A VIABILIDADE DA REALIZAÇÃO DE EXTRAÇÃO DE DADOS DE DISPOSITIVOS COMPUTACIONAIS DIRETAMENTE PELA POLÍCIA JUDICIÁRIA

THE VIABILITY OF PERFORMING DATA EXTRACTION FROM COMPUTING DEVICES DIRECTLY BY THE JUDICIAL POLICE

Renan Naspolini Bernardo[51]
Gustavo Madeira da Silveira[52]

Resumo: O presente trabalho tem como escopo central analisar de que forma a polícia judiciária poderá realizar a extração de dados de dispositivos apreendidos, de modo a contribuir para o aprimoramento da celeridade processual e da investigação policial. O artigo foi desenvolvido a partir de pesquisas bibliográficas sobre o tema. Inicialmente, conceituaram-se os vestígios e os dados digitais, além de demonstrar o quanto a tecnologia afeta a investigação criminal. Descreveu-se a cadeia de custódia dos vestígios digitais, em consonância com a Lei Federal nº 13.964/2019, popularmente conhecida como "Pacote Anticrime". Posteriormente, demonstraram-se o processo e os métodos realizados na extração desses dados digitais. Por último, discutiu-se a viabilidade e a legalidade dessa extração de dados realizada diretamente pela Polícia Civil. Concluiu-se, assim, que a forma viável da polícia judiciária realizar a extração dos dados é por meio da utilização de ferramentas forenses especializadas, com métodos explícitos e alinhados às normas legais, em especial à cadeia de custódia dos vestígios digitais.

Palavras-chave: extração de dados; evidência digital; cadeia de custódia.

Abstract: This work has a central scope to analyze how the judicial police can perform the extraction of data from seized devices in order to contribute both to the improvement of procedural speed and police investigation. The article was developed from bibliographic research on the subject. Initially, traces and digital data were conceptualized, in addition to demonstrating how technology affects criminal investigation. Also, the chain of custody of digital traces was described, in line with Federal Law No. 13,964/2019, popularly known as the "Anti-Crime Package". Subsequently, the process and methods used to extract these digital data are demonstrated. Finally, the viability and legality of this data extraction performed directly by the Civil Police are discussed. Thus, it concludes that the viable way for the judicial police to perform data extraction is through the use of specialized forensic

[51]Especialista em Gestão da Segurança Pública e Investigação Criminal Aplicada pela Academia de Polícia Civil de Santa Catarina. Graduado em Gestão Pública pela Faculdade Anhanguera – Polo Criciúma. Escrivão de Polícia Civil em Santa Catarina. E-mail: renan-bernardo@pc.sc.gov.br.

[52]Doutorando do Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento na Universidade Federal de Santa Catarina – UFSC. Mestre em Investigação Social Aplicada ao Meio Ambiente pela Universidad Pablo de Olavide - Espanha. Especialista em Direito Ambiental Nacional e Internacional pela Universidade Federal do Rio Grande do Sul – UFRGS. Especialista em Direitos Difusos e Coletivos pela Universidade do Sul de Santa Catarina – UNISUL. Especialista em Direito Ambiental pela UNISUL. Especialista em MBA Smart em Gestão Ágil de Projetos pelo Serviço Nacional de Aprendizagem Industrial – SENAI. Graduado em Direito pela Universidade Franciscana. Delegado de Polícia Civil em Santa Catarina. E-mail: gustavo-dasilvera@pc.sc.gov.br.

tools, with explicit methods and aligned with legal norms, especially regarding the chain of custody of digital traces.

Keywords: data extraction; digital evidence; chain of custody.

1 INTRODUÇÃO

Nos últimos anos, a tecnologia tem desempenhado um papel cada vez mais importante em nossas vidas, afetando praticamente todos os aspectos da sociedade, inclusive a esfera penal. Em particular, o uso de *smartphones* e dispositivos computacionais tem se tornado cada vez mais comum, transformando a maneira como as pessoas se comunicam e interagem. Esses dispositivos são capazes de armazenar uma vasta quantidade de dados que podem ser valiosos para investigações criminais.

O acesso da polícia judiciária a essas informações armazenadas em um dispositivo computacional apreendido sucede, como regra, com autorização judicial e após a realização da extração de dados dos dispositivos pelo órgão de perícia oficial. Um dos efeitos desse avanço tecnológico, como será demonstrado na pesquisa, é o aumento na quantidade de dispositivos eletrônicos apreendidos, acarretando consequências para os órgãos periciais, tornando a realização do exame pericial demorado e oneroso.

A questão é: de que forma a Polícia Civil poderá realizar a extração de dados de dispositivos apreendidos de modo a contribuir para o aprimoramento da celeridade processual e da investigação policial?

Dessa forma, esse estudo pode contribuir para o aprimoramento da celeridade processual e para uma investigação criminal mais eficiente. Pode também oportunizar um conhecimento específico para a utilização de métodos e procedimentos operacionais padrão no âmbito das polícias judiciárias. Principalmente no que diz respeito à extração de dados digitais e, até mesmo, na produção de provas digitais, bem como na cadeia de custódia de vestígios digitais.

O escopo do presente trabalho é analisar de que forma a polícia judiciária pode realizar diretamente a extração de dados de dispositivos

computacionais apreendidos. A partir disso, alguns objetivos específicos foram traçados:

1) Conceituar vestígios e dados digitais, a fim de inserir o leitor no tema, demonstrando as características e peculiaridades desses.

2) Descrever a cadeia de custódia dos vestígios digitais, apresentando a evolução histórica, o atual regramento jurídico e as normas correlatas.

3) Demonstrar o processo de extração de dados, suas características, classificações e métodos, conforme as normas empregadas.

4) Discutir a viabilidade e a legalidade da Polícia Civil realizar a extração de dados diretamente, bem como esclarecer sobre a diferença entre o laudo pericial confeccionado por um perito oficial e a produção de um relatório técnico elaborado pelos policiais responsáveis pela extração dos dados.

Parte-se da premissa de que, para polícia judiciária realizar a extração de dados, de modo a contribuir para o aprimoramento da celeridade processual e da investigação policial, necessita, primeiramente, capacitar seus policiais responsáveis pelas extrações. Além disso, lançar mão de ferramentas forenses especializadas, com uma metodologia sólida, conforme o ordenamento jurídico, em especial à cadeia de custódia dos vestígios digitais.

Para responder à pergunta de investigação e cumprir com o objetivo geral e os específicos, utilizar-se-á o método da pesquisa exploratória por meio de pesquisa bibliográfica para a coleta dos dados. O artigo está disposto em seis capítulos: introdução, metodologia, referencial teórico, extração de dados pela polícia judiciária, considerações finais e referências.

2 METODOLOGIA

Empregou-se nesse estudo o método da pesquisa exploratória valendo-se, essencialmente, da pesquisa bibliográfica para a coleta dos dados, com uma revisão de literatura narrativa. A pesquisa inicial ocorreu

por meio do sítio eletrônico Google Acadêmico. Foram utilizadas palavras-chave na pesquisa como: “extração de dados”, “computação forense”, “cadeia de custódia”, “cadeia de custódia de vestígio digital”, “prova digital”, “vestígio digital” e “forense *smartphone*”.

Essa pesquisa inicial resultou em quarenta e oito fontes bibliográficas entre artigos, normas e livros. Dezoito desses trabalhos pesquisados foram integrados a esta pesquisa. Foram utilizados como critério para integração os materiais que tratavam de diretrizes e métodos de extração de dados, além de assuntos pertinentes à persecução penal.

Importante constar que devido à especificidade do tema, boa parte do material referencial foi encontrado em publicações periódicas produzidas por organismos envolvidos na persecução criminal que tratam de ciências forenses, policiais e criminais.

3 REFERENCIAL TEÓRICO

Será discutido inicialmente o vestígio digital, seu conceito, suas classificações e suas peculiaridades, pois é esse que se pretende extrair dos dispositivos para ser analisado. Na sequência, serão abordados a cadeia de custódia, recém positivada no Código de Processo Penal pela Lei nº 13.964/2019 (Pacote Anticrime), e o seu impacto no vestígio digital. Por último, será discutido acerca da extração de dados propriamente dita.

3 .1 VESTÍGIO DIGITAL E DADOS

Antes de aprofundar no tema do vestígio digital, cabe esclarecer a diferença entre vestígio, evidência e indício. Segundo Stumvoll*et al.* (2014, p.74), “[...] qualquer marca, fato, sinal, que seja detectado em local onde haja sido praticado um fato delituoso é, em princípio, um vestígio.”. Com o advento da Lei nº 13.964, de dezembro de 2019, (Pacote Anticrime), esse instituto foi conceituado no Art. 158-A, §3º do Código de Processo Penal (CPP) como: “Vestígio é todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal.” (BRASIL, 2019).

A evidência é o "[...] vestígio analisado e depurado, tornando-se uma prova por si só em conjunto, para ser utilizada no esclarecimento dos fatos." (VELHO *et al*., 2017, p.11). Essa nomenclatura é utilizada no âmbito da investigação e da perícia e, por vezes, confundida com o conceito de indício, o qual é mais abrangente. Ou seja, está além dos elementos meramente materiais, conforme dispõe o Código de Processo Penal (CPP), em seu Art. 239: "Considera-se indício a circunstância conhecida e provada, que, tendo relação com o fato, autorize, por indução, concluir-se a existência de outra ou outras circunstâncias" (BRASIL, 1941).

Apesar de ser uma alteração recente no CPP, em 2019, o conceito de vestígio expresso pelo legislador no art. 158-A, §3° do CPP, aponta para objetos e materiais tangíveis. A título de exemplo, podem ser encontrados em um local de crime cápsulas de munição, manchas de sangue, arma de fogo e documentos, dentre outros. O Código não tratou especificamente dos vestígios digitais, mas infere-se que esse tipo de vestígio, por sua relação com as infrações penais, esteja abarcado no conceito exposto pelo CPP (NERES, 2021).

Já o vestígio digital é uma informação de natureza lógica ou física obtida de um sistema computacional que pode ser relacionado a um crime. O usuário desse sistema, ao manuseá-lo, produz esses vestígios. Assim, é possível identificar a materialidade e a dinâmica do fato (VELHO, 2016). Ocorre que não há uma padronização no termo técnico utilizado para identificar os vestígios digitais. Estes são, muitas vezes, chamados de evidências digitais ou provas digitais, especialmente por profissionais do ramo da computação forense.

A norma brasileira ABNT NBR ISO/IEC 27037:2013, a qual será utilizada como norte deste artigo, trata das diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Conceitua a evidência digital como "[...] informações ou dados, armazenados ou transmitidos em forma binária, que podem ser invocados como evidência" (ABNT, 2013, p. 2).

Os dados digitais possuem algumas peculiaridades que os tornam diferentes de outros tipos de vestígios materiais tangíveis. Segundo VAZ (2012), o vestígio digital possui as seguintes características: 1) imaterialidade e desprendimento do suporte físico; 2) volatilidade; 3) suscetibilidade de clonagem (dispersão); 4) necessidade de intermediação de equipamento para ser acessado.

O caráter imaterial, de acordo com VAZ (2012), ocorre devido aos dados, basicamente, serem informações eletrônicas não percebidas pelos olhos humanos, ou seja, de natureza impalpável. Somente após o processamento de um dispositivo computacional, que essa informação será representada para o usuário em algum formato de arquivo. Ainda, o dado digital pode existir independentemente do suporte físico que o originou, pois pode ser transferido a outros suportes e, mesmo assim, manter sua originalidade. Em outros termos, sua sequência numérica se mantém inalterada, sendo suscetível à clonagem integral.

Entende-se volatilidade como algo que possa ser instável, variável. Devido à sua imaterialidade o vestígio digital é volátil, sujeito a variações e dissipação com facilidade, podendo assim perder os dados guardados na forma digital, bem como ocorrerem alterações que comprometam a confiabilidade da informação (VAZ, 2012). Essas alterações podem ocorrer voluntariamente por parte do usuário ou, até mesmo, uma intervenção do próprio sistema informático. Minto *et al* (2021), acrescentam que os dados digitais armazenados em um dispositivo podem ser perdidos caso ocorra uma falta de alimentação de energia, uma atualização do sistema automática ou, até mesmo, devido à natureza temporária de um certo dado digital.

Outro atributo dos dados digitais diz respeito à dispersão que pode ocorrer sobre eles. Esses vestígios podem estar localizados em diferentes lugares, inclusive dentro do mesmo sistema local, por exemplo, um arquivo

em *cache*[53]. Outra forma comumente utilizada é o serviço de armazenamento em nuvem, o qual pode estar gerenciando uma cópia integral de um determinado dado digital de um cliente a partir de um servidor localizado em outro país.

Acerca da necessidade de intermediação de equipamento para os dados digitais serem acessados, Vaz (2012) explica sobre a impossibilidade de leitura desses dados, devido às suas características de imaterialidade e invisibilidade. Necessita, assim, de um sistema intermediador capaz de processar e reproduzir essa informação digital ao usuário final.

O *Request for Comments* RFC 3227[54], que trata das diretrizes para coleta e arquivamento de evidências digitais, assinala que essas evidências precisam ser: admissíveis, autênticas, completas, confiáveis e acreditáveis (BREZINSKI; KILLALEA, 2002). Para ser admissível, a evidência digital necessita estar conforme a legislação vigente e apta a ser apresentada perante o juízo (BREZINSKI; KILLALEA, 2002).

Autêntica, quando possui conexão entre o objeto da investigação e as evidências apuradas. Além do mais, pode ser testada sua imutabilidade por meio de uma função de verificação, como o *hash,* por exemplo. Essa função, basicamente, converte um dado digital (entrada) em uma sequência de bits (saída) que pode ser visualizada por meio de caracteres alfanuméricos (HASSAN, 2019). Esse valor é exclusivo para cada evidência digital, funcionando como uma espécie de DNA do arquivo digital.

Quanto à completude, a evidência digital deve estar disponível na íntegra para as partes envolvidas na persecução penal. Lopes Junior (2019) pontua que a prova deve estar acessível para defesa do acusado em sua integralidade e originalidade, no intuito de garantir o direito ao contraditório.

---

[53] Em sistemas computacionais, a memória *cache* é uma camada de armazenamento de dados temporários de alta velocidade para que solicitações futuras desses dados sejam atendidas mais rapidamente do que se os dados precisassem ser acessados a partir da localização de armazenamento principal.

[54] Request for Comments (RFC) são documentos técnicos criados por indivíduos e organizações que lidam com tecnologia, tendo como destaque a Internet Engineering Task Force (IETF).

Por sua vez, a confiabilidade da evidência, para Neres (2021, p.349), "[...] consiste em não haver fatos, relacionados à coleta e ao tratamento da evidência, que lancem dúvidas sobre a real autenticidade e veracidade".

Por último, ela deve ser acreditável, isto é, facilmente credível e compreensível para os julgadores. Por mais que a informação original se trata de uma sequência binária, esta deve ser "traduzida" para os envolvidos no processo. A título de exemplo, não basta apenas apontar que uma evidência está localizada em um determinado banco de dados de um *smartphone*. O profissional analista deve apresentá-la por meio de aplicações de texto, imagem, entre outras (NERES, 2021).

Quanto ao manuseio da evidência digital, a ABNT 27037 (2013) apontou quatro aspectos fundamentais: 1) auditabilidade, 2) repetibilidade ou reprodutibilidade e 3) justificabilidade.

A fim de se tornar auditável, todo o processo de produção dessa prova deve estar disponível para uma avaliação independente, a fim de confrontar e determinar se o método científico, a técnica ou o procedimento foi seguido, conforme os ditames técnicos e legais (ABNT, 2013).

Um terceiro deverá ser capaz de realizar os processos descritos na produção da evidência digital e de alcançar os mesmos resultados, garantindo assim a reprodutibilidade e a repetibilidade (ABNT, 2013).

Já para possibilitar a justificabilidade, o policial que analisou a evidência digital deve ser capaz de justificar todas as ações e métodos utilizados no manuseio da evidência (ABNT, 2013).

Um dos desafios da polícia judiciária é acompanhar a evolução digital, adaptando-se a uma nova realidade dinâmica. Horsman (2021) discorre sobre um conceito de local de crime moderno, uma cena de crime que muitas vezes pode ser considerada híbrida, isto é, físico-digital. Os dispositivos digitais devem ser considerados uma extensão de uma cena de crime. Um aparelho telefônico, por exemplo, pode ser tratado como um local de crime híbrido, contendo tanto vestígios digitais intangíveis, quanto potencialmente físicos no próprio dispositivo.

Esse tipo de vestígio está presente em vários dispositivos digitais, amplamente difundidos na sociedade, como *smartphones*, *tablets*, *notebooks*, *smartwatch*, sistemas de navegação móveis (GPS), câmeras digitais de vídeo e fotografias e circuito fechado de televisão (CFTV), além de dispositivos de armazenamento: nuvem, SSD, HD, DVD, *pendrive*, entre outros. Já mais recentemente, a Internet das Coisas (do inglês *Internet of Things* - IoT) vem ocupando espaço no cotidiano das pessoas. Em poucas palavras, IoT nada mais é que uma extensão da Internet atual, que proporciona aos objetos, como eletrodomésticos, carros, máquinas industriais, com capacidade computacional e de comunicação conectarem-se à Internet, podendo ser controlados remotamente. Esses objetos possuem capacidade de interação com sensores, os quais os tornam úteis para auxiliar em tarefas humanas (SANTOS *et al*., 2016).

Conforme Carvalho (2020), esses vestígios são informações armazenadas ou transmitidas eletronicamente na forma de bits, como e-mails, tráfegos de rede, fotos, vídeos, áudios, documentos, planilhas, logs de acesso e conexão, os quais podem se tornar evidências após análise. Logo, essa gama de dados digitais passa a ter relevância e importância não só para o cotidiano das pessoas, mas também para a investigação criminal.

Por possuírem conteúdo sobre a vida privada e a intimidade do investigado, esses dados são invioláveis, consoante tutelou a Carta Magna de 1988, quando tratou dos direitos e garantias fundamentais (BRASIL, 1988). Obviamente que, para a polícia judiciária poder ter acesso a esses dados, a autoridade policial deve representar ao juízo para que este, caso assim decidir, afaste o sigilo dos dados pretendidos. Em posse da autorização judicial, há que realizar a extração dos dados dos dispositivos computacionais ora apreendidos.

3.2 CADEIA DE CUSTÓDIA

A Secretaria Nacional de Segurança Pública – SENASP estabeleceu as diretrizes sobre os procedimentos a serem observados no tocante à

cadeia de custódia de vestígios, por meio da Portaria nº 82, de 16 de julho de 2014. Essa Portaria definiu cadeia de custódia como "[...] 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" (BRASIL, 2014).

Apenas em 2019, com o advento da Lei nº 13.964/2019 (Pacote Anticrime) que a cadeia de custódia ganhou maior relevância, sendo que foram inseridos seis novos artigos ao capítulo II do Código de Processo Penal, sobre esse tema. Um desses novos dispositivos, o artigo 158-A, trouxe um conceito semelhante ao da Portaria retro e denominou a cadeia de custódia como "[...] 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" (BRASIL, 2019).

Ainda, na Portaria 82/2014, consta que:

> [...] 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. [...] a garantia da cadeia de custódia confere aos vestígios certificação de origem e destinação e, consequentemente, atribui à prova pericial resultante de sua análise, credibilidade e robustez suficientes para propiciar sua admissão e permanência no elenco probatório (BRASIL, 2014).

Visto que é fundamental a manutenção da cadeia de custódia, Furlaneto Neto e Santos (2020) alertam para as eventuais consequências, caso não seja empregado esse instituto. Para os autores, o contraditório e a ampla defesa ficam comprometidos, podendo gerar, até mesmo, uma eventual nulidade da prova.

O artigo 158-B do CPP disciplinou o rastreamento do vestígio em dez etapas, a saber: reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte. O conceito de cada etapa e o seu respectivo dispositivo legal estão dispostos no quadro a seguir:

Quadro 1 – Etapas e conceitos do rastreamento do vestígio

Etapa	**Conceito**	**Dispositivo legal do CPP**
Reconhecimento	Ato de distinguir um elemento como de potencial interesse para a produção da prova pericial.	Art. 158-B, I
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.	Art. 158-B, II
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.	Art. 158-B, III
Coleta	Ato de recolher o vestígio que será submetido à análise pericial, respeitando suas características e natureza.	Art. 158-B, IV
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.	Art. 158-B, V
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.	Art. 158-B, VI

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.	Art. 158-B, VII
Processamento	Exame pericial em si, manipulação do vestígio consoante 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.	Art. 158-B, VIII
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.	Art. 158-B, IX
Descarte	Procedimento referente à liberação do vestígio, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial.	Art. 158-B, X

Fonte: o primeiro autor (2023)

O Código de Processo Penal (CPP), alterado pelo Pacote Anticrime, apesar da inovação, não tratou especificamente sobre a cadeia de custódia de vestígios digitais. No entanto, diante das especificidades desse tipo de vestígio, já apresentadas neste artigo, é imprescindível a normatização de uma prática metodológica, a fim de não comprometer o material probatório produzido. É disponibilizado, assim, aos operadores da persecução penal, policiais e peritos oficiais, um procedimento padrão a ser seguido. Tudo isso,

além de ofertar ao julgador e a defesa uma baliza, quando apresentada essa prova no processo penal.

Sobre esse tema, Machado (2020) explica que o CPP não disciplinou acerca do tratamento dado à cadeia de custódia de vestígio digital. O autor propõe, ainda, a utilização da ABNT NBR ISO/IEC 27037:2013 como diretriz para manutenção da integridade probatória.

A versão internacional dessa norma é referência para vários países no que diz respeito à perícia forense digital. Ela define uma metodologia para identificação, coleta, aquisição e preservação de evidências forenses digitais no processo de investigação. A norma faz parte da família ISO[55] 27000, que trata do Sistema de Gestão de Segurança da Informação (SGSI). Sendo assim, uma norma elaborada por organização competente e reconhecida no Brasil, desde 2013 (FURLANETO NETO; SANTOS, 2020).

O Procedimento Operacional Padrão (POP), publicado pela Secretaria Nacional de Segurança Pública (SENASP), em 2013, trouxe também orientações aos profissionais de perícia da área de informática acerca de como realizar exames que envolvam dados contidos em equipamentos computacionais portáteis. Todavia, as diretrizes do POP são genéricas e superficiais. Não especificam, por exemplo, uma metodologia de aplicação da cadeia de custódia dessa prova. Esse mesmo POP apontou como referência a versão internacional da norma ISO/IEC 27037, a qual não havia sido publicada pela ABNT(BRASIL, 2013).

Portanto, a ABNT 27037 (2013) apresenta um processo de manuseio da evidência digital que consiste em quatro etapas, a saber: identificação, coleta, aquisição e preservação do potencial evidência digital.

[55] ISO – International Organization for Standardization - Organização Internacional para Padronização, em tradução livre.

Figura 1 - Processo de manuseio da evidência digital

Fonte: o primeiro autor (2023).

Identificação: a evidência digital pode ser representada nas formas física e lógica. Essa etapa trata de reconhecer e identificar quais são os dispositivos de processamento que podem conter a potencial evidência digital relevante para investigação, bem como em quais suportes os dados digitais estão armazenados (*Smartphones*, HDs, *pen drives*, nuvem). É nessa fase que se verifica a volatilidade da evidência digital para, desta forma, garantir a correta ordem da coleta ou da aquisição, além de mitigar possível risco de dano à potencial prova (ABNT, 2013).

Coleta: após a identificação dos dispositivos, os profissionais responsáveis julgarão pela coleta ou pela aquisição dessa evidência, conforme a circunstância. Caso optem pela coleta, os dispositivos, basicamente, serão removidos fisicamente e transportados para um ambiente controlado, aguardando futura aquisição. É importante considerar se os dispositivos que serão coletados estão ligados ou desligados, pois, como já discutido, dados armazenados em uma memória RAM são bastante voláteis, ocorrendo sua perda quando desligado o sistema (ABNT, 2013).

Aquisição: é a etapa do processo que realiza a produção da cópia da evidência digital ou a extração dos dados, a depender do dispositivo computacional ou do dispositivo de armazenamento. É altamente recomendado que os métodos utilizados para extração/cópia forense sejam documentados em detalhes, especialmente as situações em que o dado será alterado inevitavelmente. O ideal é que esse processo seja o menos intrusivo possível (ABNT, 2013).

De acordo com Carvalho (2020), após a extração ou cópia forense dos dados digitais, a análise desses dados deve ser feita com uma cópia forense, evitando utilizar a evidência original. Esta deve ser protegida, a fim de assegurar sua integridade.

Preservação: esta etapa ocorre simultaneamente com as demais fases do processo de manuseio da evidência digital, desde a identificação dos dispositivos digitais até o fim da persecução criminal. Trata-se da guarda e do acondicionamento, tanto da evidência digital, como do suporte físico que a detém. Evita, assim, espoliação ou adulteração dos dados. Entende-se por espoliação as alterações físicas que podem resultar em degradação magnética ou elétrica por meio de temperatura elevada, exposição à alta ou à baixa umidade, bem como choques e vibrações. Por esta razão, é fundamental proteger a evidência digital da melhor forma (ABNT, 2013).

Algumas fases do processo de manuseio da evidência digital, propostas pela ABNT 27037 (2013), coincidem com as etapas da cadeia de custódia dispostas nos incisos do Art. 158-B do CPP, conforme demonstrado no quadro a seguir:

Quadro 2 – Comparativo entre as etapas da cadeia de custódia proposta pelo CPP e a ABNT 27037:2013

ABNT 27037:2013	**CPP - Art. 158-B**
Identificação	I - Reconhecimento
Coleta	IV - Coleta
Aquisição	VIII - Processamento
Preservação	IX - Armazenamento

Fonte: o primeiro autor (2023).

Quanto à cadeia de custódia das evidências digitais, a norma ABNT 27037 (2013) recomenda que seja instituída a partir do processo de coleta ou aquisição e que toda intervenção no procedimento seja documentada. Deve possibilitar a identificação do movimento da evidência e das pessoas responsáveis por manuseá-la durante o fluxo da cadeia.

A cadeia de custódia de um vestígio digital possui algumas peculiaridades que ensejam a realização de uma metodologia aceitável para garantir integridade e autenticidade da potencial evidência digital. A metodologia utilizada e os profissionais qualificados são os principais componentes a fornecer credibilidade à investigação (ABNT, 2013). E quanto aos profissionais que trabalham com a prova digital, a ABNT (2013) ainda recomenda que sejam capazes de demonstrar que são devidamente treinados e possuem técnica e entendimento jurídico suficientes para manusear apropriadamente a evidência digital.

3.3 EXTRAÇÃO DE DADOS

Já a extração dos dados digitais propriamente dita é realizada na etapa de processamento dos vestígios, prevista no artigo 158-B do CPP, bem como na fase da aquisição, conforme o processo de manuseio da evidência digital exposto na ABNT 27037:2013. A extração de dados, para Figueiredo e França Júnior (2022, p.76-77), pode ser definida como:

> [...] um conjunto de meios e métodos tecnológicos, providos por pessoa física e/ou jurídica devidamente registrados nos canais legais, de origem nacional ou estrangeira, que se responsabilizam pela eficácia dos métodos e meios desde que usados da forma adequada, onde há reduzida capacidade de interação humana em relação à execução do processo de extração em si, restando ao homem (operador) o papel de identificação da técnica e preparo do aparelho para fins de execução da ferramenta sobre este.

Em suma, pode-se dizer que a extração de dados é o processo de aquisição de informações armazenadas em dispositivos eletrônicos, visando obter evidências digitais que possam ser utilizadas em investigações criminais. Existem diferentes métodos de extração de dados que variam

segundo o tipo de dispositivo e a finalidade da investigação. A título de exemplo, a extração dos dados de mídia de armazenamento, como SSD, *pen drives* e HD, é diferente da extração de dados de dispositivos computacionais portáteis devido à singularidade do tipo de dispositivo (VELHO *et al*., 2016).

A extração de dados em dispositivos computacionais portáteis, como *smartphones* e *tablets*, segundo Velho *et al*. (2016) pode ser feita por meio das seguintes técnicas: extração manual, extração lógica, extração física e extração avançada. Inicialmente, a extração manual é a mais básica, não exigindo um conhecimento avançado do operador, pois implica a constatação manual dos vestígios por meio da manipulação do aparelho. Os dados podem ser transcritos manualmente para um relatório ou, até mesmo, a tela do dispositivo pode ser fotografada. A desvantagem desse método é que os dados deletados não podem ser recuperados (VELHO *et al*., 2016).

A extração lógica necessita de uma ferramenta forense específica para ser aplicada. Basicamente, é realizada a coleta de dados a partir do sistema operacional do dispositivo. Velho *et al*. (2016) explicam que esse método permite a coleta de dados que estão acessíveis pelo sistema operacional e armazenados na memória interna do dispositivo. Esse método é geralmente mais rápido e fácil de executar do que a extração física, mas pode não fornecer todos os dados relevantes para a investigação, além de não recuperar os dados apagados do dispositivo.

A extração física é uma técnica que permite a recuperação de todos os dados armazenados em um dispositivo móvel, incluindo dados que foram deletados. Nesse tipo de extração, "[..] as ferramentas forenses conseguem acesso direto ao conteúdo da memória flash dos dispositivos, funcionando como a cópia bit a bit dos exames de mídia de armazenamento convencionais." (VELHO *et al*., 2016, p. 326).

Por último, a extração avançada requer conhecimentos em eletrônica por parte do extrator, uma vez que o circuito integrado de

memória (*chip*) será removido fisicamente da placa de circuito impresso do aparelho. Posteriormente, esse chip será lido bit a bit em um equipamento apropriado. É uma técnica de difícil aplicação, pois requer especialistas na matéria, além de ter um custo elevado (VELHO *et al*., 2016).

Como visto, para realizar a extração dos dados, os órgãos responsáveis precisam utilizar as ferramentas forenses adequadas. Essas ferramentas são *softwares* ou *hardwares* especializados que possibilitam realizar atividades de extração e coleta. Além disso, também de análise dos dados de dispositivos digitais, leitores de cartão SIM, além de possuírem algoritmos de funções (*hash*), oferecendo recursos auditáveis, garantindo confiabilidade e autenticidade à evidência digital. Dentre as ferramentas forenses mais utilizadas atualmente, destaca-se o UFED da *Cellebrite*, que é também capaz de decodificar informações criptografadas (senhas de bloqueio), entre outras, como XRY da *MicroSystemation* e EnCase da *GuidanceSoftware* (VELHO *et al*., 2016).

4 EXTRAÇÃO DE DADOS PELA POLÍCIA JUDICIÁRIA

Discutir-se-á nesta etapa a realização das extrações dos dados de dispositivos computacionais apreendidos no curso da investigação, bem como sua legalidade, a diferença entre o laudo de perícia e a jurisprudência sobre o tema.

Após decisão judicial afastando o sigilo dos dados, a polícia judiciária, em regra, encaminha os dispositivos digitais apreendidos ao órgão de perícia oficial, para este realizar a extração dos dados. Em algumas unidades da federação, o órgão pericial oficial, responsável pela extração, é desvinculado da polícia civil, ou seja, um órgão autônomo, a exemplo dos três estados do sul brasileiro (SILVA *et al*., 2022).

Devido à evolução tecnológica, inclusive dos criminosos, houve um aumento na quantidade de dispositivos computacionais apreendidos. Segundo Polastro e Eleutério (2015), essa demanda por extração e análise dos órgãos periciais tem ocasionado um grande acúmulo de trabalho. Giova

(2016) esclarece que os laboratórios forenses não conseguem realizar os exames forenses com a qualidade adequada e nem entregá-los em um prazo razoável, devido à alta demanda por perícias digitais, além da capacidade reduzida desses laboratórios.

O órgão pericial muitas vezes não possui conhecimentos sobre investigação e, ao receber quesitos genéricos, acaba indo em busca de ilícitos nos dispositivos, fazendo com que o exame pericial se torne mais demorado, mais custoso e com menos resultados satisfatórios (POLASTRO; ELEUTÉRIO, 2015). Há reflexos na qualidade da investigação, pois não parece razoável que um dispositivo celular fique mais de um ano aguardando para ter seus dados extraídos. Para contornar esse problema, as polícias civis de diversas unidades federativas vêm adquirindo esses softwares forenses nos últimos anos (LEAL; FELIX, 2020).

Além disso, o próprio Ministério da Justiça e Segurança Pública, por meio da Portaria N° 26, de 9 de julho de 2020, criou o Projeto Excel, que auxilia as polícias civis com o fornecimento de *softwares* forenses e *hardwares* para dar mais celeridade às extrações e análises de celulares apreendidos de indivíduos envolvidos com o crime organizado (BRASIL, 2020).

Em seu portal eletrônico, o Ministério da Justiça divulgou que, de 2019 a 2022, já havia capacitado 130 policiais para o uso das ferramentas forenses (BRASIL, 2022). Os policiais civis responsáveis pela extração dos dados não produzem laudo pericial, salvo na falta de perito oficial, quando duas pessoas idôneas, portadoras de diploma de curso superior, preferencialmente na área de atuação, realizarão o exame de corpo de delito, conforme determina o CPP em seu art. 159 §1° (BRASIL, 1941).

O que será confeccionado pelos policiais operadores da ferramenta forense, conforme apontam Figueiredo e França Júnior (2022), consiste num relatório técnico. Nele serão descritas todas as etapas realizadas no processo de extração, atentando-se à documentação cronológica da cadeia de

custódia e, sobretudo, à demonstração da metodologia utilizada no processo.

A manipulação da evidência digital pelos policiais não a torna uma prova inviável. O que garante que essa evidência não foi modificada ou comprometida pelos policiais é a sua própria característica de auditável. Diversos meios como *hash, log* de dados e metadados podem atestar isso (FIGUEIREDO; FRANÇA JÚNIOR, 2022).

O que se pretende é produzir uma prova digital e técnica, até porque vigora no processo penal a ampla liberdade probatória. Não há hierarquia entre meios de prova, sejam eles meios nominados ou inominados. Além disso, o exame pericial não é a única forma de se comprovar a materialidade de uma prova (FIGUEIREDO; FRANÇA JÚNIOR, 2022).

Nada impede que o dispositivo computacional objeto da extração de dados seja encaminhado, após a extração efetuada pela polícia judiciária, ao órgão de perícia oficial que possui outra finalidade, ou seja, pericial. O laudo pericial tem o viés de produzir prova cautelar que garante a possibilidade do contraditório na modalidade diferida (BRASIL, 1941).

O Tribunal de Justiça do estado do Acre, por meio do Habeas Corpus nº 1000323-86.2020.8.01.0000, foi provocado a decidir sobre a legalidade de um relatório técnico, confeccionado por servidor do Ministério Público, acerca da extração de dados de um aparelho celular. Seguem os principais trechos do acórdão (ACRE, 2020):

> CONSTITUCIONAL. PENAL. PROCESSO PENAL. HABEAS CORPUS. ORGANIZAÇÃO CRIMINOSA. EMENDA À INICIAL APÓS INFORMAÇÕES DA AUTORIDADE COATORA. VIABILIDADE. REPETIÇÃO DAS TESES TRAZIDAS NA IMPETRAÇÃO. ARGUIÇÃO DE NULIDADES. AFASTAMENTO. APREENSÃO DE TELEFONE CELULAR NO INTERIOR DE ESTABELECIMENTO PRISIONAL. POSSIBILIDADE DE INVESTIGAÇÃO PELO PARQUET. **LAUDO TÉCNICO NÃO SE EQUIPARA À PERÍCIA. A MATERIALIDADE DO DELITO EM APURAÇÃO NÃO REQUER EXAME PERICIAL PARA COMPROVAÇÃO. OFENSA A DISPOSITIVO LEGAL NÃO CONFIGURADA. PROVA LEGAL**. [...] Como se pode observar, no caso desses autos, em nenhum momento houve interceptação de conversas por via telefônica ou interceptação de transmissão de fluxo de dados pela via telefônica ou telemática. **O que ocorreu foi apenas a extração de dados, notadamente arquivos de áudios com a extensão OPUS, conversas**

> **do aplicativo WhatsApp, arquivos de imagem e arquivos de vídeo, que já estavam armazenados anteriormente na memória do dispositivo móvel celular apreendido**.
> [...] Corroborando com o entendimento dos representantes do Ministério Público, os **relatórios técnicos de extração e de análise**, ou similares, produzidos na área de Computação Forense **não se confundem com perícias**, tratando-se tão somente da descrição pormenorizada dos procedimentos técnicos adotados para se conseguir acesso a um dispositivo de informática e o detalhamento do seu conteúdo.
> [...] Instado a se manifestar acerca das nulidades apontadas pela defesa, o Ministério Público com atuação no Primeiro Grau amplamente demonstrou tanto a validade do "Relatório Técnico" confeccionado por servidor do NAT/MP (Núcleo de Apoio Técnico) como também a **devida qualificação e certificação** para o desempenho da atividade forense pelo servidor daquele órgão.
> [...] Com efeito, os arquivos digitais armazenados na memória interna de um dispositivo informático se equiparam, em especial no caso dos autos, à prova da categoria documental.
> [...] Desse modo, entendo que não merece prosperar a alegação de nulidade posta pela defesa, vez que o documento elaborado pelo servidor do Parquet **não se trata de Exame pericial, mas sim de Relatório** que poderá ser utilizado como **documento probatório** nos autos, assim, voto **pela rejeição da nulidade**. [Grifo nosso]

Em suma, o Tribunal acordou que o referido relatório técnico é equiparado a uma prova da categoria documental e não pericial e, portanto, julgou legal a materialização da extração. Ademais, ainda ficou comprovada a qualificação técnica do servidor responsável pela extração e pela confecção do relatório.

5 CONSIDERAÇÕES FINAIS

O presente estudo versou sobre a forma de a polícia judiciária realizar a extração de dados de dispositivos apreendidos, de modo a contribuir para o aprimoramento da celeridade processual e da investigação policial.

Inicialmente, apresentaram-se o conceito e as características dos vestígios digitais. Esse conhecimento técnico revela-se fundamental para o policial operador, que irá delinear qual método utilizará para extrair esses dados, a partir de suas peculiaridades.

Foi demonstrada também uma forma adequada de manuseio desses vestígios, conforme diretrizes da norma brasileira ABNT NBR ISO/IEC 27037:2013. Em seguida, tratou-se da cadeia de custódia e da sua relevância

para o tratamento dos vestígios, em especial o vestígio digital. Sendo o registro desta extremamente importante em todo o processo de extração de dados.

Sequencialmente, descreveu-se o processo de extração de dados. Para tanto, é primordial o uso de ferramentas forenses para cada tipo de extração. Conclui-se, assim, que há mínima intervenção do policial operador com a evidência digital.

Discutiu-se sobre a extração de dados realizada pela polícia judiciária e foram demonstrados os problemas enfrentados pelos órgãos periciais quanto ao acúmulo de dispositivos informáticos a serem periciados.

A realização da extração de dados direta pela Polícia Civil pode ser seletiva e focada, aumentando a eficiência da investigação. Em outras palavras, as ferramentas forenses no momento da extração podem selecionar os tipos de dados que se deseja extrair. Em uma investigação de pornografia infantil, por exemplo, pode-se extrair apenas imagens, vídeos e conversas. Já num caso de homicídio, talvez seja interessante extrair apenas os dados de geolocalização ou de conexão do investigado. Providências como estas facilitam sobremaneira o trabalho dos investigadores ao procederem a análise da extração dos dados, evitando despender excessivo tempo para analisar todo o conteúdo do dispositivo apreendido.

No final, exibiu-se um julgado sobre o assunto. Apesar de ter sido realizada pesquisa, não foram encontrados outros julgados específicos sobre o tema no judiciário brasileiro. Eventualmente, a dificuldade em encontrar material bibliográfico acerca do tema pode ser atribuída ao fato de se tratar de um assunto relativamente recente, sem olvidar de sua natureza preponderantemente técnica.

Em face do exposto, é possível inferir que a polícia judiciária pode realizar a extração de dados dos dispositivos computacionais apreendidos. A forma adequada enseja a utilização de ferramentas forenses especializadas e auditáveis, bem como a demonstração da metodologia aplicada condicionada à observância das normas legais, em especial à

cadeia de custódia desses vestígios digitais. Precisa ser também lembrada a capacitação dos policiais responsáveis pelo processo de extração dos dados, de modo a contribuir para o aprimoramento da celeridade processual e da investigação policial.

Por fim, sugere-se para trabalhos futuros discutir uma metodologia no que tange à extração de dados realizada pela Polícia Civil, a fim de padronizar os procedimentos. De qualquer modo, a polícia judiciária vem se mostrando em contínuo processo de modernização e de aquisição de ferramentas forenses para otimizar os necessários e imprescindíveis avanços em suas técnicas investigativas.

REFERÊNCIAS

ACRE. Tribunal de Justiça do Estado do Acre. Câmara Criminal. **Habeas Corpus 1000323-86.2020.8.01.0000**, Relator: Des. Elcio Mendes. Data do julgamento: 02/04/2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27037 Tecnologia da informação – Técnicas de segurança – Diretrizes para identificação, coleta, aquisição e preservação de evidência digital.** Rio de Janeiro, 2013.

BRASIL. **Ação do Ministério da Justiça e Segurança Pública já causou prejuízo de R$ 1 bi ao crime organizado.** Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/acao-do-ministerio-da-justica-e-seguranca-publica-ja-causou-prejuizo-de-r-1-bi-ao-crime-organizado. Acesso em 28 mar. 2023.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 28 out. 2022.

BRASIL. **Decreto-Lei n° 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm. Acesso em 28 out. 2022.

BRASIL. **Lei n° 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em 28 out. 2022.

BRASIL. Ministério da Justiça. **Portaria n° 26**, de 09 de julho de 2020. Disponível em: https://dspace.mj.gov.br/bitstream/1/1867/1/PRT_SEOPI_2020_26.pdf. Acesso em 28 mar. 2023.

BRASIL. Ministério da Justiça**. Portarian° 82** de 16 de julho de 2014. Secretaria Nacional de Segurança Pública. DOU de 18/07/2014 (n° 136, Seção 1, pág. 42)

BRASIL. Secretaria Nacional de Segurança Pública. **Procedimento operacional padrão: perícia crimina**l. Brasília: Ministério da Justiça, 2013. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/analise-e-pesquisa/pop/procedimento-operacional-padrao. Acesso em: 28 out. 2022.

BREZINSKI, D., KILLALEA, T. **Request for Comments: 3227:Guidelines for evidencecollectionandarchiving**. Internet Engineering Task Force, 2002. Disponível em: https://www.rfc-editor.org/search/rfc_search_detail.php?rfc=3227&pubstatus%5B%5D=Any&pub_date_type=any. Acesso em: 12 out. 2022.

CARVALHO, RomulloWheryko Rodrigues de. A Importância da Cadeia de Custódia na Computação Forense **Revista Brasileira de Crimininalística**, v. 9, n.2, p.134-138, 2020. Disponível em: https://revista.rbc.org.br/index.php/rbc/article/view/463. Acesso em 14 out. 2022.

FIGUEIREDO, Jorge Ramos de; FRANÇA JÚNIOR, Fausto Faustino de**. Extração forense avançada de dados em dispositivos móveis**. Rio de Janeiro: Editora Brasport, 2022.

FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos. Apontamentos sobre a cadeia de custódia da prova digital no brasil**. Revista Em Tempo**, v. 20, n. 1, nov. 2020. ISSN 1984-7858. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3130. Acesso em: 27 fev. 2023.

GIOVA, Giuliano. **Proposta para integração de laboratórios forenses digitais via rede de weblabs**. 2016. 149 f. Tese (Doutorado em Sistemas

Eletrônicos) – Escola Politécnica, Universidade de São Paulo, São Paulo, 2016.

HASSAN, Nihad A. **Perícia Forense Digital**: guia prático com uso do sistema operacional Windows. São Paulo: Novatec Editora, 2019.

HORSMAN, Graeme. Digital evidenceandthe crime scene. **Science & Justice**
v. 61, I.6, nov. 2021, p. 761-770. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1355030621001295. Acesso em: 28 out. 2022;

LEAL, David; FELIX, Yuri. **O mercado de dados: o caso cellebrite e a investigação digital no Brasil**. Disponível em: https://ibccrim.org.br/noticias/exibir/7210/. Acesso em 28 mar. 2023.

LOPES JUNIOR, Aury. **Direito processual penal**. 16ª ed. São Paulo: Saraiva Educação, 2019.

MACHADO, Leonardo Marcondes. **Aplicação da cadeia de custódia da prova digital**. Revista Consultor Jurídico, 2020. Disponível em: https://www.conjur.com.br/2020-mar-31/academiapolicia-aplicacao-cadeia-custodia-prova-digital. Acesso em: 12 out. 2022

MINTO, Andressa Olmedo; CARVALHO, Lauro Fabiano de Souza; LIMA, Fransmar Costa. **A Prova Digital no Processo Penal**. São Paulo: Editora Liber Ars, 2021.

NERES, Winícius Ferraz. A cadeia de custódia dos vestígios digitais sob a ótica da Lei n. 13.964/2019: aspectos teóricos e práticos. **Boletim Científico ESMPU**, Brasília, ano 20, n. 56, jan./jun. 2021. ISSN 1676-4781. Disponível em: https://escola.mpu.mp.br/publicacoes/boletim-cientifico/edicoes-do-boletim/boletim-cientifico-n-56-janeiro-junho-2021/a-cadeia-de-custodia-dos-vestigios-digitais-sob-a-otica-da-lei-n-13-964-2019-aspectos-teoricos-e-praticos. Acesso em: 28 out. 2022

POLASTRO, Mateus de Castro; ELEUTERIO, Pedro Monteiro da Silva. **Um Modelo de triagem de dados digitais aplicado à perícia criminal em informática.** 15° Simposio Argentino de Informática y Derecho (SID 2015) - JAIIO 44. Rosario, 2015. Disponível em: http://sedici.unlp.edu.ar/handle/10915/55344. Acesso em 27 mar. 2023.

SANTOS, Bruno P. *et al*. **Internet das Coisas: da Teoria à Prática.** Minicursos SBRC -Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. Porto Alegre: SBC, 2016. Disponível em: http://sbrc2016.ufba.br/minicurso/minicurso-1/#collapseminicurso. Acesso em: 27 mar. 2023.

SILVA, Tiago F. *et al*. Perícia Criminal e a Legislação Brasileira. **Revista Brasileira de Crimininalística**, v. 11, n.2, p.14-23, 2022. Disponível em: https://revista.rbc.org.br/index.php/rbc/article/view/415. Acesso em 27 mar. 2022.

STUMVOLL, Victor Paulo *et al*. **Criminalística**. Campinas: Editora Millennium, 6ª ed., 2014.

VAZ, Denise Provasi. **Provas digitais no processo penal**: formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. 168 f. Tese (Doutorado em Direito Processual) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012.

VELHO, Jesus Antônio *et al*. **Ciências forenses - uma introdução às principais áreas da criminalística**. Campinas: Editora Millennium, 3ª ed., 2017.

VELHO, Jesus Antônio *et al*. **Tratado de computação forense**. Campinas: Editora Millennium, 2016.