A cadeia de custódia dos vestígios digitais sob a ótica da Lei n. 13.964/2019: aspectos teóricos e práticos

Winícius Ferraz Neres

Analista do MPU – suporte e infraestrutura de TIC, lotado na Assessoria Nacional de Perícia em TIC da Procuradoria-Geral da República. Engenheiro de Computação. Especialista em Segurança da Informação e em Computação Forense.

Resumo: Este artigo versa sobre a promulgação da Lei n. 13.964/2019, que trouxe com ela, um conjunto de consequências teóricas e práticas. Especificamente no âmbito do Código de Processual Penal (CPP), os arts. 158-A a 158-F acrescentaram dispositivos relacionados ao tratamento da prova pericial, em especial à manutenção da cadeia de custódia. Esses artigos, em certos momentos, foram taxativos acerca do tratamento do vestígio penal, mas, por outro lado, deixaram lacunas, principalmente quando se vislumbra um vestígio digital. Esse tipo de vestígio é naturalmente mais volátil e passível de adulteração quando comparado aos das outras áreas de conhecimento. Portanto, cabe às forças da lei e aos demais envolvidos o desenvolvimento de procedimentos e de estrutura necessários para a adequação legal, bem como a garantia da integridade e da manutenção da cadeia de custódia dessa categoria de vestígio, que se torna cada vez mais importante numa sociedade em que os crimes informáticos proliferam. Nesse contexto, é fundamental a busca por fontes de conhecimento complementares e confiáveis. Destaque para as normas nacionais e internacionais acerca do tratamento dos vestígios digitais, bem como os procedimentos operacionais já desenvolvidos por diversos institutos de criminalística. Concluindo, como produto desta pesquisa seguem, no formato de apêndice, três compilados que objetivam apoiar de alguma forma os responsáveis em conduzir a missão de adequar a manutenção da cadeia de custódia do vestígio informático à Lei n. 13.964/2019.

Palavras-chave: Cadeia de custódia. Crime informático. Lei n. 13.964/2019. Vestígio digital.

Abstract: This article deals with the enactment of Law 13.964/2019, which brought with it a set of theoretical and practical consequences. Specifically within the scope of the Criminal Procedure Code, the articles 158-A to 158-F were added provisions related to the treatment of expert evidence, in particular the maintenance of the chain of custody. These articles, at certain times, were definitive about the treatment of the criminal vestige, but on the other hand, they left gaps, especially when dealing with a digital trace. This type of vestige is naturally more volatile and susceptible to adulteration when compared to other areas of knowledge. Therefore, it is the responsibility of the law enforcement agencies and others involved to develop the necessary procedures and structure for legal adequacy, as well as to guarantee the integrity and maintenance of the chain of custody of this category of vestige, that is becoming increasingly important in a society where computer crimes proliferate. Due this, the search for complementary and reliable sources of knowledge is fundamental. Highlight for the national and international norms about the treatment of digital traces, as well as the operational procedures already developed by several criminology institutes. In conclusion, as a product of this research, three compilations are presented as appendices that aim to support in some way those responsible for carrying out the mission of adapting the maintenance of the chain of custody of the computer trace to Law 13.964/2019.

Keywords: Chain of custody. Computer crime. Law 13.964/2019. Digital trace.

Sumário: 1 Introdução. 2 Crimes informáticos. 3 Vestígios digitais. 3.1 Especificidades dos vestígios digitais. 3.2 Manuseio dos vestígios digitais. 3.3 Cadeia de custódia dos vestígios digitais. 3.4 Boas práticas para a manutenção da cadeia de custódia dos vestígios digitais. 4 Conclusão.

1 Introdução

Em junho de 2018, foi apresentado na Câmara dos Deputados o Projeto de Lei n. 10.372/2018, que objetivava "[...] agilizar e modernizar a investigação criminal e a persecução penal".[1] Em 24 de dezembro de 2019, enfim, o Presidente Jair Bolsonaro, após vetar 25 itens do texto final aprovado pelo Parlamento, sancionou e promulgou a Lei n. 13.964/2019, conhecida popularmente como Pacote Anticrime.

1 Brasil. Câmara dos Deputados. *Projeto de Lei n. 10.372/2018*. Disponível em: https://www.camara.leg.br/propostas-legislativas/2178170. Acesso em: 20 abr. 2020.

A Lei n. 13.964/2019 alterou diversos dispositivos legais, entre eles o Código de Processo Penal (Decreto-Lei n. 3.689/1941), do qual têm especial interesse para este estudo os arts. 158-A a 158-F, inseridos no capítulo relativo ao exame de corpo de delito, cadeia de custódia e perícias.

Não obstante a preservação da prova não ser uma inovação no ordenamento jurídico brasileiro, é senso comum que os mencionados artigos conferiram maior importância à manutenção da cadeia de custódia dos vestígios penais. Indo adiante, ao analisar mais atentamente os supracitados artigos, também se percebe que em alguns dispositivos há um detalhamento minucioso de certos procedimentos. Por outro lado, também ficam expostas algumas lacunas operacionais que não foram abordadas pela legislação.

Esse hiato de certa forma é esperado, afinal, não seria razoável que o legislador descrevesse taxativamente todos os mecanismos relativos à manutenção e garantia da cadeia de custódia dos vestígios penais das mais diversas as áreas do conhecimento. Isso, no entanto, obriga a que as forças da lei se atentem e criem os devidos procedimentos e as necessárias estruturas de trabalho.

Essa situação fica ainda mais latente ao se tratar dos vestígios, evidências ou provas digitais, afinal esses ativos exigem cautela especial, uma vez que, de forma geral, dados armazenados são mais passíveis de adulteração do que os vestígios físicos existentes em outras áreas do conhecimento.[2]

De todo modo, a promulgação da Lei n. 13.964/2019, no tocante ao gerenciamento da cadeia de custódia, ainda vem impondo mudanças nas estruturas físicas e organizacionais das forças da lei que necessitam lidar com essa questão. Nessa conjuntura apresentada, este trabalho intenta ter natureza aplicável, de maneira que, além de apresentar conceitos associados e propor reflexões acerca do tema, enuncia um compilado de boas práticas, com vistas ao apoio da adequada manutenção da cadeia de custódia de alguns dos mais comuns vestígios digitais tratados no contexto pericial da Tecnologia da Informação e Comunicação (TIC).

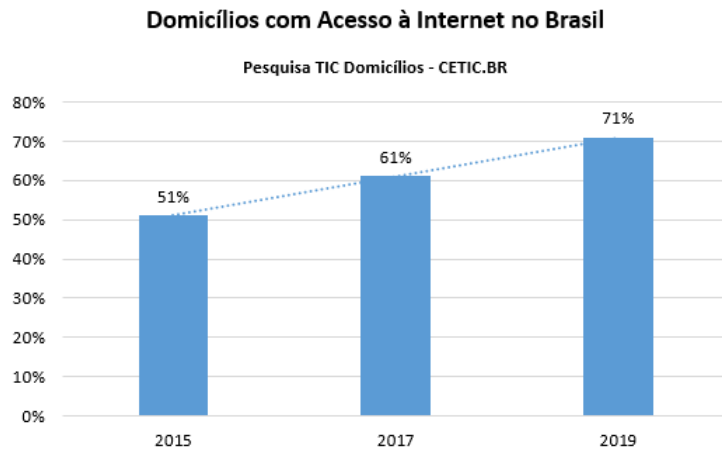
2 Cunha, Rogério Sanches. *Pacote Anticrime*: Lei 13.964/2019 – Comentários às alterações no CP, CPP e LEP. Salvador: JusPodivm, 2020.

2 Crimes informáticos

Neste século, o uso da internet e dos recursos tecnológicos associados tornou-se imprescindível às organizações (públicas e privadas), aos indivíduos e à sociedade de forma geral. As pessoas buscam conhecimento, procuram novas relações pessoais, executam atividades profissionais ou simplesmente intentam se divertir a partir de um dispositivo conectado à rede mundial. As corporações, por sua vez, também são cada vez mais dependentes da TIC para se comunicarem com parceiros, fornecedores e clientes, bem como para otimizarem os processos de produção e prestação de serviços.

A respeito do acesso à tecnologia no Brasil, convém mencionar alguns indicadores da pesquisa intitulada "TIC Domicílios", realizada periodicamente pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC.BR). Segundo essa pesquisa, em 2019, 71% dos lares brasileiros possuíam acesso à internet. Em 2017, havia um apontamento de 61% para esse mesmo indicador e, em 2015, apenas 51% das residências brasileiras dispunham de acesso à rede mundial de computadores. A figura a seguir ilustra esses números e a tendência de crescimento.[3]

Figura 1 • Percentual de domicílios brasileiros com acesso à internet



3 Comitê Gestor de Internet no Brasil, 2016; 2018; 2020. Acesso em: 18 ago. 2020.

Outro interessante indicador se refere à quantidade de indivíduos no Brasil que já tiveram contato direto com a internet. Em 2019, a pesquisa "TIC Domicílios – Indivíduos" concluiu que 80% dos brasileiros já haviam acessado a internet alguma vez na vida, independentemente do meio. Já em 2017, a pesquisa afirmou que 74% das pessoas possuíam essa experiência e, em 2015, esse índice chega a apenas 66%.[4]

Sob outra perspectiva, a reboque do maior acesso à tecnologia neste século e dos inúmeros benefícios gerados por ela, cresceram as práticas ilícitas utilizando direta ou indiretamente os sistemas informatizados. Do mesmo modo, é fato notório que as tecnologias novas, responsáveis por permitirem o desenvolvimento e a automação dos processos de negócio, por outro lado também possibilitam formas do inadequado uso dos computadores e afins.[5]

Mister registrar que esse tipo de delito e as tentativas de enfrentamento vêm ganhando força neste século. No entanto, segundo o jurista alemão Ulrich Sieber, há registros do início da década de 1970 dos primeiros tipos penais destinados a proteger a vida privada diante das novas formas de armazenamento, transmissão e processamento de dados que surgiam naquela época.[6]

Sobre a tipologia dos crimes informáticos, existem algumas correntes divergentes. Uma forma de abordar essa questão seria visualizar a cibercriminalidade em sentido amplo e em sentido estrito. A primeira abarcaria toda e qualquer atividade criminosa executada por meios informáticos, seja ela direcionada especificamente a siste-

4 Comitê Gestor de Internet no Brasil, 2016, 2018, 2020.

5 Welch, 2007, p. 2781-2782 *apud* Caiado, Felipe B.; Caiado, Marcelo. Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse. *In:* Domingos, Fernanda Teixeira Souza *et al.* (coord.). *Crimes Cibernéticos*: coletânea de artigos. v. 3. Brasília: Ministério Público Federal – 2ª Câmara de Coordenação e Revisão, 2018. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos. Acesso em: 18 ago. 2020.

6 Kist, Dário José. *A prova digital no processo penal*. Leme-SP: JH Mizuno, 2019.

mas cibernéticos, seja apenas como instrumento-meio para a prática de um crime comum. A segunda, mais estrita, abraça a tese de que crimes informáticos contemplariam apenas os delitos em que o elemento digital esteja presente como objeto principal de proteção.[7]

Há quem opte por categorizar os crimes cibernéticos tendo por base o bem jurídico tutelado. Ulrich Sieber, por exemplo, propôs que esses delitos fossem classificados como:[8]

a) crimes econômicos;

b) ataques à privacidade;

c) transmissão de conteúdos ilegais;

d) outros delitos, incluindo os crimes contra a vida.

Como outro exemplo de observância e classificação dos crimes informáticos, o autor Túlio Vianna[9] inicialmente considera que o mero uso de um dispositivo computacional para a execução de um delito, por si só, não configuraria um crime informático, caso o bem afetado não seja objetivamente um dado ou uma informação automatizada. Ainda nas palavras de Vianna,[10] "em rigor, para que um delito seja considerado de caráter informático, é necessário que o bem jurídico por ele protegido seja a inviolabilidade de informações e dados [...]".

Por outro lado, esse autor reconhece que muitos outros literatos também consideram crimes informáticos aquelas infrações penais em que o ativo de TIC sirva apenas como um instrumento-meio e, portanto, também não descarta esse entendimento comum. Dessa forma, ele resolveu classificar os crimes informáticos em quatro espécies: a) crimes informáticos próprios; b) crimes informáticos impróprios; c) crimes informáticos mistos; d) crimes informáticos mediatos ou indiretos.

7 Kist, 2019.

8 Sieber *apud* Kist, 2019.

9 Vianna, Túlio; Machado, Felipe. *Crimes informáticos:* conforme a Lei nº 12.737/2012. Belo Horizonte: Fórum, 2013.

10 Vianna; Machado, 2013, p. 29.

Crimes informáticos próprios seriam aqueles delitos em que o bem protegido pela norma é a inviolabilidade das informações em trânsito ou armazenadas. Um exemplo clássico desse tipo de delito seria o crime de invasão de dispositivo informático e o crime de inserção de dados falsos em sistema de informações por parte de funcionário público (art. 313-A do Código Penal – CP).

Ainda sob a ótica desse autor, crimes informáticos impróprios seriam aqueles em que o dispositivo computacional é utilizado como mero instrumento para a execução do crime, mas não existe ofensa à inviolabilidade da informação automatizada. Um exemplo seria o crime de ameaça (art. 147 do CP), passível de ser executado via correio eletrônico ou rede social. Nesse caso, em regra, não há qualquer ataque à inviolabilidade de informações automatizadas.

Já os crimes cibernéticos mistos "[...] são crimes complexos[11] em que, além da proteção da inviolabilidade dos dados, a norma visa tutelar bem jurídico de natureza diversa".[12] São delitos derivados do ataque ao sistema informatizado. Essa espécie pode ser ilustrada pelo crime de acesso a sistema do serviço eleitoral, a fim de alterar a apuração ou a contagem de votos (Lei. n. 9.504, art. 72, inciso I).

Finalmente, crimes informáticos mediatos (ou indiretos) seriam conceituados como delitos-fim não informáticos que herdaram essa característica do delito-meio informático para possibilitar sua execução. Dessa forma, por exemplo, se determinada pessoa invadir o sistema computacional de um banco e transferir indevidamente recursos financeiros para conta alheia, esse indivíduo estaria cometendo dois diferentes delitos: o crime de invasão de dispositivo informático e o crime de furto, sendo aquele um crime informático e este um delito contra o patrimônio. De todo modo, nesse caso hipotético, o agente somente seria apenado pelo furto, aplicando-se ao caso o princípio da consunção.[13]

11 Crimes complexos são os delitos em que há uma fusão unitária de mais de um tipo de crime (Hungria, 1958, p. 53 *apud* Vianna; Machado, 2013).

12 Vianna; Machado, 2013, p. 34.

13 Vianna; Machado, 2013.

Outra perspectiva acerca desse assunto, aparentemente a mais difundida, ao menos no Brasil, e a preferida deste articulista, é classificar os crimes informáticos simplesmente em próprios ou puros e impróprios ou impuros. Aqueles abrangeriam os delitos cometidos necessariamente em virtude da existência do ciberespaço. Acesso não autorizado a um sistema informático, interceptação ilegal de comunicação telemática e criação de *malwares* com fins ilícitos são bons exemplos de crimes informáticos próprios ou puros.[14]

Por fim, os cibercrimes impróprios ou impuros seriam aqueles passíveis de objetivamente ser executados de forma tradicional no mundo físico, mas no caso concreto foram praticados via sistemas informatizados. Como exemplo é possível mencionar os estelionatos praticados via internet, os ataques à honra ou as ameaças por meio de dispositivos tecnológicos e a difusão de conteúdo proibido na rede mundial de computadores.[15]

3 Vestígios digitais

Primeiramente, durante esta pesquisa, percebeu-se que muitas obras mencionam os temos vestígio digital, evidência digital e prova digital praticamente como sinônimos. Assim, convém aclarar esses conceitos e suas diferenças sutis, pois em certas situações essa questão não será um mero preciosismo.

Nos termos do § 3º do art. 158-A da Lei n. 13.964/2019, "vestígio é todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal". Com base nessa definição e no entendimento deste articulista, é cabível entender vestígio digital como todo material de cunho informático ou digital, visível ou latente, constatado ou recolhido, que se relaciona a um crime informático.

Na mesma linha, vestígio digital também pode ser apresentado como "[...] um registro digital que existe em decorrência de

14 Kist, 2019.

15 Kist, 2019.

uma prévia intervenção humana, tratada aqui como agente motivador direto ou indireto daquele evento".[16]

Já uma evidência digital representa o vestígio digital que, após analisado pelo corpo técnico (geralmente um perito), se mostra diretamente relacionado ao caso investigado. A partir do momento que estiver ratificado o vínculo entre o vestígio digital e o delito, esse vestígio pode ser denominado de fato uma evidência digital. Supletivamente a essa explicação, convém citar o conceito de evidência digital proposto por Casey:[17]

> Uma evidência digital pode ser entendida como qualquer dado armazenado ou transmitido utilizando-se um computador, de maneira que com este dado seja possível demonstrar ou refutar uma hipótese acerca de um evento; ou ainda que este forneça elementos críticos determinantes num caso investigado, tal como premeditação, dolo, álibi etc.

Nessa linha de desenvolvimento, a depender do caso concreto, uma evidência digital poderá se tornar uma prova digital, que pode ser definida como uma informação transmitida ou memorizada, em formato binário, apta a ser utilizada como parte do conjunto probatório no âmbito de uma ação penal, cível ou administrativa.

Em resumo, podemos entender o vestígio digital como um dado digital que possa ter relação com o fato investigado. Já a evidência digital pode ser considerada um vestígio digital analisado e comprovadamente relacionado ao caso investigado. A prova digital, por sua vez, é a evidência digital formalizada no âmbito processual.

3.1 Especificidades dos vestígios digitais

Os ativos digitais intrinsicamente possuem atributos que os tornam peculiares quando comparados aos objetos de outras áreas

16 Brasil. Ministério Público Federal. *Roteiro de atuação de crimes cibernéticos*. 3. ed. Brasília: Ministério Público Federal, 2ª Câmara de Coordenação e Revisão, 2016. Disponível sob demanda em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes. Acesso em: 20 ago. 2020.

17 Casey, 2004 *apud* Brasil, 2016, p. 163.

de conhecimento. Algumas dessas especificidades são:[18] a) imaterialidade ou invisibilidade; b) volatilidade; c) fragilidade; d) dispersão.

Em que pese um computador ou smartphone consiga criar e armazenar dados telemáticos de inúmeros tipos, caso esses dispositivos fossem desmontados, esses dados não estariam visíveis a olho nu. Aquilo que o usuário escreve, lê ou ouve utilizando um dispositivo de TIC envolve um complexo processo eletrônico de forma quase invisível ao ser humano. Enquanto um vestígio analógico, em regra, é material por natureza, o digital é essencialmente composto por bits.

Um vestígio digital é volátil, pois a partir de uma ação do usuário (intencional ou não) ou do próprio sistema informático, pode ele facilmente desparecer. Por exemplo, uma sequência de bits que, num certo instante, esteja armazenada na memória RAM de um computador pode sumir no milésimo de segundo seguinte devido à gestão do sistema operacional ou à interrupção do fornecimento de energia elétrica.

Em relação à fragilidade, o digital carrega esse atributo, pois os dados ou os metadados associados podem ser facilmente manipulados quando em comparação às provas físicas comuns. De igual forma, essa manipulação pode acontecer por responsabilidade do próprio usuário (intencionalmente ou não) ou do sistema operacional.

Outro predicado consiste na possibilidade de partes da mesma prova digital estarem localizadas em locais diferentes. Essa dispersão existe em duas dimensões. De um lado, certos vestígios ou provas digitais podem estar mantidos em diferentes locais, mas inseridos no mesmo sistema informático. Por exemplo, é factível que parte de uma prova digital esteja armazenada em disco rígido e outra parte na memória RAM.

De outro lado, a segunda dimensão da dispersão está relacionada à natureza geográfica. Ou seja, as partes que compõem o todo de uma prova podem estar mantidas em locais físicos totalmente

18 Kist, 2019.

distintos. Os melhores exemplos são os serviços de nuvem, que atualmente mantêm suas estruturas e dados dispersos em vários locais do mundo.

Ainda acerca das especificidades dos ativos digitais, é salutar mencionar o documento *Request for Comments 3227* (RFC 3227), que apresenta as diretrizes para coleta e manutenção de evidências digitais. Segundo essa norma técnica, é basal que uma prova digital detenha as seguintes características:[19] a) admissibilidade; b) autenticidade; c) completude; d) confiabilidade; e) acreditabilidade.

Uma prova digital é considerada admissível quando está em plena conformidade com a legislação local, afinal de nada adianta a obtenção de uma prova por meios ilícitos. O segundo atributo, a autenticidade, deve ser capaz de interligar positivamente o material probatório ao fato investigado. Complementarmente, na interpretação do advogado Thiago Vieira (2019),[20] esse atributo também contempla a integridade da evidência. Essa qualidade "diz respeito à imutabilidade da evidência e pode ser aferida através de comparações de resumos matemáticos".[21]

O terceiro aspecto, a completude, tem o objetivo de relatar o fato na integralidade, não apenas sob a ótica de uma das partes. Nesse sentido, segue valorosa lição do professor Geraldo Prado:[22]

> O conhecimento das fontes de prova pela defesa é fundamental, porque a experiência histórica que precede a expansão da estrutura trifásica de procedimento penal, adequada ao modelo acusatório, contabi-

19 Internet Engineering Task Force. *RFC 3227:* Guidelines for evidence collection and archiving. Fremont, 2002. Disponível em: https://www.ietf.org/rfc/rfc3227.txt. Acesso em: 19 ago. 2020.

20 Vieira, Thiago. *Aspectos técnicos e jurídicos da prova digital no processo penal*. Disponível em: https://medium.com/@tocvieira/aspectos-t%C3%A9cnicos-e-jur%C3%ADdicos-da-prova-digital-no-processo-penal-aa22ef05fb30. Acesso em: 30 mar. 2021.

21 Também conhecidos no meio computacional como valores *hash* ou *messages digest*.

22 Prado, Geraldo. *A cadeia de custódia de prova no processo penal*. São Paulo: Marcial Pons, 2019. p. 72.

liza a supressão de elementos informativos como estratégia das agências de repressão que fundam as suas investigações em práticas ilícitas.

Não custa sublinhar que apenas inadvertidamente eventual autor de ilicitudes probatórias permitiria a chegada ao processo de traços das referidas ilicitudes.

Por isso, o exame da legalidade da investigação criminal concentrado com exclusividade no material apresentado pelo acusador em juízo é, de regra, inócuo ou no mínimo insuficiente.

Adicionalmente, interligada à completude, mister citar a Súmula Vinculante 14 do Supremo Tribunal Federal:

> É direito do defensor, no interesse do representado, ter acesso amplo aos elementos de prova que, já documentados em procedimento investigatório realizado por órgão com competência de polícia judiciária, digam respeito ao exercício do direito de defesa.

Nesses termos, de forma inequívoca, o STF ratificou o direto do defensor ao acesso amplo, irrestrito, de forma integral às provas, inclusive às digitais, utilizadas ao longo do procedimento investigatório. Ademais, esse entendimento cria algumas responsabilidades diretas para os órgãos de investigação, em especial para os ministérios públicos e as polícias judiciárias, principalmente no tocante à manutenção da cadeia de custódia.

A confiabilidade, por sua vez, consiste em não haver fatos, relacionados à coleta e ao tratamento da evidência, que lancem dúvidas sobre a real autenticidade e veracidade. Essa necessária característica está ligada intimamente à capacitação dos profissionais envolvidos e aos métodos utilizados ao longo do trabalho pericial.

Por fim, o quinto traço, a acreditabilidade, propõe que a evidência seja compreensível por seus julgadores. Nesse sentido, vale este trecho redigido por Vacca:[23]

> Não faz sentido apresentar a saída binária se o júri não tiver ideia do que tudo isso significa. Da mesma forma, se você apresentá-los com

23 Vacca, 2005 *apud* Vieira, 2019.

uma versão formatada e compreensível do humano, você deve ser capaz de mostrar a relação com o original binário, caso contrário, não há como o júri saber se você o falsificou.

3.2 Manuseio dos vestígios digitais

Percebe-se que, ao longo da exposição das especificidades do vestígio digital, algumas delas estão intimamente vinculadas à qualidade do tratamento ou manuseio do ativo digital. Acerca desse tema, em âmbito penal, é fundamental aos operadores do tema o entendimento da seção "Do Exame de Corpo de Delito, da Cadeia de Custódia e das Perícias em Geral", registrada no Código de Processo Penal. De todo modo, é possível destacar alguns pontos.

Primeiramente, o art. 158 do CPP ratifica 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". Além disso, o art. 159 é taxativo ao afirmar que o exame pericial em âmbito penal deve ser realizado por perito oficial,[24] portador de diploma de curso superior.[25]

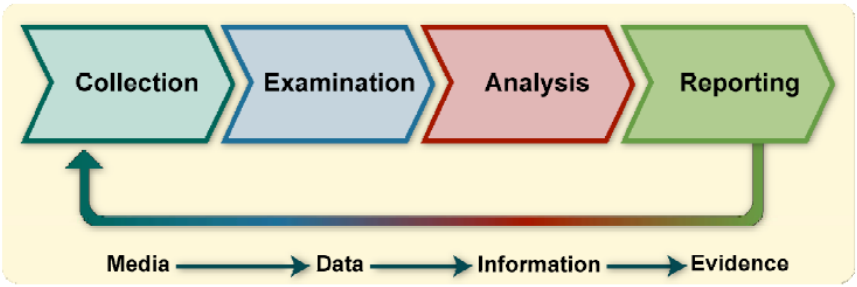
Em relação ao aspecto técnico, é fundamental que a prova ou potencial prova digital seja tratada conforme os procedimentos forenses adequados. As orientações e diretrizes acerca do tratamento desse tipo de prova costumam variar, a depender da fonte pesquisada. O National Institute of Standards and Technology (NIST), por exemplo, a partir da publicação do documento Special Publication 800-86,[26] defende que esse processo deva ocorrer em quatro etapas: a) coleta; b) exame; c) análise; d) formalização.

24 Na esfera federal e em âmbito criminal, perito oficial é o Perito Criminal Federal, cargo vinculado ao Departamento de Polícia Federal.

25 O CPP também aponta algumas exceções a essa regra.

26 National Institute of Standards and Technology. *Guide to integrating forensic techniques into incident response*. NIST Special Publication 800-86. Gaithersburg: NIST, 2006. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-86/final. Acesso em: 18 ago. 2020.

Figura 2 • Fluxo de tratamento da prova digital



Fonte: Guide to integrating forensic techniques into incident response. NIST SP 800-86.

Na primeira etapa, os dados relacionados a um evento específico são identificados, rotulados, registrados e coletados, observando-se com especial cuidado a manutenção da integridade. Na fase denominada exame, ferramentas e técnicas forenses apropriadas para cada tipo de dado coletado são utilizadas para extrair informações relevantes.

A próxima fase, a análise, envolve o estudo dos resultados da fase anterior com o objetivo de obter informações específicas do caso que deu origem ao tratamento da evidência. A etapa seguinte, a formalização, aborda o relatar dos resultados de todo o trabalho, podendo incluir a descrição das ações executadas, procedimentos e ferramentas utilizadas.

Em igual sentido, o documento RFC 3227 também apresenta diretrizes para coleta e arquivamento das evidências digitais. Na seção denominada "Procedimentos de Coleta", o documento sugere que as organizações mantenham um procedimento de coleta tão detalhado quanto possível com o objetivo de minimizar a quantidade de tomadas de decisão necessárias durante o processo de execução da coleta.

Adicionalmente, essa RFC destaca que o procedimento de coleta da evidência deve ser transparente e reprodutível. Os executores devem estar preparados para repetir com precisão os métodos utilizados e ter esses métodos testados por especialistas independentes. Além disso, é estabelecida uma coleção de passos técnicos

para a coleta da evidência, que pode ser consultada diretamente na seção 3.2 desse documento.

Em relação ao arquivamento, a RFC 3227 defende que sejam utilizadas mídias já comumente manipuladas para armazenamento da evidência na organização, evitando assim tecnologias obscuras. Por fim, também existe orientação no sentido de que o acesso à evidência digital seja estritamente restrito e claramente documentado.

De maneira complementar, vale citar o processo de manuseio de evidências digitais indicado pela norma ABNT NBR ISO/IEC 27037:2013. Ela destaca que seu escopo se refere somente ao processo inicial de manuseio digital, composto por: a) identificação; b) coleta; c) aquisição; d) preservação.

A fase de identificação contempla a pesquisa, o reconhecimento e a documentação da potencial evidência digital, considerando também a priorização da coleta baseada na volatilidade da evidência. Uma vez identificadas, as evidências estão aptas à fase de coleta. Coleta é a etapa ou subprocesso do processo de manuseio da evidência digital na qual evidências digitais em potencial são removidas de sua localização original para um laboratório ou ambiente controlado. Nessa etapa, abordagens diferentes podem ser necessárias, a depender do estado do ativo.

A terceira etapa, aquisição, contempla a produção da cópia da evidência digital e a documentação dos métodos utilizados nessa atividade. Aspectos como situação da evidência, custo de execução da etapa e tempo devem ser considerados pelo perito, bem como registrados os motivos de cada decisão. Segundo a norma, é recomendável que todos os métodos utilizados para adquirir uma evidência digital sejam reproduzíveis ou verificáveis por profissional independente e capacitado.

A última etapa, preservação, numa tradução livre da norma ABNT NBR ISO/IEC 27037, prega que a "[...] evidência digital seja preservada para garantir sua utilidade na investigação". Essa fase envolve o armazenamento da potencial prova digital com o objetivo primário de protegê-la contra espoliação ou adulteração. Ademais,

um ponto importante citado na norma que merece destaque: "recomenda-se que o processo de preservação seja iniciado e mantido durante o processo de manuseio da evidência digital, começando da identificação do dispositivo digital que contém a potencial evidência digital". Assim, considerando essas definições, a figura a seguir ilustra, de forma macro, o processo de manuseio de evidência digital proposto pela ABNT NBR ISO/IEC 27037:2013. Destaque especial para o fato de que a preservação da evidência digital deve permear todas as etapas de manuseio do bem questionado.

Figura 3 • Processo de tratamento forense da evidência digital NBR ISO/IEC 27037:2013

Fonte: ABNT NBR ISO/IEC 27037:2013.

3.3 Cadeia de custódia dos vestígios digitais

Já inicialmente, importante consignar que, apesar de algumas diferenças na abordagem do manuseio da evidência digital, todas as normas de boas práticas citadas na seção anterior apresentam algo em comum: a ratificação da necessidade da adequada manutenção da cadeia de custódia do vestígio digital. Esse requisito torna-se ainda mais imprescindível ao considerar as tipicidades desse tipo de vestígio e as inovações apresentadas pelos arts. 158-A a 158-F da Lei n. 13.964/2019.

O documento Special Publication 800-86, por exemplo, define perícia digital como a aplicação da ciência aos atos de identificação, coleta, exame e análise de dados, preservando a integridade das informações e a estrita manutenção da cadeia de custódia.[27]

27 National Institute of Standards and Technology, 2006, p. ES-1 (tradução livre).

O documento RFC 3227, por seu lado, afirma, na seção 4.1, que uma adequada cadeia de custódia deve ser capaz de descrever claramente como a evidência foi localizada e tratada. Ademais, ainda segundo a norma técnica ABNT NBR ISO/IEC 27037:2013, é recomendado que a pessoa autorizada para agir no local de incidente, na execução de coleta e aquisição da evidência digital, seja capaz de descrever todas as aquisições de dados e dispositivos custodiados. Tudo isso também deve ser fichado num documento chamado registro de cadeia de custódia, que é o registro da cronologia de movimento e do manuseio da potencial evidência.

Em âmbito prático nacional, especificamente em 2012, o então Ministério da Justiça entendeu que as unidades de perícia do País necessitavam de procedimentos minimamente padronizados para a produção da prova técnica. Nesse sentido, foi lançado o programa Brasil Mais Seguro, que previu como uma de suas ações de fortalecimento da perícia a padronização de alguns procedimentos relacionados à atividade pericial.[28]

A seção 3 desse documento, que também aborda a informática forense, pode ser considerada um marco quanto à padronização das atividades periciais no País, no entanto ela não possui como principal foco o tratamento da cadeia de custódia, bem como não vincula a atuação do perito. Objetivamente, trata-se de um (valoroso) manual para nortear o trabalho técnico.[29]

Como um dos efeitos da produção do Procedimento Operacional Padrão - Perícia Criminal, o então Ministério da Justiça, também mediante a Secretaria Nacional de Segurança Pública, em julho de 2014, publicou a Portaria n. 82, que estabeleceu as diretrizes sobre os procedimentos a serem observados no tocante à cadeia de custódia de vestígio. Enfim, essa portaria definiu cadeia de cus-

28 Brasil. Ministério da Justiça. *Procedimento operacional padrão:* perícia criminal. Brasília: Ministério da Justiça, 2013. Disponível em: https:// https://www.novo.justica.gov.br/sua-seguranca-2/seguranca-publica/analise-e-pesquisa/download/pop/procedimento_operacional_padrao-pericia_criminal.pdf. Acesso em: 20 jun. 2020.

29 Cunha, 2020.

tódia nos seguintes termos:[30] "Denomina-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte".

Além disso, o mesmo documento ampliou categoricamente a importância da cadeia de custódia ao qualificá-la da seguinte forma já na parte introdutória do documento normativo: "[...] a cadeia de custódia é fundamental para garantir a idoneidade e a rastreabilidade dos vestígios, com vistas a preservar a confiabilidade e a transparência da produção da prova pericial até a conclusão do processo judicial".

Ainda em relação à Portaria n. 82/2014 do Ministério da Justiça, esse instrumento normativo infralegal também definiu taxativamente as etapas que compreendem uma adequada cadeia de custódia: reconhecimento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte.

Por outro lado, uma portaria ministerial é um instrumento que estabelece instruções e procedimentos necessários à execução de leis, decretos e regulamentos. Em regra, os efeitos de uma portaria ministerial vinculam apenas as atividades desse ministério e os órgãos hierarquicamente subordinados. Ou seja, exceto em relação à Polícia Federal, a Portaria n. 82/2014 do Ministério da Justiça também não criou efeitos vinculativos sobre as atividades periciais. Ficou claro que a cadeia de custódia e a busca pela padronização dos exames periciais ganhavam força no País, no entanto havia uma lacuna legislativa que deveria ser preenchida.

Em 2019, com a promulgação e publicação da Lei n. 13.964, a manutenção das etapas relativas à cadeia de custódia ganhou força vinculativa em nosso ordenamento. O art. 158-A do Pacote Anticrime definiu cadeia de custódia da seguinte forma:

30 Brasil. Ministério da Justiça. *Portaria n. 82, de 16 de julho de 2014*. Estabelece as diretrizes sobre os procedimentos a serem observados no tocante à cadeia de custódia de vestígios. Brasília: Ministério da Justiça, 2014. Disponível em: http://sintse.tse.jus.br/documentos/2014/Jul/18/diario-oficial-da-uniao-secao-1/portaria-no-82-de-16-de-julho-de-2014-estabelece. Acesso em: 5 abr. 2021.

> Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte.

Nas palavras de Rogério Sanches Cunha, o conceito de cadeia de custódia apresentado pela Lei n. 13.964/2019 é "em suma, a sistematização de procedimentos que objetivam a preservação do valor probatório da prova pericial caracterizada, mais precisamente, da sua autenticidade".[31]

Ainda segundo esse autor, o art. 158-A do CPP se preocupa em certificar a preservação dos vestígios desde o contato inicial até o descarte dos elementos coletados, atestando-se a sua qualidade mediante a documentação cronológica dos atos executados em consonância às normas técnicas previstas. Cunha vai além, e de forma mais incisiva afirma que a prova pericial que observa fielmente a cadeia de custódia pode ser considerada uma prova irrefutável, assumindo caráter ímpar frente ao juízo.[32]

O art. 158-B do Pacote Anticrime, por sua vez, definiu que a cadeia de custódia equivale ao rastreamento do vestígio nas dez seguintes etapas:[33]

> I - reconhecimento: ato de distinguir um elemento como de potencial interesse para a produção da prova pericial;
>
> II - isolamento: ato de evitar que se altere o estado das coisas, devendo isolar e preservar o ambiente imediato, mediato e relacionado aos vestígios e local de crime;
>
> III - fixação: descrição detalhada do vestígio conforme se encontra no local de crime ou no corpo de delito, e a sua posição na área de

31 Cunha, 2020, p. 174.

32 Cunha, 2020.

33 Cabe salientar que essas etapas são praticamente as mesmas mencionadas pela Portaria n. 82/2014 do então Ministério da Justiça (atualmente Ministério da Justiça e Segurança Pública), exceção à etapa de isolamento.

exames, podendo ser ilustrada por fotografias, filmagens ou croqui, sendo indispensável a sua descrição no laudo pericial produzido pelo perito responsável pelo atendimento;

IV - coleta: ato de recolher o vestígio que será submetido à análise pericial, respeitando suas características e natureza;

V - acondicionamento: procedimento por meio do qual cada vestígio coletado é embalado de forma individualizada, de acordo com suas características físicas, químicas e biológicas, para posterior análise, com anotação da data, hora e nome de quem realizou a coleta e o acondicionamento;

VI - transporte: ato de transferir o vestígio de um local para o outro, utilizando as condições adequadas (embalagens, veículos, temperatura, entre outras), de modo a garantir a manutenção de suas características originais, bem como o controle de sua posse;

VII - recebimento: ato formal de transferência da posse do vestígio, que deve ser documentado com, no mínimo, informações referentes ao número de procedimento e unidade de polícia judiciária relacionada, local de origem, nome de quem transportou o vestígio, código de rastreamento, natureza do exame, tipo do vestígio, protocolo, assinatura e identificação de quem o recebeu;

VIII - processamento: exame pericial em si, manipulação do vestígio de acordo com a metodologia adequada às suas características biológicas, físicas e químicas, a fim de se obter o resultado desejado, que deverá ser formalizado em laudo produzido por perito;

IX - armazenamento: procedimento referente à guarda, em condições adequadas, do material a ser processado, guardado para realização de contraperícia, descartado ou transportado, com vinculação ao número do laudo correspondente;

X - descarte: procedimento referente à liberação do vestígio, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial.

O art. 158-D da Lei n. 13.964/2019, também incorporado ao CPP, explana as determinações relativas ao acondicionamento dos vestígios. Na sequência, o art. 158-E apresenta um ponto muito

importante. Ele assenta que todos os Institutos de Criminalística "deverão ter uma central de custódia destinada à guarda e controle dos vestígios, e sua gestão deve ser vinculada diretamente ao órgão central de perícia oficial de natureza criminal".

Na literalidade do registro, apenas os Institutos de Criminalística devem se adequar a esse ponto. Contudo, considerando que outros órgãos e entidades poderão desenvolver atividades de cunho pericial (por exemplo, os Ministérios Públicos), surge para o autor uma dúvida acerca da necessidade de criação da central de custódia por parte dessas outras entidades. Por fim, o art. 158-F ratifica que todo o material retirado da central de custódia para exame pericial deve ser devolvido a esse ambiente após a conclusão do procedimento.

3.4 Boas práticas para a manutenção da cadeia de custódia dos vestígios digitais

Ainda no desenvolver deste artigo, detectou-se a existência de um montante razoável de leis, portarias, normas técnicas e procedimentos operacionais voltados ao adequado tratamento e manutenção da cadeia de custódia dos vestígios digitais. Dessa forma, num viés prático, esta seção objetiva apresentar três compilados que intentam apoiar a manutenção da cadeia de custódia de vestígios digitais associados às seguintes fontes: a) computadores e dispositivos de armazenamento; b) dispositivos móveis; c) dados telemáticos oriundos de prestadoras de serviço de aplicação na internet.

Cada um dos compilados de boas práticas relativos à manutenção da cadeia de custódia está estruturado nas dez etapas definidas pelo art. 158-B do Código Processual Penal brasileiro. Ademais, cada uma dessas etapas está explanada mediante sugestões de ações práticas e objetivas embasadas na legislação ou em outros documentos pertinentes.

Importante destacar que o resultado apresentado não vislumbra ser um modelo plenamente assertivo e rígido, afinal cada organização possui a sua necessidade, mas pretende sim servir de apoio neste momento de necessária mudança. Por fim, com o objetivo de facilitar a compreensão, os produtos finais desta seção estão apresentados como apêndices.

4 Conclusão

A promulgação da Lei n. 13.964/2019 apresentou uma série de inovações jurídicas que necessitaram e ainda necessitam ser absorvidas pelas forças da lei e operadores do direito. Dentre essas mudanças legislativas, destacam-se os arts. 158-A a 158-F, que serviram de motivação para esta pesquisa.

No tocante aos aspectos relacionados ao tratamento da prova pericial e à manutenção da cadeia de custódia, em que pese a atenção a esse tipo de prova não ser uma inovação absoluta no arcabouço jurídico do nosso País, é inegável que as mudanças apresentadas pela Lei n. 13.964/2019 foram relevantes.

Os artigos supracitados, por vezes, apresentaram detalhes procedimentais minuciosos; por outro lado, de forma compreensível, deixaram um certo vácuo, forçando, assim, os envolvidos a criarem os devidos procedimentos com vistas à manutenção da integridade da prova pericial e à garantia da manutenção da cadeia de custódia.

Adicionalmente, durante as inúmeras leituras dos arts. 158-A a 158-F, ficou claro, ao menos aos olhos deste articulista, que o legislador delineou o vestígio penal como algo material, físico, concreto, palpável. Não há qualquer menção direta ou sugestão de que esses artigos foram redigidos considerando as particularidades dos vestígios informáticos.

Ainda assim, apesar da inexistência de qualquer aspecto desenhado claramente para os vestígios informáticos, não é possível que as forças da lei e demais envolvidos ignorem os arts. 158-A a 158-F, afinal não há na lei essa exceção. Dessa forma, objetivamente convém aos envolvidos, principalmente às forças da lei: entender o cerne das alterações legislativas; seguir o dispositivo infraconstitucional naquilo que for aplicável; criar e respeitar os procedimentos voltados à manutenção da cadeia de custódia dos vestígios digitais.

A especificidade do vestígio digital fica ainda mais cristalina quando estudadas as normas técnicas nacionais e internacionais, bem como os procedimentos operacionais já existentes em algumas

forças da lei acerca do assunto. Portanto, ao desenvolver os adequados procedimentos operacionais, são condições básicas buscar fontes de conhecimento complementares ao ordenamento jurídico infraconstitucional e adaptar esses redigidos aos casos concretos e práticos. Dentre essas fontes, destaque para a NBR ISO/IEC 27037, a RFC 3227, as publicações 800-86 e 80-101 R1 do NIST e o Procedimento Operacional Padrão de Perícia Criminal do Ministério da Justiça e Segurança Pública.

Finalmente, nesse cenário de tempestiva mudança, foram produzidos e disponibilizados por esta pesquisa três compilados de boas práticas que objetivam apoiar as mudanças organizacionais que buscam a adequação à legislação processual penal.

Referências

Associação Brasileira de Normas Técnicas. *NBR ISO/IEC 27037: Diretrizes para identificação, coleta, aquisição e preservação de evidência digital*. Rio de Janeiro, 2013. Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=307273. Acesso em: 10 mar. 2020.

Ayers, Rick; Brothers, Sam; Jansen, Wayne. *National Institute of Standards and Technology Special Publication 800-101:* Revision 1. Guidelines on Mobile Device Forensics. Maio 2014. Disponível em: https://www.nist.gov/publications/guidelines-mobile-device-forensics. Acesso em: 1º out. 2020.

Brasil. Câmara dos Deputados. *Projeto de Lei n. 10.372/2018*. Disponível em: https://www.camara.leg.br/propostas-legislativas/2178170. Acesso em: 20 abr. 2020.

Brasil. *Decreto-Lei n. 2.848, de 7 de dezembro de 1940*. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 30 abr. 2020.

Brasil. *Decreto-Lei n. 3.689, de 3 de outubro de 1941*. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 30 abr. 2020.

Brasil. *Lei n. 13.964, de 24 de dezembro de 2019*. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13964.htm. Acesso em: 4 mar. 2020.

Brasil. Ministério da Justiça. *Portaria n. 82, de 16 de julho de 2014*. Estabelece as diretrizes sobre os procedimentos a serem observados no tocante à cadeia de custódia de vestígios. Brasília: Ministério da Justiça, 2014. Disponível em: http://sintse.tse.jus.br/documentos/2014/Jul/18/diario-oficial-da-uniao-secao-1/portaria-no-82-de-16-de-julho-de-2014-estabelece. Acesso em: 5 abr. 2021.

Brasil. Ministério da Justiça. *Procedimento operacional padrão:* perícia criminal. Brasília: Ministério da Justiça, 2013. Disponível em: https://https://www.novo.justica.gov.br/sua-seguranca-2/seguranca-publica/analise-e-pesquisa/download/pop/procedimento_operacional_padrao-pericia_criminal.pdf. Acesso em: 20 jun. 2020.

Brasil. Ministério Público Federal. *Roteiro de atuação de crimes cibernéticos*. 3. ed. Brasília: Ministério Público Federal, 2ª Câmara de Coordenação e Revisão, 2016. Disponível sob demanda em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes. Acesso em: 20 ago. 2020.

Caiado, Felipe B.; Caiado, Marcelo. Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse. *In:* Domingos, Fernanda Teixeira Souza *et al*. (coord.). *Crimes Cibernéticos*: coletânea de artigos. v. 3. Brasília: Ministério Público Federal – 2ª Câmara de Coordenação e Revisão, 2018. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos. Acesso em: 18 ago. 2020.

Comitê Gestor da Internet no Brasil. *TIC Domicílios 2015*. São Paulo, 2016. Disponível em: https://cetic.br/pt/tics/domicilios/2015/domicilios/A4/expandido. Acesso em: 18 ago. 2020.

Comitê Gestor da Internet no Brasil. *TIC Domicílios 2015* – Indivíduos. São Paulo, 2016. Disponível em: https://www.cetic.br/pt/tics/domicilios/2015/individuos/C1/. Acesso em: 18 ago. 2020.

Comitê Gestor da Internet no Brasil. *TIC Domicílios 2017.* São Paulo, 2018. Disponível em: https://cetic.br/pt/tics/domicilios/2017/domicilios/A4/expandido. Acesso em: 18 ago. 2020.

Comitê Gestor da Internet no Brasil. *TIC Domicílios 2017* – Indivíduos. São Paulo, 2018. Disponível em: https://www.cetic.br/pt/tics/domicilios/2017/individuos/C1/. Acesso em: 18 ago. 2020.

Comitê Gestor da Internet no Brasil. *TIC Domicílios 2019.* São Paulo, 2020. Disponível em: https://cetic.br/pt/tics/domicilios/2019/domicilios/A4/expandido. Acesso em: 18 ago. 2020.

Comitê Gestor da Internet no Brasil. *TIC Domicílios 2019 – Indivíduos.* São Paulo, 2020. Disponível em: https://www.cetic.br/pt/tics/domicilios/2019/individuos/C1. Acesso em: 18 ago. 2020.

Cunha, Rogério Sanches. *Pacote Anticrime*: Lei 13.964/2019 – Comentários às alterações no CP, CPP e LEP. Salvador: JusPodivm, 2020.

Internet Engineering Task Force. *RFC 3227:* Guidelines for evidence collection and archiving. Fremont, 2002. Disponível em: https://www.ietf.org/rfc/rfc3227.txt. Acesso em: 19 ago. 2020.

Kist, Dário José. *A prova digital no processo penal.* Leme-SP: JH Mizuno, 2019.

National Institute of Standards and Technology. *Guide to integrating forensic techniques into incident response.* NIST Special Publication 800-86. Gaithersburg: NIST, 2006. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-86/final. Acesso em: 18 ago. 2020.

Prado, Geraldo. *A cadeia de custódia de prova no processo penal.* São Paulo: Marcial Pons, 2019.

Vianna, Túlio; Machado, Felipe. *Crimes informáticos:* conforme a Lei nº 12.737/2012. Belo Horizonte: Fórum, 2013.

Vieira, Thiago. *Aspectos técnicos e jurídicos da prova digital no processo penal.* 2019. Disponível em: https://medium.com/@tocvieira/aspectos-t%C3%A9cnicos-e-jur%C3%ADdicos-da-prova-digital-no-processo-penal-aa22ef05fb30. Acesso em: 30 mar. 2021.

Apêndice I • Manutenção da cadeia de custódia de computadores e dispositivos de armazenamento

Exemplos de ativos	Desktops, notebooks, Hard Drive Disks, Solid State Drives, cartões de memória e pendrives.
Premissa	• O dispositivo encontrava-se desligado (não energizado) no momento do primeiro contato com o agente. • O dispositivo em questão foi alvo de execução de busca e apreensão.

Reconhecimento	
Ação	**Fundamentação**
Reconhecer e identificar elementos como de potencial interesse para a produção de prova pericial.	a) CPP, art. 158-B, I. b) NBR ISO/IEC 27037/2013, item 5.4.2. c) NIST Special Publication 800-86, item 3.1.1.

Isolamento	
Ação	**Fundamentação**
Isolar e preservar o ambiente imediato, mediato e relacionado ao vestígio e local de crime. Atentar-se ao fato de que os equipamentos podem conter vestígios físicos que podem ser de interesse ou exigir cuidados de manipulação, tais como impressões digitais, resíduos orgânicos (cabelo, pele, sangue etc.) ou outros materiais contaminantes.	a) CPP, art. 158-B, II. b) NBR ISSO/IEC 27037/2013, item 6.2.1. c) Procedimento Operacional Padrão – MJSP, POP n. 3.1, item 4.1.
Questionar os prováveis proprietários do dispositivo sobre possíveis senhas de descriptografia e, caso elas sejam fornecidas, registrá-las em documento.	a) Sugestão do autor.
Remover possível fonte de alimentação conectada ao dispositivo.	a) NBR ISO/IEC 27037/2013, item 7.1.2.2.
Etiquetar, desconectar e proteger todos os cabos e portas do dispositivo.	a) NBR ISO/IEC 27037/2013, item 7.1.2.2.

Fixação	
Ação	**Fundamentação**
Descrever detalhadamente, em documento, o dispositivo encontrado no local da operação. Convém registrar, minimamente, os seguintes pontos: • data e hora da operação; • localização do ativo no ambiente; • identificação dos envolvidos na operação, inclusive as testemunhas; • indicação do provável proprietário do dispositivo; • descrição do ativo, contemplando, marca, modelo, número de série, cor e aparente estado de conservação.	a) CPP, art. 158-B, III. b) RFC 3227, item 3.2.

Coleta	
Ação	**Fundamentação**
Recolher o dispositivo que será submetido à análise pericial. Adicionalmente, é importante que o agente responsável por essa ação colete qualquer material que possa estar relacionado a potencial informação, por exemplo: papel com senhas registradas, carregadores, conectores e adaptadores de conexão.	a) CPP, art. 158-B, IV. b) CPP, art. 158-C. c) NBR ISO/IEC 27037/2013, item 5.4.3.

Acondicionamento	
Ação	**Fundamentação**
Acondicionar o dispositivo em embalagem para proteção contra impactos físicos e eletromagnéticos.	a) CPP, art. 158-D, § 2º.
Acondicionar individualmente o dispositivo em sacola plástica transparente inviolável, numerada e com identificação da instituição. Convém registrar nessa sacola, minimamente, os seguintes pontos: • data e hora da ação; • descrição sucinta do ativo apreendido; • nome e assinatura do responsável pelo acondicionamento. Por fim, a sacola deve ser lacrada.	a) CPP, art. 158-B, V. b) CPP, art. 158-D. c) CPP, art. 158-D, § 1º. d) CPP, art. 158-D, § 3º. e) CPP, art. 158-D, § 4º. f) CPP, art. 158-D, § 5º. g) NBR ISO/IEC 27037/2013, item 5.4.5. h) NBR ISO/IEC 27037/2013, item 6.9.3.

Transporte	
Ação	**Fundamentação**
Transportar o dispositivo à Central de Custódia da força da lei.	a) CPP, art. 158-B, VI. b) NBR ISO/IEC 27037/2013, item 6.9.4.

Recebimento	
Ação	**Fundamentação**
Transferir formalmente a posse do dispositivo, por exemplo, à Central de Custódia. Convém que o documento de registro contemple, minimamente, os seguintes pontos: • número do procedimento relacionado à apreensão do dispositivo; • unidade da força da lei relacionada; • local de origem do dispositivo; • identificação do responsável pela entrega do dispositivo; • identificação do responsável pelo recebimento do dispositivo.	a) CPP, art. 158-B, VII.

Processamento	
Ação	**Fundamentação**
Identificar o dispositivo. Essa identificação deve conter, minimamente: marca, modelo, número de série, cor, registro fotográfico e aparente estado de conservação.	a) Procedimento Operacional Padrão – MJSP, POP n. 3.1, item 4.1.

Processamento	
Ação	**Fundamentação**
Executar a duplicação do dispositivo de armazenamento e documentar as atividades, os métodos e as ferramentas utilizadas. Sugere-se a utilização de arquivo imagem para armazenamento da duplicação forense. Observação 1: Convém utilizar ferramentas e técnicas forenses com vistas à execução da duplicação do dispositivo de armazenamento sem adulteração do dispositivo questionado. Observação 2: Nos termos da NBR ISO 27037:2013, essa ação descrita é denominada como aquisição. Observação 3: Convém calcular e registrar no laudo técnico o valor *hash* SHA-256, ou SHA-512, do arquivo imagem gerado a partir do dispositivo questionado (*vide* observação 1).	a) CPP, art. 158-B, VIII. b) NBR ISO/IEC 27037/2013, item 5.4.4. c) NIST Special Publication 800-86, item 3.1.2. d) Procedimento Operacional Padrão – MJSP, POP n. 3.1, item 4.2.
Realizar o processamento de dados necessários à análise a partir da imagem coletada. Essa etapa pode envolver, por exemplo, a recuperação dos arquivos apagados, a checagem de assinatura de arquivos, a categorização e a indexação dos dados.	a) CPP, art. 158-B, VIII. b) NIST Special Publication 800-86, item 3.2. c) Procedimento Operacional Padrão – MJSP, POP n. 3.1, item 4.3.

Processamento	
Ação	**Fundamentação**
Analisar os dados apresentados na busca da resposta ao quesito formulado pelo demandante.	a) CPP, art. 158-B, VIII. b) NIST Special Publication 800-86, item 3.3. c) Procedimento Operacional Padrão – MJSP, POP n. 3.1, item 4.4.
Formalizar o exame pericial mediante, por exemplo, laudo técnico.	a) CPP, art. 158-B, VIII. b) NIST Special Publication 800-86, item 3.4. c) Procedimento Operacional Padrão – MJSP, POP n. 3.1, item 4.5.

Armazenamento	
Ação	**Fundamentação**
Armazenar o dispositivo em local adequado, por exemplo, na Central de Custódia. Um local adequado deve contemplar, minimamente: • registros de entrada e saída de vestígios, incluindo data, hora e responsável pela ação; • acesso restrito e controlado a pessoas autorizadas.	a) CPP, art. 158-B, IX. b) CPP, art. 158-E, § 1º. c) CPP, art. 158-E, § 2º. d) CPP, art. 158-E, § 3º. e) CPP, art. 158-E, § 4º. f) CPP, art. 158-F. g) NBR ISO/IEC 27037/2013, item 5.4.5.

Descarte	
Ação	**Fundamentação**
Liberação do equipamento, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial.	a) CPP, art. 158-B, IX.

Apêndice II • Manutenção da cadeia de custódia de dispositivos móveis

Exemplos de ativos	Smartphones e tablets.
Premissa	• O dispositivo encontrava-se desligado (não energizado) no momento do primeiro contato com o agente. • O dispositivo em questão foi alvo de execução de busca e apreensão.

Reconhecimento	
Ação	**Fundamentação**
Reconhecer e identificar elementos como de potencial interesse para a produção de prova pericial.	a) CPP, art. 158-B, I. b) NBR ISO/IEC 27037/2013, item 5.4.2. c) NIST Special Publication 800 -101 r 1, item 4.1.

Isolamento	
Ação	**Fundamentação**
Isolar e preservar o ambiente imediato, mediato e relacionado ao vestígio e local de crime. Atentar-se para o fato de que os equipamentos podem conter vestígios físicos que podem ser de interesse ou exigir cuidados de manipulação, tais como impressões digitais, resíduos orgânicos (cabelo, pele, sangue etc.) ou outros materiais contaminantes.	a) CPP, art. 158-B, II. b) NBR ISO/IEC 27037/2013, item 6.2.1. c) Procedimento Operacional Padrão – MJSP, POP n. 3.1, item 4.1.

Isolamento	
Ação	**Fundamentação**
Remover o cartão SIM, caso esteja presente no equipamento, ou ativar o "modo avião".	a) Procedimento Operacional Padrão – MJSP, POP n. 3.2, item 4.1. b) NIST Special Publication 800-101 r 1, item 4.3.
Questionar os prováveis proprietários do dispositivo sobre possíveis senhas de descriptografia ou bloqueio de tela. Caso elas sejam fornecidas, validá-las na prática e registrá-las em documento.	a) Sugestão do autor.
Verificar, se possível, a configuração dos aplicativos de mensageria acerca da função "duplo fator de autenticação" e desativá-la, caso esteja ativada.	a) Sugestão do autor.

Fixação	
Ação	**Fundamentação**
Descrever, em documento, detalhadamente o dispositivo encontrado no local da operação. Convém registrar, minimamente, os seguintes pontos: • data e hora da operação; • localização do ativo no ambiente; • identificação dos envolvidos na operação, inclusive as testemunhas; • indicação do provável proprietário do dispositivo; • descrição do ativo, contemplando marca, modelo, número de série, cor e aparente estado de conservação.	a) CPP, art. 158-B, III. b) RFC 3227, item 3.2. c) NIST Special Publication 800-101 r 1, item 4.2.

Coleta	
Ação	**Fundamentação**
Recolher o dispositivo que será submetido à análise pericial. Adicionalmente, é importante que o agente responsável por essa ação colete qualquer material que possa estar relacionado a potencial informação, por exemplo: papel com senhas registradas, carregadores, conectores e adaptadores de conexão.	a) CPP, art. 158-B, IV. b) CPP, art. 158-C. c) NBR ISO/IEC 27037/2013, item 5.4.3.

Acondicionamento	
Ação	**Fundamentação**
Acondicionar individualmente o dispositivo em sacola plástica transparente inviolável, numerada e com identificação da instituição. Convém registrar nessa sacola, minimamente, os seguintes pontos: • data e hora da ação; • descrição sucinta do ativo apreendido; • nome e assinatura do responsável pelo acondicionamento. Por fim, a sacola deve ser lacrada.	a) CPP, art. 158-B, V. b) CPP, art. 158-D. c) CPP, art. 158-D, § 1º. d) CPP, art. 158-D, § 3º. e) CPP, art. 158-D, § 4º. f) CPP, art. 158-D, § 5º. g) NBR ISO/IEC 27037/2013, item 5.4.5. h) NBR ISO/IEC 27037/2013, item 6.9.3.

Transporte	
Ação	**Fundamentação**
Transportar o dispositivo à Central de Custódia da força da lei.	a) CPP, art. 158-B, VI. b) NBR ISO/IEC 27037/2013, item 6.9.4. c) NIST Special Publication 800-101 r 1, item 4.4.

Recebimento	
Ação	**Fundamentação**
Transferir formalmente a posse do dispositivo, por exemplo, à Central de Custódia. Convém que o documento de registro contemple, minimamente, os seguintes pontos: • número do procedimento relacionado à apreensão do dispositivo; • unidade da força da lei relacionada; • local de origem do dispositivo; • identificação do responsável pela entrega do dispositivo; • identificação do responsável pelo recebimento do dispositivo.	a) CPP, art. 158-B, VII.

Processamento	
Ação	**Fundamentação**
Identificar o dispositivo. Essa identificação deve conter, minimamente: marca, modelo, número de série, cor, registro fotográfico, ICCID,[34] IMEI,[35] IMSI,[36] MSISDN[37] e aparente estado de conservação.	a) Procedimento Operacional Padrão – MJSP, POP n. 3.2, item 4.1. b) NIST Special Publication 800-101 r 1, item 5.1.
Carregar a bateria do dispositivo.	a) Procedimento Operacional Padrão – MJSP, POP n. 3.2, item 4.1.
Remover o cartão SIM, caso ainda esteja presente no equipamento.	a) Procedimento Operacional Padrão – MJSP, POP n. 3.2, item 4.1. b) NIST Special Publication 800-101 r 1, item 4.3.
Clonar ou extrair os dados do cartão SIM, caso esteja disponível.	a) CPP, art. 158-B, VIII. b) Procedimento Operacional Padrão – MJSP, POP n. 3.2, item 4.1.

34 *Integrated Circuit Chip Card Identification* é o número identificador único e global do cartão SIM.

35 *International Mobile Equipment Identity* é o número de identificação único e global do equipamento de telefonia.

36 *International Mobile Subscriber Identity* é um número de 15 dígitos que determina a identidade internacional da linha de telefonia/dados. Ele é formado pelos códigos MCC (*Mobile Country Code*) + MNC (*Mobile Network Code*) + MSIN (*Mobile Station Identification Number*).

37 *Mobile Service ISDN Number* é o número provido pela operadora que representa o número discado associado ao assinante. Ele é formado pelos códigos CC (*Country Code*) + NDC (*National Destination Code*) + SN (*Subscriber Number*).

Processamento	
Ação	**Fundamentação**
Realizar a extração dos dados do dispositivo em nível lógico, sistema de arquivos e (ou) físico. Observação 1: *A priori*, caso exista algum cartão de memória associado, ele deve estar inserido no dispositivo móvel no momento da extração dos dados. Observação 2: *A priori*, o equipamento deverá ser ligado para execução dessa extração. Portanto, é importante confirmar se o dispositivo encontra-se em "modo avião". Observação 3: Convém registrar no laudo técnico o valor *hash* do arquivo imagem do dispositivo ou do relatório gerado pela ferramenta forense. Observação 4: A extração manual deve ser executada somente como última alternativa.	a) CPP, art. 158-B, VIII. b) Procedimento Operacional Padrão – MJSP, POP n. 3.2, itens 4.2 e 5. c) NIST Special Publication 800-101 r 1, item 5.3.
Realizar o processamento de dados necessários à análise a partir dos dados coletados. Essa etapa pode envolver, por exemplo, informações acerca do usuário, agenda de contatos, listas de chamadas, calendários, áudios, vídeos, registros de localização e aplicativos de mensageria.	a) CPP, art. 158-B, VIII. b) Procedimento Operacional Padrão – MJSP, POP n. 3.2, item 4.3. c) NIST Special Publication 800-101 r 1, item 6.1.
Analisar os dados apresentados na busca da resposta ao quesito formulado pelo demandante.	a) CPP, art. 158-B, VIII. b) Procedimento Operacional Padrão – MJSP, POP n. 3.2, item 4.3.

Processamento	
Ação	**Fundamentação**
Formalizar o exame pericial mediante, por exemplo, laudo técnico.	a) CPP, art. 158-B, VIII. b) NIST Special Publication 800-101 r 1, item 7. c) Procedimento Operacional Padrão – MJSP, POP n. 3.4, item 4.4.

Armazenamento	
Ação	**Fundamentação**
Armazenar o dispositivo em local adequado, por exemplo, na Central de Custódia. Um local adequado deve contemplar, minimamente: • registros de entrada e saída de vestígios, incluindo data, hora e responsável pela ação; • acesso restrito e controlado a pessoas autorizadas.	a) CPP, art. 158-B, IX. b) CPP, art. 158-E, § 1º. c) CPP, art. 158-E, § 2º. d) CPP, art. 158-E, § 3º. e) CPP, art. 158-E, § 4º. f) CPP, art. 158-F. g) NBR ISO/IEC 27037/2013, item 5.4.5.

Descarte	
Ação	**Fundamentação**
Liberação do equipamento, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial.	a) CPP, art. 158-B, IX.

Apêndice III • Manutenção da cadeia de dados telemáticos oriundos de provedoras de serviço de aplicação na internet

Exemplos de ativos	Arquivos com dados telemáticos que contemplem, por exemplo, *e-mails*, histórico de localização, *backup* de aplicação de smartphones e demais arquivos armazenados em nuvem.
Premissa	• Os arquivos foram disponibilizados pela provedora de serviço de aplicação, mediante ordem judicial, via internet. Ou seja, não foram disponibilizadas pelas empresas mídias com esses arquivos.

Reconhecimento	
Ação	**Fundamentação**
Reconhecer e identificar a forma de disponibilização dos arquivos por parte da provedora. Em regra, as empresas apresentam duas soluções: portal próprio para *download* ou disponibilização de *link* direto para *download* dos arquivos.	a) CPP, art. 158-B, I. b) NBR ISO/IEC 27037/2013, item 5.4.2. c) NIST Special Publication 800-06, item 3.1.1.

Isolamento	
Ação	**Fundamentação**
Isolar os arquivos baixados com vistas a evitar adulterações e acessos indevidos.	a) CPP, art. 158-B, IV.

Fixação	
Ação	**Fundamentação**
Descrever detalhadamente, em documento, as informações associadas aos dados disponibilizados. Convém registrar, minimamente, os seguintes pontos: • data e hora da disponibilização dos arquivos por parte da provedora de aplicação; • forma de disponibilização dos arquivos; • identificação do caso perante a provedora de aplicação.	a) CPP, art. 158-B, III. b) RFC 3227, item 3.2.

Coleta	
Ação	**Fundamentação**
Realizar o *download* dos arquivos disponibilizados, inclusive documentos informativos. Além disso, caso esteja disponível, registrar os valores *hashes* dos arquivos apresentados pela provedora de aplicação.	a) CPP, art. 158-B, IV. b) CPP, art. 158-C. c) NBR ISO/IEC 27037/2013, item 5.4.3.

Acondicionamento	
Ação	**Fundamentação**
Não se aplica.	-

Transporte	
Ação	**Fundamentação**
Não se aplica.	-

Recebimento	
Ação	**Fundamentação**
Não se aplica.	-

Processamento	
Ação	**Fundamentação**
Calcular os valores *hashes* dos arquivos coletados. Ademais, convém manter em local isolado os arquivos originais baixados perante a provedora de aplicação.	a) Sugestão do autor.
Executar, quando necessário, a descriptografia dos arquivos.	a) Sugestão do autor.

Processamento	
Ação	**Fundamentação**
Realizar o processamento de dados necessários à análise a partir da imagem coletada. Essa etapa pode envolver, por exemplo, a recuperação dos arquivos apagados, checagem de assinatura de arquivos, categorização e indexação dos dados.	a) CPP, art. 158-B, VIII. b) NIST Special Publication 800-06, item 3.2.
Analisar os dados apresentados na busca da resposta ao quesito formulado pelo demandante.	a) CPP, art. 158-B, VIII. b) NIST Special Publication 800-06, item 3.3.
Formalizar o exame pericial mediante, por exemplo, laudo técnico.	a) CPP, art. 158-B, VIII. b) NIST Special Publication 800-06, item 3.4.

Armazenamento	
Ação	**Fundamentação**
Armazenar os arquivos em sistema de armazenamento adequado. Esse ambiente deve contemplar, minimamente: • registros de acesso aos vestígios, incluindo data, hora e responsável pela ação; • acesso restrito e controlado a pessoas autorizadas.	a) CPP, art. 158-B, IX. b) CPP, art. 158-E, § 1º. c) CPP, art. 158-E, § 2º. d) CPP, art. 158-E, § 3º. e) CPP, art. 158-E, § 4º. f) CPP, art. 158-F. g) NBR ISO/IEC 27037/2013, item 5.4.5.

Descarte	
Ação	**Fundamentação**
Exclusão definitiva dos arquivos, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial.	a) CPP, art. 158-B, IX.