecimento do interesse investigativo e possibilidade de manifestação da parte afetada é, desse modo, requisito a ser considerado para que – pelo contraditório – possibilite ao imputado um protagonismo na formação da decisão judicial que determinará ou negará mandado judicial complementar.

Embora possa parecer uma restrição *ex ante* descabida, não é disso que se trata. O "protocolo de pesquisa" deve ser visto como limite primeiro à restrição gradual de um direito fundamental quando da fase de pesquisa de fontes de prova armazenadas em dispositivos informáticos. A delimitação permite que se coloque objetividade na identificação de fontes de prova relevantes como garantia de eficiência investigativa diante de todas as informações contidas no dispositivo, ao mesmo tempo em que simboliza a restrição de direitos fundamentais de forma razoável, adequada e necessária.

Possibilita-se, assim, a imposição de limites para uma atuação investigativa lícita, em que a pesquisa capaz de identificar as fontes de prova digital visadas, se pauta na descrição do mandado judicial. Tal protocolo se mostra requisito específico necessário, pois possibilita um controle maior da diligência investigativa tanto pela autoridade julgadora que apreciará o "protocolo de pesquisa" como justificativa metodológica investigatória, quanto pela parte afetada que pelo exercício do contraditório pode apontar se a metodologia e abrangência se mostram necessárias, adequadas e proporcionais na representação da autoridade investigativa. A proposição é semelhante ao que Polansky[18], a partir de Berman, aponta.

18. POLANSKY, Jonathan A. *Garantías constitucionales del procedimiento penal en el entorno digital*. Buenos Aires: Hammurabi, 2020. p. 205-207. "Estas restricciones no deberían resultar estáticas, sino que podrían ir ampliando en la medida en que avance la ejecución del análisis de la información digital, y tal ampliación se encontrara justificada. […] en una primera etapa se deberían extraer únicamente los archivos encontrados mediante la

Chama-se atenção, entretanto, para o exercício do contraditório pela parte afetada na possibilidade de influência na formação cognitiva do julgador que apreciará a representação investigativa que objetiva mandado judicial de pesquisa e recolha da *fonte de prova digital,* cuja participação também é fundamental na fiscalização da observância de limites investigativos no cumprimento dos mandados judiciais, apontando sempre que ocorrer eventual abuso. Assim, documentado estará qualquer ato investigativo de pesquisa que exorbitar a autorização judicial, o que poderá resultar em sanção processual de inadmissibilidade probatória[19]. Ou seja, as restrições *ex ante* no cumprimento de mandados judiciais, notadamente quanto à aplicação dos "protocolos de pesquisa" funcionam como ferramentas de minimização da intrusão estatal.

3. *Best Practices* da ciência forense digital e o acertamento técnico informático para aquisição e recolha de fontes de prova digital

A aquisição de provas digitais é o objetivo pretendido em investigações informáticas cujos alvos são sistemas informáticos. Se são os dados, as informações e programas informáticos ou sistemas informáticos ou telemáticos os objetos visados pela investigação tecnológica preliminar e, notadamente, a partir deles se buscam realizar pretensões probatórias, deve-se adotar medidas técnicas capazes de assegurar a sua conservação e impedir, assim, sua alteração mediante procedimento que assegure sua originalidade e inalterabilidade.

Nesse sentido, é a Ciência Forense Digital[20] que orienta a investigação preliminar e serve de base para as discussões probatórias[21] que se inserem nos processos

aplicación de los filtros dispuestos, y, en una segunda, se podrían analizar cada uno de ellos. De esta forma, quienes ejecuten la medida no tendrían acceso a toda la información secuestrada, sino solamente a aquella que surgiera de la aplicación de los filtros, los cuales se podrían ir ampliando con las correspondientes autorizaciones judiciales".

19. Embora ciente das repercussões quanto aos "conhecimentos fortuitos de prova", não será abordado neste trabalho as discussões relacionadas à temática.

20. Assim como Ramalho, opta-se por discorrer quanto à Ciência Forense Digital "como categoria genérica que abrange, em sentido amplo, as atividades de identificação, recolha e análise de prova digital e que inclui, entre outros ramos, a Ciência Forense Computacional". RAMALHO, David Silva. *Métodos ocultos de investigação criminal em ambiente digital.* Almedina: Coimbra, 2017. p. 111.

21. Diversas são as abordagens técnicas para a análise de sistemas informáticos, por tal razão é que a Ciência Forense Digital deve guiar as investigações e a constituição probatória. Como apontado por Costabile, as técnicas podem variar desde o estado de funcionamento dos

judiciais[22]. Conforme Walker, esta se compõe pela "aplicabilidade de técnicas de investigação e análise computacional com o objetivo de determinar ou identificar possíveis fontes de prova penal"[23].

Logo, nesse cenário o aspecto mais importante da fonte de prova penal digital é a confiabilidade das informações que possuem, destacando-se dois propósitos essenciais: a i) integralidade probatória, que consiste em garantia de manter a inalterabilidade dos dados armazenados e a conservação dos suportes físicos de armazenamento; e a ii) continuidade probatória, como característica de possibilidade de acompanhamento do procedimento de coleta e análise em cada uma das etapas, por meio de relatórios detalhados[24].

---

sistemas em análise. Destaca o autor, por exemplo, que a "Análise post-mortem: refere-se a uma análise realizada com a máquina desligada, realizada após a prática de uma infração. Esse tipo de atividade é mais frequente em ações de polícia judiciária, quando, por exemplo, um disco rígido ou outra memória é apreendido para ser analisado posteriormente em laboratório (ou em um consultor técnico)". Por outro lado, a "Análise Forense ao Vivo: inclui técnicas de análise em sistemas ativos, desenvolvidas nos últimos anos; no caso, por exemplo, de um crime flagrante por acesso não autorizado a sistemas informáticos, muitas vezes não há muitos vestígios no disco rígido, mas a informação pode ser alocada na memória RAM (a temporária). Tais dados seriam perdidos ao desligar o aparelho com os métodos conhecidos no setor; além disso, muitas vezes os dispositivos de memória são protegidos por mecanismos de criptografia, e as chaves também estão contidas na memória temporária" COSTABILE, Gerado. Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008. *Ciberspazio e Diritto,* vol. 11, n. 3, 2010. p. 495-497. "Al di là delle classificazioni, che potrebbero differenziarsi o arricchirsi per tipologia e per tecnica, è necessario in ogni caso considerare ortogonali le due classificazioni proposte, in quanto ad ogni specifico campo di applicazione della computer forensics si associa una scelta preferenziale sullo stato di funzionamento del sistema (in determinati casi la scelta è obbligata, ad esempio Live Forensics per il recupero dei dati in RAM)".

22. Como aponta Lupária, a computação forense é "la disciplina che si occupa della preservazione, dell'identificazione, dello studio, delle informazioni contenute nei computer, o nei sistemi informativi in generale, al fine di evidenziare l'esistenza di prove utili allo svolgimento dell'attività investigativa". Portanto, uma nova especialização da atividade de polícia científica. LUPÁRIA, Lucas; ZICCARDI, Giovanni. *Investigazione penale e tecnologia informatica*: l'accertamento del reato tra progresso scientifico e garanzie fondamentali. Milano: Giuffrè Editore, 2007. p. 46-47.
23. WALKER, Cornell. *Computer forensics*: bringing the evidence to court. Acesso em: 06.2018. Disponível em: [www.infosecwriters.com/text_resources/pdf/Computer_Forensics_to_Court.pdf]. p. 1.
24. LUPÁRIA, Lucas; ZICCARDI, Giovanni. *Investigazione penale e tecnologia informatica*: l'accertamento del reato tra progresso scientifico e garanzie fondamentali. Milano: Giuffrè Editore, 2007. p. 65.

De modo geral, o procedimento de investigação desenvolvido pela Digital Forense é composto, não exclusivamente, por etapas sequenciais ou concomitantes. Afirmam Marcella e Guillossou que o contato inicial, como primeira etapa, decorre do requerimento, em que se estabelece uma base e uma justificativa para o procedimento especializado. A autorização judicial, portanto, em casos criminais, deve demarcar o escopo do trabalho investigativo, fixando a atuação especializada e demarcando seus limites, apontando "parâmetros específicos da investigação, a amplitude e profundidade das áreas investigativas pretendidas, critérios de pesquisa, legislação aplicável e etc."[25]

A segunda etapa é definida pelo tratamento das fontes de prova digital, cujo objetivo é a preservação da integridade do dado que poderá ser utilizada em um processo judicial. O registro, desde as condições do objeto de análise até a metodologia adotada permite a avaliação, posterior, da lisura do procedimento adotado. Destacam os autores que um princípio geral é a cautela excessiva no registro procedimental, passando inclusive pelo apontamento de quais equipamentos são utilizados, mídias de conexão, *hardwares* e *softwares*[26]. É o registro adequado e pormenorizado que atribui confiabilidade à cadeia de custódia[27].

25. MARCELLA, Albert J.; GUILLOSSOU, Frederic. *Cyber forensics: from data to digital evidence.* New Jersey: Wiley, 2012. p. 214. "At a minimum the search criteria may include several components: 1) Keywords associated with the case being investigated (personnel names, company project code names, competitor names, phrases, etc.); 2) Dates or date ranges during which the act under investigation is reported to have taken place; 3) Filetypes (.docx, .doc, .xls, .pdf, .nef, .tif, .png, .jpg, .wav, .mp4, etc.) associated with the case being investigated".

26. "Any equipment the cyber forensic investigator uses to conduct an investigation on the evidence needs to be documented; this includes hardware, software, and connecting media. This equipment should be properly maintained and in working order. Names, versions, upgrades, models, and any other relevant information pertaining to the equipment used (hardware and software) can be considered important and therefore documented per case. As months and perhaps years pass after an investigation, it may not be easy to recall which version of software was used for an investigation". MARCELLA, Albert J.; GUILLOSSOU, Frederic. *Cyber forensics*: from data to digital evidence. New Jersey: Wiley, 2012. p. 218.

27. Reforçam os autores que "o principal objetivo do tratamento das fontes de prova digital é garantir que os dados não sejam alterados, manipulados ou alterados de qualquer forma em relação à sua forma originalmente adquirida, preservando e rastreando as fontes de prova". Logo, "a cadeia de custódia precisa ocorrer antes, durante e após a transferência de qualquer fonte de prova. O início de um processo de cadeia de custódia não deve ocorrer após a fonte de prova ter sido examinada, pois ser capaz de provar quem teve acesso ao objeto examinado, permitirá a responsabilização sobre a integridade da fonte de prova. Essa responsabilidade é um passo essencial na preservação do objeto de análise". MARCELLA,

Definido o objeto alvo da investigação, passa-se para a implementação dos procedimentos comprovadamente eficientes seja para análise de sistemas, seja para análise de arquivos[28]. Como dito, a apreensão do dispositivo informático físico é por vezes momento inicial para a investigação, uma vez que se trata do suporte detentor da informação pretendida. A transportação do material que será submetido ao procedimento para ambiente controlado de laboratório é aspecto primordial para que se possa prevenir riscos de contágio e corrompimento de informações digitais[29].

Uma terceira etapa é a aquisição da fonte de prova digital, cujo objetivo é obter uma imagem forense e preservar a integridade e originalidade da fonte de prova alcançada. Como esclarece Gammarota[30], o procedimento de aquisição e cópia

---

Albert J.; GUILLOSSOU, Frederic. *Cyber forensics*: from data to digital evidence. New Jersey: Wiley, 2012. p. 219.

28. MARCELLA, Albert J.; GUILLOSSOU, Frederic. *Cyber forensics*: from data to digital evidence. New Jersey: Wiley, 2012. p. 209. "Any one of the steps done incorrectly, carelessly, or skipped could thwart and invalidate the entire investigation, regardless of the eventual investigative findings".

29. LUPÁRIA, Lucas; ZICCARDI, Giovanni. *Investigazione penale e tecnologia informatica*: l'accertamento del reato tra progresso scientifico e garanzie fondamentali. Milano: Giuffrè Editore, 2007. p. 63-64. "Il manuale del dipartimento di Giustizia degli stati uniti d'America contenente le line guida in tema di search and seizure prevede, nel chapter 2, che le circostanze possano spesso richiedere che gli investigatori sequestrino i computer e analizzino il contenuto off site, ovvero lontano dal luogo. Successivamente nel laboratorio di forensics viene realizzata una bistream o mirror image del disco fisso, un esatto duplicato non solo dei file ma di ogni bit del disco fisso".

30. GAMMAROTA, Antonio. Informatica forense e processo penale: la prova digitale tra innovazione normativa e incertezze giurisprudenziali. *Dottorato di Ricerca in Diritto e nuove tecnologie*, Università di Bologna, 2016. p. 98-100. "La cancellazione dei dati da una memoria mediante le procedure standard fornite dai sistemi operativi, salvo che non sia effettuata con particolari tecniche di c.d. wiping che vadano a sovrascrivere i dati, riguarda solo l'indice che consente di ricostruire i documenti cosicché l'utente non riesce più ad accedervi. Tuttavia, i dati c.d. cancellati, fino a quando non vengono sovrascritti, sono ancora archiviati sulla memoria e quindi potenzialmente recuperabili e analizzabili. Stesso discorso va fatto per i dati registrati nei c.d. slack space. Per comprendere il fenomeno bisogna partire dall'organizzazione della memoria la quale è strutturata in blocchi (settori) di dimensione fissa. Su tali blocchi vengono archiviati i bit, a prescindere dalle dimensioni del file. Allorquando i file sono di dimensioni inferiori a quella dei blocchi, rimarrà un'area di memoria inutilizzata, più o meno vasta. Ma se in tale area erano stati già archiviati dati dei file successivamente cancellati, nell'area all'interno dei blocchi rimasta inutilizzata dall'archiviazione dei file successivi continueranno ad insistere dati dei file precedentemente archiviati e continueranno ad essere ivi archiviati finché lo spazio non verrà sovrascritto a seguito di allocazione di nuovi file o di operazioni di wiping".

de dados constitui um momento fundamental na investigação informática, sendo atualmente reconhecido que o melhor método para aquisição de dados armazenados em memória (estática) é o chamado *bit stream* ou *image bit a bit*. Trata-se de cópia forense completa e integral da memória na qual os *bits* estão armazenados, incluindo os espaços livres, em uma perspectiva que não envolva alteração de dados e metadados. Há casos, como já informado, que dados e metadados não estão visíveis, foram deletados, estão arquivados ou ocultos.

Logo, o procedimento de cópia *bit stream* ou *image bit a bit* define-se como "procedimento de criação de imagem cópia do disco inteiro, exatamente como está, com a mesma organização de arquivos, os pedaços de arquivos, arquivos danificados, fragmentos de arquivos". Tal imagem permite que um técnico de informática recrie ou monte todo o disco usado para armazenamento e tenha um disco idêntico ao original[31].

O procedimento de cópia consiste, portanto, na garantia de inalterabilidade de *bits* da memória original e deve ser integral, representando perfeitamente a sequência de *bits* original. Nesse ponto, ressalta o autor para a importância da utilização de *hardware* e *software* adequados e interpostos para impedir a manipulação da memória que se pretende copiar, impedindo, por consequência, a modificação de dados originais. A verificação da conformidade dar-se-á por meio da função *hash*. Destaca Lupária[32] que um dos princípios fundamentais do procedimento operatório da análise forense é que todo o trabalho do especialista seja feito sob a cópia alcançada, pois assim evitar-se-á que a originalidade seja perdida, danificada ou alterada.

Como quarta etapa, apontam Marcella e Guillossou[33] a preparação dos dados, propriamente dita, cujo objetivo é preparar e identificar dados para a análise e investigação forense. Segundo os autores, tal etapa se subdivide em "pré-processamento" e "pesquisa". É no "pré-processamento" que se possibilita, pela montagem de sistemas de arquivo, a visualização e organização dos dados, a recuperação de arquivos deletados. Também é nele que se possibilita verificar o tipo de arquivo (.pdf, .docx,

31. LUPÁRIA, Lucas; ZICCARDI, Giovanni. *Investigazione penale e tecnologia informatica*: l'accertamento del reato tra progresso scientifico e garanzie fondamentali. Giuffrè Editore: Milano, 2007. p. 63-64.

32. LUPÁRIA, Lucas; ZICCARDI, Giovanni. *Investigazione penale e tecnologia informatica*: l'accertamento del reato tra progresso scientifico e garanzie fondamentali. Milano: Giuffrè Editore, 2007. p. 63-64.

33. MARCELLA, Albert J.; GUILLOSSOU, Frederic. *Cyber forensics*: from data to digital evidence. New Jersey: Wiley, 2012. p. 229.

por exemplo), bem como se existem arquivos ocultos na memória do dispositivo visado. A indexação, a partir do "pré-processamento", permite uma pesquisa rápida pelo arquivo desejado. Já a sub-etapa da "pesquisa" possibilita essencialmente uma refinação da fonte de prova digital em conjuntos menores de dados passíveis de investigação, geralmente se utilizando de "filtros" de pesquisas mais avançados para que se alcance com maior precisão a informação desejada.

Como já salientado, a metodologia deve ser documentada de maneira integral para que possa ser verificável pelas partes processuais em análise adequada. Dessa forma, garante-se o exercício do Direito de Defesa, notadamente quanto ao seu exercício do contraditório. A documentação de toda a etapa de cópia, possibilita a exposição de erros procedimentais. A cópia integral e em conformidade com a técnica reflete fator fundamental, posto que como se afirma, uma vez que sua execução não obedeceu aos parâmetros próprios da *computação forense*, tornar-se-á inviável o critério de confiabilidade do método, resultando assim na inutilização do material em contexto probatório.

Por fim, como quinta etapa, os autores[34] apontam a "investigação" dos dados objetos do mandado de busca, que se preocupa em encontrar e recolher aquilo que foi requerido. Trata-se de etapa cujo risco da subjetividade aumenta. Conforme expõem Lupária e Ziccardi, embora se imagine que todo o procedimento de análise deve ser exposto por meio de relatório especializado, que possui dois componentes distintos, um técnico e um investigativo[35], em uma análise mais atenta à técnica informático-científica, importa salientar que o investigador especialista ou perito informático possui o dever de apresentar sua análise técnica de maneira objetiva, na observância de procedimentos metodológicos que impedem uma análise subjetiva.

Assim, a abordagem firma-se na análise da avaliação da preservação das fontes de prova objeto de investigação e materiais adquiridos por meio de técnicas corretas e ferramentas adequadas. Conforme Casey, assim o especialista possui papel

34. MARCELLA, Albert J.; GUILLOSSOU, Frederic. *Cyber forensics*: from data to digital evidence. New Jersey: Wiley, 2012. p. 235.

35. LUPÁRIA, Lucas; ZICCARDI, Giovanni. *Investigazione penale e tecnologia informatica*: l'accertamento del reato tra progresso scientifico e garanzie fondamentali. Milano: Giuffrè Editore, 2007. p. 67. O componente técnico é o exame propriamente dito da memória de massa, a determinação e a extração dos dados em agrupamentos, recuperação de arquivos excluídos, quebra de senhas, determinação de senhas de arquivos ou pastas, ataques de força bruta, ataques direcionados ou descriptografia. Já o componente investigativo consistiria na disposição de exposições que caracterizam a conduta delitiva investigada, desde o fornecimento de diagramas de análise, como na comparação de elementos resultantes das operações e diligências policiais.

fundamental na produção da prova penal digital em momento processual oportuno, posto que para além de técnico na recolha do material pretendido é também, testemunha especializada. Portanto, a aplicação de altos níveis de objetividade em todas as etapas procedimentais é o que garante a eficácia do processo investigativo e, notadamente, probatório[36-37].

Como apontado por Iovene[38], são três as soluções possíveis para as hipóteses em que não houve a observância das indicações procedimentais adequadas às melhores práticas forenses. A primeira teria como resultado a decretação da nulidade do ato de aquisição ou recolha pelas violações às garantias de defesa no tocante à ausência de confiabilidade, posto que as medidas técnicas destinadas a assegurar a conservação dos dados originais e evitar sua alteração integraria um requisito especial – com finalidade de garantia – que deve ser respeitado na realização de

36. É evidente que não se desconhece que como pessoas, os especialistas, também possuem reações emocionais, abrigam preconceitos, e estão sujeitos a diversos fatores de influência, todavia, o procedimento metodológico seguido deve se preocupar em blindar eventuais influências na análise especializada. Casey aponta que há um conjunto de regras no Procedimento Criminal do Reino Unido que se lançam com a intenção de evitar que os investigadores especializados ou peritos informáticos possam incorrer em análises subjetivas. Dirá o autor que i) o perito deve auxiliar o Tribunal a atingir o objetivo primordial, dando opinião objetiva e imparcial sobre assuntos de sua competência, ii) este dever deve prevalecer sobre qualquer obrigação para com a pessoa de quem recebe instruções ou por quem é remunerado e, dessa forma, iii) o perito possui obrigação de informar todas as partes e o tribunal se sua análise mudar do que consta no relatório servido como fonte de prova ou dado como uma declaração. Dirá o autor que jamais um especialista deve imputar definitivamente uma conduta tida como criminosa a um suspeito, esse não é o papel do especialista. A competência do perito não se confunde com a competência do Tribunal. CASEY, Eoghan. *Digital Evidence and Computer Crime*: Third Edition. San Diego: Elsevier, 2011. p. 51.

37. No mesmo sentido, apontam Lupária e Ziccardi, em referência à Ghirardini, que a computação forense é a disciplina que lida com a preservação, identificação, estudo, documentação de computadores ou sistemas de informação em geral, com o objetivo de identificar fontes de prova para fins investigativos. Por vezes, a disciplina é erroneamente confundida como um novo "ramo" da segurança informática o que termina por resumir sua funcionalidade. Trata-se, em verdade, de um setor que exige conhecimentos informáticos muito elevados e que refina competências de análise, observação e paciência. LUPÁRIA, Lucas; ZICCARDI, Giovanni. *Investigazione penale e tecnologia informatica*: l'accertamento del reato tra progresso scientifico e garanzie fondamentali. Giuffrè Milano: Editore, 2007. p. 68.

38. IOVENE, Federica. *Prova informatica e diritti fondamentali della persona nel processo penale*. Tesi di Dottorato, Università degli Studi di Trento. 2014. p. 68.

uma identificação de fontes de provas digitais em sistemas informáticos ou telemáticos[39]. A segunda, conforme aponta a doutrina italiana, decorreria da adoção do critério de inutilidade probatória, na constatação de que uma vez não observada as técnicas forenses, resultar-se-ia na inidoneidade probatória do resultado e de qualquer outro meio destinado à análise do resultado, razão pela qual o julgador deveria excluí-la na fase de admissibilidade[40].

Por fim, aponta a autora que há entendimentos que se firmam sob a perspectiva da valoração probatória, em que se reconhece uma impossibilidade de nulidade probatória ou inutilidade da prova. Nesse sentido, caberia ao julgador, com o auxílio da perícia e assistentes técnicos da defesa, valorar se a investigação foi conduzida corretamente e se a cadeia de custódia foi respeitada[41], bem como utilizando da busca de elementos externos que combinem com o material informático probatório "deficitário"[42].

No Direito Processual Penal Brasileiro, a impossibilidade de reconhecer-se como confiável uma fonte de prova, pela patologia procedimental de sua aquisição ou pela violação de qualquer direito fundamental ou garantia processual, deve incorrer na aplicabilidade do Artigo 157 do Código de Processo Penal[43]. Assim, a

39. No mesmo sentido, PITTIRUTI, Marco. *Digital evidence e procedimento penale.* Torino: G. Giappichelli Editore, 2017. p. 156-157.

40. A inutilidade probatória é procedimento próprio da legislação processual penal italiana. No Direito Processual Penal Brasileiro não há procedimento semelhante, resultando apenas na declaração da ilicitude probatória cuja consequência é, ou a sua inadmissibilidade ou o seu desentranhamento dos autos processuais conforme preconiza o artigo 157 do Código de Processo Penal.

41. IOVENE, Federica. *Prova informatica e diritti fondamentali della persona nel processo penale.* Tesi di Dottorato, Università degli Studi di Trento. 2014. p. 68-69. "Infine, alcuni Interpreti ritengono che la questione si risolva sotto il profilo della valutazione della prova (art. 192 c.p.p.)257. Non sarebbe, infatti, possibile ravvisare né un caso di nullità né un'ipotesi di inutilizzabilità in quanto ciò equivarrebbe a ricavare divieti probatori dalla sola lesione dell'interesse tutelato dalla legge, ma privi in realtà di un'espressa copertura normativa258. Spetterebbe quindi al giudice, avvalendosi dell'apporto dei periti e dei consulenti tecnici della difesa, valutare se le indagini siano state condotte in maniera corretta e se sia stata rispettata la chain of custody".

42. PITTIRUTI, Marco. *Digital evidence e procedimento penale.* Torino: G. Giappichelli Editore, 2017. p. 157.

43. Como apontado por Albert J. Marcella e Frederic Guillossou: "In some cases, not following your own written procedures may be comparable to not following the law". MARCELLA,

constatação da patologia procedimental implica na determinação da inadmissibilidade probatória.

Ademais, todo o procedimento investigativo que se baseia na orientação científica da Ciência Forense Digital é, efetivamente, um *método de apuração fática* que – embora auxiliar ao Direito Processual Penal, notadamente ao *método de produção probatória* – independe de juízo de valor quanto à sua utilidade processual. É dizer, em que pese possa existir opiniões que discordem do *método científico*, trata-se de elemento imprescindível para determinar a confiabilidade probatória[44]. Não por acaso, o artigo 158 do Código de Processo Penal, destaca a indispensabilidade de toda a documentação e registro do procedimento adotado para fins de confiabilidade processual.

Na jurisprudência do Superior Tribunal de Justiça[45] é possível encontrar entendimento de modo diverso, no sentido de que uma vez inexistente a previsão legal que impõe observância estrita a determinado procedimento, não há que se falar em ilicitude probatória. Porém, tal entendimento afasta a análise da própria fragilidade e volatilidade como características da *fonte de prova digital* que se pretende alcançar. Não é inapropriado dizer que é a Ciência Forense Digital que determina as diretrizes procedimentais do método, cabendo o Direito Processual Penal adequar sua metodologia de produção probatória ao método científico indicado. Nesse sentido, importa salientar que

> "qualquer entrada num sistema informático, ainda que efetuada com os métodos mais avançados, pode alterar os dados nele contidos, gerando mutações que, ainda que mínimas, correm o risco de ser decisivas se se tratar de circunstâncias factuais relevantes para a afirmação da responsabilidade do acusado."[46]

Albert J.; GUILLOSSOU, Frederic. *Cyber forensics*: from data to digital evidence. New Jersey: Wiley, 2012. p. 210.

44. BRASIL. *Superior Tribunal de Justiça – STJ,* Habeas Corpus – HC 160.662/RJ, 6ª T., j. 18.02.2014.

45. BRASIL. *Superior Tribunal de Justiça – STJ*, REsp 1.435.421/RS, 6ª T., rel. Maria Thereza de Assis Moura. "Ementa: Recursos especiais. Penal e processo penal. Evasão de divisas. Dosimetria. Pena-base. Elevado montante evadido. Circunstância judicial negativa. Lei 12.850/13. Norma supervenieentee. Ausência de prequestionamento. Disco rígido. Acesso direto. Ilicitude. Inexistência. [...] 3. O espelhamento das mídias de informática são providências de perpetuação da prova destinadas a atestar, com a maior confiabilidade possível, a idoneidade da prova, mas não há determinação legal de que não sejam acessadas diretamente. [...]."

46. DANIELE, Marcelo. La prova digitale nel processo penale. *Rivista di Diritto Processuale Anno LXVI,* (Seconda Serie), n. 2, Marzo-Aprile, 2011. p. 295.

Ou seja, como aponta Daniele[47], os procedimentos de cópia de fontes de provas digitais, mesmo quando não digam respeito a dados em via de alteração – condição que, por si só, permitiria a realização do procedimento de avaliações técnicas não repetíveis – podem resultar tais mutações irreversíveis do objeto.

Há, portanto, duas situações importantes que afetam a análise do tema. De um lado, na hipótese em que a investigação se utiliza de método distinto do sugerido pela Ciência Digital Forense, caberá a defesa pelo exercício do contraditório em momento prévio à decisão de admissibilidade da fonte de prova digital apontar – em abstrato – que o *método de apuração fática* adequado e confiável é outro. Diz-se, em abstrato, pois não deve se impor a carga probatória à defesa na indicação concreta de alteração de dados. De outro, o apontamento da inadequação do método utilizado torna presumível a alteração da *fonte de prova digital*. Logo, não há que se falar em demonstração de prejuízo pela defesa, uma vez que a comprovação da alteração do dado impõe uma inversão da carga probatória incompatível aos ditames processuais. Assim, impõe-se à parte acusatória o dever da comprovação da fiabilidade da prova penal.

Essa orientação, como salienta Pittiruti, parte da consciência de que o dado informático possui características próprias e peculiares de fragilidade e volatilidade. De tal modo, de forma presumida, afirma-se que "o uso de métodos de aquisição incorretos altera a própria natureza da *fonte de prova digital*, que perde irremediavelmente, a capacidade de provar"[48]. A orientação reforça, portanto, a ideia de uma necessária proteção ainda mais avançada para a autenticidade da informação comprobatória que ingressará ao processo judicial, resguardando a confiabilidade da informação para sua utilização tanto em relação ao acertamento fático, como em relação à valoração judicial. Logo, a indicação do método apropriado pela Ciência

47. DANIELE, Marcelo. *La prova digitale nel processo penale. Rivista di Diritto Processuale,* Anno LXVI, (Seconda Serie), n. 2, Marzo-Aprile, 2011. p. 295.

48. PITTIRUTI, Marco. *Digital evidence e procedimento penale.* Torino: Giappichelli Editore, 2017. p. 158. "Detto altrimenti, occorre evidenciare che, con riferimento alla digital evidence, eventuali violazioni nelle modalità di ricerca, apprensione e formazione della prova incidono inevitabilmente sull'essenza del dato informatico, poiché il contenuto viene modificato. Tali violazioni, dunque, si riverberano sul risultato probatorio. Insomma, con riguardo alla prova digitale, i vizi dell'attività di raccolta della prova diventano vizi dell'atto probatorio in sé. Alla luce di quest'ultima precisazione, i canoni di genuinità e non alterazione della prova legislativamente imposti dall L. n. 48/2008 assumono la giusta valenza: non già mere indicazioni operative prive di alcuna sanzione, ma veri e propri divieti impliciti presidiati dalla sanzione dell'inutilizzabilità".

Forense Digital é, para além de uma definição de proibição probatória, uma preocupação com o resultado genuíno e imutável[49].

4. A rastreabilidade da fonte de prova penal digital: *discovery* e *softwares*

Falar em rastreabilidade da fonte de prova digital é em um primeiro momento relacionar a aquisição da fonte de prova ao pressuposto da atribuição de carga probatória à acusação no processo penal. A presunção de inocência, como dito, possui faceta de regra probatória e isso é determinante no processo penal, na medida em que atribui à acusação a carga probatória de sua hipótese criminal desconstituindo os argumentos defensivos. Nesse sentido, rastreabilidade da fonte de prova é vinculada à carga probatória, pois impõe também o dever à acusação na demonstração do método de aquisição, uma documentação necessária que comprove sua atuação lícita que decorre da probidade processual e investigativa. O que, verdadeiramente, atrela-se ao próprio devido processo legal e à ampla defesa no tocante à sua preparação e ao seu exercício.

Assim, aponta Prado[50] que há dispositivos próprios para o controle da legalidade das atividades de investigação que não podem ser ignorados em um processo acusatório, sendo certo que o Direito Processual Penal Brasileiro reconhece a relevância do controle judicial acerca da legalidade da persecução penal. Nesse sentido, importa salientar que a rastreabilidade da fonte de prova é, sensivelmente, um dispositivo próprio vinculado ao direito de conhecimento quanto as descobertas (*discovery*) ou à obtenção de acesso a elementos de prova coletados por agentes e órgãos públicos.

A descoberta aqui apontada não se limita às fontes de prova alcançadas, mas ao conhecimento de todo o procedimento que possibilitou o alcance. É dizer, a fonte de prova alcançada surge nos autos processuais a partir de algo, logo a partir da aquisição da fonte de prova deve-se possibilitar, como uma retroanálise, o conhecimento

49. PITTIRUTI, Marco. *Digital evidence e procedimento penale.* Torino: G. Giappichelli Editore, 2017. p. 160. "Proprio l'obbligo di adottare determinate accortezze a tutela della genuinità ed immodificabilità della prova rappresenta, dunque, un vero e proprio divieto probatorio, sia que pure espresso in forma implicita, a protezione dell'affidabilità dell'accertamento. Ben lungi dal rappresentare mere indicazioni di metodo agli operanti, tali disposizioni sono caratterizzate da una finalità ben più rilevante, vale a dire evitare risultati probatori inquinati.(Grifo nosso)

50. PRADO, Geraldo. *A cadeia de custódia da prova no processo penal.* São Paulo: Marcial Pons, 2019. p. 76-77.

acerca do percurso investigativo que possibilitara a identificação da fonte de prova e, portanto, da informação de valor probatório que carrega.

Trata-se, pois, de uma concepção que aponta um dever às autoridades investigativas em documentar toda a sua atividade procedimental – incluindo a coleta de informações de valor probatório, perfazendo-se como uma matéria não apenas ética acusatória[51], mas como uma "obrigação processual"[52], ou seja, como cumprimento normativo que garanta a observância dirigida à paridade de armas cuja premissa fundamental é o alcance de um julgamento justo.

Pontua Prado[53], a partir de menções ao Direito Norte-Americano, que não há mais espaço – em um procedimento que se pretende com protagonismo às partes – manobras que busquem o fator "surpresa" para que se garanta uma vantagem estratégica na fase judicial. Por tais razões, no ordenamento jurídico Brasileiro, por exemplo, toda informação já documentada em sede de investigação preliminar deve ser fornecida à parte afetada pela investigação, ressalvadas as diligências em andamento[54].

51. Sobre ética acusatória LANGER, Máximo; ROACH, Kent. Direitos no processo penal: um estudo de caso sobre convergência e direitos de disclosure = *Rights in Criminal Procedure: a case study about convergence and rights to disclosure.* In: *Revista Brasileira de Ciências Criminais: RBCCrim*, São Paulo, v. 23, n. 116, p. 239-257, set.-out. 2015. p. 245.

52. PRADO, Geraldo. *A cadeia de custódia da prova no processo penal.* São Paulo: Marcial Pons, 2019. p. 76-77.

53. PRADO, Geraldo. *A cadeia de custódia da prova no processo penal.* São Paulo: Marcial Pons, 2019. p. 78.

54. BRASIL, Supremo Tribunal Federal – STF, Sumula 14: "É direito do defensor, no interesse do representado, ter acesso amplo aos elementos de prova que, já documentados em procedimento investigatório realizado por órgão com competência de polícia judiciária, digam respeito ao exercício do direito de defesa". Nesse sentido, destaca-se o precedente representativo: "Há, é verdade, diligências que devem ser sigilosas, sob risco de comprometimento do seu bom sucesso. Mas, se o sigilo é aí necessário à apuração e à atividade instrutória, a formalização documental de seu resultado já não pode ser subtraída ao indiciado nem ao defensor, porque, é óbvio, cessou a causa mesma do sigilo. (...) Os atos de instrução, enquanto documentação dos elementos retóricos colhidos na investigação, esses devem estar acessíveis ao indiciado e ao defensor, à luz da Constituição da República, que garante à classe dos acusados, na qual não deixam de situar-se o indiciado e o investigado mesmo, o direito de defesa. O sigilo aqui, atingindo a defesa, frustra-lhe, por conseguinte, o exercício. (...) 5. Por outro lado, o instrumento disponível para assegurar a intimidade dos investigados (...) não figura título jurídico para limitar a defesa nem a publicidade, enquanto direitos do acusado. E invocar a intimidade dos demais investigados, para impedir o acesso aos autos, importa restrição ao direito de cada um dos envolvidos, pela razão manifesta de que os impede a todos de conhecer o que, documentalmente, lhes seja contrário. Por

Apesar disso, é preciso salientar que o direito à descoberta das fontes de prova deve ter vinculação quanto à origem daquilo que se documenta, sob pena de não ser possível uma plena consciência – por parte do sujeito afetado – do caminho percorrido pela investigação no alcance das informações que servem de base para sustentação da hipótese acusatória (ex. "informação decorrente de serviços de inteligência"). Ou seja, a informação alcançada deve ter procedência certa, para que se mostre confiável à tomada de decisão. Ainda que os autos de investigação não sejam compartilhados ou incluídos nos autos processuais que serão encaminhados ao juízo sentenciante, há que se ter procedência certa e – portanto – lícita das informações decorrentes de provas cautelares, antecipadas e irrepetíveis que se comunicará da investigação aos autos processuais[55].

A *Discovery,* portanto, é mecanismo capaz de tornar possível o direito à prova pela defesa[56]. No tocante às fontes de prova penal digital, o direito ao conhecimento acerca da "descoberta" e, por decorrência, à rastreabilidade da fonte de prova, está diretamente vinculado não apenas quanto à utilização das novas tecnologias de investigação informática, mas prioritariamente quanto à utilização de tecnologias de aquisição ou cópia forense das *fontes de prova digital* que serão inseridas nos autos processuais.

Como já exposto, a aquisição das fontes de prova digital armazenadas em dispositivos informáticos é somente possível a partir da execução de *softwares* que permitem a exata criação de cópia forense e posterior inspeção e aquisição das *fontes de prova digital* com relevante valor probatório. Portanto, entendido esse procedimento preliminar, importa salientar que a cópia forense é sempre uma *fonte de prova*

isso, a autoridade que investiga deve, mediante expedientes adequados, aparelhar-se para permitir que a defesa de cada paciente tenha acesso, pelo menos, ao que diga respeito a seu constituinte" HC 88.190, voto do rel. min. Cezar Peluso, 2ª T, j. 29.08.2006, *DJ* 06.10.2006.

55. PRADO, Geraldo. *A cadeia de custódia da prova no processo penal*. São Paulo: Marcial Pons, 2019. p. 78-79. "o funcionamento eficaz das *Discovery devices* depende, porém, da estruturação do procedimento penal que tenha aptidão para viabilizar o controle pelas partes da atividade probatória do adversário – e sua consequente licitude – e também da prescrição ao juiz criminal de papel destacado de fiscalização da regularidade procedimental, em um contexto em que a atividade jurisdicional penal concebida como de tutela da Constituição e das leis. [...] No caso do processo penal a nova arquitetura acusatória aos poucos aproxima os concretos sistemas de justiça criminal e redesenha a face destes sistemas, assemelhando-os em termos de estrutura básicas, 'estrutura' aqui concebida como 'conexão entre elementos, etapas ou fases'".

56. PRADO, Geraldo. *A cadeia de custódia da prova no processo penal*. São Paulo: Marcial Pons, 2019. p. 81.

derivada. É dizer, os dados, arquivos e programas, visíveis ou ocultos, armazenados em um dispositivo informático são *fontes de prova originárias* cuja aquisição pela cópia forense é efetivada por *software*. Ou seja, uma programação executada por instruções previamente elaboradas por um programador. Assim, a autenticidade e credibilidade auferida à *fonte de prova derivada* somente pode ser categoricamente confirmada a partir do conhecimento de que as instruções do *software,* que executa a tarefa de cópia ou aquisição, são precisas.

Sobre a matéria, aponta Mason[57] que um dispositivo informático digital não alcança sua funcionalidade sem que o *hardware* possua um *software* instalado. Este segundo, portanto, escrito por programadores e alimentado por usuários. Desse modo, o autor assinala que toda prova digital pode ser tratada como uma declaração conjunta que é "parcialmente feita pela pessoa que insere dados" e "parcialmente feita pelas centenas de programadores responsáveis por escrever o *software* que produz os dados". Por tais razões, aponta o autor que toda forma de prova digital alcançada por *software*, pela imprecisão e inconfiabilidade permanece como *hearsay*, ou aqui adotado como "conjectura" por presunção, uma vez que é o código do *software* que alcança a informação originária e a transmite de modo inteligível.

É dizer, de acordo com Teppler[58], há uma incompreensão daquilo que pode ser entendida como "informação gerada por computador" e o que constitui uma "informação de origem". Salienta o autor que os dados de origem de todas as informações geradas por computador são de natureza binária, e os dados processados, visualizados, impressos ou armazenados são compostos decorrentes de conjuntos ordenados de zeros e uns. Estes últimos, são processados por outros conjuntos ordenados de dados binários que compõem o sistema operacional e outros aplicativos

57. MASON, Stephen. Software code as the witness. In: Stephen Mason and Daniel Seng (eds.). *Electronic Evidence* (4th edn, University of London 2017) 88-100.

58. TEPPLER, Stephen W. Digital data as hearsay. *Digital Evidence and Electronic Signature Law Review 7*, v. 6. 2009. p. 7-9. Disponível em: [https://sas-space.sas.ac.uk/5334/1/1853-2571-1-SM.pdf]. "Os dados (ou informações) realmente lidos ou percebidos por um leitor humano (ou membros de um júri) devem, portanto, ser considerados a última 'visão' em um conjunto de 'visões de visões' e não a 'fonte' ou dados de origem. Em outras palavras, enquanto uma pessoa pode ler, ouvir ou ver dados gerados por computador, é impossível ler, ouvir ou ver os dados de origem ou de origem gerados por computador. Para perceber os dados do computador de origem como dados nativos, é necessário interpretar o idioma em que esses dados são gravados (como 'C' ou 'Visual Basic'). Para interpretar a linguagem em que os dados são escritos, é necessário, por sua vez, entender a linguagem em que eles são escritos. O objetivo final em entender ou examinar informações geradas por computador é entender as afirmações, ou discurso, dos programadores de computador (todos os quais são humanos) que, por código-objeto ou código-fonte, fornecem instruções aos computadores para fazer declarações condicionais". [tradução livre].

de *software* de processamento de dados para produzir o que é comumente chamado de arquivos de dados.

Nesse sentido, os dados de origem são, portanto, sempre compostos por "zeros e uns" e, necessariamente, são processados ou renderizados pelo sistema operacional e vários aplicativos para que se produza os arquivos. Por sua vez, os arquivos são processados por outros aplicativos para produzir imagens que podem ser visualizadas em uma tela, ou podem ser visualizadas por impressões.

Logo, mesmo que a extração dos dados de dispositivo informático for comprovadamente autêntica pelo *software* utilizado para a aquisição, para que seja incluída em um processo judicial deve ser apontada como "fonte de prova" concreta, ou seja, afastado o seu grau de "conjectura" por presunção. Do contrário, o caráter de "conjectura" por presunção é vetor responsável para a decretação da sua inconfiabilidade e, consequentemente, sua exclusão ou inadmissibilidade pela ausência de credibilidade.

Tais informações permitem afirmar que sem a ciência do código-fonte[59] do *software* utilizado para a aquisição, cópia forense, dos dados armazenados em um dispositivo informático não é possível garantir que a informação decorrente possui credibilidade. Como aponta Teppler[60], um computador ou programa de computador somente produzirão informações dentro do alcance das instruções contidas no código-fonte do aplicativo ou programa utilizado. Ou seja, aplicativos e programas de computador produzem informações destinadas a ser criadas pela instrução elaborada pelo programador. Logo, a ciência quanto ao código-fonte à parte imputada necessariamente permite com que se avalie – sob o crivo do contraditório – a identificação de possíveis erros, proposital ou acidentalmente inseridos[61], nas instruções de programação e execução de tarefas.

---

59. Sobre o Código-fonte, aponta Mason, a partir de Svein Willasseen que "o *software* é escrito como código-fonte. O código-fonte é escrito pelo programador, inserindo instruções em um editor. A sequência de instruções define a função do programa, como receber *input* do usuário, realizar cálculos, mostrar *output* na tela e assim por diante. Esse código-fonte é geralmente compilado em um programa executável (um arquivo executável faz com que um computador execute tarefas de acordo com as instruções), que é distribuído aos usuários do programa. O código-fonte não pode ser derivado completamente do programa executável" [tradução livre]. MASON, Stephen. Software code as the witness. In: Stephen Mason and Daniel Seng (eds.). *Electronic Evidence* (4th edn, University of London 2017). p. 89.

60. TEPPLER, Stephen W. Digital data as hearsay. *Digital Evidence and Electronic Signature Law Review 7*, v. 6. 2009. p. 15-16. Disponível em: [https://sas-space.sas.ac.uk/5334/1/1853-2571-1-SM.pdf].

61. "'Human-made faults' are, in turn, divided into malicious faults and 'nonmalicious' or guileless faults. These faults can be introduced during the development of the system by a

Os erros[62] podem estar inseridos em qualquer das etapas do processamento. A partir desse panorama, quando não identificados os erros pela auditoria do código-fonte do *software*, as informações geradas pelo *software* forense serão incorporadas em um processo judicial e posteriormente valoradas inadequadamente em decisão. É dizer, as informações legíveis a partir de *softwares* que possibilitam a extração de dados, ou cópia forense, apresentam-se com maior credibilidade quando se possibilita o afastamento das hipóteses de que são enganosas ou não confiáveis. Máxime, quando se está a falar de *softwares* de decodificação das informações criptografadas ou codificadas.

É a partir, portanto, do código-fonte do *software* que se possibilita apontar que as informações alcançadas são, categoricamente, precisas e não tendenciosas. Como salienta Mason, se o código do *software* for impreciso, ou se uma instrução elaborada pelo programador atuar sobre uma informação ou outra instrução incorreta, então o código provavelmente falhará em instruir o computador da maneira que o

developer or during use by an external third party. Guileless faults can be classified as faults due to mistakes, and deliberate faults that are brought about because of bad decisions – usually caused when choices are made to accept having less of one thing in order to get more of something else, for instance, to preserve acceptable performance, or because of economic considerations. Developers who commit such faults may deliberately violate an operating procedure without understanding the consequences of their action". MASON, Stephen. The presumption that computers are 'realiable'. In: Stephen Mason and Daniel Seng (eds.). *Electronic Evidence* (4th ed, University of London 2017). p. 132.

62. Mason aponta que: "O professor Thomas observa que 'A principal maneira de os desenvolvedores de software garantirem a qualidade de seu trabalho é executando testes, embora os cientistas da computação tenham dito nos últimos quarenta anos que os testes nunca podem mostrar que o software é seguro ou correto'. Mesmo para sistemas relativamente pequenos, o número de possíveis casos de teste necessários para testes abrangentes é enorme. Também nem sempre é certo se o teste foi aprovado ou reprovado, sendo necessário repetir os testes após qualquer alteração de software. Além disso, um único caso de teste só pode expor um sistema a um conjunto muito específico de condições e valores de dados. O número de variações é, em termos práticos, ilimitado porque um teste robusto deve considerar, entre outros, diferentes valores de dados, o número de tarefas simultâneas em execução, a configuração da memória do sistema, a configuração do hardware, todos os dispositivos ou sistemas conectados, a ações dos operadores, erros do usuário, erros de dados, mau funcionamento do dispositivo e assim por diante. No entanto, porque o teste é um assunto complexo, não significa que o teste não deva ser realizado". Neste sentido, aponta ainda que "a fonte primária de erros de software está em seu processo de desenvolvimento". MASON, Stephen. The presumption that computers are 'realiable'. In: Stephen Mason and Daniel Seng (eds.). *Electronic Evidence* (4th edn, University of London 2017). p. 131. [tradução livre].

programador pretendia[63]. O grau de confiabilidade e credibilidade de que a "fonte de prova derivada" necessita para ser admitida em um processo judicial somente poderá ser alcançado a partir da ciência de que o código-fonte do *software* utilizado na etapa de aquisição, cópia forense, não possui erros de instrução.

Dito isso, é preciso se ter consciência de que não há espaços para obviedades, quer-se dizer, "nem sempre será óbvio se a confiabilidade da fonte de prova gerada por computador é imediatamente detectável sem o recurso para estabelecer se o código-fonte do *software* não possui defeitos"[64]. A confiabilidade do código-fonte do *software*, de suas atualizações e revisões, portanto, não é pautada em presunção de funcionalidade regular.

5. Considerações finais

Diante de todo o exposto, constatou-se que o entendimento firmado pelo Superior Tribunal de Justiça no Informativo de Jurisprudência 763 demarca avanço significativo quanto à aquisição e admissibilidade de dados informáticos como prova penal digital. Não sem razão, é a confiabilidade da prova e o registro documental do método de extração que garante maior acertamento decisório ao caso penal. Logo, devem ser consideradas inadmissíveis todas as provas digitais que não são acompanhadas de registro documental quanto aos procedimentos adotados para a preservação de sua integralidade e autenticidade.

Todavia, como resposta à pergunta problema formulada no presente artigo, relacionada aos pressupostos que devem ser observados pela Autoridade Investigativa e Judicial na aquisição e produção da prova penal extraída de dispositivos digitais, merece destaque algumas questões.

Quanto à aquisição do Dado Informático, observou-se que diante do risco de Mandados Judiciais Genéricos, é importante verificar que tal medida deve ocorrer primeiro pela autorização da apreensão de seu suporte, o que não se relaciona com uma autorização judicial para utilização de todos os dados informáticos, nele contidos, como fonte de prova digital.

É dizer, o mandado judicial para apreensão do Suporte Informático possui delimitações próprias. Um segundo Mandado Judicial se faz necessário, estabelecendo

63. MASON, Stephen. Software code as the witness. In: Stephen Mason and Daniel Seng (eds.). *Electronic Evidence* (4th edn, University of London 2017). p. 91.

64. [Tradução livre] MASON, Stephen. The presumption that computers are 'realiable'. In: Stephen Mason and Daniel Seng (eds.). *Electronic Evidence* (4th edn, University of London 2017). p. 182.

delimitações *ex ante* para a proteção de Direitos Fundamentais afetados e à obediência do critério da especialidade da prova. Dessa forma, evita-se buscas genéricas que caracterizam a "pesca probatória".

Assim, como ferramenta para evitar devassas probatórias, sugere-se a implementação do detalhamento na representação investigativa que pretende o alcance de dados informáticos, materializada pelo "protocolo de pesquisa". Essa limitação *ex ante* não impede autorizações complementares, porém, importa salientar que uma vez feita a cópia forense de dados constantes nos Sistemas Informáticos, não há mais que se falar em risco de frustração processual de natureza probatória por parte do sujeito visado. Logo, não há razão para o afastamento da atuação defensiva em contraditório, seja na formação cognitiva do juízo competente para conceder a autorização, seja no acompanhamento das diligências investigativas de alcance dos Dados Informáticos. É o acompanhamento da Defesa nessa fase que demarca a fiscalização dos limites expressos no Mandado Judicial e sua obediência.

De mesmo modo, foi possível perceber que o acertamento técnico da atividade de aquisição e recolha de dados armazenados em Sistemas Informáticos deve observância às Boas Práticas da Ciência Forense Digital. Se a Prova Penal Digital é, notadamente, uma prova científica, há que se ter como pressuposto básico o rigor no cumprimento de técnicas próprias para atestar a confiabilidade e autenticidade da fonte de prova penal digital. Embora tais recomendações possam não constar em Lei Processual Penal, são estas que possibilitam a execução acertada do denominado método de apuração fática, cuja função precípua é auxiliar o método de produção da prova penal digital, como prova em espécie. Não se trata de mero capricho, mas de metodologia que serve à diminuição dos riscos de perdas probatórias, tornando as fontes de prova digital em fontes confiáveis e, portanto, admissíveis.

Nesse panorama, também foi constatado que há uma necessária relevância quanto à revelação do código-fonte do *software* utilizado na metodologia probatória. Somente com a ciência do código-fonte é possível se atestar devida credibilidade à fonte de prova penal digital, pois é pelo código-fonte que se possibilita a identificação de erros, proposital ou acidentalmente inseridos, nas instruções de programação e execução das tarefas.

Toda a diligência deve ser detalhadamente registrada, não há espaço para uma "presunção de fidedignidade". Portanto, a cadeia de custódia da prova é requisito de admissibilidade da fonte de prova penal digital. A demonstração de que todas as etapas foram cumpridas com rigor possibilita uma atribuição de confiabilidade à informação e, por decorrência, à decisão judicial que pretende utilizá-la.

6. Referências

CASEY, Eoghan. *Digital Evidence and Computer Crime*: Third Edition. Elsevier: San Diego, 2011.

COSTABILE, Gerado. Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008. *Ciberspazio e Diritto*, v. 11, n. 3, p. 465-508, 2010.

DANIELE, Marcelo. La prova digitale nel processo penale. *Rivista di Diritto Processuale*, Anno LXVI, (Seconda Serie), n. 2, Marzo-Aprile, 2011. p. 295.

GAMMAROTA, Antonio. *Informatica forense e processo penale*: la prova digitale tra innovazione normativa e incertezze giurisprudenziali. Dottorato di Ricerca in Diritto e nuove tecnologie, Università di Bologna, 2016.

GLOECKNER, Ricardo; EILBERG, Daniela Dora. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. R*evista Brasileira de Ciências Criminais*, v. 156/2019, 2019.

IOVENE, Federica. *Prova informatica e diritti fondamentali della persona nel processo penale.* Tesi di Dottorato, Università degli Studi di Trento, 2014.

KERR, Orin S. Executing warrants for digital evidence: the case for use restrictions on nonresponsive data. *Texas Tech Law Review*, vol. 48:1, 2015.

LANGER, Máximo; ROACH, Kent. Direitos no processo penal: um estudo de caso sobre convergência e direitos de disclosure = *Rights in Criminal Procedure: a case study about convergence and rights to disclosure.* In: *Revista Brasileira de Ciências Criminais: RBCCrim,* São Paulo, v. 23, n. 116, p. 239-257, set.-out. 2015.

LUPÁRIA, Lucas; ZICCARDI, Giovanni. *Investigazione penale e tecnologia informatica*: l'accertamento del reato tra progresso scientifico e garanzie fondamentali. Milano: Giuffrè Editore, 2007. p. 46-47.

MARCELLA, Albert J.; GUILLOSSOU, Frederic. *Cyber forensics*: from data to digital evidence. New Jersey: Wiley, 2012.

MASON, Stephen. Software code as the witness. In: Stephen Mason and Daniel Seng (eds.). *Electronic Evidence* (4th edn, University of London 2017) 88-100.

MASON, Stephen. The presumption that computers are 'realiable'. In: Stephen Mason and Daniel Seng (eds.). *Electronic Evidence* (4th ed, University of London 2017).

MENDES, Carlos Hélder Carvalho Furtado. *Prova penal digital*: direito à não autoincriminação e contraditório na extração de dados armazenados em sistemas informáticos. Tese (Doutorado) – Programa de Pós-graduação em Ciências Criminais – PUCRS, 2023.

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

POLANSKY, Jonathan A. *Garantías constitucionales del procedimiento penal en el entorno digital.* Buenos Aires: Hammurabi, 2020.

PRADO, Geraldo. *A cadeia de custódia da prova no processo penal.* São Paulo: Marcial Pons, 2019. p. 76-77.

RAMALHO, David Silva. *Métodos ocultos de investigação criminal em ambiente digital.* Almedina: Coimbra, 2017.

SOUSA MENDES, Paulo de. A privacidade digital posta à prova no processo penal. In: *Quaestio facti. Revista Internacional sobre Razonamiento Probatorio*, n. 2, 2021. p. 225-250.

TEPPLER, Stephen W. Digital data as hearsay. *Digital Evidence and Electronic Signature Law Review 7*, v. 6, p. 7-9, 2009. Disponível em: [https://sas-space.sas.ac.uk/5334/1/1853-2571-1-SM.pdf].

WALKER, Cornell. *Computer forensics*: bringing the evidence to court. Disponível em: [www.infosecwriters.com/text_resources/pdf/Computer_Forensics_to_Court.pdf]. p. 1. Acesso em: 06.2018.

7. Jurisprudência

BRASIL. Superior Tribunal de Justiça – STJ, AgRg no Recurso em Habeas Corpus 143.169 – RJ (2021/0057395-6), 5ª T., rel. Min. Jesuíno Rissato (Des. convocado do TJDFT), rel. p/acórdão Min. Ribeiro Dantas, *DJe* 02.03.2023.

BRASIL. Superior Tribunal de Justiça – STJ, Habeas Corpus – HC 160.662/RJ, 6ª T., j. 18.02.2014.

BRASIL. Superior Tribunal de Justiça – STJ, REsp 1.435.421/RS, 6ª T., rel. Maria Thereza de Assis Moura.

PESQUISAS DO EDITORIAL

Áreas do Direito: Digital; Penal; Processual

Veja também Doutrinas relacionadas ao tema

- Admissibilidade das provas digitais: o que se faz na nuvem; fica na nuvem, de Fernanda Antunes Marques Junqueira e Flávio da Costa Higa – *RDT* 229/75-95;
- A cadeia de custódia como elemento fundamental da validade e utilidade das provas digitais, de Maurício Tamer – *Boletim Revista dos Tribunais Online* 36/2023;
- A proteção dos dados sensíveis no ordenamento jurídico brasileiro, de Graziela Harff e Marcelo Schenk Duque – *RDCC* 29/57-88;
- O regime jurídico das provas digitais no direito brasileiro, de João Paulo Lordelo Guimarães Tavares – *RePro* 316/373-387;
- Fundamentos à aplicação do incidente de autenticidade ao elemento probatório informático: a ineficiência da simples captura de tela como meio probatório, de Spencer Toth Sydow e Agenor Alexsander C. Costa – *RDTec* 13/2021;
- Recomendação sobre a ética da inteligência artificial da UNESCO e sua aplicação no judiciário, de Luciane Cardoso Barzotto – *RDT* 225/221-241; e
- Sequestro de dados e ataque cibernético na sociedade da informação, de Emerson Penha Malheiro, Eduardo Sorrentino de Alcântara e Nathalia Esteves – *RT* 1043/149-164.

Mendes, Carlos Hélder Carvalho Furtado; Felix, Yuri. Aquisição das fontes de prova penal digital: reflexões a partir do informativo de jurisprudência 763 do STJ.
Revista Brasileira de Ciências Criminais. vol. 197. ano 31. p. 215-247. São Paulo: Ed. RT, jul./ago. 2023.
DOI: [https://doi.org/10.54415/rbccrim.v197i197.504].