Parecer: investigação criminal digital e processo penal

Legal opinion: digital criminal investigation and criminal process

Geraldo Prado

Doutor em Direito. Concluiu estudos de Pós-doutoramento em História das Ideias e Cultura Jurídicas pela Universidade de Coimbra. Investigador do Instituto de Direito Penal e Ciências Criminais da Faculdade de Direito da Universidade de Lisboa e do Ratio Legis – Centro de Investigação e Desenvolvimento em Ciências Jurídicas, da Universidade Autónoma de Lisboa, e Professor visitante da Universidade Autônoma de Lisboa. Consultor Sênior Associado do JusticiaLatinoAmerica – JusLat.
Lattes: [http://lattes.cnpq.br/0340918656718376].
ORCID: [https://orcid.org/0000-0002-4738-780X].
geraldoprado@terra.com.br

DOI: [https://doi.org/10.5281/zenodo.8381070].

Autor convidado

Áreas do Direito: Penal; Processual; Digital

Resumo: Creio que o interesse na publicação do parecer reside no fato de o estudo diferenciar as duas etapas da persecução penal sob o ângulo do processo digital: a investigação criminal digital e o processo penal digital em sentido estrito. A abordagem reforça o que se tem investigado relativamente ao tema da prova digital, no entanto deslocando a ênfase da prova digital para o procedimento em si. Uma investigação criminal digital tem nuances que a autonomizam e que exigem tratamento jurídico adequado a ela. A correta compreensão do fenômeno pode auxiliar o intérprete no que toca à definição dos efeitos jurídicos da violação das regras do devido processo legal digital, examinando hipótese de contaminação dos atos do processo pelos da investigação.

Palavras-chave: Investigação criminal digital – Prova digital – Cadeia de custódia das provas digitais.

Abstract: I believe that the interest in publishing this legal opinion lies in the fact that the study differentiates the two stages of criminal prosecution from the angle of the digital process: the digital criminal investigation and the digital criminal process in the strict sense. The approach reinforces what has been investigated regarding the issue of digital evidence, however shifting the emphasis from digital evidence to the process itself. A digital criminal investigation has nuances that make it autonomous and that require adequate legal treatment. The correct understanding of the phenomenon can help the interpreter in terms of defining the legal effects of violating the rules of digital due process, examining the hypothesis of contamination of the acts of the process by those of the investigation.

Keywords: Digital criminal investigation – Digital evidence – Chain of custody of digital evidence.

Sumário: 1. Consulta. 2. Breve descrição dos fatos pertinentes ao parecer. 3. A prova digital: segurança e autenticidade. A tutela constitucional da privacidade e a proteção de dados. Considerações iniciais. 3.1. Introdução. 3.2. A investigação digital e a prova digital: segurança e autenticidade sob controle na primeira etapa da persecução penal. 4. Quesitos.

"Na prática do juízo processual, a estrutura peculiar do dado digital engendra a ilusão de que o que é digitalmente representado é indiscutível, assim como o sentido atribuível a tal representação. Isso nos conduz a acreditar de maneira acrítica que uma exibição digital é adequada para apoiar o raciocínio lógico-probatório do juiz"

(Raffaella Brighi e Michele Ferrazzano).[1]

1. Consulta

Os cultos advogados F. E, N. C. e R. M apresentam consulta sobre questões atinentes ao regime jurídico-constitucional brasileiro da admissibilidade da prova, com especial ênfase à problemática da prova digital concernente à instauração e preservação da cadeia de custódia de material que, de acordo com o que alegam, ingressou indevidamente em processo, em trâmite na 1ª Vara Federal Cível e Criminal da Subseção Judiciária da Comarca de "X".

Assim é que o estudo solicitado pelos Consulentes é pertinente à instauração e preservação ou não da cadeia de custódia de conteúdo consistente em dispositivos e arquivos digitais relativos à apreensão ordenada em 30 de abril de 2018 no âmbito da Vara Especializada em Crimes contra a Criança e o Adolescente da Comarca de "Y" (Justiça Estadual).

O processo criminal corre hoje perante a 1ª Vara Federal Cível e Criminal da Subseção Judiciária da Comarca de "X", imputando-se ao interessado N. C., denunciado em 03 de novembro de 2020, a prática dos crimes previstos nos arts. 241-A[2] e 241-B da Lei 8.069/1990 (Estatuto da Criança e do Adolescente), c/c art. 71 do CP.

A indagação dos Consulentes centra-se nas consequências jurídicas da violação dos cuidados próprios à espécie de diligência técnica.

O tema, pois, está circunscrito à "integridade", "autenticidade" e "auditabilidade" de provas digitais em um determinado contexto de apreensão, preservação, exame e

1. Tradução livre. BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. In: CAIANIELLO, Michele; CAMON, Alberto (ed.). *Digital forensic evidence*: towards common European standards in antifraud administrative and criminal investigations. Milano: Cedam, 2021. p. 14. Raffaella Brighi é Professora associada de *Informatica giuridica* e *Informatica forense* na *Università di Bologna*. Michele Ferrazzano é Professor de *Informatica* na *Università di Modena e Reggio Emilia*.

2. Art. 241-A, Lei 8.069/1990. "Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. (Incluído pela Lei 11.829, de 2008)."

emprego probatório desses elementos, não cabendo juízo de valor sobre quaisquer outros aspectos do caso.

2. Breve descrição dos fatos pertinentes ao parecer

Ao que interessa penso que a questão controvertida, submetida a análise, está definida no acórdão emitido no processo de *habeas corpus* e nos laudos periciais elaborados pelo assistente técnico P. P. em 22 de março de 2022 e 25 de novembro de 2021.

Com efeito, é incontroverso que os laudos periciais oficiais, confeccionados quer na esfera estadual, quer na federal, incluem informações hipoteticamente armazenadas em dispositivos digitais não apreendidos na execução da medida cautelar (um *notebook* Dell e um HD Samsung).

Saliente-se que os citados laudos oficiais apoiam a denúncia no que diz respeito a N. C.

O conteúdo digital desses equipamentos foi considerado prova obtida por meios ilícitos no julgamento do *habeas corpus*, em 06 de junho de 2022.

O tribunal federal, no entanto, não determinou a exclusão dos demais elementos digitais atribuídos na acusação a N. C., enquanto os laudos de autoria do assistente técnico sublinham "violação da cadeia de custódia" também em relação a esses elementos.

Assim, além da prova já considerada obtida de forma ilícita pelo tribunal, questiona-se a remanescente, e a impugnação dos Consulentes centra-se em problemas referidos à cadeia de custódia dessas provas.

As indagações dos Consulentes são:

1) Conforme a documentação do processo apresentada e os laudos emitidos, é possível afirmar que no tocante à internação processual, por ordem judicial, das informações digitais adquiridas, o procedimento de instauração e preservação de sua cadeia de custódia foi observado?

2) Na hipótese de constatação da quebra da cadeia de custódia das provas, que consequências jurídicas advêm disso?

O tema não é inédito, mas apenas nos últimos nove anos a doutrina nacional passou a lhe dedicar mais significativa atenção apesar de sua inegável filiação ao processo penal constitucional.

Merece, pois, o enfrentamento teórico destacado que terá lugar em seguida, em perspectiva analítica.

Desde logo, no entanto, um resumo fiel do tema central do estudo jurídico pode ser este: o crescente papel que os elementos probatórios digitais exercem nos processos criminais implica compreender que investigação digital e processo penal digital configuram duas fases da persecução penal, ambas com imensa relevância epistêmica e jurídica, mas com funções próprias.

O sucesso do processo penal digital, no sentido de adjudicar a melhor solução jurídica à causa penal, depende de garantias de integridade e autenticidade dos elementos informativos digitais em geral obtidos durante a investigação criminal.

No processo penal digital o "contraditório digital" é constituído pela possibilidade concreta de que os elementos probatórios digitais sejam "auditáveis". Essa "auditabilidade", que marca o contraditório processual digital, é dependente da integridade e autenticidade dos elementos probatórios que são adquiridos na fase de investigação. Se não é possível assegurar que esses elementos são íntegros e autênticos, a parte contrária àquela que os produziu na etapa da investigação não estará em condições de, no curso do processo criminal, percorrer retrospectivamente a trilha probatória, pois essa não mais existe.

Por isso, os mecanismos de controle da integridade e autenticidade desses elementos probatórios digitais formam parte dos dispositivos jurídico-epistêmicos que definem *se* e *quando* há justa causa para a ação penal baseada em meios probatórios digitais.

A natureza *manipulável* e *volátil* do elemento digital – da sequência de *bits*, como acentuam Raffaella Brighi e Michele Ferrazzano – requisita sejam incorporadas práticas técnico-científicas de investigação criminal digital que de modo algum podem ser escanteadas.

As "boas práticas" de aquisição da prova digital são inerentes à própria prova. Será visto que o "corpo de delito informático" é complexo porque dependente do próprio método de sua verificação.

Quando surgem indícios de manipulação de dados contidos em arquivos digitais, manipulação acidental ou intencional, todo o esquema jurídico-epistemológico sobre o qual se funda a prova digital é abalado.

Uma diferença de *milhares* de arquivos de imagem entre uma perícia oficial e outra ou a *comprovação* de que o dispositivo digital apreendido por ordem judicial posteriormente foi alvo de uma manipulação que alterou seu conteúdo digital são informações relevantes no processo penal digital para excluir do seu âmbito a prova impugnada.

E se a constatação da manipulação vem acrescida da notícia de que dispositivos digitais *não apreendidos* foram empregados processualmente, o que se tem é um caso paradigmático de violação do devido processo legal digital.

O objetivo de busca da verdade no processo penal digital está condicionado pelo respeito escrupuloso às chamadas "boas práticas técnico-científicas".

Isso não é novidade no direito brasileiro, tampouco remonta à reforma processual penal de 2019.

Em tema de investigação de crimes relacionados à pornografia infantil pela Internet, a *indispensabilidade* da instauração da cadeia de custódia das provas digitais é muito bem tratada pela tese portuguesa de mestrado de 2015, do Delegado de Polícia Federal Stenio Sousa Santos (Universidade Autónoma de Lisboa).[3]

No caso concreto, antes mesmo de se falar em "violação da cadeia de custódia" é inevitável reconhecer que a cadeia de custódia das provas digitais sequer foi instaurada quando era devido e pertinente, no momento da apreensão dos dispositivos digitais.

Isso já diz tudo.

Bem... vamos à teoria e sua aplicação ao caso examinado.

3. SOUSA, Stenio Santos. *Investigação criminal cibernética*: por uma política criminal de proteção à criança e ao adolescente na Internet. Porto Alegre: Núria Fabris, 2015.

3. A prova digital: segurança e autenticidade. A tutela constitucional da privacidade e a proteção de dados. Considerações iniciais

3.1. Introdução

Em obra de referência sobre o tema Jonathan A. Polansky, professor da Universidade de Buenos Aires, indaga: "Como em um mundo virtual é possível assegurar que os agentes estatais não introduzam informação em um disco rígido apreendido?"[4]

É possível parafrasear Polansky e indagar: como em um mundo virtual é possível assegurar que os agentes estatais não introduzam ou suprimam informação em um contexto de apreensão de dados digitais provenientes de qualquer fonte?

O objetivo deste estudo consiste em responder a essa indagação, que hoje é comum aos vários ordenamentos jurídicos.

O caso submetido à análise é paradigmático sob vários ângulos.

Com efeito, transversalmente à questão da preservação de elementos probatórios obtidos em sequência de investigações tendo como alvo várias pessoas, com a apreensão de dispositivos digitais, suscitam-se também problemas relacionados a tutelas constitucionais clássicas – privacidade, proteção das comunicações, devido processo legal – e a outras que configuram direitos fundamentais da nova era biodigital, como é o caso da proteção constitucional especial dos sistemas de tecnologia de informação e comunicação.[5]

Antecipam-se aqui, como chave de leitura, alguns dos argumentos que serão desenvolvidos ao longo do estudo e que justificam que a aplicação das regras ao caso concreto esteja pavimentada pelo domínio de conceitos de base que, dada a expansão da prova digital, praticamente convertem o direito probatório em direito probatório digital.

A inevitabilidade dessa transformação decorre do fenômeno inconteste da convergência de tecnologias de informação e comunicação que toma corpo em dispositivos informáticos cuja função não é mais redutível à de mero instrumento de comunicação entre duas ou mais pessoas. Além dos telefones móveis, é incontroverso que os computadores pessoais há muito transcenderam a função de dispositivos de comunicação.

Em realidade, o conjunto dos dispositivos digitais modernos – incluindo, naturalmente, aqueles que operacionalizam a chamada "Internet das Coisas" – armazena informações pessoais que em grande medida são informações situadas no campo juridicamente protegido da privacidade e da intimidade e são também informações suscetíveis de serem alteradas à revelia do titular do "banco de dados digital", haja vista sua característica de volatilidade.

O acelerado desenvolvimento das tecnologias de comunicação e informação a partir da expansão do conhecimento no campo da inteligência artificial e da descoberta e emprego de materiais que transformaram os dispositivos digitais, com as sucessivas revoluções

4. POLANSKY, Jonathan A. *Garantías constitucionales del procedimiento penal en el entorno digital*. Buenos Aires, Hammurabi, 2020. p. 170.

5. HOFFMANN-RIEM, Wolfgang. *Teoria geral do direito digital*. Transformação digital. Desafios para o direito. Trad. de Italo Fuhrmann. Rio de Janeiro: Forense, 2021. p. 49.

tecnológicas 2.0, 3.0, 4.0, chegando nos dias em que essas linhas são escritas à concretização da 6.0 (o 5G já é uma realidade *ultrapassável*), *aposentaram* a antiga fórmula da intromissão nas comunicações alheias e a substituíram por um conjunto integrado "humano-máquina", altamente complexo e perigosamente manipulável.

Nos últimos 15 anos há pouca diferença – irrelevante mesmo para os fins da análise – entre a interceptação de conversas telefônicas ou de dados, pois que os sistemas digitais de comunicação telefônica substituíram os analógicos e a "aquisição e preservação" de conversas telefônicas interceptadas corresponde tecnicamente à interceptação de dados, esfumaçando a distinção constitucional estabelecida pelo inciso XII do art. 5º da CRFB.[6]

Mais até, é necessário que se diga, essa convergência tecnológica produziu um fenômeno com o qual certamente sonharam os governantes autocráticos europeus dos tempos posteriores à Paz de Vestfália (1648), com a *nova diplomacia* associada à espionagem de inimigos *internos* e *externos*: a capacidade de intromissão e controle massivo das populações por meio do domínio das informações.

O mundo descrito pelo escritor russo Ievguêni Ivánovitch Zamiátin em seu romance de 1924, intitulado "Nós",[7] que, segundo George Orwell, o inspirou em "1984" e a Aldous Huxley, em "Admirável Mundo Novo",[8] profecia a vida devassada, de janelas físicas e mentais eternamente abertas e acessíveis aos governantes.

A intromissão nas comunicações hoje é conceitualmente uma interceptação de dados que são convertidos em formato de áudio e que funciona à semelhança das ficcionais janelas físicas e mentais permanentemente abertas.

O exemplo das comunicações telefônicas digitais é muito importante mesmo no contexto da aquisição de arquivos de imagens, que é do que trata o caso examinado, porque sons, imagens, palavras no universal digital não são outra coisa senão dados.

O poder imagético que impregna o arquivo digital é exercido visual ou sonoramente sem que o público-alvo – juiz, partes, autoridade policial e as pessoas em geral – se dê conta de que está diante de *bits* organizados de uma determinada maneira a formar aquilo que *aparece* e que, em verdade, é o resultado algorítmico de um determinado arranjo desses *bits*.

Por esse ângulo releva considerar o conceito de "dado", que é o ponto de partida de tudo mais que está envolvido no universo digital. De acordo com Brighi e Ferrazzano:

---

6. Art. 5º, CRFB. "Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal."
7. ZAMIÁTIN, Ievguêni Ivánovitch. *Nós*. Trad. de Gabriela Soares e Ana Resende. São Paulo: Editora Aleph, 2017 (publicado originalmente em 1924 com o título em russo "Mbl"). p. 20-314.
8. ORWELL, George. Resenha de Nós, de Ievguêni Ivánovitch Zamiátin (publicada originalmente em 04 de janeiro de 1946 na Revista Tribune, Londres). In: ZAMIÁTIN, Ievguêni Ivánovitch. *Nós*. Trad. de Gabriela Soares e Ana Resende. São Paulo: Editora Aleph, 2017. p. 317-323.

> "*Dado digital* é uma representação que usa uma sequência binária de bits que não são compreensíveis por humanos. Portanto, requer uma série de operações pelas quais se realiza uma transformação que pode levar a diferentes resultados (exibidos como texto na tela ou como vídeo, ou ainda como imagem impressa no papel). Sem interpretação, os dados não podem ter nenhum significado."[9]

Acentuam esses autores que o "dado digital" consiste em representação de sequências binárias de *bits* incompreensíveis para os humanos, a demandar uma série de operações técnicas carregadas de variáveis que os transformam em diferentes resultados possíveis, de voz, imagem, texto etc., conforme sejam processadas essas sequências de *bits*.[10]

"Sem interpretação, dados não podem ter nenhum significado", lecionam corretamente Brighi e Ferrazzano.[11]

É nesse sentido que se afirma que o "corpo de delito informático" é complexo porque dependente do próprio método de sua verificação, em uma espécie de movimento circular que caracteriza a chamada "prova digital".

A operação técnica e a interpretação humana são vetores essenciais no processo hoje rotineiro de digitalização da vida.

E o binômio "humano-máquina" é inevitável, mesmo em ambientes dominados por intensa aplicação prática de recursos de inteligência artificial (p. e., com a *programação* de seleção de trechos captados correspondentes a "palavras-chave" para pesquisas), porque diferentemente do que fazem as chamadas *Big Techs*, com seu *arrastão tecnológico de informações pessoais via Inteligência Artificial* (*IA*), o uso que os agentes estatais pretendem dar às informações colhidas esbarra em uma série de garantias constitucionais tradicionais e novas que interditam as devassas.

O "controle informacional" da vida das pessoas, para fins de investigação e processo criminal, é, por razões óbvias, escrupulosamente regulado em lei. Seus aspectos objetivo (método, técnica, *alvo* etc.) e subjetivo (as comunicações a que excepcionalmente o acesso de terceiros está autorizado) são incompatíveis com uma espécie de "delegação automática às máquinas", requisitando permanente intervenção e supervisão do elemento «humano».

A garantia constitucional do contraditório é a *essência* do devido processo legal. No mundo híbrido digital-analógico essa garantia toma forma complexa de: *i)* possibilidade

9. Tradução livre. BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. In: CAIANIELLO, Michele; CAMON, Alberto (ed.). *Digital forensic evidence*: towards common European standards in antifraud administrative and criminal investigations. Milano: Cedam, 2021. p. 14.
10. BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. In: CAIANIELLO, Michele; CAMON, Alberto (ed.). *Digital forensic evidence*: towards common European standards in antifraud administrative and criminal investigations. Milano: Cedam, 2021. p. 14.
11. Tradução livre. BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. In: CAIANIELLO, Michele; CAMON, Alberto (ed.). *Digital forensic evidence*: towards common European standards in antifraud administrative and criminal investigations. Milano: Cedam, 2021. p. 14.

concreta de identificação, verificação e conferência das técnicas empregadas para adquirir e preservar as informações, com suas nuances de conversibilidade tanto de suportes como de programas (criptografia, decodificação, conversão áudio-imagem e imagem-áudio etc.); *ii)* rastreabilidade concreta de todos os procedimentos técnicos empregados, com a identificação das pessoas envolvidas em cada etapa, seu nível de autorização para intervenção e descrição das atividades praticadas por cada uma delas; *iii)* e a "repetibilidade" da diligência, que deve ser compreendida em conformidade com cada *espécie de aplicação tecnológica*, mas que deve assegurar às partes e ao juiz ou juíza que a informação originalmente obtida é aquela examinada por todos os envolvidos durante a persecução penal.

Como sublinhado no preâmbulo deste estudo, autenticidade e integridade da prova garantidas por sua auditabilidade.

A *fé* na palavra do investigador que ouvia as conversas no alto do poste da companhia telefônica não pode ser substituída pela *fé ilusória da irrefutabilidade do resultado da diligência tecnológica*, como adverte Marcello Daniele.[12]

O conhecimento dos métodos de aquisição de elementos probatórios digitais e a rastreabilidade da aplicação das técnicas são imperativos da eleição da ingerência em dispositivos informáticos que não apenas na chamada *Cloud Forensic*, mas em todas as formas de perícia digital (*Digital Forensic*) para fins processuais, conduzem à consideração da tripla dimensão referida em 2013 por Keyun Ruan, Joe Carthy, Tahar Kechadi e Ibrahim Baggili: a) dimensão técnica; b) dimensão organizacional; c) e dimensão jurídica.[13]

Para fins de processo penal, no âmbito da validade jurídica dos atos probatórios, as três dimensões são indissociáveis, pois, salientam Brighi e Ferrazzano, todo dado digital é útil para apoiar ou rejeitar teses acerca do cometimento do crime ou da existência de um álibi.[14]

Nesse contexto é possível destacar o *primeiro aspecto* a ser enfrentado na prática, nas hipóteses em que, ainda que demandando a investigação criminal informações contidas *nos* ou obtidas a partir *de* dispositivos digitais, o acesso às referidas informações pela Polícia não haja sido realizado adequadamente.

Será visto que esse primeiro aspecto, relacionado à forma de acesso às plataformas de processamento das informações cobra a escrupulosa observância de certos protocolos técnicos porque, como salientaram no caso concreto tanto o perito T. S., da Unidade Técnico-Científica da Delegacia de Polícia Federal de Uberlândia, em 02 de abril de 2020, quanto o

12. DANIELE, Marcello. Prova scientifica e regole di esclusione. In: CANZIO, Giovanni; DONATI, Luca Lupária (Ed.). *Prova scientifica e processo penale*. 2. ed. Milão: Wolters Kluwer, 2022. p. 447.

13. RUAN, Keyun; CARTHY, Joe; KECHADI, Tahar; BAGGILI, Ibrahim. Cloud forensics definitions and critical criteria for cloud forensic capability: an overview of survey results. *Digital investigation*, v. 10, 2013. p. 37. Os três primeiros membros do *Center for Cyber Security and Cyber Crime Investigation, University College Dublin*, e Baggili membro do *Tagliatela College of Engineering, Department of Computer Science, University of New Haven*.

14. BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. In: CAIANIELLO, Michele; CAMON, Alberto (Ed.). *Digital forensic evidence*: towards common European standards in antifraud administrative and criminal investigations. Milano: Cedam, 2021. p. 14-15.

assistente técnico, nos dois laudos já referidos, a pluralidade de operações técnicas envolvidas em cada etapa, do *input* ao *output*, estabelece um "processo de apreensão do dado digital" irredutível a um só *ato*.

Vale observar o cuidado adotado pelo perito federal, em abril de 2020, orientado a "possibilitar a posterior verificação da integridade do material examinado". Com o propósito de viabilizar a rastreabilidade e auditabilidade do próprio trabalho pericial, T. S. gerou o arquivo *hash* relativamente a todos os arquivos que examinou.

Em palavras mais simples, o perito federal "lacrou" o material digital que examinou, atento às características próprias às perícias digitais.

E que características são essas? Brighi e Ferrazzano respondem que a perícia digital deve seguir o caminho: *a)* de preservação da integridade do dado digital; *b)* de verificação de sua autenticidade quanto à originalidade e aquisição; *c)* completude do material digital examinado, de sorte a permitir que as partes tenham acesso ao *contexto* em que os dados digitais estão inseridos; *d)* a confiabilidade quanto a não terem sido esses dados alterados, modificados, suprimidos ou aditados; *e)* pertinência probatória para o caso; *f)* adequação em termos de contribuição informacional; e, finalmente, *g)* a documentação de todo o processo acima referido, que se faz por meio da instauração e preservação da cadeia de custódia.[15]

Quando percebido o processo como um todo, sem a ilusão de que se trata de uma intervenção direta, imediata e instantânea, sem quaisquer desdobramentos, compreende-se o imenso cuidado que há pelo menos duas décadas origina protocolos técnicos nacionais e internacionais que, à semelhança da Norma ABNT ISO/IEC 27037:2013 (NRP ISSO/IEC 27037), espelha metodologias internacionalmente consagradas dirigidas à preservação da prova eletrônica.[16]

O órgão antifraude da União Europeia justamente adota esses cuidados quando cuida da investigação digital de graves crimes econômico-financeiros, conforme proposta de seu manual de boas práticas (Guidelines on Investigation Procedures for OLAF Staff).[17]

15. BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. In: CAIANIELLO, Michele; CAMON, Alberto (Ed.). *Digital forensic evidence*: towards common European standards in antifraud administrative and criminal investigations. Milano: Cedam, 2021. p. 17-18.
16. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ISO/IEC 27037. Tecnologia da informação – Técnicas de segurança – Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Primeira edição: 09 dez. 2013. Válida a partir de 09 jan. 2014. Disponível para aquisição em: [www.normas.com.br/visualizar/abnt-nbr-nm/33821/nbriso-iec27037-tecnologia-da-informacao--tecnicas-de-seguranca-diretrizes-para-identificacao-coleta-aquisicao-e-preservacao-de-evidencia--digital]. Acesso em: 15.06.2023. A norma ISO/IEC 27037 é mencionada por Brighi e Ferrazzano: BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. In: CAIANIELLO, Michele; CAMON, Alberto (Ed.). *Digital forensic evidence*: towards common European standards in antifraud administrative and criminal investigations. Milano: Cedam, 2021. p. 20, 28 e 37).
17. EUROPEAN ANTI-FRAUD OFFICE. *Guidelines on investigations for OLAF staff*. Data: 11 out. 2021. Disponível em: [https://anti-fraud.ec.europa.eu/guidelines-investigations-olaf-staff_en]. Consultado em 10 de junho de 2023.

O *segundo aspecto* é instrumental ao primeiro, como em abril de 2016 o Tribunal Federal Constitucional alemão reconheceu, ao tratar do direito fundamental especial à integridade dos sistemas de tecnologia de informação e comunicação.[18]

Como mencionado, a volatilidade e a característica manipulabilidade dos dados digitais, capazes de serem alterados sem deixar rastros,[19] fomentam rigorosos protocolos internacionais de tratamento de fontes de prova digital.[20]

Polansky, após apresentar extenso rol de normativas para o resguardo da prova em dispositivos de armazenamento digital, alerta para a orientação predominante acerca da intervenção *ex ante*, visando à adoção de protocolos e critérios que sejam aptos a validar a prova digital no momento de sua *obtenção*, cercada de cuidados para que a informação que as caracteriza não seja colocada em dúvida.[21]

As provas digitais, realçam Brighi e Ferrazzano, são intangíveis, alteráveis anonimamente porque compostas de sequências binárias, modificáveis pelo seu *manuseio* incorreto, voláteis e com potencial ilimitado de reprodutibilidade.[22]

É certo que ao condicionar a validade jurídica dos elementos probatórios à constatação de que as melhores práticas foram adotadas, o modelo da "prova digital" articula as três dimensões referidas por Ruan, Carthy, Kechadi e Baggili: a dimensão técnica, a organizacional e a dimensão jurídica, conferindo à perícia forense papel primordial na determinação da admissibilidade da prova.

Diane Barret, professora da Bloomsburg University of Pennsylvania, adverte, a respeito da perícia forense digital, que sua definição existe há muitos anos. Assevera Barrett:

---

18. ALEMANHA. Bundesverfassungsgericht (Tribunal Constitucional Federal da Alemanha). BVerfGE 141, 220. 1 BvR 966/09; 1 BvR 1140/09. Decisão. Data: 20 abr. 2016. Versão em inglês disponível em: [www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2016/04/rs20160420_1bvr096609en.html]. Acesso em: 19.01.2021.
19. FÉRNANDEZ MARTÍNEZ, Juan Carlos. Especialidades de la prueba cuando, esta, es tecnológica. In: ORTEGA BURGOS, Enrique (Ed.). *Actualidad:* Nuevas Tecnologías. Valencia: Tirant lo Blanch, 2020. p. 333.
20. International Organization for Standardization. ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. Norma técnica. Publicada em outubro de 2012. Revisada e confirmada em 2018. Versão vigente. Disponível para aquisição em: [www.iso.org/standard/44381.html]. Acesso em: 20.01.2021; Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27037:2013. Tecnologia da informação – Técnicas de segurança – Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Identifica a: ISO/IEC 27037:2012. Norma técnica. Publicada em 09 dez. 2013. Confirmada em 26 nov. 2018. Versão vigente. Disponível para aquisição em: [www.abntcatalogo.com.br/norma.aspx?ID=307273]. Consultado em: 20.01.2021.
21. POLANSKY, Jonathan A. *Garantías constitucionales del procedimiento penal en el entorno digital*. Buenos Aires: Hammurabi, 2020. p. 173-174.
22. BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. In: CAIANIELLO, Michele; CAMON, Alberto (Ed.). *Digital forensic evidence*: towards common European standards in antifraud administrative and criminal investigations. Milano: Cedam, 2021. p. 16.

"O processo de perícia digital consiste na coleta, preservação, análise e apresentação de resultados dos elementos probatórios colhidos na cena do crime".[23]

Importante ressaltar o que salienta, em seguida, a professora da Universidade da Pensilvânia: "O processo tradicional de aquisição da prova digital inclui a manutenção do controle da cadeia de custódia dos dados probatórios forenses".[24] E acrescenta a mesma autora, em ponto crucial para a conclusão acerca do caso examinado no presente estudo: "A ciência por detrás da perícia digital requer processos repetíveis produzindo resultados consistentes."[25]

Essa é conclusão unânime na doutrina, que domina o cenário da prova digital em todo o mundo, cabendo acrescentar, com Brighi e Ferrazzano, que o paradigma da cadeia de custódia segue *todo o ciclo vital* da prova digital, com o registro de cada etapa do manuseio da prova, da aquisição formal à verificação final, de sorte a tornar apta a repetibilidade da trilha processual da prova.[26]

Não existe uma cadeia de custódia da prova digital pela metade.

A auditabilidade da prova digital que viabilize a sua rastreabilidade, reconstituindo-se as etapas com a confirmação da integridade e autenticidade da informação colhida, revela-se condição *sine qua non* de validade jurídica do ato probatório.

A dimensão técnica e a dimensão jurídica da prática probatória digital encontram-se nessa *esquina* da validade jurídica e, em atividades complexas, como sucede ser a da aquisição e preservação dos arquivos de imagens, a dimensão organizacional deverá oferecer "respostas consistentes", perdoada a redundância, às eventuais *inconsistências* verificadas.

Hoje a literatura a respeito da garantia da integridade e autenticidade da prova digital é rica, em especial no direito norte-americano, mas também no Brasil, conforme será visto. Este é o *terceiro aspecto* a ser considerado no caso concreto. A Polícia adotou os protocolos vigentes de garantia da integridade, autenticidade e auditabilidade da prova consistente na aquisição dos dispositivos informáticos e arquivos digitais?

Vimos que a Norma ABNT ISO/IEC 27037:2013 é de 2013.

Como é irrespondível no laudo derradeiro do assistente técnico, da apreensão de dispositivos eletrônicos, em 17 de maio de 2018, com realização de perícia na mesma data, passando pelas perícias de junho de 2018, no Instituto de Criminalística de Belo Horizonte, pelas de julho daquele ano, no mesmo Instituto, até chegar à perícia na esfera federal, em abril de 2020, algo de fato ocorreu *e é impossível determinar o que tenha sido*, porque a cadeia de custódia dos dispositivos eletrônicos (supostamente 9) e a dos arquivos digitais (a critério do perito variando de 41.650 a 2.000 arquivos de imagem) *não foi instaurada*.

23. BARRETT, Diane. Cloud Based Evidence Acquisitions in Digital Forensic Education. *Information Systems Education Journal*, v. 18, n. 6, p. 46-56, 2020. p. 46.
24. BARRETT, Diane. Cloud Based Evidence Acquisitions in Digital Forensic Education. *Information Systems Education Journal*, v. 18, n. 6, p. 46-56, 2020. p. 46.
25. BARRETT, Diane. Cloud Based Evidence Acquisitions in Digital Forensic Education. *Information Systems Education Journal*, v. 18, n. 6, p. 46-56, 2020. p. 46.
26. BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. In: CAIANIELLO, Michele; CAMON, Alberto (Ed.). *Digital forensic evidence*: towards common European standards in antifraud administrative and criminal investigations. Milano: Cedam, 2021. p. 18.

A cadeia de custódia das provas digitais deve seguir *todo o ciclo vital da prova digital*. Isso é consensual até porque é intuitivo à luz das características já referidas dos elementos digitais e o seu processo técnico de conversão em *prova digital*.

O que o perito federal T. S. examinou foi o que entregaram em 02 de abril de 2020. Ninguém pode afirmar que o que T. S. periciou corresponda ao que foi apreendido na residência de N. C.

Ao revés, é possível afirmar categoricamente o contrário.

Como destacou o eminente Desembargador relator do *habeas corpus*, ao determinar a exclusão de parte da prova digital, "restou incontroverso nos autos que, dentre os materiais encaminhados pela PCMG para elaboração da perícia pela Polícia Federal, foram incluídos itens não apreendidos com o paciente [N. C]".

Além disso também é possível fazer duas afirmações factualmente incontestáveis: não há documentação que registre, esclareça ou historie a instauração da cadeia de custódia dos dispositivos eletrônicos apreendidos em tese com N. C.; e a brutal diferença da quantidade de arquivos de imagens, cuja origem, autenticidade e integridade não são demonstráveis, reforça a conclusão pericial do assistente técnico de que um computador "foi utilizado e modificado após a sua apreensão no dia 17/05/2018".

Dificilmente no direito brasileiro, na investigação de crimes do gênero, se encontrará um caso parecido de não instauração de cadeia de custódia de prova digital.

Releva notar que em relação às *tradicionais* provas digitais, Polansky alerta para o fato de que a apreensão deste tipo de elemento probatório – a execução da medida, propriamente dita – envolve duas etapas: a primeira, de apreensão do dispositivo eletrônico físico; a segunda etapa consiste na extração e análise da informação digital contida no dispositivo.[27]

Como tive a ocasião de mencionar,[28] o rápido desenvolvimento tecnológico impacta o mundo da vida e o transforma, pois que a cada dia nos deparamos com novos dispositivos materiais e digitais que acumulam e processam milhares de informações pessoais de cada um de nós.

Seria frustrante buscar definir uma taxinomia desses dispositivos quando se sabe que mesmo o e-mail hoje é considerado um "quase dinossauro", em termos de comunicação, após ter condenado as antigas cartas de papel ao sótão de nossas mais românticas memórias...

Visto por aí, em termos de obsolescência o *e-mail* se assemelha ao "investigador pendurado no poste ouvindo conversas telefônicas"...

Ainda assim, convém levar em conta a advertência de Fernández Martínez: de que o primeiro passo para que se possa dispor processualmente de uma prova digital é assegurar que não se questione sua integridade e autenticidade, "ya que todos sabemos de la facilidad de su manipulación, así como de su volatilidad".[29]

27. POLANSKY, Jonathan A. *Garantías constitucionales del procedimiento penal en el entorno digital*. Buenos Aires: Hammurabi, 2020. p. 168.

28. PRADO, Geraldo. *A cadeia de custódia da prova no processo penal*. 2. ed. São Paulo: Marcial Pons, 2021. p. 194 e ss.

29. FÉRNANDEZ MARTÍNEZ, Juan Carlos. Especialidades de la prueba cuando, esta, es tecnológica. In: ORTEGA BURGOS, Enrique (Dir.). *Actualidad*: nuevas tecnologías. Valencia: Tirant lo Blanch, 2020. p. 333.

Afirmei no livro sobre a cadeia de custódia das provas que as fontes da prova digital denotam, pela própria estrutura, o grau de dificuldade da tarefa de preservar a integridade do elemento probatório digital e de verificar sua autenticidade, além de determinar o cuidado extremado que se deve ter, haja vista os riscos concretos de manipulação e alteração dos dados.[30]

Na oportunidade lembrei a lição de Joaquín Delgado Martín, de que a informação digital está disponível: a) nas redes sociais e páginas da Web; b) em dispositivos eletrônicos; c) armazenados em provedores de serviços.[31]

Os dados podem ainda estar *nas nuvens* (*in the cloud*) em sistemas privados, públicos, híbridos, móveis e comunitários,[32] alimentados em redes abertas ou fechadas que cada dia com maior frequência se caracterizam pela ubiquidade.

As "nuvens digitais" não são *nuvens* em sentido literal, mas, como referido, espaços de armazenamento de dados digitais cujo acesso é ou deve ser controlado em primeiro lugar pelo titular dos dados.

O acesso do próprio titular ou de terceiros aos dados digitais é, pois, um processo técnico que *sempre* lida com as delicadas características de volatilidade e possibilidade de manipulação. Isso demanda do processo técnico que seja realizado cercado de cuidados.

Que os cuidados necessários tenham sido adotados pelo responsável pela manutenção dos sistemas privados, públicos, híbridos, móveis e comunitários, não é algo dado. Ao revés, deve ser demonstrado e isso é especialmente mais necessário quando se trata de dados criptografados que deverão servir de prova em processos judiciais e que, para tanto, ao final, deverão estar reconvertidos em condições de serem objeto de interpretação.

Desnecessário frisar que o ônus de realizar corretamente a diligência probatória digital é da Polícia ou de quem executa a ordem judicial de apreensão dos dispositivos eletrônicos ou das informações digitais.

É assim em sistema processual penal acusatório regido pela presunção de inocência, mas o fato é que na prática também é intuitivo que seja dessa forma porque somente quem

30. Para ilustrar, mais uma vez, Ahmed e Roussev destacam as dificuldades inerentes à perícia em face de novas tecnologias: "A perícia forense digital é fundamentalmente reativa por natureza – não podemos investigar sistemas e artefatos que não existem; não podemos ter *melhores práticas* antes de um período experimental durante o qual diferentes abordagens técnicas são experimentadas, testadas (perante os tribunais) e validadas. Isso significa que sempre há um atraso entre a introdução de um objeto de tecnologia da informação e o tempo em que uma capacidade forense correspondente adequada é implementada. A evolução da infraestrutura das tecnologias da informação é impulsionada pela economia e pela tecnologia; a perícia forense apenas identifica e segue as migalhas digitais deixadas para trás." Tradução livre. AHMED, Irfan; ROUSSEV, Vassil. Analysis of Cloud Digital Evidence. In: CHEN, Lei; TAKABI, Hassan; LE-KHAC, Nhien-An (Ed.). *Security, Privacy, and Digital Forensics in the Cloud*. Hoboken, Singapura: John Wiley & Sons, 2019. p. 302.

31. DELGADO MARTÍN, Joaquín. *Judicial-Tech, el proceso digital y la transformación tecnológica de la justicia*: Obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 55-56.

32. DELGADO MARTÍN, Joaquín. *Judicial-Tech, el proceso digital y la transformación tecnológica de la justicia*: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 55.

se apropria do dispositivo judicial e domina o acesso formal aos dados, com o dever de os apresentar em juízo, detém o poder de fato de *cuidar da coisa custodiada*, mais uma vez com o perdão pela redundância.

No "percurso técnico" que caracteriza o processo de acesso aos dados digitais, o cuidado haverá de se estender às atividades de terceiros, ou seja, a de todos os agentes que foram os destinatários progressivos do conjunto de elementos digitais disponibilizado pelo guardião do sistema ou de alguma maneira terão que participar do processo.

O caminho digital percorrido pela informação deve estar protegido contra manipulações acidentais ou intencionais, supressões ou acréscimos gerados pelas citadas características e nisso não é relevante a diferença entre o acesso a dispositivos físicos – telefones celulares, notebooks ou computadores de grande porte – comunicações telefônicas ou sistemas operacionais *in the cloud*.

A integridade, autenticidade e auditabilidade dos dados convoca o cuidado com os dois aspectos referidos e o verbo "dever", empregado linhas atrás, não é mera figura de linguagem.

Trata-se, portanto, de se comprovar a instauração e preservação de duas distintas cadeias de custódia, imbricadas porque ao serem violadas, ou mesmo não instauradas, podem demonstrar: a) supressão indevida de arquivos; b) indícios de sua manipulação; c) comprometimento da autenticidade dos elementos de informação; d) inviabilidade do material de ser auditado. É o que se observa no caso concreto.

No Anexo II consta esquema da proposta de 2013, dos professores Ilyoung Hong, Hyeon Yu, Sangjin Lee e Kyungho Lee, orientado às diligências de busca e apreensão de elementos probatórios digitais que ilustram bem o caráter tridimensional mencionado nas linhas antecedentes.[33]

Os autores, membros *Center for Information Security Technologies* (*CIST*) e da University Korea, sugerem um modelo de triagem das informações digitais que se revela dinâmico, dado o caráter flexível inerente às diligências, permanentemente supervisionado que compatibilize os interesses da investigação e descoberta da verdade com a garantia do contraditório própria ao ambiente digital.

O citado modelo triádico e as inúmeras outras boas práticas existentes há mais de uma década e conhecidas internacionalmente em geral são compatíveis com o ordenamento jurídico brasileiro.

O que realmente é incompatível com a nossa Constituição é a agregação de uma "fé processual irrestrita" aos executores das medidas cautelares de intromissão. A atividade probatória digital, pelo seu caráter de devassa, é e deve ser objeto de controle de forma contínua.

Releva notar o julgado de 17 de abril de 2013, do Tribunal Supremo da Espanha (STS 342/2013 – RJ 2013, 3296), mencionado por Federico Bueno da Mata, que fixou que a "presença de notário judicial no ato de transferência de dados não atua como pressuposto de validade de sua prática."[34]

---

33. HONG, Ilyoung; YU, Hyeon; LEE, Sangjin; LEE, Kyungho. A new triage model conforming to the needs of selective search and seizure of electronic evidence. *Digital investigation*, v. 10, p. 175-192, 2013.

34. BUENO DE MATA, Federico. *Las Diligencias de Investigación Penal en la Cuarta Revolución Industrial*: principios teóricos y problemas prácticos. Navarra: Aranzadi, 2019. p. 176.

Assevera o tribunal espanhol: "O decisivo é que, seja por meio da intervenção do notário durante a diligência de busca e apreensão dos computadores, ou mediante qualquer outro meio de prova, fiquem descartadas as dúvidas sobre a integridade dos dados e sobre a correlação entre a informação apreendida no ato de intervenção e a que se obtém mediante a transferência."[35]

Exatamente é o mesmo processo de garantia constitucional da autenticidade, integridade e auditabilidade inerente à aquisição das provas digitais, processo impositivo da cadeia de custódia.

A cadeia de custódia da prova consiste em método por meio do qual se pretende preservar a integridade do elemento probatório e assegurar sua autenticidade em contexto de investigação e processo. Realizada em conformidade com as boas práticas de cada área específica, a cadeia de custódia das provas permite que os elementos probatórios sejam auditáveis, concretizando o que se convencionou chamar de "contraditório da prova digital".

A violação da cadeia de custódia implica a impossibilidade de valoração da prova, configurando seu exame – de verificação da cadeia de custódia – um dos objetos do juízo de admissibilidade do meio de prova ou do meio de obtenção de prova, conforme o caso. A consequência jurídica da quebra da cadeia de custódia das provas consiste em não se submeter a juízo de *peso probatório*, sequer de *relevância* da prova, os vestígios que não tenham sido adequadamente preservados.

Não é diferente quando a análise envolve as chamadas provas digitais.[36] Esse é o *quarto aspecto* a considerar.[37]

Com efeito, Federico Lucio Godino e Christian Andrés Pérez Sasso identificam na violação da cadeia de custódia das provas lesão ao devido processo legal, no tocante à obtenção e/ou preservação do elemento probatório, a interditar sua valoração pelo juiz.[38]

---

35. BUENO DE MATA, Federico. *Las Diligencias de Investigación Penal en la Cuarta Revolución Industrial*: principios teóricos y problemas prácticos. Navarra: Aranzadi, 2019. p. 176.
36. Sem embargo da afirmação, o trabalho pericial também poderá contribuir para a identificação de provas relevantes contidas em dispositivos informáticos, como salientam Irfan Ahmed e Vassil Roussev: "A noção de *relevância* é inerentemente específica a cada caso e uma grande parte da competência de um analista forense é a capacidade de identificar provas relevantes a um caso. Frequentemente, um componente crítico da análise forense é a *atribuição* causal de uma sequência de eventos a atores humanos específicos do sistema (tais como usuários e administradores). Quando utilizados em processos judiciais, a *proveniência*, a *confiabilidade* e a *integridade* dos dados utilizados como prova são de suma importância. Em outras palavras, consideramos todos os esforços para realizar análises de sistema ou de artefatos após o fato como uma forma de perícia forense. Isso inclui atividades comuns tais como a resposta a incidentes e investigações internas, que quase nunca resultam em quaisquer processos judiciais. Em geral, somente uma pequena fração das análises forenses chega às salas de audiência como provas formais." Tradução livre. AHMED, Irfan; ROUSSEV, Vassil. Analysis of Cloud Digital Evidence. In: CHEN, Lei; TAKABI, Hassan; LE-KHAC, Nhien-An (ed.). *Security, Privacy, and Digital Forensics in the Cloud*. Hoboken, Singapura: John Wiley & Sons, 2019. p. 301-302.
37. Nesse sentido a recente decisão veiculada no Informativo 763 do Superior Tribunal de Justiça, de 14 de fev. de 2023. Agravo Regimental no Habeas Corpus 143.169/RJ. 5ª Turma. Rel.: Min. Messod Azulay Neto. Rel. para acórdão: Min. Ribeiro Dantas. Julgamento em: 07 fev. 2023.
38. GODINO, Federico Lucio; PÉREZ SASSO, Christian Andrés. *Cadena de Custodia*: procedimientos para resguardar los elementos probatorios. Buenos Aires: Hammurabi, 2020. p. 41.

O fato de serem constitutivas do denominado *corpo de delito* as submete ao regime legal previsto de longa data no direito brasileiro, de acordo com o disposto no art. 158 do Código de Processo Penal (CPP), leito onde o estatuto da cadeia de custódia veio a repousar pela via da Lei 13.964/2019.

Com efeito, o direito brasileiro contempla a determinação do corpo de delito por meio de perícia, nos casos em que a conduta deixa vestígios. Era assim à luz das regras originais do CPP de 1941 e isso se tornou incontroverso após a minirreforma do processo penal, em 2008, por meio da edição da Lei 11.690.

Entre as alternativas possíveis – sistema de perícia de partes e sistema oficial de perícias – o processo penal brasileiro optou pelo segundo e o aperfeiçoou, facultando aos interessados (durante a investigação criminal) e às partes (ao longo do processo) a constituição de assistentes técnicos.

O modelo de perícia oficial cumpre função de garantia fundamental no contexto da prova digital, mas é imprescindível rematar aqui que a cadeia de custódia dos elementos probatórios é uma consequência inevitável e obrigatória do paradigma escolhido, porque a etapa prévia de acertamento do fato é dependente da segurança na preservação dos vestígios.

Violada a cadeia de custódia do elemento probatório, não é mais possível assegurar a autenticidade da prova e sua integridade, sendo a prova inadmissível e, pois, insuscetível de exame de peso ou força probatória.

Isso é assim na hipótese de violação da cadeia de custódia de armas, drogas ou quaisquer outros vestígios, incluindo os elementos digitais, elementos probatórios insuscetíveis de valoração ainda que a título de corroboração por outras provas. Trata-se de atividades probatórias funcionalmente distintas e inconfundíveis.

Favorecerá o entendimento do tema relembrar as lições de João Mendes de Almeida Junior sobre a amplitude do objeto que caracteriza o *corpo de delito* por certo.[39]

Não há dúvida de que a cadeia de custódia é condição de procedibilidade do exame de corpo de delito. Por isso, como mencionado, no Brasil o instituto mereceu ser regulado pela Lei 13.964/2019 no art. 158-A-F do CPP.

Devem ser extraídas consequências jurídicas incontornáveis, próprias e adequadas às hipóteses de proibição probatória, pois que o elemento probatório afetado pela violação da cadeia de custódia é insuscetível de valoração.

Assim é que as provas diretamente derivadas destes elementos em tese manipuláveis, inseguros quanto à autenticidade e integridade, são contaminadas pela ilicitude que deriva das que resultaram da violação da cadeia de custódia.

Este é o *quinto aspecto* a ser levado em conta no presente estudo. As provas que hajam derivado das informações em tese obtidas sem que tenham sido instauradas ou adequadamente preservadas as cadeias de custódia respectivas também não podem ser valoradas porque contaminadas pela mesma ilicitude da fonte.

39. ALMEIDA JUNIOR, João Mendes de. *O Processo Criminal Brazileiro*. 3. ed. Rio de Janeiro: Typ. Baptista de Souza, 1920. v. II, p. 9-11 e 16, com menção, para a ação penal, à imprescindibilidade do exame de corpo de delito nos crimes que deixam vestígios.

3.2. A investigação digital e a prova digital: segurança e autenticidade sob controle na primeira etapa da persecução penal

Ao lecionar sobre a "prova tangível", no clássico livro sobre análise da prova, Terence Anderson, David Schum e William Twining indicam que estas «provas tangíveis» nem sempre são o que parecem ser. Por isso, acrescentam os autores, coloca-se a questão da credibilidade da prova tangível, a ser considerada, entre outros aspectos, pelo viés da autenticidade.[40]

Com base na experiência jurídica norte-americana Anderson, Schum e Twining, pelo que compreendo, sustentam duas formas cumulativas de determinação da autenticidade da prova: a aplicação da regra 901 das *Federal Rules of Evidence* (FRE),[41] que estabelece para a parte que propõe introduzir a prova que ofereça respaldos para que seja assumida a autenticidade do elemento probatório; e a cadeia de custódia da prova, que previne manipulações intencionais ou imprudentes do referido elemento que alterem a informação que ele veicula.[42]

40. ANDERSON, Terence; SCHUM, David; TWINING, William. *Análisis de la prueba*. Trad. coord. por Flavia Carbonell y Claudio Agüero. Madrid: Marcial Pons, 2015. p. 99.
41. "Regra 901. Autenticação ou identificação de provas (a) Em geral. Para satisfazer a exigência de autenticação ou identificação de um item de prova, o proponente deve produzir prova suficiente para sustentar a conclusão de que o item é o que o proponente alega ser. (b) Exemplos. A seguir são apresentados apenas exemplos – não uma lista completa – de provas que satisfaçam a exigência: (1) *Depoimento de uma Testemunha com Conhecimento.* Depoimento de que um item é o que se afirma ser. (2) *Opinião de um "não-especialista" sobre a caligrafia.* A opinião de um não-especialista de que a caligrafia é genuína, baseada em uma familiaridade com ela que não foi adquirida para o litígio atual. (3) *Comparação por uma Testemunha Perita ou pelo Juiz [trier of fact].* Uma comparação com um espécime autenticado por uma testemunha perita ou pelo juiz [trier of fact]. (4) *Características distintivas e semelhantes.* A aparência, conteúdo, substância, padrões internos ou outras características distintivas do item, consideradas em conjunto com todas as circunstâncias. (5) *Opinião sobre uma Voz.* Uma opinião que identifica a voz de uma pessoa – seja ouvida em primeira mão ou através de transmissão ou gravação mecânica ou eletrônica – com base na audição da voz a qualquer momento, em circunstâncias que a liguem ao suposto orador. (6) *Prova sobre uma conversação telefônica.* Para uma conversa telefônica, prova de que foi feita uma chamada para o número atribuído no momento para: (A) uma determinada pessoa, se as circunstâncias, incluindo autoidentificação, mostrarem que a pessoa que atende foi a chamada; ou (B) um determinado negócio, se a chamada foi feita para um negócio e a chamada era relativa a negócio razoavelmente transacionado pelo telefone. (7) *Provas sobre os registros públicos.* Prova de que: (A) um documento foi registrado ou arquivado em um escritório público como autorizado por lei; ou (B) um suposto registro ou declaração pública é do escritório onde itens deste tipo são mantidos. (8) *Prova sobre documentos antigos ou compilações de dados.* Para um documento ou compilação de dados, prova de que o mesmo: (A) está em uma condição que não cria nenhuma suspeita sobre sua autenticidade; (B) estava em um lugar onde, se autêntico, provavelmente estaria; e (C) tem pelo menos 20 anos de idade quando apresentado. (9) Prova *sobre um processo ou sistema.* Prova descrevendo um processo ou sistema e mostrando que ele produz um resultado preciso. (10) *Métodos Fornecidos por um Estatuto ou Regra.* Qualquer método de autenticação ou identificação permitido por um estatuto federal ou por uma regra prescrita pela Suprema Corte." Tradução livre. ESTADOS UNIDOS. Federal Rules of Evidence. Rule 901. Authenticating or Identifying Evidence. Data da última alteração até o momento: 1º de dezembro de 2020. Disponível em: [www.law.cornell.edu/rules/fre/rule_901]. Acesso em: 30.06.2021.
42. ANDERSON, Terence; SCHUM, David; TWINING, William. *Análisis de la prueba*. Trad. coord. por Flavia Carbonell y Claudio Agüero. Madrid: Marcial Pons, 2015. p. 99.

Salientam os citados autores que a opinião expressada por *experts*, convocados a examinar determinado elemento probatório, dependerá dos atributos de credibilidade do próprio elemento.

Não há aqui uma cisão jurídico-prática entre a perícia, que é o exame de corpo de delito, e a condição de possibilidade da perícia em si, que depende da autenticidade e integridade do elemento probatório que será examinado.

Assim, quando o art. 158 do CPP assinala que "[quando] a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado", o pressuposto é de que o exame será realizado sobre *os vestígios*, garantida a sua autenticidade e integridade.

Para os antigos, que lidavam com poucas infrações penais – homicídio, lesões, roubo, furto, falsificação de moeda, lesa-majestade etc. – conforme a complexidade da sua época, esta garantia de autenticidade e integridade do elemento probatório vinha associada à inspeção ocular do inquisidor e, aí sim, posteriormente, pelas conclusões do *expert* (médico, engenheiro etc.).

Na atualidade vivenciamos um salto quântico, quer na quantidade de delitos, quer no que toca às distintas e complexas formas de sua execução, quer ainda pelo potencial imenso de manipulação dos vestígios em circunstâncias que tornam impraticável o rastreamento da alteração deliberada do elemento probatório, como adverte Gustavo Badaró em sua análise das chamadas provas digitais.[43]

Nesse sentido a Lei 13.964/2019, que introduziu os arts. 158-A a 158-F do CPP, não inova na matéria.

A integridade e autenticidade do elemento probatório é um pressuposto para o conhecimento do exame do corpo de delito e sua interpretação crítica pelas partes e pelo juiz, independentemente de o CPP recentemente ter passado a exigir a documentação da "história cronológica do vestígio", conforme está claro da leitura do art. 158-A do Código.

Esta história cronológica documentada será variável, consoante são distintas as espécies de vestígios. Isso é assim basicamente porque o processo de coleta deve levar em conta o tipo de vestígio coletado e o método de coleta, armazenamento e transporte e as possibilidades concretas de alteração do elemento probatório em virtude da técnica de coleta, do método de armazenamento e de transporte (terceirizado? etc.) e da proteção do elemento probatório contra a interferência de terceiros enquanto estiver depositado sob a responsabilidade do Estado.

A documentação da história cronológica da custódia do elemento probatório, a demonstrar que muito provavelmente foi cumprido o mandado jurídico de garantia de integridade e autenticidade da prova, não configura um simples relato temporal, mas em atenção à complexidade do elemento probatório cumpre funções relevantes, uma vez que deve descrever:

43. BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. *Boletim IBCCRIM*, ano 29, n. 343, p. 7-9, jun. 2021. Disponível em: [www.ibccrim.org.br/publicacoes/edicoes/747/8544]. Acesso em: 29.06.2021.

a) os protocolos de coleta/extração do dado, de sorte a comprovar que não houve supressão, inclusão ou alteração de elementos que afete a qualidade de "prova autêntica e íntegra", em atenção ao princípio da "mesmidade"; b) os cuidados que foram adotados, voltados à transparência do processo anterior, que igualmente demonstrem que houve controle por terceiros da coleta/extração, acondicionamento, transporte e preservação do elemento probatório, isso em reverência ao princípio da "desconfiança"; c) a cadeia de pessoas que tiveram contato com o elemento probatório e os respectivos títulos e motivos, se funcionário público ou terceiro à administração, se para transporte ou exame do vestígio etc.

Nesse sentido, no caso concreto, os esclarecimentos adicionais prestados pelo *expert* constituído pela parte informam acerca da não adoção dos protocolos de correta e adequada aquisição de elementos digitais no momento da realização da busca e apreensão e mesmo posteriormente, quando realizadas as perícias.

Como sublinhei desde o prólogo do parecer, a cadeia de custódia das provas digitais sequer foi instaurada oportunamente no caso concreto.

E a cadeia de custódia da prova como método é a um tempo garantia e condição de possibilidade do exame de corpo de delito à luz do conjunto de direitos que caracterizam o devido processo legal.

Pelo ângulo da defesa, no processo criminal, não há dúvida que sendo o conjunto probatório essencial para a superação do estado de incerteza imposto pela presunção de inocência, é correta a conclusão de Álvarez Buján e Gustavo Badaró, para as provas digitais, de que em um sistema que respeite a presunção de inocência esta ficará afetada, "devendo a prova [digital] ser destituída de valor probatório".[44]

Caio Badaró Massena também ressalta a ilogicidade de se trabalhar em um nível de insegurança jurídico-epistêmica provocado pela violação da cadeia de custódia da prova.

Vale observar o que salienta o autor:

> "fato é que nenhuma delas permite a conclusão, não raro adotada pelos juízes e tribunais, de deixar a análise da observância da cadeia de custódia integralmente para a sentença: quem defende a inadmissibilidade entende que a análise da demonstração da integridade da prova deve ser feita logo ao momento da conformação do conjunto probatório; por sua vez, quem defende a admissibilidade entende que a apreciação do grau de contaminação da prova deve ser resolvida no momento posterior da valoração. Mas fato é que nem mesmo a partir dessa segunda construção se pode anuir com a insegurança de se descobrir apenas ao fim do processo se a prova foi considerada íntegra ou com sua cadeia de custódia não demonstrada pela acusação. Até porque, embora a sentença seja a decisão que dá sentido à unidade do procedimento, não custa lembrar que esta não é a única decisão judicial sobre os fatos tomada durante todo o procedimento/processo penal."[45]

44. BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. *Boletim IBCCRIM*, ano 29, n. 343, jun. 2021. p. 9. Disponível em: [www.ibccrim.org.br/publicacoes/edicoes/747/8544]. Acesso em: 29.06.2021.

45. BADARÓ MASSENA, Caio; MATIDA, Janaina. Exame da cadeia de custódia é prejudicial a todas as decisões sobre fatos. *Revista Consultor Jurídico*. 13 ago. 2021. Disponível em: [www.conjur.com.

Se há consensos nessa matéria, dois sobrelevam os demais: os vestígios digitais são voláteis; e sua apreensão e análise demandam a aplicação das melhores práticas (*best practices*) por profissionais altamente capacitados.

Ana Di Iorio, em alentado estudo sobre os protocolos de preservação da prova digital, assevera que os cuidados específicos reclamados em âmbito internacional para este tipo de prova consideram o propósito de "evitar a contaminação da prova", em geral resultante de atuação indevidas de identificação, aquisição e preservação da prova digital, cumprindo "minimizar a manipulação da prova digital", "documentar qualquer ação que implique mudança irreversível" na mencionada prova, separar rigidamente a função pericial de quaisquer outras associadas à investigação digital ("Não atuar além de suas competências e não tomar decisões sem a autorização correspondente") e, vale salientar, "aderir às regulações e leis locais".[46]

O "controle da cadeia de custódia", sublinha Di Iorio, configura uma "série de cuidados destinados a traçar a origem, identidade e integridade da prova para que esta não se perca, seja destruída ou alterada".[47]

Daí, conclui a Diretora do InfoLab do Ministério Público da Província de Buenos Aires que para a intervenção sobre a prova é imprescindível a adoção de protocolo específico, formado pelo "conjunto de regras estabelecidas por norma ou costume que detalhem o processo de *atuação científica*, técnica, médica etc." (grifo nosso).[48]

E entre os princípios gerais de manejo da prova digital Di Iorio aponta a necessidade de atuação do "informático forense", distinguindo-se na investigação digital os papéis de assessoramento, investigação e perícia.[49]

Com efeito, na linha do mencionado consenso acerca das boas práticas relativas à prova digital, o jurista italiano Silvio Marco Guarriello define algumas premissas que socorrem o entendimento do caráter cogente das regras brasileiras sobre a cadeia de custódia das provas.

Em primeiro lugar, Guarriello situa as provas produzidas no contexto das investigações digitais no gênero das "provas científicas". Como já mencionado, as características das atividades periciais em questão, das *computer forensics* e *digital forensics*, sublinha Guarriello,

---

br/2021-ago-13/limite-penal-exame-cadeia-custodia-prejudicial-todas-decisoes-fatos]. Acesso em: 17.06.2023.

46. DI IORIO, Ana. Protocolos de preservación de evidencia digital y cuestiones forenses. In: DUPUY, Daniela (Dir.); KIEFER, Mariana (Coord.). *Cibercrimen II*. Buenos Aires-Montevideo: Editorial B de F, 2018. p. 341-343.
47. Tradução livre. DI IORIO, Ana. Protocolos de preservación de evidencia digital y cuestiones forenses. In: DUPUY, Daniela (Dir.); KIEFER, Mariana (Coord.). *Cibercrimen II*. Buenos Aires-Montevideo: Editorial B de F, 2018. p. 344.
48. Tradução livre. DI IORIO, Ana. Protocolos de preservación de evidencia digital y cuestiones forenses. In: DUPUY, Daniela (Dir.); KIEFER, Mariana (Coord.). *Cibercrimen II*. Buenos Aires-Montevideo: Editorial B de F, 2018. p. 345.
49. DI IORIO, Ana. Protocolos de preservación de evidencia digital y cuestiones forenses. In: DUPUY, Daniela (Dir.); KIEFER, Mariana (Coord.). *Cibercrimen II*. Buenos Aires-Montevideo: Editorial B de F, 2018. p. 348.

as localizam na sede da prova científica informático-digital que emprega técnicas "da melhor ciência e experiência".[50]

O autor – como os e as demais – ressalta a natureza volátil dos elementos probatórios digitais a impor rigoroso estatuto que considere a natureza dessa prova e a necessidade de assegurar a sua integridade e autenticidade (não alteração).

Na lição compartilhada pelo magistrado italiano, professor da Universidade de Campania L. Vanvitelli, trata-se de uma "atividade investigativa técnico-científica" que tem por objeto prova digital "constituída em um 'ambiente' particular cujos elementos são imateriais e sujeitos a modificação".[51]

Acrescenta Guarriello que a complexidade da prova digital é agravada pelo estado de permanente transformação tecnológica e pelas características do "ambiente digital". A volatilidade do elemento probatório digital, acentua, resulta da pouca *estabilidade* e definitividade dos dados digitais.[52]

Por essa razão é imprescindível que o *expert* responsável pela produção da prova digital seja um perito forense "com especialização técnico-científica elevada e confiável, constantemente atualizado em relação aos métodos de análise das provas digitais".[53]

O consenso sobre a natureza complexa da "investigação digital" e o caráter técnico da respectiva intervenção probatória, em uma era claramente digital, reforçam a compreensão de que a tutela jurídica incidente na hipótese não está apenas orientada à privacidade, intimidade e direitos gerais de personalidade.

Mais ainda, e neste ponto convergem o direito processual penal e a epistemologia, o avanço da digitalização da vida repercute na persecução penal de sorte a convertê-la em uma persecução penal digital.

O efeito prático dessa conversão, ditada pelas tantas vezes já acentuadas características dos elementos probatórios digitais, consiste em atribuir à primeira fase da persecução penal digital uma função bastante específica: a de ser a etapa procedimental responsável pelo recolhimento – recolha, diriam os portugueses – dos vestígios digitais, sua organização, preservação e análise de modo a apoiar o exercício futuro da ação penal na hipótese de se comprovar a justa causa.

Esta função específica – de aquisição, preservação e análise dos vestígios digitais – transforma a primeira etapa da persecução penal digital em uma fase sujeita a controles de legalidade que condicionam o exercício futuro da acusação e sua admissibilidade no momento em que a denúncia é apresentada em juízo.

50. GUARRIELLO, Silvio Marco. Le best practices in materia di computer forensics. In: LASELLI, Michele (a cura di). *Investigazioni digitali*. Milano: Giuffrè Francis Lefebvre, 2020. p. 77.
51. GUARRIELLO, Silvio Marco. Le best practices in materia di computer forensics. In: LASELLI, Michele (a cura di). *Investigazioni digitali*. Milano: Giuffrè Francis Lefebvre, 2020. p. 79.
52. GUARRIELLO, Silvio Marco. Le best practices in materia di computer forensics. In: LASELLI, Michele (a cura di). *Investigazioni digitali*. Milano: Giuffrè Francis Lefebvre, 2020. p. 80.
53. GUARRIELLO, Silvio Marco. Le best practices in materia di computer forensics. In: LASELLI, Michele (a cura di). *Investigazioni digitali*. Milano: Giuffrè Francis Lefebvre, 2020. p. 80.

A investigação criminal digital assenhora-se de um espaço jurídico-epistemológico próprio, inconfundível com o que é pertinente ao processo de conhecimento condenatório.

Entendo que nestes termos é válida a conceituação de investigação digital proposta por Brighi e Ferrazzano:

> "Investigações digitais são definidas como o 'uso de métodos cientificamente derivados e comprovados para a identificação, coleta, transporte, armazenamento, análise, interpretação, apresentação, distribuição, devolução e/ou destruição de prova digital derivada de fontes digitais, preservando a prova digital e mantendo a cadeia de custódia' (ISO/IEC 27043). Compõe-se de várias etapas e duas fases principais."[54]

Os autores italianos desdobram a própria investigação digital em duas etapas: a do processo de aquisição dos vestígios digitais e a posterior, que envolve a análise técnico-científica desses vestígios.[55]

Conforme defendem corretamente, a primeira etapa da investigação digital consiste na identificação, coleta, aquisição e preservação do "potencial vestígio digital", enquanto a segunda etapa concerne à análise do elemento probatório digital, a interpretação dos resultados da mencionada análise, a emissão do laudo e a apresentação desses resultados em juízo, com a indicação precisa das ferramentas e métodos empregados.[56]

Cada fase da investigação digital, lecionam Brighi e Ferrazzano, deve observar criteriosamente as próprias etapas sequenciais requisitadas pela natureza dos vestígios que formam o objeto da pesquisa criminalística.[57]

54. Tradução livre. BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. In: CAIANIELLO, Michele; CAMON, Alberto (Ed.). *Digital forensic evidence*: towards common European standards in antifraud administrative and criminal investigations. Milano: CEDAM, 2021. p. 33.
55. BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. In: CAIANIELLO, Michele; CAMON, Alberto (Ed.). *Digital forensic evidence*: towards common European standards in antifraud administrative and criminal investigations. Milano: CEDAM, 2021. p. 34.
56. BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. In: CAIANIELLO, Michele; CAMON, Alberto (ed.). *Digital forensic evidence*: towards common European standards in antifraud administrative and criminal investigations. Milano: Cedam, 2021. p. 34.
57. BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. In: CAIANIELLO, Michele; CAMON, Alberto (Ed.). *Digital forensic evidence*: towards common European standards in antifraud administrative and criminal investigations. Milano: Cedam, 2021. p. 34.

Figura I: Processo de investigação digital[58]

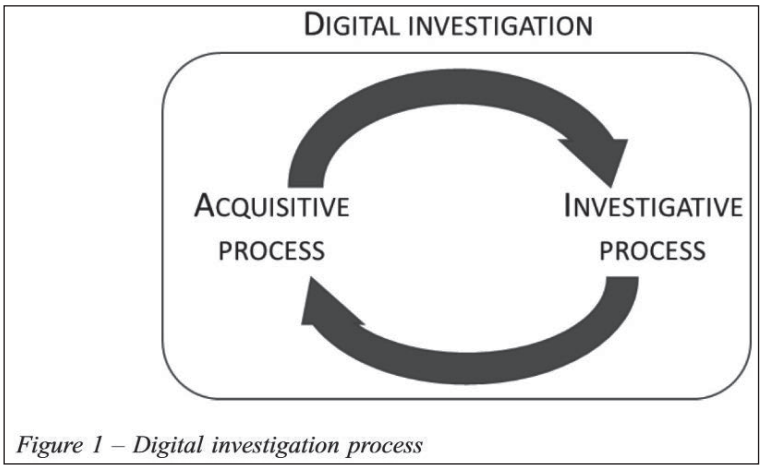

Figure 1 – Digital investigation process

Figura II: Principais fases da investigação digital[59]

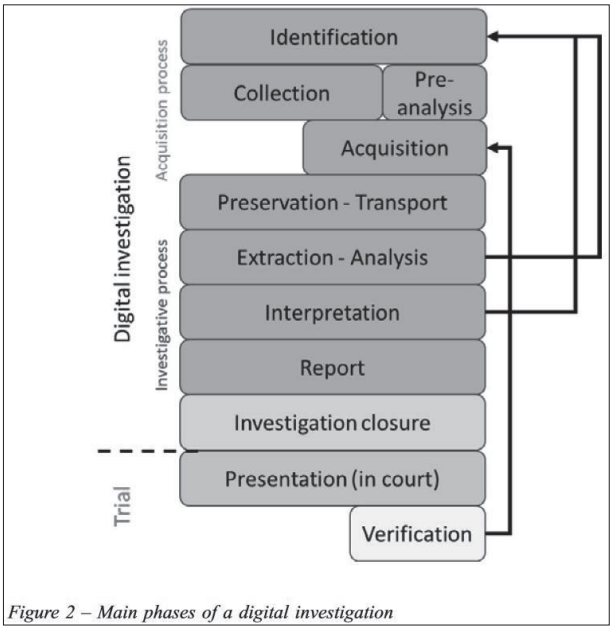

Figure 2 – Main phases of a digital investigation

58. BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. In: CAIANIELLO, Michele; CAMON, Alberto (Ed.). *Digital forensic evidence*: towards common European standards in antifraud administrative and criminal investigations. Milano: Cedam, 2021. p. 34.
59. BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. In: CAIANIELLO, Michele; CAMON, Alberto (Ed.). *Digital forensic evidence*: towards common European standards in antifraud administrative and criminal investigations. Milano: Cedam, 2021. p. 35.

Assim compreendida a função da investigação digital, lógica e juridicamente não há como se sustentar que os controles exercidos sobre o pressuposto da prova digital – a segurança sobre seus elementos formativos – possam ser *fundidos* com a *análise de resultado*.

Não custa recordar que do ponto de vista pericial o *resultado* é uma conclusão matemática acerca da sequência binária de *bits* que constitui o arquivo digital e não a imagem que nós, como leigos, enxergamos como a aplicação prática dessa sequência.

Nós vemos uma *imagem* que pode ou não ter sido manipulada e interpretamos *essa imagem*. Se a imagem foi manipulada de sorte a nos levar a uma *representação* distinta da que corresponderia à imagem originalmente capturada pelo dispositivo digital, nossa percepção leiga é incapaz de discernir a manipulação. E nossa conclusão – interpretação da *representação* da imagem, som, texto etc. – terá sido artificiosamente conduzida em outra direção.

Proliferam os programas de edição de arquivos de imagens, sons ou textos usados recreativamente por milhões de pessoas no mundo a cada minuto.

Hoje não é mais possível ignorar que um arquivo digital é algo *manipulável*. Daí que não é possível confundir a *imagem* que vemos com a *realidade supostamente retratada*. Ou mesmo a *voz* ou o *texto*...

A possibilidade de manipulação de elementos probatórios digitais concerne ao "entorno digital" dos envolvidos e pode afetar mesmo terceiros, indevidamente inseridos na dinâmica de uma investigação criminal não pautada por critérios éticos ou ainda em virtude de uma contaminação involuntária e acidental dos referidos elementos probatórios digitais.

O episódio suspeito retratado no processo e mencionado pelo culto desembargador relator do *habeas corpus* é significativo, reforçando-se a conclusão pela afirmação incontestável do assistente técnico de que mesmos os arquivos digitais que o magistrado presumiu aptos a demonstrar a justa causa e os preservou da declaração de ilicitude não foram devidamente resguardados por meio da instauração da sua cadeia de custódia.

O que o magistrado do tribunal regional identificou como *equívoco*, *engano* reconhecido pelo Ministério Público Federal (MPF) consistente em atribuir a N. C. dispositivos digitais não apreendidos, é, na verdade, a constatação da "não adoção dos protocolos de constituição da prova digital" relativamente a *todo o material* hipoteticamente apreendido na diligência ordenada pela juíza estadual.

Nenhuma afirmação de validade jurídica da prova digital pode ser formulada no presente caso porque a *formação da prova digital* é dependente da instauração de sua cadeia de custódia, o que não ocorreu.

A alegação de que N. C. admitiu que eram seus os dispositivos digitais apreendidos e hipoteticamente examinados pelos peritos estaduais e pelo perito federal não supre a necessidade legal e epistêmica de instauração da cadeia de custódia tanto dos equipamentos como dos arquivos.

N. C. perdeu o domínio sobre dispositivos eletrônicos e arquivos digitais no momento em que foi executada a diligência de busca e apreensão. A partir desse instante a responsabilidade pela tutela da integridade do sistema digital foi transferida aos agentes estatais, que deveriam ter instaurado as respectivas cadeias de custódia conforme os sobejamente conhecidos protocolos da prova digital.

As inconsistências verificadas pelo tribunal federal e mais amplamente pelo assistente técnico, sem embargo de o perito federal ter constatado que não havia cadeia de custódia instaurada quanto ao material que lhe foi enviado, demonstram a falta de tutela da integridade do sistema digital.

E a tutela da integridade do sistema digital aparece como premissa de qualquer juízo fático da espécie que esteja na base de um modelo de justiça criminal que fundamente a persecução penal na busca da verdade.

Ademais, hoje se reconhece o caráter fundamental do direito à proteção de dados, consoante preconiza o inc. LXXIX, do art. 5º da Constituição da República (CRFB), assim como o inciso XXVI do art. 21 e o XXX do art. 22, incorporados pela EC 115, de 2022.

Vale reproduzir os dispositivos citados:

> "Art. 5º, CRFB: [...] LXXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais."
>
> "Art. 21, CRFB. Compete à União: [...] XXVI – organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei."
>
> "Art. 22, CRFB. Compete privativamente à União legislar sobre: [...] XXX – proteção e tratamento de dados pessoais."

Dada a multiplicidade de elementos probatórios que produzem vestígios materiais ou digitais, alguns dos quais resultantes da limitação concreta de bens jurídicos de terceiros individualizáveis e até de coletividades ou grupos difusos de pessoas, e a variedade de empregos de um mesmo elemento probatório em contextos díspares, alguns dos quais não necessariamente apenas processuais, não me parece possível, portanto, limitar à presunção de inocência o fundamento da cadeia de custódia.

Creio que a cadeia de custódia das provas está mais bem abrigada na ampla cláusula do devido processo legal, quer por sua dimensão procedimental, dimensão que convive com a presunção de inocência, o contraditório e o direito de defesa, quer à vista de sua vertente material, que por sua vez configura obstáculo à incriminação generalizada e ilegal.

De toda maneira, é a raiz constitucional mesma da limitação do poder punitivo que tem na cadeia de custódia das provas uma concretização independente e anterior ao regramento da sua documentação, instituído pela lei de 2019.

É possível que a cadeia de custódia das provas tenha sido rompida ou não preservada – vale lembrar, trata-se de um conceito epistêmico e jurídico, e não de uma *coisa real* – em casos anteriores à entrada em vigor da Lei 13.964/19, resultando na inadmissibilidade do elemento probatório que não goza da chancela da "mesmidade" e daquela que resulta da aferição e controle do emprego dos métodos atinentes a este singular elemento.

Ao disciplinar "a cadeia de custódia das provas" no CPP, o legislador tão somente incorporou à lei processual protocolos gerais que historiam todo o processo de ingresso e ampla preservação da prova no âmbito da persecução penal, sem, todavia, interferir nas técnicas que de fato a caracterizam.

E isso é perfeitamente compreensível. Na segunda edição do livro sobre a cadeia de custódia das provas no processo penal mencionei o universo de protocolos do gênero existentes

no Brasil, que reclamam tratamento harmônico. Sem embargo, quando se trata de prova digital, como é o caso do presente estudo, as indicações dos arts. 158-A a 158-F do CPP são necessárias, mas não suficientes.

Relembre-se que, em se tratando de provas digitais, com frequência a prática cobra a definição de duas distintas cadeias de custódia: a do dispositivo digital (hardware – sistemas de armazenamento) e a de seu conteúdo (arquivos, programas etc.).

A verificação do estado dos dispositivos digitais e o processo de extração dos dados e de sua transferência para algum dispositivo hoje claramente não são consideradas ações que para fins probatórios possam ser levadas a cabo sem controle e sem a descrição da técnica fiável de migração do dado eletrônico, seja ele som ou imagem, ou ambos, com a correta datação e constatação de que o equipamento de origem está aferido e é igualmente fiável também no tocante aos metadados.

A volatilidade da prova digital é de quase impossível detecção e à semelhança da prova de DNA manipulada, a inversão do ônus da prova para exigir dos acusados que demonstrem o dano causado por eventual modificação intencional dos dados consistiria na temível "prova diabólica", isto é, naquela inatendível.

Como salienta Álvarez Buján, sobre a prova do DNA, que compartilha com a prova digital esta condição de quase não rastreabilidade, se a prova defensiva pudesse ser realizada o seria,[60] mas na enorme maioria dos casos – e este não é diferente – isso é impossível, tomando a aparência o lugar da verdade.

Aqui sequer é necessário argumentar que a inversão do ônus da prova viola a presunção de inocência.

As providências previstas nos arts. 158-A a 158-F do CPP não são regras processuais penais em sentido estrito, mas apenas explicitam protocolos historiadores da cadeia de custódia da prova, esta sim um instituto processual penal.

Reitere-se que esta, como método de garantia da autenticidade e integridade do elemento probatório, é parte fundamental da "doutrina do corpo de delito", que considera essencial determinar o corpo de delito revelado por vestígios materiais ou digitais pelo emprego de práticas e técnicas que lhe confiram certeza jurídica e epistêmica.

O que vai significar este "corpo de delito" no contexto do debate processual em contraditório é assunto para a valoração da prova (se houve crime, se o fato estava justificado etc.). O "corpo de delito" como ponto de partida, porém, deve passar no teste da fiabilidade probatória para ser admitido como prova no processo.

Seguramente o caso concreto permite que se vá mais além no que se refere à segurança epistêmica exigida quanto às provas digitais.

O fato de o acesso às informações decorrer da incorporação de elementos probatórios digitais em tese obtidos por meio de busca e apreensão requisita um refinamento daquela distinção entre as duas distintas cadeias de custódia – a do dispositivo digital (hardware – sistemas de armazenamento) e a de seu conteúdo (arquivos, programas etc.) – que a mera referência a "sistemas de armazenamento" não dá conta sem maiores explicações.

60. ÁLVAREZ BUJÁN, María Victoria. *La prueba de ADN como prueba científica.* Su Virtualidad Jurídico-Procesal. Valencia: Tirant lo Blanch, 2018. p. 448.

Por este ângulo Federico Bueno de Mata ressalta que uma distinção baseada em "suportes" já não atende à realidade das tecnologias ordinariamente em uso. Não se trata de falar apenas em "suporte físico" e "suporte imaterial", e sim em "canais ou vias pelas quais estas provas podem transitar para incorporar-se ao processo."[61]

E Bueno da Mata ilustra o fato com o exemplo dos elementos digitais armazenados nas nuvens, *in the cloud*, salientando que a já clássica distinção baseada em suportes foi elaborada "sem ter em conta todo o sistema de *cloud computing* e que, portanto, faz com que muita informação fique localizada na nuvem sem necessidade de passar a formato físico."[62]

Apesar de que imagens em tese são *canalizadas* para um formato digital, a identidade com as informações digitais *in the cloud* decorre da impossível rastreabilidade daquelas à origem, porque esta é a transmissão da imagem em seu tempo presente, e a quase não rastreabilidade da prova digital *in the cloud*, criptografada e difusa e pelos dispositivos de armazenamento do provedor.

O autor da Universidade de Salamanca recorre à definição de "prova digital" adotada pelo Instituto Nacional de Tecnologias de Comunicação da Espanha (INTECO), posto nestes termos, realçando o binômio *software-hardware* que é peculiar a certos elementos probatórios digitais:

> "datos que de manera digital se encuentran almacenados o fueran transmitidos mediante equipos informáticos y que son recolectados mediante herramientas técnicas especializadas empleadas por un perito en una investigación informática. Tienen la función de servir como prueba física, por encontrarse dentro de un soporte, de carácter intangible (no modificables) en las investigaciones informáticas."[63]

Não há dúvida, e neste ponto coincido com Bueno da Mata, que a especialidade da "prova digital" resulta de que necessariamente é composta por um "*elemento técnico* que fará referência bem a um *hardware* em sede judicial ou bem a um canal eletrônico quando se apresente por meio de um sistema de gestão informatizado" e por um "*elemento lógico* ou *software* que terá natureza intangível"[64] (grifos nossos).

Com efeito, é indispensável entender que a *e-evidence*, prova eletrônica ou prova digital se caracteriza por ser "qualquer classe de informação (dados) que tenha sido produzida, armazenada ou transmitida por meios eletrônicos".[65]

---

61. BUENO DE MATA, Federico. *Las Diligencias de Investigación Penal en la Cuarta Revolución Industrial*: principios teóricos y problemas prácticos. Navarra: Aranzadi, 2019. p. 132-133.
62. BUENO DE MATA, Federico. *Las Diligencias de Investigación Penal en la Cuarta Revolución Industrial*: principios teóricos y problemas prácticos. Navarra: Aranzadi, 2019. p. 133.
63. BUENO DE MATA, Federico. *Las Diligencias de Investigación Penal en la Cuarta Revolución Industrial*: principios teóricos y problemas prácticos. Navarra: Aranzadi, 2019. p. 133.
64. BUENO DE MATA, Federico. *Las Diligencias de Investigación Penal en la Cuarta Revolución Industrial*: principios teóricos y problemas prácticos. Navarra: Aranzadi, 2019. p. 133.
65. DELGADO MARTÍN, Joaquín. *Judicial-Tech, el proceso digital y la transformación tecnológica de la justicia*: Obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 55.

A variedade de «provas digitais» e sua constante transformação e complexidade reforçam a ideia do caráter indispensável da adoção dos procedimentos corretos para a sua aquisição, preservação, emprego processual e auditabilidade (contraditório efetivo) conforme a espécie de prova digital de que se trata.

Volto a insistir em um ponto que considero crucial: as boas práticas técnicas consolidadas nos protocolos nacionais e internacionais de tratamento das provas digitais *não configuram filigranas jurídicas*, não são meras etapas que possam ser levadas a cabo sem a delimitação de que prática cabe para cada espécie de prova digital.

Não se trata de mera formalidade. Tampouco, na maioria das vezes as técnicas previstas para um modelo de prova podem ser livremente intercambiadas para modelo distinto. Ou ainda, não atende à imperiosidade de instauração da cadeia de custódia a menção ao fato de que o código *hash* foi calculado em relação a determinado «dispositivo», quando não se comprova que este dispositivo é a fonte original da informação digital e não simples cópia.

Na hipótese examinada neste estudo, não há acordo sequer quanto ao número de dispositivos eletrônicos apreendidos. 9, 13, 14?!!!

Anteriormente me referi a "dispositivo" sem distinção de suporte ou canal, *hardware* ou *software*. O fundamento do raciocínio vale para informações de interceptações telefônicas, *in the cloud*, captadas por *drones*, contidos em eletrodomésticos *inteligentes* ou registradas por aparelhos biotecnológicos incorporados ao organismo humano para substituir órgãos humanos disfuncionais, amputados ou definitivamente afetados.

Nada obstante as dificuldades que possam surgir, dada a digitalização da vida, que afeta todas as suas dimensões, é possível buscar alguma sistematização a partir das fontes da prova digital, revelando-se, pela mera exposição, o grau de dificuldade da tarefa de preservar a integridade do elemento probatório digital e verificar sua autenticidade, além de determinar o cuidado extremado que se deve ter, haja vista os riscos concretos de manipulação e alteração dos dados.

O tema da "prova digital" é inconfundível com o da liberdade individual e as possibilidades de manipulação e alteração da prova digital, intencionalmente ou por acidente, requerem extremado cuidado no âmbito da jurisdição penal.

Luigi Cuomo, Procurador Substituto Geral na Corte de Cassação italiana, adverte que dadas as características da prova digital, o "baricentro de um processo fundado sobre prova científica se coloca sempre mais na investigação preliminar, no âmbito da qual o dado digital em regra vem adquirido pela polícia judiciária e é sucessivamente analisado pelo pessoal técnico."[66]

Em livro específico sobre a cadeia de custódia de dados digitais, Jacob Heilik destaca a necessidade de autenticação e da demonstração da proveniência desses dados. Pela clareza e importância das observações, reproduz-se o trecho da obra do autor canadense:

> "A proveniência é importante porque fornece uma ligação clara entre a informação apresentada e a fonte legalmente adquirida da qual provém. A autenticação é importante para

66. CUOMO, Luigi. La prova digitale. In: CANZIO, Giovanni; DONATI, Luca Lupária (Ed.). P*rova Scientifica e Processo Penale*. 2. ed. Milão: Wolters Kluwer, 2022. p. 629.

> estabelecer que a informação apresentada não foi alterada desde o momento em que foi coletada – ou seja, não é nem mais nem menos do que os dados da fonte original."[67]

Os cuidados de coleta não se confundem com a hipotética autorização espontânea de acesso ao conteúdo digital da mesma maneira que a permissão de acesso a um domicílio é inconfundível com o que fazem os agentes *no* domicílio enquanto lá se encontram.

O rigor no procedimento de coleta da prova digital é condição de validade do elemento probatório desta natureza porque a característica principal deste elemento é sua *volatilidade*, isto é, a sua condição de "elemento manipulável" sem que fiquem rastros dessa manipulação.

Assim é que a exigência de documentação detalhada, precisa e rigorosa de toda a fase de coleta da prova eletrônica é exigida por outros órgãos internacionais, como a *Association of Chief Police Officers* (ACPO), o *National Institute of Standards and Technology* (NIST) e o *Internet Engineering Task Force* (IETF).[68]

Neste sentido, compreende-se a imensa preocupação de legislação e doutrina, em nível internacional, com a preservação da cadeia de custódia da prova digital, inadmitindo-se a prova à vista da demonstração de sua violação.

Vale lançar mão das palavras da Procuradora da República Fernanda Teixeira Souza Domingos:

> "A completude ou a integridade da prova digital é o terceiro requisito de validade das evidências digitais. [...] Técnicas especiais periciais são aptas a identificar a assinatura digital do arquivo ou *hash* de forma a verificar a integralidade da prova. Caso algum bit tenha sido alterado, é como o DNA do arquivo, sua integralidade terá sido violada ou corrompida, não se prestando a ser avaliada em juízo.
>
> A fim de não se comprometer a integralidade da prova digital, seu conteúdo original juntamente com seus *hashes* (assinatura digital) devem ser preservados e efetuada a análise na cópia".[69]

No caso concreto as boas práticas não foram observadas. E as inconsistências não são irrelevantes.

---

67. Tradução livre. HEILIK, Jacob. *Chain of Custody for Digital Data:* A Practitioner's Guide. Canada: Independently published, 2019. p. 16-17.
68. ACPO. *Good Practice Guide for Digital Evidence*. Association of Chief Police Officers of England, Wales & Nothern Ireland. Mar. 2012. p. 6-7. Disponível em: [http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf]. Acesso em: 20.08.2020. NIST. *Guide to Integrating Forensic Techniques into Incident Response*. Karen Kent, Suzanne Chevalier, Tim Grance e Hung Dang. Special Publication 900-86. Ago. 2006. p. 3-4/3-5. Disponível em: [https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf]. Acesso em: 20.08.2020; IETF. *Guidelines for Evidence Collection and Archiving* (RFC 3227). Fev. 2002. p. 5. Disponível em: [https://tools.ietf.org/html/rfc3227]. Acesso em: 20.08.2020.
69. DOMINGOS, Fernanda Teixeira Souza. As provas digitais nos delitos de pornografia infantil na internet. In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro (Org.). *A prova no enfrentamento à macrocriminalidade*. 3. ed. Salvador: JusPodivm, 2015. p. 197.

Não há sequer como saber com segurança se o perito federal examinou dispositivos e arquivos originais porque estes não estavam custodiados. Em outras palavras, a autoridade policial, por razões desconhecidas, não instaurou a cadeia de custódia, apesar da normativa vigente desde 2013.

O que parece evidente, no caso concreto, é que a formação da prova digital se apartou por completo da fórmula citada pelas autoras e autores referidos ao longo do presente estudo, que defendem que a constituição dessa prova é da ordem da perícia, e não da *polícia*.

Não se trata de preservar um cadáver, o mantendo intocado até a chegada da perícia ao local e o disponibilizando da mesma maneira aos *experts* do Instituto Médico Legal.

No exemplo do cadáver a teórica separação entre "suporte" e "elementos ou informações de natureza probatória que estão no corpo" é visível e mais facilmente identificável. O desdobramento cronológico entre aquisição e formação da prova em geral permite constatar se foi respeitada a intangibilidade do cadáver e detectar eventual não instauração ou preservação da sua cadeia de custódia.

No caso das informações digitais, a não aplicação dos protocolos de 2013 obstou a constituição da cadeia de custódia das provas, porque em realidade os peritos oficiais terminam trabalhando sem a segurança imprescindível de que o material examinado pudesse corresponder *integralmente* e de *forma autêntica* aos elementos probatórios originais.

Para a validade jurídica da prova não basta calcular o código *hash* da cópia entregue ao perito federal.

Com base na análise ofertada pelo *expert* contratado pela Defesa, o que se constata é que a instauração da cadeia de custódia das provas digitais não se configurou e por isso não é possível certificar a fiabilidade probatória do material empregado na denúncia.

O laudo do assistente técnico indicia mesmo uma manipulação de dispositivos eletrônicos após a apreensão judicial que não permite que se descarte a interpretação de que arquivos não originais passaram a fazer parte do material examinado.

É incompreensível e inexplicável a enorme discrepância entre a quantidade de arquivos de imagem identificados por um e outro peritos estaduais.

Observe-se que em paralelo com as "normas penais em branco", aquelas tratadas pelos preceitos dispositivos dos arts. 158-A e 158-F do CPP funcionam como "normas processuais penais em branco", como compreendeu o Superior Tribunal de Justiça no paradigmático julgamento da sua 5ª Turma.[70]

E a consequência jurídica a ser pronunciada é a mesma: a inadmissibilidade da referida prova.

Não faria sentido o legislador cogitar uma determinada tipicidade probatória (art. 158-A e ss. do CPP), orientada por critérios de segurança epistemológica e jurídica, e assumir de bom grado que o ato probatório valerá e será valorado ao final do processo, apesar de praticado em desconformidade com o modelo legal.

70. Informativo 763 do Superior Tribunal de Justiça, de 14 de fev. de 2023. Agravo Regimental no Habeas Corpus n. 143.169/RJ. 5ª Turma. Rel.: Min. Messod Azulay Neto. Rel. para acórdão: Min. Ribeiro Dantas. Julgamento em: 07 fev. 2023.

A inadmissibilidade de uma prova implica em algo mais que a proibição de emprego de meio de prova ou do meio de obtenção de prova. O juízo de inadmissibilidade pretende de forma especial que o destinatário da prova para o fim de decidir não tenha efetivo contato com o elemento probatório inidôneo.

O "não conhecimento" é da essência da "*admissibility*" e da "*exclusion*", sendo imprescindível a exclusão para prevenir o efeito de contaminação psicológica que mesmo provas com baixo grau de sustentação empírica podem produzir.[71]

Em trabalho clássico sobre a prova no direito processo penal brasileiro, Antonio Magalhães Gomes Filho destaca que "ao *direito à prova* corresponde, como verso da mesma medalha, um *direito à exclusão* das provas que contrariem o ordenamento"[72].

Na mesma obra, o professor titular da Universidade de São Paulo adverte para o fato de que a manifestação primeira do direito à participação contraditória nas atividades probatórias consiste na faculdade que deve ser assegurada às partes de dialogar a respeito da admissão das provas.[73]

Por óbvio, seria inútil conferir à defesa este direito se porventura fosse permitido ao magistrado simplesmente evitar decidir sobre a questão da admissibilidade, tratando toda matéria como questão de valoração.

Valorar prova a que faltam os requisitos da integridade e autenticidade leva à emissão de sentença e acórdão que, tomando por certo o conhecido, mas ignorando se este conhecido está completo ou foi modificado, pode levar a que preferira a versão à verdade. Não se deve esquecer que a versão de um fato é a visão parcial desse fato.

A qualidade da decisão penal é a meta a ser perseguida, pois dela dependerá a justiça da solução que o Estado oferece ao caso.

A medida desta qualidade, cumpre acentuar, é aferida: a) pela compatibilidade dos procedimentos, entre eles o probatório, ao estado de direito; b) pela definição do Ministério Público como sujeito processual protagonista da ação penal – e não mais o juiz –; c) pela afirmação categórica da principal função judicial como sendo de custódia do complexo dispositivo de construção da decisão penal; d) e, por fim, pela identificação e delimitação dos métodos de demonstração empírica do fundamento das alegações das partes.

Por este ângulo, e seguindo tendência de aproximação dos modelos jurídicos, cabe extrair dos novos princípios do direito probatório, no âmbito do processo penal brasileiro, regra semelhante àquela que, nas *Federal Rules of Evidence (FRE)*, nos Estados Unidos da América, está prevista na Seção IV: a da melhor prova para determinar o fato, como exigência para a acusação ultrapassar a presunção de inocência.[74]

---

71. JACKSON, John D.; SUMMERS, Sarah J. *The Internationalisation of Criminal Evidence*: beyond the common law and civil law traditions. Nova Iorque, Cambridge: Cambridge University Press, 2012. p. 72.
72. GOMES FILHO, Antonio Magalhães. *Direito à prova no processo penal*. São Paulo: Ed. RT, 1997. p. 93.
73. GOMES FILHO, Antonio Magalhães. *Direito à prova no processo penal*. São Paulo: Ed. RT, 1997. p. 173.
74. Vide: COLOMER, Juan-Luis (Coord.). *Introducción al proceso penal federal de los Estados Unidos de Norteamérica*. Valencia: Tirant lo Blanch, 2013. p. 356-357.

Como sublinhou Alberto Binder, a tarefa de construção da verdade no processo penal, sob o estado de direito, está ordenada por meio de requisitos de verificação dos fatos da causa, conforme standards probatórios ("regras orientadoras fortes") que tenham a capacidade de limitar a discricionariedade, em um procedimento complexo que precede a tomada de decisão, de acordo com diferentes etapas e dimensões, a saber: a análise da legalidade da prova, a determinação de sua pertinência e utilidade, o "peso" das distintas proposições e a construção do relato judicial de justificação da escolha procedida.[75]

Por este ângulo, nos dias atuais processo civil e processo penal se aproximam.

Alerta Michele Taruffo que, ao ser adotada uma concepção racional-legal de justiça, o processo judicial está orientado à investigação da verdade possível, pois que "uma reconstrução verídica dos fatos da causa é uma condição necessária da justiça e da legalidade da decisão".[76]

Sublinha o professor italiano que a exigência de busca da verdade dos fatos desponta como condição de veracidade, validade e aceitação da decisão judicial. Segundo este autor, isso recomenda que o conhecimento de circunstâncias relevantes para a decisão recorra quando possível ao emprego de meios científicos, de modo a "reduzir a área na qual o juízo sobre os fatos pode ser formulado somente sobre bases cognoscitivas não científicas".[77]

E arremata: "a influência das provas científicas se apresenta mais amiúde no processo penal".[78]

A indiscutível centralidade da questão de mérito do processo – o fato definido como infração penal atribuído ao acusado – adquire relevância concreta porque no lugar da alegação do crime e da condição de criminoso justificar a condenação de alguém ("direito penal do autor"), será a prova deste fato, produzida em respeito aos mencionados *standards* probatórios ("regras orientadoras fortes"), que legitimará a punição conforme o caso ("direito penal do fato").

A defesa, por sua vez, tem o direito de conhecer a totalidade dos citados elementos informativos para rastrear a legalidade da atividade persecutória e contestar a procedência da pretensão acusatória.

A possibilidade de refutação pela defesa constitui elemento indispensável à validade jurídica de um processo penal estribado na verificação do fato como condição para a punição do acusado.

---

75. BINDER, Alberto. Prólogo. In: SCHIAVO, Nicolás. *Valoración racional de la prueba em materia penal*: un necesario estándar mínimo para La habilitación del juicio de verdad. Buenos Aires: Del Puerto, 2013. p. 9-10. A noção de "regras orientadoras fortes", que são os *standards probatórios*, não é totalmente desconhecida do direito brasileiro. A título de exemplo convém fazer referência ao art. 158 do CPP e a exigência de exame de corpo de delito relativamente aos crimes que deixam vestígios.
76. TARUFFO, Michele. Conocimiento científico y criterios de la prueba judicial. In: ORTEGA GOMERO, Santiago (Dir.). *Proceso, prueba y estándar*. Lima: ARA, 2009. p. 33.
77. TARUFFO, Michele. Conocimiento científico y criterios de la prueba judicial. In: ORTEGA GOMERO, Santiago (Dir.). *Proceso, prueba y estándar*. Lima: ARA, 2009. p. 34-35.
78. TARUFFO, Michele. Conocimiento científico y criterios de la prueba judicial. In: ORTEGA GOMERO, Santiago (Dir.). *Proceso, prueba y estándar*. Lima: ARA, 2009. p. 34-35.

O arco de informações submetidas ao contraditório no processo penal à luz do estado de direito é amplo, portanto, e não está limitado ao conjunto de informações que a acusação disponibiliza ao juízo e à defesa.

Há significativa diferença de ordem conceitual e prática entre aquilo que a acusação pode empregar no processo, que delimita a temática que estabelece e condiciona a decisão, por meio da imputação, por um lado, e, por outro, a totalidade dos elementos informativos recolhidos na investigação criminal e até no processo penal, pelas agências públicas de repressão.

Estes elementos são aptos a indicar à defesa a correção ou incorreção da trajetória da própria persecução penal e se não assiste razão à acusação.

Quando avaliada em perspectiva a não integridade da prova digital colhida, conforme juízo do assistente técnico, a conclusão corrobora a suspeição da defesa acerca da ineficácia probatória resultante da não instauração – no extremo – ou da quebra da cadeia de custódia, porque inviabiliza o exercício do direito de defesa.

Verificada a quebra da cadeia de custódia relativamente às provas digitais referidas, todos os elementos probatórios que se conectam aos arquivos digitais estão contaminados e igualmente não são válidos.

A contaminação gerada pela quebra da cadeia de custódia das provas tem tratamento no art. 157 do CPP, que estabelece a inadmissibilidade das provas derivadas das ilícitas, salvo quando houver rompimento do nexo de causalidade entre umas e outras, o que não é o caso.

É o que se observa no caso concreto.

A causalidade naturalística própria da cadeia das provas ilícitas impede a avaliação das provas posteriores à declarada ilícita e impõe sua exclusão do processo (art. 157, § 1º, do CPP).

A causalidade normativa, que tem ainda maior peso relativamente à proteção que incumbe à proibição de prova ilícita, produz o mesmo efeito ao interditar o emprego dos conhecimentos obtidos pela prova ilícita para "interpretar" provas aparentemente produzidas sem uma filiação direta e imediata com a prova declarada ilícita.

O tratamento da prova obtida mediante violação da cadeia de custódia é simétrico ao oferecido às provas ilícitas como ressaltado ao longo do estudo.

Vale sublinhar, por fim, que a tradição de controle da ilicitude probatória tem o mérito de incorporar um "efeito dissuasório" – *deterrent effect* – que serve de desestímulo às agências repressivas quanto à tentação de recorrerem a práticas ilegais para obter a punição.

Esta posição de rigor contra as ilicitudes probatórias tem pautado a atuação de nossos tribunais superiores.

No julgamento do HC 160.662-RJ,[79] a 6ª Turma do Superior Tribunal de Justiça por unanimidade acolheu a tese da cadeia de custódia e declarou a ilicitude da prova.

79. STJ. Habeas Corpus 160.662/RJ. 6ª Turma. Relatora: Ministra Assusete Magalhães. Impetrante: Fernando Augusto Fernandes e outros. Pacientes: Luis Carlos Bedin e Rebeca Daylac. Data do julgamento: 18 fev. 2014.

Por sua vez, ao julgar caso em que a infiltração da ilicitude probatória contaminou o processo em alto grau, a Quinta Turma do Superior Tribunal de Justiça firmou primoroso precedente.[80]

4. Quesitos

À vista do exposto é possível passar a responder aos quesitos formulados no sentido de que:

1) Conforme a documentação do processo apresentada e os laudos emitidos é possível afirmar que no tocante à internação processual, por ordem judicial, das informações digitais adquiridas, o procedimento de instauração e preservação de sua cadeia de custódia foi observado?

Respondido no corpo do parecer. O assistente técnico identificou: *i)* a não instauração da cadeia de custódia das informações digitais, desatendendo-se às boas práticas periciais pertinentes; *ii)* e apontou indícios de não integridade dos elementos digitais empregados na acusação.

A inconfiabilidade técnica desses elementos e a impossibilidade de sua adequada auditabilidade afetam a autenticidade dessa prova e prejudicam o contraditório.

2) Na hipótese de constatação da quebra da cadeia de custódia das provas, que consequências jurídicas advêm disso?

Respondido no corpo do parecer.

Em virtude da constatação da não instauração correta da cadeia de custódia das provas digitais e dos indícios que o assistente técnico também apontou, de quebra da cadeia de custódia das provas digitais, os elementos probatórios dessa natureza empregados no processo inequivocamente constituem prova ilícita.

Eventual prova derivada destes elementos está contaminada porque fundada em dado probatório inválido e inadmissível.

Ressalvado melhor entendimento, este é o parecer.

Rio de Janeiro, 18 de junho de 2023.

80. Ementa e trechos do voto condutor no: STJ, HC 149.250 SP. 5ª Turma (STJ). Relator: Ministro Adilson Vieira Macabu. Impetrante: Andrei Zenkner Schmidt e outros. Julgamento em: 07 de jun. 2011. *DJe* 05.09.2011.

Anexo
Modelo de Triagem[81]

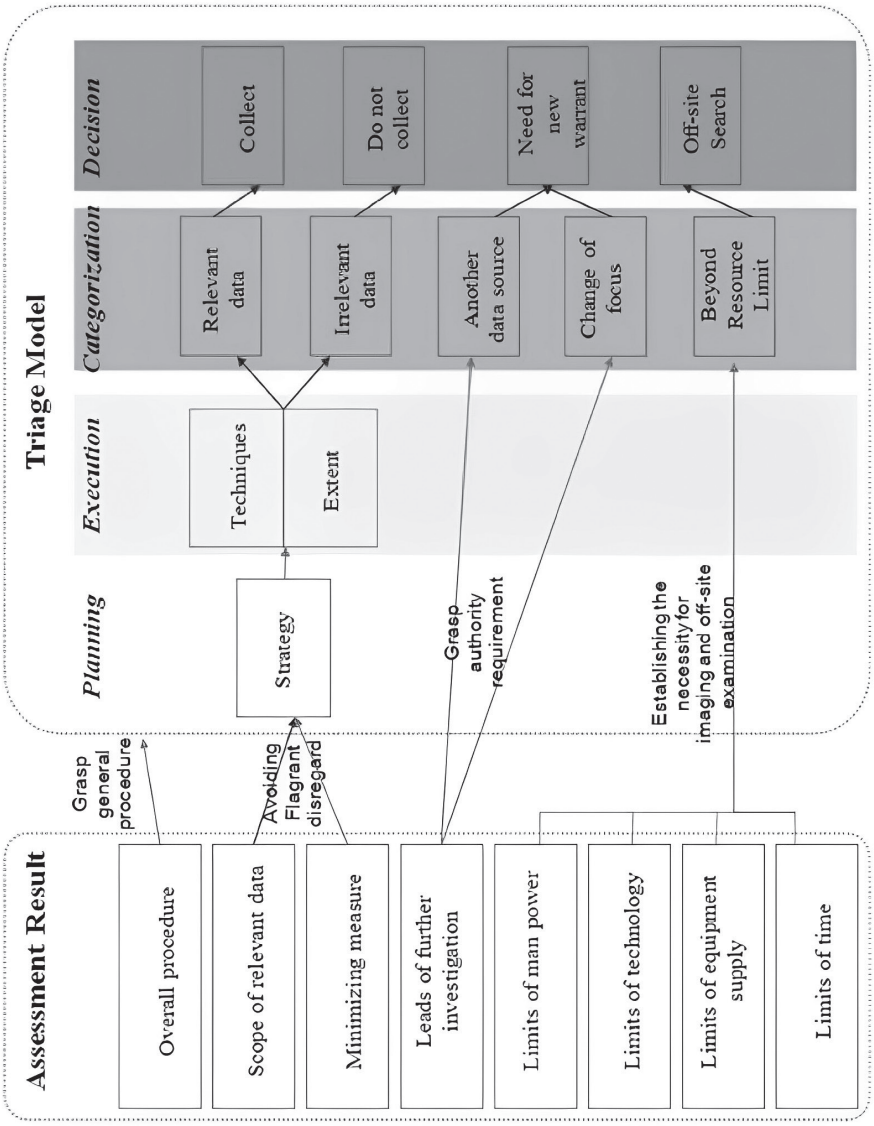

Fig. 3. Graphical representation of relationship between assessment results and triage model.

81. Original retirado de: HONG, Ilyoung; YU, Hyeon; LEE, Sangjin; LEE, Kyungho. A new triage model conforming to the needs of selective search and seizure of electronic evidence. *Digital investigation*, v. 10, p. 175-192, 2013. p. 180.

PESQUISAS DO EDITORIAL

Áreas do Direito: Penal; Processual; Digital

Veja também Doutrinas relacionadas ao tema

- A cadeia de custódia como elemento fundamental da validade e utilidade das provas digitais, de Maurício Tamer – *Boletim Revista dos Tribunais Online* 36/2023;
- 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 investigação criminal no Brasil: uma proposta de avaliação de desempenho com base na experiência internacional, de Nefi Cordeiro e Elton Luiz Bueno Candido – *RBCCrim* 189/269-288;
- Existem limites probatórios na era digital? – a validade processual penal e constitucional das provas digitais, de Guilherme Machado de Castilhos e Aline Pires de Souza Machado de Castilhos – *RT* 1010/275-294; e
- Promotores e provas digitais: tecnologias na nuvem oferecem uma solução, de Gina Jurva – *Boletim Revista dos Tribunais Online* 27/2022.

Prado, Geraldo. Parecer: investigação criminal digital e processo penal.
Revista Brasileira de Ciências Criminais. vol. 199. ano 31. p. 315-350. São Paulo: Ed. RT, nov./dez. 2023.
DOI: [https://doi.org/10.5281/zenodo.8381070].