APONTAMENTOS SOBRE A CADEIA DE CUSTÓDIA DA PROVA DIGITAL NO BRASIL

NOTES ON THE DIGITAL TEST CUSTODY CHAIN IN BRAZIL

Mário Furlaneto Neto[1]

José Eduardo Lourenço dos Santos[2]

RESUMO

A Lei nº 13.964, de 24 de dezembro de 2019, modificou representativamente o Código de Processo Penal. Dentre as alterações mais relevantes pode-se citar a regulamentação da cadeia de custódia no direito processual penal brasileiro. Utilizou-se o método dedutivo e procedimentos de revisão doutrinária, legislativa e jurisprudencial objetivando debater metodologias para padronizar a recuperação de dados armazenados em dispositivos informáticos no Brasil. Concluiu-se ser necessária prévia ordem judicial para a realização de perícia computacional forense, assim como a adoção da norma ABNT NBR ISO/IEC 27037:2012 e Procedimento Operacional Padrão (POP/SENASP), veiculado pela Secretaria Nacional de Segurança (SENASP), enquanto referenciais teóricos para a realização das periciais computacionais forenses visando a produção da prova digital íntegra e autêntica. Impõe-se, ainda, a necessidade do aparelhamento e especialização de policiais e peritos computacionais forenses para atender o crescente aumento dos índices de crimes digitais.

PALAVRAS-CHAVE: cadeia de custódia da prova penal, perícia forense digital, vestígio tecnológico, investigação criminal cibernética, evidência eletrônica.

ABSTRACT

Law No. 13,964, of December 24, 2019, significantly modified the Code of Criminal Procedure. Among the most relevant changes can be cited the chain of custody regulation in Brazilian criminal procedural law. The deductive method and procedures for doctrinal, legislative and jurisprudential review were used to discuss methodology to standardize the recovery of data stored on computer devices in Brazil. It was concluded that a prior court order was necessary to carry out computer forensic expertise, as well as the adoption of the ABNT NBR ISO/IEC 27037: 2012 standard and Standard Operating Procedure (SOP), published by the National Security Secretariat (SENASP), while theoretical references for conducting those of computer forensic experts aiming at producing

[1]Doutorado em Ciência da Informação pela Universidade Estadual Paulista Júlio de Mesquita Filho (2008). Graduado em Direito pela Faculdade de Direito de Marília Fundação Eurípides Soares da Rocha (1990), Mestrado (2003). Atualmente é professor titular da graduação e do Mestrado em Direito do Centro Universitário Eurípides de Marília (UNIVEM), mantido pela Fundação de Ensino Eurípides Soares da Rocha, Delegado de Polícia da Polícia Civil do Estado de São Paulo, professor da Academia da Polícia Civil do Estado de São Paulo, atuando principalmente nos seguintes temas: crimes informáticos, furto mediante fraude, pornografia infantil na internet, inquérito policial eletrônico e biobancos.

[2] Doutorado em Direito pela Universidade Federal do Paraná (UFPR - 2013) e Pós-Doutorado na Universidade de Coimbra (área de Democracia e Direitos Humanos - 2016). Graduado em Direito pela Fundação de Ensino Eurípides Soares da Rocha (1988), Mestrado em Direito pela Fundação de Ensino Eurípides Soares da Rocha (2002),Atualmente é professor do Centro Universitário Eurípides de Marília, Graduação e Mestrado. Tem experiência na área de Direito, com ênfase em Direito Penal, atuando principalmente nos seguintes temas: Direito Penal, Criminologia, Direito e Internet, Direito Processual Penal, Direitos Fundamentais, Derrotabilidade Normativa e Novos Direitos.

full and authentic digital evidence. There is also a need for the equipping and specialization of police and computer forensic experts in order to meet for growing increase in digital crime rates.

KEYWORDS: chain of custody of criminal evidence, digital forensic expertise, technological trace, cybercriminal investigation, electronic evidence.

INTRODUÇÃO

A Lei nº 13.964, de 24 de dezembro de 2019 (BRASIL, 2019a), em vigor desde 23 de janeiro de 2020, aperfeiçoou a legislação vigente e modificou representativamente o Código de Processo Penal. As alterações mais relevantes foram: criação da cadeia de custódia no direito processual penal, consolidação do acordo de não persecução criminal pelo Ministério Público, bem como infiltrações de agentes na repressão de crimes específicos[3].

O instituto da cadeia de custódia, previsto a partir do artigo 158-A da Lei nº 13.964/ 2019 (BRASIL, 2019a), conceituou a medida como sendo o conjunto de procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes visando rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte.

Destaca-se que no processo penal a preservação da cadeia de custódia objetiva tutelar "a identidade, integridade e autenticidade dos elementos da prova", inclusive no que tange a eventual necessidade de contraprova (GIACOMOLLI, 2016, p.209). Portanto, a inobservância da cadeia de custódia pode comprometer o contraditório e a ampla defesa, assim como causar consequências relevantes à persecução penal, a gerar, inclusive, eventual nulidade da prova e, consequentemente inviabilizar a prova da materialidade da infração penal.

Nucci (2020) aduz que a inobservância dos procedimentos pertinentes à cadeia de custódia geram nulidades relativas, havendo, portanto, necessidade de arguição no momento processual oportuno, com demonstração de prejuízo efetivo.

Ainda, em relação à prova, insta frisar que, hodiernamente, os conteúdos virtuais armazenados em dispositivos informáticos passaram a influenciar e ter relevância não só no cotidiano das pessoas como, também, na esfera penal e processual penal, no que tange ao esclarecimento da prova da existência do crime e indícios de autoria.

No entanto, diante da escassez de normatização na legislação brasileira relacionada à materialização de vestígios digitais, justamente por sua complexidade, já que vestígios podem estar em diversos suportes e linguagens, assim como ocultados em meios a inúmeros dados ou

[3] Inovou-se, ainda, quanto a instituição do juízo de garantias, cujos dispositivos que o regulamentam estão suspensos por decisão do STF (BRASIL, 2020).

informações, faz-se primordial o debate científico sobre métodos para padronização da recuperação de vestígios digitais armazenados em dispositivos informáticos no âmbito do Brasil.

Adotou-se o método dedutivo, mediante procedimentos de revisão bibliográfica, legislativa e jurisprudencial. Utilizou-se para coleta dos dados a revisão integrativa da literatura (BOTELHO *et al*., 2011) e publicações científicas nacionais. Os resultados foram apresentados na forma descritiva voltados à realidade brasileira.

1 AVANÇOS NA LEGISLAÇÃO BRASILEIRA RELACIONADOS AOS CRIMES VIRTUAIS

No que tange aos tipos penais, partindo do pressuposto de que a maior parte das infrações penais são abertas e podem ser perpetradas por qualquer meio eleito pelo sujeito ativo, o poder legiferante promoveu alterações pontuais no Código Penal como, por exemplo, a recente inserção dos parágrafos 4º e 5º ao artigo 122 do Código Penal, pela Lei Federal nº 13.968/2019 (BRASIL, 2019b), estipulando majorantes quando a instigação, induzimento e auxílio ao suicídio se der por meio da rede mundial de computadores, de rede social ou transmitida em tempo real, ou quando o agente for líder ou coordenador de grupo ou de rede virtual.

Ainda que de forma mais limitada, a legislação processual penal brasileira tem sofrido atualizações para adequar-se a esta nova realidade, em especial no que tange à possibilidade de produção da prova. A Lei Federal 9.296/1996 estipulou no artigo 1º, § único (BRASIL, 1996) a possibilidade da interceptação do fluxo das comunicações de informática e telemática.

Em 2014, a Lei Federal nº 12.965 (BRASIL, 2014), denominada de Marco Civil da Internet, regulamentou o armazenamento dos registros de acesso ao provedor de conexão e ao provedor de aplicação de Internet, assim como a forma para obtenção de tais informações para fins de produção de prova (FURLANETO NETO; GARCIA, 2014).

Em 2017, a Lei Federal nº 13.441 introduziu a figura do agente virtual infiltrado[4] para fins de repressão a crimes contra a dignidade sexual da criança e do adolescente, em cujo contexto se insere, dentre outros, os previstos nos artigos 240, 241, 241-A a D do Estatuto da Criança e do Adolescente (BRASIL, 2017a).

Mais recentemente, a Lei Federal nº 13.964/2019 - Lei Anticrime (BRASIL, 2019a), inseriu o artigo 10-A na Lei Federal nº 12.850/2013 (BRASIL, 2013a) que ampliou a possibilidade

[4] Agente virtual infiltrado: consiste em meio de prova subsidiária, qualificada pela atuação dissimulada (com ocultação da real identidade) e sigilosa de agente policial, seja de forma presencial ou virtual, face a um criminoso ou grupo de criminosos, visando localizar fontes de prova, identificar criminosos e obter elementos de convicção para elucidar o delito e desarticular associação ou organização criminosa, auxiliando também na prevenção de ilícitos penais (BRASIL, 2017a).

de adoção do agente virtual infiltrado enquanto meio de prova para fins de investigar crimes previstos na referida lei e a eles conexos, praticados por organizações criminosas.

A mesma norma modificou o capítulo II do Código de Processo Penal e passou a disciplinar, nos artigos 158-A a F, o instituto da cadeia de custódia. No que diz respeito à preservação das informações coletadas, a cadeia de custódia possibilita documentar a cronologia das evidências, em especial os responsáveis pela coleta e manuseio. Assim, procedimentos como acondicionar evidências em invólucro lacrado e restringir o acesso às evidências apenas aos profissionais responsáveis pela custódia minimizam a possibilidade da manipulação indevida e tornam as evidências mais confiáveis.

Destaca-se que a produção da prova no processo penal, em especial diante de crimes praticados por meio da internet, seja por agentes virtualmente infiltrados ou em face da quebra de dados ou mesmo interceptação do fluxo das comunicações de informática ou telemática, necessita respeitar a cadeia de custódia e adequar-se às novas exigências legais, em especial diante da necessidade de se ter um processo eminentemente garantista, a respeitar os direitos e garantias individuais da pessoa humana (FERRAJOLI, 2013).

A expressão “dispositivo informático” utilizada pelo direito penal refere-se a todo e qualquer dispositivo apto a armazenar dados e informações, interligados ou não à rede mundial de computadores. Logo, um cartão de memória acoplado a um smartphone, com finalidade de ampliar a capacidade de seu armazenamento, deve ser considerado um dispositivo informático por extensão, pois sua funcionalidade está interligada ao dispositivo informático em que está instalado.

Para fins de caracterização de infração penal, o direito penal estabelece a necessidade de indevida violação de mecanismo de segurança assim como exige o elemento subjetivo do injusto, consubstanciado na finalidade específica do agente de obter, adulterar ou destruir dados ou informações. Verifica-se, portanto, que o legislador infraconstitucional, por meio da criminalização da invasão de dispositivo informático alheio, buscou tutelar a liberdade individual na forma da inviolabilidade da intimidade e da vida privada (SCARMANHÃ; FURLANETO NETO; SANTOS, 2014).

Bitencourt (2019) inclusive, sustenta que no âmbito da liberdade individual, a pessoa deve ter a opção de manter alguns aspectos de sua vida em sigilo, em cujo contexto se insere as informações mantidas em dispositivos informáticos, enquanto “princípio de ordem pública”. Parte-se do pressuposto de que se a comunicação por meio de sistema de informática é sigilosa, o produto desta comunicação também deve ser, em observância aos incisos X e XII do artigo 5º da Constituição Federal. Na visão do autor, a tutela penal abrange a “privacidade individual, pessoal ou profissional do ofendido”.

Em que pese haver decisões de alguns tribunais apontando a desnecessidade de ordem judicial para o acesso a dados e informações armazenadas em dispositivos informáticos, o posicionamento contemporâneo do STJ e do STF é no sentido de exigir-se prévia ordem judicial fundamentada para possibilitar o acesso a tais conteúdos (BRASIL, 2018; BRASIL, 2017b; BRASIL 2012; BRASIL, 2019d), em tutela ao direito à intimidade e vida privada, previstos no artigo 5º, inciso X, da CF, em especial por conta do disposto no artigo 7º , III, da Lei nº 12.965/2014 (BRASIL, 2014), que estabelece a inviolabilidade e sigilo das comunicações privadas armazenadas, salvo por ordem judicial

O processo penal brasileiro, que prima pela busca à verdade, evidencia-se, em regra, pela liberdade probatória. Assim, qualquer meio de prova é admitido, desde que não viole a lei, a moral e os bons costumes. Veda-se a prova ilícita, incluindo as que violam regras de ordem processual (provas ilegítimas) e de direito material (provas ilegais). Logo, para o ordenamento jurídico brasileiro, em especial no que tange à prova digital, objeto da presente discussão, a observância do princípio da vedação da prova ilícita é corolário do devido processo legal (ÁVILA; BORRI, 2019).

Nota-se, portanto, que o tema das provas digitais aborda assunto suscetível de discussão, pois envolve o interesse público em obter provas para resolução de ilícitos penais, ao mesmo tempo deve primar pela observância dos direitos fundamentais dos indivíduos envolvidos na demanda, principalmente os que englobam a intimidade e vida privada.

2 CONCEITO E CARACTERÍSTICAS DAS PROVAS DIGITAIS

A prova digital relevante para o processo penal contempla os arquivos informáticos que podem estar em poder do investigado ou de terceiros que contém informações úteis à busca da verdade. Importante ressaltar que as provas digitais compreendem todos os dados ou informações armazenadas em dispositivos informáticos. No entanto, existem algumas informações contempladas pelo processo penal enquanto provas documentais e que estão, a princípio, armazenadas em bancos de dados digitais, como por exemplo, os dados cadastrais do cliente do provedor de conexão à internet (FURLANETO NETO; SANTOS; GIMENES, 2018).

Em outra hipótese, as informações decorrentes da quebra do sigilo bancário de um suspeito, inicialmente armazenadas pela instituição financeira, pode ser enviada digitalmente ao Laboratório de Lavagem de Dinheiro do Departamento de Inteligência da Polícia Civil (LAB-LD) ou fisicamente ao processo onde se decretou a quebra do sigilo, já que referido feito cautelar ainda permanece físico e não está inserido no protocolo do processo digital, ao menos quando a medida é postulada e decretada na fase da investigação criminal.

No Brasil, os meios de obtenção das provas puramente digitais ocorrem por meio de requisição, busca e apreensão, interceptação do fluxo das comunicações de informática e perícia.

Ressalta-se, ainda, que a prova digital pode permanecer por pouco tempo disponível para acesso. Ao mesmo tempo, pode ser de fácil dispersão e armazenamento, com isso, ser de curta durabilidade. Pode, ainda, ser facilmente modificada e/ou dificilmente acessada, dependendo do meio pelo qual foi produzida. Além disso, pode ser transmitida a qualquer dispositivo digital (PEREIRA, 2019).

Sendo assim, as principais características das provas digitais são: imaterialidade, volatilidade, suscetibilidade de clonagem e facilidade de dispersão, necessidade de dispositivo informático para transmissão, conforme descrito na tabela 1 (VAZ, 2012).

Tabela 1- Características da prova digital.

Característica	Descrição
Imaterialidade	A ausência de representação física facilita a transmissão e contribui para o grande armazenamento de conteúdos nos sistemas informáticos. Podem ser transmitidos sem a necessidade de movimentação física.
Volatilidade	Refere-se ao fato de sofrer constantes mudanças. Apresenta-se frágil, facilmente se submete a alterações ou desaparecimento, bastando à modificação da sequência numérica que a compõe.
Suscetibilidade de clonagem e facilidade de dispersão	Em decorrência da imaterialidade torna-se extremamente suscetível ao processo da clonagem. Pode ser facilmente copiada e transmitida a outros dispositivos eletrônicos oferecendo risco à preservação da originalidade do arquivo utilizado como meio de prova.
Necessidade de dispositivo para transmissão	Mesmo sendo imaterial e independente do meio físico onde está armazenada, não se pode eliminar a importância do objeto físico para a repercussão do conteúdo probatório, tendo em vista que é o único meio pelo qual ocorre a exposição, extração ou transmissão da prova. A prova digital ao ser constituída por combinações numéricas, restritas ao ambiente digital, necessita de dispositivos físicos para o processamento e exteriorização. Portanto, dispositivo para transmissão é a única forma de acesso ao teor da prova.

Fonte: Adaptado de Vaz (2012).

Considerando as particularidades da prova digital descritas acima, observa-se que a sua preservação na cadeia de custódia requer procedimentos específicos. Dessa forma, a seguir serão debatidas formas de rastreamento, manuseio e tratamento das evidências digitais.

3 PRESERVAÇÃO DA PROVA DIGITAL NA CADEIA DE CUSTÓDIA

Os artigos 158-A ao 158-F do Código de Processo Penal (BRASIL, 2019a) definiram o conceito da cadeia de custódia e reconheceram sua relevância. Os procedimentos a serem utilizados

para manter e documentar a história cronológica do vestígio[5] coletado em locais ou em vítimas de crimes visando rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte encontram-se na tabela 2.

Tabela 2- Etapas do rastreamento dos vestígios na cadeia de custódia, de acordo com a Lei nº 13.964, de 24 de dezembro de 2019.

Etapa	Descrição
Reconhecimento	Ato de distinguir um elemento como de potencial interesse para a produção da prova pericial.
Isolamento	Procedimento para evitar que se altere o estado das coisas, devendo isolar e preservar o ambiente imediato, mediato e relacionado aos vestígios e local de crime.
Fixação	Descrição detalhada do vestígio conforme se encontra no local de crime ou no corpo de delito, e a sua posição na área de exames, podendo ser ilustrada por fotografias, filmagens ou croqui, sendo indispensável a sua descrição no laudo pericial produzido pelo perito responsável pelo atendimento.
Coleta	Recolhimento de vestígio que será submetido à análise pericial, respeitando suas características e natureza.
Acondicionamento	Processo 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.
Transporte	Transferência do 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.
Recebimento	Ato formal de mudança 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.
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.
Armazenamento	Refere-se 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.
Descarte	Liberação do vestígio, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial.

Fonte: Adaptado de Brasil (2019a).

Nota-se que o início da cadeia de custódia dar-se-á com a preservação do local de crime ou com procedimentos policiais ou periciais que constatam a existência de vestígios. O agente público que reconhecer um elemento como de potencial interesse para a produção da prova pericial fica responsável por sua preservação.

[5] Art. 158-A, § 3º. Vestígio: todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal (BRASIL, 2019a).

A coleta dos vestígios deverá ser realizada preferencialmente por perito oficial, que dará o encaminhamento necessário para a central de custódia, mesmo quando for necessária a realização de exames complementares. Todos os Institutos de Criminalística (IC) deverão ter uma central de custódia destinada à guarda e controle dos vestígios. A gestão deve ser vinculada diretamente ao Órgão Central de Perícia Oficial de natureza criminal.

Verifica-se que o legislador descreveu normas genéricas relativas à cadeia de custódia não contemplando práticas metodológicas referentes aos vestígios digitais. Nesse sentido, Machado (2020) defende a aplicação da Norma ABNT NBR ISO/IEC 27037:2012 (ABNT, 2013), publicada em 09/12/2013 e que entrou em vigência em 09/01/2014, com a finalidade de padronizar o tratamento de evidências digitais.

As normas ISO/IEC são elaboradas pela Organização Internacional de Padronização (ISO) em conjunto com a Comissão Eletrotécnica Internacional (IEC) com o objetivo de melhorar a qualidade de produtos e serviços. No Brasil, estas normas são compostas pela sigla NBR (Norma Brasileira), sendo revisadas e gerenciadas pela Associação Brasileira de Normas Técnicas (ABNT).

Destaca-se que a norma ABNT NBR ISO/IEC 27037:2012 (ABNT, 2013) é referência internacional para identificação, coleta, aquisição e preservação de evidências forenses digitais em todas as etapas no processo de investigação. Faz parte das normas da família ISO 27000 - Gestão da Segurança da Informação, sendo a mais relevante na área de perícia forense digital.

Em vigor no Brasil desde janeiro de 2014, a norma define e descreve as diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Apesar de não se tratar de norma obrigatória, por não haver, ainda, um reconhecimento explícito em lei, é, de fato, a única norma elaborada por organismos competentes e reconhecida no Brasil que trata sobre o tema, além de ser a norma que, em sua versão internacional (ISO), descreve os procedimentos adotados nos ordenamentos de vários países.

Vale frisar, também, que referida norma serve de alicerce e referencial teórico do Procedimento Operacional Padrão (POP) adotado pela Secretaria Nacional de Segurança Pública (SENASP) para fins de estabelecer metodologia padrão para realização de perícia informática forense envolvendo perícias em mídia de armazenamento computacional, em equipamentos computacionais portáteis, em local de informática e em local de internet (BRASIL, 2013b).

A evidência digital considerada na norma ABNT NBR ISO/IEC 27037:2012 (ABNT, 2013) pode ser produzida através de diferentes tipos de dispositivos digitais como HD, disquetes, CD/DVD, pen-drive, smartphones, tabletes, assistentes digitais pessoais (PDA), dispositivos eletrônicos pessoais (PED), cartões de memória, sistemas de navegação móveis (GPS), sistemas embarcados, câmeras digitais de vídeo e fotografias (incluindo CFTV), desktops, notebooks, redes

baseadas em TCP/IP e outros protocolos digitais, bem como dispositivos com funções semelhantes das descritas acima.

De acordo com a norma, toda evidência digital válida deve apresentar três características fundamentais: a) relevância: quando se destina a provar ou refutar um elemento de um caso específico que está sendo investigado, b) confiabilidade: representa o grau de fidelidade de uma informação em relação ao original e c) suficiência: significa que a evidência digital deve ser suficiente para permitir que elementos questionados sejam adequadamente examinados ou investigados.

Detalha, ainda, que a evidência digital pode ser dividida em duas categorias: dados voláteis e dados não voláteis, estas definições são aplicadas às memórias (componentes de armazenamento de informações). A memória RAM[6] é considerada um tipo de memória "volátil", pois os dados que não foram guardados de forma permanente serão apagados após desligamento do computador. A memória ROM[7] e os outros dispositivos de armazenamento de dados são considerados "não voláteis" (como pendrive, HD e SDCard).

A norma ressalta, ainda, quatro aspectos principais no manuseio da evidência digital, sendo eles: auditabilidade, justificabilidade, repetibilidade e reprodutibilidade, conforme apresentado na tabela 3.

Tabela 3- Tratamento da evidência digital de acordo com a Norma ABNT NBR ISO/IEC 27037:2012.

Item	Descrição
Auditabilidade	Identifica se o método científico, técnica ou o procedimento foi adequadamente seguido. Possibilita o processo de exame e validação de um sistema, atividade ou informação. Recomenda-se documentação de todos os processos executados no tratamento da evidência digital.
Repetibilidade	Permite repetição dos resultados dos testes a qualquer tempo depois do teste original utilizando os mesmos procedimentos, métodos de medição e instrumentos, sob as mesmas condições.
Reprodutibilidade	Verifica se os mesmos resultados são produzidos utilizando diferentes instrumentos, diferentes condições e a qualquer tempo.
Justificabilidade	Analisa se todas as ações e métodos utilizados para o tratamento da evidência digital foram adequados para obtenção dos resultados.

Fonte: ABNT (2013).

[6] Existem dois tipos de memórias: RAM e ROM. A memória RAM (*Random Access Memory* - Memória de Acesso Aleatório) é aquela que permite a gravação e a regravação dos dados. É responsável pela leitura dos conteúdos quando requeridos, ou seja, de forma não-sequencial. É uma memória transitória e volátil. Se o computador for desligado, as informações são perdidas (VECCHIA, 2019).

[7] De acordo com o mesmo autor, a memória ROM (*Read Only Memory* - Memória Apenas de Leitura) permite a gravação de dados uma única vez, não sendo possível apagar ou editar a informação, somente acessar a mesma. A memória ROM armazena informações do equipamento, além de ter as instruções de reconhecimento dos diversos periféricos associados. Os dados armazenados, normalmente, são gravados pelo fabricante do equipamento.

O processo de manuseio da evidência digital é composto pelas seguintes etapas: identificação, coleta, aquisição e preservação. Em relação à identificação salienta-se que a evidência digital é representada pela forma física e lógica. A forma física inclui a representação de dados dentro de um dispositivo tangível. A forma lógica da evidência digital refere-se à representação virtual dos dados dentro do dispositivo.

A técnica de identificação envolve a pesquisa, reconhecimento e documentação da evidência digital. Sendo assim, torna-se fundamental iniciar o processo de identificação detectando os dispositivos de processamento que podem conter a evidência digital. Esse procedimento inclui, também, priorizar a coleta das evidências baseada em sua volatilidade. Recomenda-se que a volatilidade dos dados seja identificada para garantir a correta ordem dos métodos de coleta e aquisição para minimizar o risco de dano à prova digital. Convém destacar a necessidade de buscas visando localizar prováveis evidências digitais ocultas como arquivo apagado e/ou adulterado.

Em relação a identificação de mídias, o processo diz respeito tanto à identificação física quanto a identificação lógica que é realizada através do cálculo do valor (ou código) *hash*[8], utilizando funções como MD5[9] (*Memory Digest Algorithm* - Resumo da memória), SHA1[10] (*Secure Hash Algorithm* - Algoritmo de hash seguro) ou SHA2 - mais utilizada atualmente.

Em relação à preservação da prova digital, a norma diz respeito à proteção de sua integridade para garantia de sua utilidade e validade probatória. O processo de preservação envolve a guarda da evidência digital e do dispositivo digital visando garantir a autenticidade da evidência digital.

Deve ser minimizado o manuseio da evidencia e dispositivo informático. Todas as alterações e ações devem ser documentadas. Salienta-se, ainda, que o perito forense deve praticar ações somente dentro de sua área de competência.

Tabela 4- Síntese das etapas do manuseio da evidência digital, de acordo com Norma ABNT NBR ISO/IEC 27037:2012.

Etapa	Descrição
Coleta	Isolar a área, coletar, garantir a integridade, identificar equipamento, embalar e etiquetar evidências digitais.

[8] Código *hash*: corresponde a uma sequência única de letras e número que garantem a integridade dos dados compartilhados.

[9] MD5: é um método que transforma uma palavra em um código. Por meio de um código MD5 *hash* não é possível encontrar a palavra que o originou. É muito utilizado no caso de armazenamento de senhas pessoais.

[10] SHA: a função *hash* gera um valor ou valores de uma sequência de texto usando uma função matemática. É uma maneira de ativar a segurança durante o processo de transmissão de uma mensagem para um destinatário específico. Quando um usuário envia uma mensagem através da segurança SHA, é gerado um *hash* criptografado e enviado junto com a mensagem. O *hash* e a mensagem são decifrados pelo receptor e em seguida é gerado outro *hash* à partir da mensagem. Se os dois *hashes* gerados são semelhantes quando feita a comparação, a transmissão segura foi efetuada (VECCHIA, 2019).

Exame	Localizar, extrair, filtrar e documentar evidências digitais.
Análise	Identificar (pessoas e locais), correlacionar (pessoas e locais), reconstruir a cena e registrar evidências digitais.
Resultados	Redigir laudo, anexar evidências/demais documentos e gerar código Hash de todas evidências digitais.

Fonte: ABNT (2013).

Partindo-se do pressuposto de que todos os crimes que deixam vestígios devem ser alvo de perícia, nos termos do previsto no artigo 158 do CPP (BRASIL, 2019a), importante evidenciar que, eventualmente, haverá a necessidade de coleta de vestígios digitais em empresas ou repartições públicas. Na primeira hipótese, poderá haver interesse de terceiros que não tem qualquer relação com a infração investigada. Na segunda situação, tem-se que o serviço público não pode ser comprometido, havendo então necessidade de coleta dos vestígios digitais no local onde o dispositivo informático estiver instalado minimizando impactos negativos a direitos de terceiros de boa-fé e ao interesse público.

Para tanto, a legitimação da ação investigativa deve estar amparada por mandado de busca e apreensão com expressa autorização judicial para a realização da perícia no dispositivo informático. Defende-se que o Delegado de Polícia responsável pelo cumprimento do mandado de busca e a equipe de policiais civis que o acompanha dirija-se o local do crime em companhia de equipe de peritos computacionais forenses. Os peritos devem ter conhecimento prévio do conteúdo do mandado de busca e apreensão a fim de viabilizar o ato com eficiência.

Segundo o POP veiculado pela SENASP, a equipe computacional forense deve estar munida de equipamento fotográfico, *case* externo de leitura e escrita, *case* externo protegido contra escrita, mídias de inicialização contendo *softwares* forenses, equipamento computacional portátil equipado com *softwares* forenses, assim como *hardwares* para armazenamento dos vestígios digitais a serem coletados (BRASIL, 2013b).

Vale frisar que o exame pericial pode ser *live* ou *post mortem*, isto se o dispositivo informático estiver ligado ou desligado. O POP (BRASIL, 2013b) estabelece modelo para descrever e materializar como os dispositivos foram localizados no ambiente da perícia, como também adotar protocolo para a coleta de vestígios, sem que haja alteração de seu conteúdo a ser assegurado com o emprego de código *hash.*

CONCLUSÃO

Os autores defendem que o conteúdo de dados e informações armazenados em dispositivos informáticos são sigilosos, em observância aos princípios da intimidade e vida privada, impondo-se ordem judicial prévia para fins de realização da perícia computacional forense, consoante

entendimento assentado no STJ e em consolidação no STF, para fins de prova na investigação criminal ou instrução processual penal.

Tanto assim, que os dados e informações armazenados em dispositivos informáticos foram tutelados pelo Código Penal, que criminalizou a invasão, ao tutelar a liberdade individual, nos aspectos relacionadas à privacidade individual, tanto pessoal quanto profissional do titular do hardware onde o conteúdo está armazenado.

O sigilo dos dados e informações armazenados em dispositivos informáticos foi reforçado pelo disposto no artigo 7º, III, da Lei nº 12.965/2014, que prevê expressamente a inviolabilidade e sigilo das comunicações privadas armazenadas, exigindo ordem judicial para a sua revelação.

Há necessidade de emprego das regras de cadeia de custódia para fins de preservação, coleta e armazenamento da prova digital. Para tanto, em caso de busca e apreensão, apontam enquanto modelo ideal, que o perito computacional forense acompanhe a autoridade policial e seus agentes visando a coleta dos vestígios digitais dentro dos padrões estabelecidos pela norma ABNT NBR ISO/IEC 27037:2012 viabilizando a produção de prova íntegra e autêntica, o que poderá, eventualmente, viabilizar a prisão em flagrante do investigado, como, por exemplo, em crimes permanentes, cujo contexto se inserem os casos de posse ou compartilhamento por redes P2P de material pornográfico infanto-juvenil, sem riscos de prejudicar a prova da materialidade da infração.

Salientam, ainda, a adoção da norma ABNT NBR ISO/IEC 27037:2012 em conjunto com o Procedimento Operacional padrão veiculado pela SENASP enquanto referência metodológica para fins da produção da prova pericial em dispositivos informáticos.

Diante do crescimento exponencial da criminalidade informática, impõe-se a especialização de policiais federais e civis, bem como peritos computacionais forenses para viabilizar maior qualidade na repressão criminal de tais infrações penais. Ressaltam que, além do aperfeiçoamento e especialização, há necessidade de aparelhamento de Delegacias de Polícias e Núcleos de Criminalísticas visando para atender a crescente demanda de crimes digitais.

O aparelhamento e especialização de equipes de peritos computacionais forenses para atuar no âmbito da Superintendência da Polícia Técnico Científica, com sede em municípios que comportam Delegacias Seccionais de Polícia, vem ao encontro das exigências contemporâneas para a repressão de crimes que empregam altas tecnologias.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27037:2012 - Tecnologia da informação - Técnicas de segurança - Diretrizes para identificação, coleta,**

aquisição e preservação de evidência digital. 2013. Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=307273. Acesso em: 02 abr. 2020.

ÁVILIA, Gustavo Noronha; BORRI, Luiz Antonio. A cadeia de custódia da prova no "Projeto de Lei Anticrime": suas repercussões em um contexto de encarceramento em massa. **Revista de Direito Univille**, v.16, n.89, p.114-132, 2019.

BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte especial**. 19. ed. São Paulo: Saraiva, 2019. E-Book. Disponível em: app.saraivadigital.com.br/leitor/ebook:648355. Acesso em: 04 abr. 2020.

BOTELHO, Louise Roedel; CUNHA, Cristiano Castro de Almeida; MACEDO, Marcelo. O método da revisão integrativa nos estudos organizacionais. **Gestão e Sociedade**, v.5, n.11, p.121-136, 2011.

BRASIL. Constituição. **Constituição da República Federativa do Brasil**. 1988. Brasília: Senado Federal: Centro Gráfico, 1988.

BRASIL. Lei 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do artigo 5º da Constituição Federal. **Diário Oficial da República Federativa do Brasil**, Brasília: DF, 25 jun. 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L9296.htm. Acesso em: 04 jan. 2020.

BRASIL. Lei 12.850 de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. **Diário Oficial da República Federativa do Brasil**, Brasília: DF, 5 ago. 2013a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/ Lei/L12850.htm. Acesso em: 22 jan. 2020.

BRASIL. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. **Diário Oficial da República Federativa do Brasil**, Brasília: DF, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 jan. 2020.

BRASIL. Lei 13.441, de 8 de maio de 2017. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente. **Diário Oficial da República Federativa do Brasil**, Brasília: DF, 08 maio. 2017a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13441.htm. Acesso em: 25 jan. 2020.

BRASIL. Lei 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. **Diário Oficial da República Federativa do Brasil**, Brasília: DF, 24 dez. 2019a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm. Acesso em: 18 jan. 2020.

BRASIL. Lei Federal 13.968, de 26 de dezembro de 2019. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para modificar o crime de incitação ao suicídio e incluir as condutas de induzir ou instigar a automutilação, bem como a de prestar auxílio a quem a pratique. **Diário Oficial da República Federativa do Brasil**, Brasília: DF, 26 dez. 2019b. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13968.htm>. Acesso em: 15 jan. 2020.

BRASIL. Secretaria Nacional de Segurança Pública. **Procedimento operacional padrão: perícia criminal**. Secretaria Nacional de Segurança Pública: Ministério da Justiça, 2013b.

BRASIL. Superior Tribunal de Justiça de Minas Gerais (5ª Câmara Criminal). Habeas Corpus nº 89.981. Recorrente: Junio Guedes Ferreira. Recorrido: Ministério Público do Estado de Minas Gerais. Relator: Ministro Reynaldo Soares da Fonseca. **Diário de Justiça Eletrônico**, Brasília: DF, 27 set. 2017b. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/505880324/recurso-em-habeas-corpus-rhc-89981-mg-2017-0250966-3?ref=juris-tabs. Acesso em: 30 mar. 2020.

BRASIL. Superior Tribunal de Justiça de Santa Catarina (5ª Câmara Criminal). AgRg nº Recurso em Habeas Corpus nº 92.801. Agravante: Ministério Público do Estado de Santa Catarina. Agravado: Leonardo Vieira Gonçalves. Relator: Ministro Felix Fischer. **Diário de Justiça Eletrônico**, Florianópolis: SC, 26 mar. 2018. Disponível em: https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1689703&num_registro=201703226407&data=20180326&formato=PDF. Acesso em: 25 mar. 2020.

BRASIL. Superior Tribunal de Justiça de Santa Catarina (5ª Câmara Criminal). Apelação criminal nº 0018245-88.2016.8.24.0023. Apelante: Maysa Bosio Martins e outros. Apelado: Ministério Público do Estado de Santa Catarina. Relatora: Cinthia Beatriz da Silva Bittencourt Schaefer. **Diário de Justiça Eletrônico**, Florianópolis: SC, 22 ago. 2019c. Disponível em: https://tj-sc.jusbrasil.com.br/jurisprudencia/747898098/apelacao-criminal-apr-18245882016824 0023-capital-0018245-8820168240023?ref=juris-tabs. Acesso em: 28 mar. 2020.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade ADI nº 6.299. Requerente: Partido Trabalhista Nacional e outros. Relator: Ministro Luiz Fux. **Diário de Justiça Eletrônico**, Brasília: DF, 22 jan. 2020. Disponível em: https://www.conjur.com.br/dl/fux-liminar-juiz-garantias-atereferendo.pdf. Acesso em: 28 mar. 2020.

BRASIL. Supremo Tribunal Federal. Habeas Corpus nº 91.867. Recorrente: Davi Resende Soares. Recorrido: Superior Tribunal de Justiça. Relator: Ministro Gilmar Mendes. **Diário de Justiça Eletrônico**, Brasília: DF, 24 abr. 2012. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=2792328. Acesso em: 28 mar. 2020.

BRASIL. Supremo Tribunal Federal. Habeas Corpus nº 168.052. Recorrente: Rodrigo Ricardo Laurindo. Recorrido: Superior Tribunal de Justiça. Relator: Ministro Gilmar Mendes. **Diário de Justiça Eletrônico**, Brasília: DF, 11 jun. 2019d. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5635177. Acesso em: 02 abr. 2020.

FERRAJOLI, Luigi. **Derecho e razão: teoria do garantismo penal**. São Paulo: Revista dos Tribunais, 2013.

FURLANETO NETO, Mário; GARCIA, Bruna Pinotti. Da guarda de registro de acesso a aplicações de internet na provisão de aplicações. In: LEITE, George Salomão; LEMOS, Ronaldo (Coords.). **Marco Civil da Internet**. São Paulo: Atlas, 2014.

FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos; GIMENES, Eron Veríssimo. 2. ed. **Crimes na internet e inquérito policial eletrônico**. 2. ed. São Paulo: Edipro, 2018.

GIACOMOLLI, Nereu Jusé. **O devido processo penal: abordagem conforme a Constituição Federal e o Pacto de São José da Costa Rica**. 3. Ed. São Paulo: Atlas, 2016.

MACHADO, Leonardo Marcondes. Aplicação da cadeia de custódia da prova digital. **Revista Consultor Jurídico**, 2020. 6p. Disponível em: https://www.conjur.com.br/2020-mar-31/academia-policia-aplicacao-cadeia-custodia-prova-digital. Acesso em: 28 mar. 2020.

NUCCI, Guilherme de Souza. **Pacote anticrime comentado: Lei 13.964, de 24.12.2019**. Rio de Janeiro: Forense, 2020.

PEREIRA, Marcos Tupinambá Martin Alves. **Investigação policial de crimes eletrônicos: doutrina, legislação, procedimentos e modelos**. São Paulo: Acadepol, 2019.

SCARMANHÃ, Bruna de Oliveira da Silva Guesso; FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos. Invasão de dispositivo informático: aporte com a legislação espanhola. **Revista Em Tempo**, v.13, p.231-251, 2014.

VAZ, Denise Provazi. **Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório**. 2012. 198f. Tese (Doutorado em Direito) - Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012.

VECCHIA, Evandro Dalla. **Perícia digital: da investigação à análise forense**. 2. ed. Campinas: Editora Millennium, 2019.