A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais

Does obtaining digital evidence in criminal proceedings require its own legal discipline? An analysis of the concept, characteristics and peculiarities of digital evidence

Marta Saad[1]
Universidade de São Paulo – São Paulo/SP, Brasil
martasaad@usp.br
http://lattes.cnpq.br/3199855414351538
http://orcid.org/ 0000-0001-5363-390X

Helena Costa Rossi[2]
Universidade de São Paulo – São Paulo/SP, Brasil
helena.rossi@usp.br
http://lattes.cnpq.br/6022530640899053
https://orcid.org/0009-0004-3436-9807

Pedro Henrique Partata[3]
Universidade de São Paulo – São Paulo/SP, Brasil
pedro.mortoza@usp.br
http://lattes.cnpq.br/9431614773439500
https://orcid.org/0009-0008-1318-8950

[1] Professora Doutora de Direito Processual Penal da Faculdade de Direito da Universidade de São Paulo, nos cursos de graduação e pós-graduação. Doutora (2007) e Mestre (2002) em Direito Processual Penal pela Faculdade de Direito da Universidade de São PauloConselheira do InternetLab. Coordenadora adjunta da ESEM – Escola de Segurança Multidimensional, da USP. Ex-Presidente e ex-Conselheira do Instituto Brasileiro de Ciências Criminais (IBCCRIM). Ex-Presidente da Rede Ibero Americana de Advocacia Criminal. Advogada.

[2] Graduada em Direito pela Faculdade de Direito da Universidade de São Paulo e mestranda em Direito Processual Penal no Programa de Pós-Graduação da mesma instituição, vinculada ao Departamento de Direito Processual. Advogada.

[3] Graduado em Direito pela Faculdade de Direito da Universidade de São Paulo e mestrando em Direito Processual Penal no Programa de Pós-Graduação da mesma instituição, vinculado ao Departamento de Direito Processual. Advogado.

Resumo: O presente artigo analisa o tema das provas digitais, e objetiva responder à pergunta: a obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Mediante estudo bibliográfico e legislativo, o artigo busca responder à pergunta analisando, em particular, as caraterísticas distintivas das provas digitais, os principais direitos fundamentais afetados pelas medidas de obtenção dessas provas, e duas formas de obtenção de dados digitais específicas, a saber, a busca e a apreensão de dispositivos informáticos e o acesso oculto e remoto mediante *hacking* governamental e uso de *malware*. Ao fim, conclui-se que a legislação deve prever requisitos mínimos para a obtenção de provas digitais, a balizar as decisões judiciais que autorizam o emprego dos meios de obtenção dessas provas, ou seja, responde-se à pergunta positivamente: a obtenção de provas digitais demanda uma disciplina jurídica própria no processo penal brasileiro.

Palavras-Chave: Prova digital; direitos fundamentais; disciplina legal; formas de obtenção de dados digitais.

Abstract: *This article analyzes the theme of digital evidence, and aims to answer the question: does obtaining digital evidence in Brazilian criminal proceedings require its own legal discipline? Through bibliographic and legislative study, the article seeks to answer the question by analyzing, in particular, the distinctive characteristics of digital evidence, the fundamental rights affected by measures to obtain this evidence, and two ways of obtaining specific digital data, namely, the search and seizure of computer devices and hidden and remote access through government hacking and malware. In the end, it is concluded that the legislation must provide minimum requirements for obtaining digital evidence, to guide judicial decisions that authorize the means of obtaining this evidence, that is, the question is answered positively: digital evidence does require a legal discipline of its own in Brazilian criminal proceedings.*

Keywords: *Digital evidence; fundamental rights; legal discipline; ways of obtaining digital data.*

Introdução

O presente artigo científico pretende analisar o tema das provas digitais no âmbito do processo penal, e objetiva responder à seguinte pergunta: a obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria?

Para responder a questão, em primeiro lugar, o artigo analisa o que são as provas digitais, objetivando atingir maior clareza terminológica sobre as principais questões atinentes às provas digitais, com especial atenção às características que marcam essa espécie de prova e as diferenciam daquelas classificadas como analógicas.

Em segundo lugar, o estudo analisa os principais direitos fundamentais afetados a partir do acesso a dados digitais, destacando-se as garantias expressamente positivadas pelo texto constitucional – como as inviolabilidades da intimidade, da vida privada, do domicílio e dos sigilos das diversas formas de comunicação, bem como a autodeterminação informativa –, e outras decorrentes do princípios constitucionais e do Direito Internacional dos Direitos Humanos, como a integridade e a confiabilidade dos sistemas informáticos.

Em terceiro lugar, o estudo analisa duas das principais formas de obtenção de dados digitais no âmbito do processo penal: a primeira, que pressupõe a apreensão do suporte físico no qual as informações estão armazenadas; e a segunda, que permite o acesso aos dados de forma remota e oculta (destacando-se as práticas de *hacking* governamental e utilização de *malware*). Neste ponto, serão discutidos, em termos práticos, as especificidades de cada uma dessa formas de acesso, bem como serão apontados os indicadores da insuficiência normativa da legislação brasileira para regulamentar a execução desses meios de obtenção de prova.

Finalmente, o estudo desenvolvido no artigo permite responder à pergunta originalmente formulada no sentido de que a obtenção de provas digitais no processo penal exige disciplina jurídica própria, que preveja hipóteses, requisitos e procedimentos particulares.

A presente análise foi baseada em estudo bibliográfico, amparado em artigos científicos e na doutrina especializada, assim como na revisão das disposições legais existentes no ordenamento jurídico brasileiro atual. Para responder à pergunta formulada e atingir o objetivo central do presente artigo foram instrumentais, portanto, a abordagem crítica da doutrina pertinente ao tema e dos marcos normativos vigentes, subsumindo-se as situações concretas das diferentes formas de obtenção das provas digitais ao direito posto, destacando-se os principais impasses e as possíveis formas de resolução condicionadas à legalidade.

1. O QUE SÃO PROVAS DIGITAIS?

Define-se prova digital, ou *digital evidence*, como "os dados em forma digital (no sistema binário) constantes de um suporte eletrônico ou transmitidos em rede de comunicação, os quais contêm a representação de fatos ou ideias".[4] A definição, como proposta, designa *fonte de prova,5* isto é, "pessoas ou coisas das quais pode-se conseguir a prova (*rectius*, o elemento de prova)".[6] Todavia, não é incomum que a expressão também seja utilizada para designar *elemento de prova*, ou seja, os "dados objetivos que confirmam ou negam uma asserção a respeito de um fato que interessa à decisão da causa".[7]

---

[4] VAZ, Denise Provasi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório*. Tese (Doutorado em 2012) – Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012, p. 63.

[5] *Idem, ibidem*, p. 63.

[6] GOMES FILHO, Antonio Magalhães. *Notas sobre a terminologia da prova* (reflexos no processo penal brasileiro). In: YARSHELL, Flávio Luiz; DE MORAES, Zanoide (Coods.), *Estudos em homenagem à Professora Ada Pellegrini Grinover*. São Paulo: Editora DPJ, 2005, p. 308.

[7] *Idem, ibidem*, p. 307.

O atributo "digital" não decorre da simples utilização de dispositivo informático no encaminhamento ou na produção do elemento de prova. Do contrário, quaisquer documentos poderiam ser classificados como provas digitais. Essa qualificação é relativa apenas ao próprio arquivo informático, pois liga diretamente o conteúdo da informação (que importa à persecução penal) à manipulação eletrônica de números. A capacidade representativa de fatos ou ideias vincula-se, portanto, a um processo interpretativo, que atribui um sentido humanamente compreensível a uma linguagem não natural.[8]

A prova digital, contrapondo-se às provas ditas *analógicas*, é marcada por características distintivas.[9] A *imaterialidade*, por exemplo, diz respeito à "natureza impalpável" da prova, pois os dados em formato digital não são nada além de impulsos de corrente elétrica,[10] aos quais se atribui um sentido informacional após um processo de interpretação de uma linguagem não natural.[11] Por ser imaterial, aponta-se também a *volatilidade* como característica: os dados digitais são frágeis e podem sofrer variações (propositais ou involuntárias), bastando, para tanto, a simples modificação da sequência numérica que os compõe.[12]

As provas digitais também apresentam integral *desprendimento do suporte físico* onde estão registradas, de modo que as informações produzidas e/ou armazenadas podem ser transferidas para outros dispositivos ou formas de armazenamento sem perder sua essência.[13] Esta característica liga-se diretamente com a *suscetibilidade de clonagem*, o que

---

8 BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. *Boletim IBCCRIM*, São Paulo, ano 29, n. 343, jun. 2021, p. 7.

9 VAZ, Denise. *Op. cit.*, p. 67 a 70 (nota 4). Em regra, aponta-se como características a imaterialidade, a volatilidade, o desprendimento do suporte físico, a suscetibilidade de clonagem e a necessidade de intermediação. Todavia, outros autores apontam características adicionais. Marcello Daniele menciona a dispersão, a promiscuidade e a modificabilidade, dentre outras. DANIELE, Marcello. La prova digitale nel processo penale. *Rivista di Diritto Processuale*, v. 66, n. 2, 2011, p. 283 a 298.

10 VAZ, Denise. *Op. cit*., p. 68 (nota 4).

11 BADARÓ, Gustavo. *Op. cit*., p. 7 (nota 8).

12 *Idem, ibidem,* p. 7.

13 VAZ, *Op. cit.,* p. 148 (nota 4).

significa dizer que estes dados permitem a realização de cópias – fiéis, idênticas e infinitas – dos arquivos digitais,[14] desde que se promova o espelhamento dos elementos coletados. Por fim, aponta-se a *necessidade de intermediação*[15] de equipamento: como o dado digital é uma simples sequência numérica que, isoladamente, pouco significa para o ser humano, torna-se necessário o uso de equipamentos que processem essas informações e as disponibilizem em linguagem natural, compreensível ao ser humano.[16]

Em razão dessas características típicas, a utilização das provas digitais na persecução penal exige cuidados procedimentais com objetivo de assegurar a confiabilidade e a autenticidade dos elementos de prova.[17] Afinal, se o processo, em uma concepção racionalista,[18] serve como instrumento de reconstrução histórica de um fato pretérito com objetivo de atingir uma resposta judicial que se aproxime, na maior medida possível, à verdade, os elementos de prova devem ser autênticos e confiáveis. Assim, importa estabelecer rigorosos critérios de cadeia de custódia da prova digital, eis que as suas características distintivas informam que são vulneráveis a erros (conscientes ou não) e exigem, via de regra, intervenção técnica para a sua coleta.[19]

---

[14] *Idem, ibidem,* p. 69.

[15] *Idem, ibidem,* p. 69 e 70.

[16] BADARÓ, Gustavo. *Op. cit*., p. 7 (nota 8).

[17] Especificamente sobre a cadeia de custódia das provas digitais, cf.: BADARÓ MASSENA, Caio. A propósito da cadeia de custódia das provas digitais no processo penal: breves notas sobre lógica da desconfiança, assimetria informacional e direito de defesa. *Boletim IBCCRIM*, São Paulo, v. 31, n. 368, 2023. Disponível em: <https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/506>. Acesso em: 17 jun. 2024.

[18] Ferrer-Beltrán afirma que "há uma relação teleológica entre prova e verdade, de modo que a verdade se configura como objetivo institucional a ser alcançado mediante a prova no processo judicial". FERRER-BELTRÁN, Jordi. Prova sem convicção: standards de prova e devido processo. Tradução: Vitor de Paula Ramos. São Paulo: JusPodivm, , 2022, p. 22.

[19] BADARÓ MASSENA, Caio. *Op. cit.,* p. 19 (nota 17).

2. Quais direitos fundamentais são afetados na obtenção de provas digitais?

A obtenção de provas digitais tensiona uma série de direitos fundamentais[20] positivados no texto constitucional e outros decorrentes dos princípios constitucionais e do direito internacional dos direitos humanos, como os analisados a seguir.

Antes, convém destacar que a afetação a direitos fundamentais não é exclusividade das provas digitais. As ditas provas analógicas também afetam uma série de direitos e garantias. Com a realização de uma busca domiciliar, por exemplo, para viabilizar a apreensão de um contrato simulado, a intimidade do investigado é inegavelmente restringida. No entanto, considerando-se os avanços tecnológicos das últimas três décadas e a popularização das novas tecnologias, uma série de problemas jurídicos relativos ao uso dos dados e metadados produzidos durante utilização de aparelhos eletrônicos surgiu.

Hoje em dia, com a possibilidade de obtenção e monitoramento de conversas privadas travadas entre dois ou mais interlocutores, da localização (por vezes em tempo real) de usuários de determinados dispositivos ou aplicativos, dos padrões de comportamento e de consumo, dentre outras informações potencialmente dotadas de relevância social e interesse econômico, a afetação a aspectos sensíveis da dignidade humana, como a privacidade e a intimidade, além da própria proteção de dados, aumentou exponencialmente, gerando a necessidade de tutela e alguma espécie de regulamentação jurídica.

Em síntese, em razão da massiva quantidade de informações produzidas e armazenadas em dispositivos eletrônicos, o potencial de afetação aos direitos fundamentais exacerbou-se. Esse contexto colocou em xeque a suficiência do arcabouço legislativo e da interpretação jurisprudencial para fazer frente às novas demandas, em nível nacional

[20] Joaquín Delgado Martín, por exemplo, destaca a intimidade pessoal, o segredo das comunicações, o direito à autodeterminação informativa, bem como a inviolabilidade do domicílio e o direito à imagem. DELGADO MARTÍN, Joaquín. La prueba digital. Concepto, clases, aportación al proceso y valoración. Diario La Ley, n. 6, Sección Ciberderecho, abr. 2017.

e internacional, a partir da análise dos direitos fundamentais atingidos mediante a obtenção de provas digitais.

2.1. Inviolabilidade da intimidade e vida privada

Nos termos do artigo 5º, X, da Constituição da República, são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação. O direito à vida privada também está previsto nas convenções internacionais de direitos humanos, como a Convenção Americana de Direitos Humanos (artigo 11.2)[21], o Pacto Internacional sobre Direitos Civis e Políticos (17.1)[22] e a Convenção Europeia de Direitos Humanos (artigo 8º).[23] Vale lembrar que todas elas garantem a proteção da lei contra ingerências a tal direito.[24]

Segundo José Afonso da Silva, o direito consagrado no texto constitucional abarca todas as manifestações da esfera íntima, privada e da personalidade, razão pela qual a privacidade pode ser entendida como o conjunto de informações que o indivíduo mantém sob seu controle, podendo decidir se as comunicará a terceiros e em quais condições.[25]

A conceituação do direito à privacidade (entendido em seus âmbitos mais ou menos reservados, da intimidade à vida privada), como

---

[21] Artigo 11. Proteção da honra e da dignidade 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.

[22] Artigo 17.1. Ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação.

[23] Artigo 8º 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

[24] Convenção Americana de Direitos Humanos: "Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas." (11.3); Pacto Internacional sobre Direitos Civis e Políticos: "Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas." (17.2) e Convenção Europeia de Direitos Humanos: "Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei (...)" (8.2).

[25] SILVA, José Afonso da. *Curso de direito constitucional positivo*, 11ª ed. São Paulo, Malheiros, 1996, p. 202.

faculdade de impedir com que terceiros tenham acesso a esferas de exclusividade do particular,[26] dialoga com o que a doutrina brasileira identifica como a origem histórica do direito à privacidade.[27]. Especificamente, remonta à publicação, em 1890, do artigo *The right to privacy* na *Harvard Law Review,* em que os autores Samuel Warren e Louis Brandeis buscaram compreender os limites para a exposição da imagem das pessoas na imprensa. Os autores concluíram que essa proteção dizia menos respeito à propriedade e mais à inviolabilidade da personalidade, conceituando a privacidade como o "direito de ser deixado só".[28]

Sob essa perspectiva, o direito à privacidade assume um aspecto de liberdade negativa, que é própria do particular, e pode ser imposta a terceiros. O intenso fluxo de dados digitais, porém, reclama atualização dessa perspectiva para que o direito continue a proteger o indivíduo em toda a extensão de sua personalidade, que hoje existe também no mundo digital.

Assim, a doutrina atualizada entende que o direito à privacidade deve assumir uma perspectiva mais relacional e positiva, no sentido de exigir-se do Estado prestações positivas para a proteção do direito e para garantia do controle pessoal das próprias informações.[29] Nesse sentido, o direito à privacidade passa a relacionar-se com os demais direitos que asseguram a proteção aos dados pessoais no ordenamento jurídico, deles não podendo se dissociar.

---

[26] FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito da Universidade de São Paulo*. São Paulo, v. 88, jan./dez. 1993, p. 439-459.

[27] COSTA JÚNIOR, Paulo José da. *O direito de estar só:* tutela penal da intimidade. 4. ed. São Paulo: Revista dos Tribunais, 2011 e GRINOVER, Ada Pellegrini. *Liberdades públicas e processo penal: as interceptações telefônicas.* 2. ed. São Paulo: Malheiros, 1983.

[28] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. *Harvard Law Review,* v. 4, n. 5, pp. 193-220, 1890.

[29] DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. *Espaço Jurídico*, Joaçaba, v. 12, n. 2, jul./dez. 2011 e GLOECKNER, Ricardo Jacobsen; EILBERG, Daniela Dora. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. *Revista Brasileira de Ciências Criminais,* São Paulo, ano 27, v. 156, jun. 2019, p. 353 a 393.

Assim, ainda que não haja previsão expressa nesse sentido no artigo 5º, X, da Constituição da República, a limitação desse direito fundamental deve rigorosamente estar prevista em lei, o que é reforçado pelo inciso LXXIX do mesmo artigo 5º, inserido ao rol de direitos fundamentais pela Emenda Constitucional n.º 115/2022, como tratado a seguir, uma vez que a privacidade, como não poderia deixar de ser, dialoga hoje com a proteção mais ampla conferida aos dados pessoais.

2.2. Inviolabilidade do domicílio

A Constituição, em seu artigo 5º, inciso XI, determina que a casa é asilo inviolável do indivíduo. O domicílio delimita um espaço físico em que o indivíduo desfruta da sua privacidade em suas várias expressões, onde não deve sofrer a intromissão de terceiros.[30]

A busca domiciliar e, eventualmente, a busca pessoal restringem esse direito.

Cleunice Pitombo ensina que a restrição dos direitos afetados pelas buscas e apreensões apenas se justifica pela "necessidade e imprescindibilidade da perquirição criminal", sendo indispensável, para que seja válida e eficaz, "a reta observância dos requisitos e dos limites legais" a fim de evitar buscas infundadas e exploratórias. Assim, a autora conclui que melhor seria que, além das modalidades conhecidas, fossem disciplinadas "outras formas de busca diminuindo o abuso e arbítrio, na persecução penal". [31]

Em diálogo com o tema dos dados digitais, convém ponderar que a tecnologia permite o armazenamento de dados em uma proporção inigualável às coisas de existência material, que podem ser obtidas em medidas de busca e apreensão de objetos materiais.

Uma vez que as normas que disciplinam as buscas domiciliares (artigo 240 e seguintes do Código de Processo Penal) são baseadas no mundo de existência física e material, cujo grau de invasividade entendemos

---

[30] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional*. São Paulo: Editora Saraiva, 2011, p. 289.

[31] PITOMBO, Cleunice. *Da busca e da apreensão no processo penal*. 2. ed. São Paulo: Revista dos Tribunais, 2005, p. 125.

ser significativamente menor, a equiparação do acesso a dados digitais com uma busca domiciliar é imprópria e insuficiente, e dá ensejo à relativização inadequada e desproporcional de direitos,[32] desrespeitando a singularidade que deveria ser exigida no caso.

2.3. Inviolabilidade do sigilo das comunicações

O artigo 5º, XII, da Constituição da República, prevê que é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

A Lei n.º 9.296/1996 regulamentou a questão, dispondo sobre os requisitos para execução das interceptações telefônicas e telemáticas. Segundo o seu artigo 2º da referida Lei, a interceptação só poderá ocorrer quando houver indícios razoáveis da autoria ou participação em infração penal (inciso I), a prova não puder ser feita por outros meios disponíveis (inciso II) e o fato investigado constituir infração penal punida com pena de reclusão (inciso III). A medida deverá ser autorizada de forma fundamentada, não podendo exceder o prazo de quinze dias, renováveis uma vez comprovada a sua indispensabilidade (artigo 5º).

A edição da Lei de Interceptações foi fruto de entendimento jurisprudencial firmado no *Habeas Corpus* nº 69.912/RS, no sentido de que o Código de Telecomunicações não previa as *hipóteses* e a *forma* capazes de legitimar a exceção à inviolabilidade das comunicações prevista no inciso XII do artigo 5º da Constituição da República, não possuindo "densidade normativa suficiente"[33] e não suprindo exigência de lei específica.

---

[32] ZILLI, Marcos. A prisão em flagrante e o acesso de dados em dispositivos móveis. Nem utopia, nem distopia. Apenas a racionalidade. In: ANTONIALLI, Dennys; ABREU, Jacqueline de Souza. *Direitos fundamentais e processo penal na era digital*: doutrina e prática em debate, São Paulo: InternetLab, v. 1, 2018, p. 88.

[33] SIDI, Ricardo. *A interceptação das comunicações telemáticas no processo penal*. Belo Horizonte: D'Plácido, 2016, p. 230-231.

Com relação à interceptação das comunicações telemáticas, há, portanto, regramento a estabelecer minimamente os parâmetros para a execução desse meio de obtenção de prova.

Com relação às comunicações armazenadas em caixas de correio eletrônico ou aplicativos de mensagem instantânea, todavia, há divergência doutrinária acerca da proteção conferida a esses dados.[34] Isso porque, com o avanço das tecnologias, torna-se virtualmente impossível a distinção entre o momento de fluxo de uma comunicação e o momento de seu armazenamento.[35]

Assim, ainda que se admita que o direito à inviolabilidade do sigilo das comunicações esteja suficientemente regulado em lei, há uma parcela das comunicações humanas, aquelas já armazenadas, que constituem dados digitais sensíveis, hoje desprotegidos por lei infraconstitucional e sujeitos a acessos desmedidos em razão da falta de limites legais específicos e próprios.[36]

---

[34] QUITO, Carina. As quebras de sigilo telemático no processo penal e o paradoxo do acesso irrestrito às comunicações armazenadas. In: LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro; LAUX, Francisco de Mesquita; RAVAGNANI, Giovani dos Santos (Coord.). *Direito, processo e tecnologia*. São Paulo: Revista dos Tribunais, 2020.

[35] FERRAZ JÚNIOR, Tércio Sampaio. O alcance da proteção do sigilo das comunicações no Brasil. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). *Direitos fundamentais e processo penal na era digital*: doutrina e prática em debate, São Paulo:InternetLab, v. 4, 2021, p. 97-105.

[36] Acerca do tema, argumentando pela necessidade de atualização da proteção conferida às comunicações armazenadas, assim como por um maior rigor nas disposições legais destinadas a regulamentar as intervenções mais graves em direitos fundamentais, ver: MENDES, Gilmar Ferreira; PINHEIRO, Jurandi Borges. Interceptações e privacidade: novas tecnologias e a Constituição. In: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (Coord.). *Direito, inovação e tecnologia,* São Paulo: Saraiva, v. 1, 2015; BADARÓ, Gustavo Henrique. O debate constitucional sobre privacidade, intimidade e proteção de dados no Brasil. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). *Direitos fundamentais e processo penal na era digital:* doutrina e prática em debate, São Paulo: InternetLab, v. 4, 2021 e MENDES, Laura Schertel Ferreira. *Uso de softwares espiões pela polícia:* prática legal? Jota, publicado em 04/06/2015, atualizado em 07/06/2015. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espioes-pela-policia-pratica-legal-04062015>. Acesso em: 26 fev. 2023.

2.4. Autodeterminação informativa e inviolabilidade dos dados pessoais, inclusive nos meios digitais

O direito à autodeterminação informativa tem origem na doutrina e na jurisprudência alemãs.[37] Embora o desenvolvimento conceitual do mencionado direito fundamental tenha ocorrido de forma gradual, o caso concreto submetido ao Tribunal Constitucional Alemão (*Bundesgerichtshof, ou BVerfG*)[38] que motivou o reconhecimento expresso da autodeterminação informativa envolvia uma lei, promulgada em 1982, que previa a realização de um censo populacional no ano seguinte.[39] Tal dispositivo teve sua constitucionalidade questionada perante a Suprema Corte, que reconheceu a constitucionalidade parcial da norma, declarando a inconstitucionalidade de algumas disposições.[40]

Naquela oportunidade, o *BVerfG* reconheceu que, "tendo em vista as condições do moderno processamento de dados, a proteção do indivíduo contra levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais é abrangida pelo direito geral da personalidade".[41] Especificamente sobre o conteúdo do direito fundamental, o Tribunal estabeleceu que a autodeterminação informativa "garante o poder do indivíduo de decidir ele mesmo, em princípio, sobre a exibição e o uso de seus dados pessoais".[42]

Considerando-se que a autodeterminação informativa está diretamente vinculada à sistemática de proteção conferida à privacidade e aos dados pessoais, pode-se dizer que esse direito fundamental encontra

---

[37] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. *Revista Pensar*, Fortaleza, v. 25, n. 4, out./dez. 2020, p. 10 a 13.

[38] O precedente é mencionado na doutrina e na jurisprudência alemãs como "BVerfGE 65, 1 (Volkszählung)".

[39] MARTINS, Leonardo (org.). *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal alemão*. Montevideo: Konrad-Adenauer-Stiftung, 2005, p. 233 e 234.

[40] *Idem, ibidem*, p. 234.

[41] *Idem, ibidem*, p. 234.

[42] *Idem, ibidem*, p. 234.

guarida constitucional decorrente do regime e dos princípios adotados pela Constituição da República.[43]

Esse direito fundamental encontra ainda relação direta com a própria dignidade da pessoa humana, em sua dimensão de autodeterminação individual e decorre da indissociável necessidade de proteção do indivíduo ante à sua contínua exposição aos riscos de comprometimento da sua autodeterminação informacional em um contexto de processamento massivo de dados pessoais em meios digitais.

A propósito, os dados pessoais correspondem a toda informação relacionada a uma pessoa identificada ou identificável, incluindo nome, sobrenome, endereço, estado civil, filiação, endereços IP, dados de localização, informações de navegação e pesquisa na internet, histórico de compras, de interações em redes sociais, entre outras.[44]

Nos termos da Lei Geral de Proteção de Dados (nº 13.709/2018), dado pessoal é toda "informação relacionada a pessoa natural identificada ou identificável" (artigo 5º, I). Adota-se concepção ampla sobre o conceito, que inclui as informações que permitem a associação direta com a pessoa e aquelas que permitem a sua identificação mediante processos de cruzamento de dados, desde que esse procedimento ocorra dentro de parâmetros de razoabilidade.[45]

A possibilidade de acesso a dados digitais de diversas naturezas, somada ao seu cruzamento massivo, levou ao gradual reconhecimento de que os dados pessoais merecem proteção constitucional específica, o que ocorreu em 2022 com a inclusão do inciso LXXIX ao rol de direitos fundamentais do artigo 5º da Constituição da República, o qual assegura o direito à proteção dos dados pessoais, inclusive nos meios digitais, nos termos da lei, sendo certo que ainda não há, no ordenamento jurídico

---

[43] Confira-se: BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 6393/DF. Relatora: Min. Rosa Weber. Brasília, 07 de maio de 2020. Disponível em: https://encurtador.com.br/qyHW3. Acesso em: 07 dez. 2023.

[44] PINHEIRO, Patrícia Peck. *Proteção de dados pessoais:* Comentários à Lei n. 13.709/2018 - LGPD. Editora Saraiva, 2020, p. 25 e 26.

[45] BIONI, Bruno. *Xequemate:* o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI/USP, 2015, p. 17, 27 e 31.

brasileiro, lei geral de proteção de dados para tratamento de dados para fins de segurança pública e investigação criminal

2.5. Integridade e confiabilidade dos sistemas informáticos

O direito fundamental à confiabilidade e integridade dos sistemas informáticos também tem origem germânica.[46] O seu surgimento e reconhecimento expresso está diretamente relacionado com a implementação de novos métodos ocultos de investigação: de forma resumida, o caso que culminou no reconhecimento deste direito fundamental pelo *BVerfG* versava sobre a edição de uma lei que previa a possibilidade de infiltração em dispositivos informáticos, aproveitando-se de vulnerabilidades, para obtenção de elementos informativos que pudessem subsidiar a atuação dos órgãos de inteligência estatal.[47]

Em 2008, a inconstitucionalidade da norma foi reconhecida pelo Tribunal Constitucional. Naquela oportunidade, também a partir do direito geral de personalidade, a Corte reconheceu o direito fundamental à garantia da confiabilidade e integridade de sistemas informáticos, por considerar que o direito à autodeterminação informativa não seria suficientemente protetivo aos cidadãos.[48]

Gleizer, Montenegro e Viana lecionam que esse direito assegura que "o indivíduo precisa ter uma mínima confiança de que o Estado não pode, na ausência de base legal e de certos pressupostos, monitorá-los e acessá-los arbitrariamente". Ou seja, ao passo que o direito à autodeterminação informativa protege os dados em si, isto é, as próprias informações, o direito à integridade e confiabilidade protege os dispositivos utilizados rotineiramente pelos cidadãos de ingerências estatais sem base legal .[49]

---

[46] GRECO, Luís; GLEIZER, Orlandino. *A infiltração online no processo penal:* notícia sobre a experiência alemã. *Revista Brasileira de Direito Processual Penal,* v. 5, n. 3, 2019, p. 1.488. Disponível em: <https://revista.ibraspp.com.br/RBDPP/article/view/278>. Acesso em: 2 mai. 2023.

[47] *Idem, ibidem,* p. 1.488.

[48] *Idem, ibidem,* p. 1.493.

[49] GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. *O direito de proteção de dados no processo penal e na segurança pública*. São Paulo: Marcial Pons, 2021, p. 130-131.

O artigo 5º, §2º, da Constituição da República, prescreve que "os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte". Trata-se de uma cláusula geral, de caráter abrangente, que permite o reconhecimento de direitos fundamentais não expressamente previstos pelo constituinte originário.[50] Por força desse dispositivo, reconhece-se a integridade e a confiabilidade dos sistemas informáticos, por sua relevância para a própria proteção de dados, como direito fundamental materialmente integrante da ordem constitucional, o qual pode vir a ser restringido em casos de obtenção de dados digitais.

3. Como as provas digitais podem ser obtidas?

Uma vez descritos o direitos possivelmente vulnerados em razão da utilização de provas digitais, impõe-se analisar as formas mediante as quais as provas digitais podem ser obtidas, em especial considerando-se os diversos e variados meios, como (i) interceptação telemática; (ii) coleta após apreensão do dispositivo eletrônico; (iii) requisição a terceiros, usualmente os provedores de conexão e aplicações da internet[51] e (iv) instalação sub-reptícia de *softwares* espiões para acesso direto ao dispositivo eletrônico (*malware*).[52] De maneira mais detalhada, serão

---

[50] PIOVESAN, Flavia. *Direitos humanos e o direito constitucional internacional*, 14ª Ed. São Paulo: Saraiva, 2013, p. 115.

[51] Essa divisão é semelhante à divisão que propõe Orin Kerr em: KERR, Orin S. *Digital Evidence and the new Criminal Procedure*. Columbia Law Review. v. 105, 2005, p. 279-318. Disponível em: https://www.jstor.org/stable/4099310?read-now=1&seq=15#page_scan_tab_contents>. Acesso em: 23 abr. 2023.

[52] Maria Thereza Rocha de Assis e Daniel Marchionatti também indicam como formas de acesso a dados digitais a interceptação telemática e a requisição de informações a terceiros, acrescentando a busca e apreensão on-line, o mandado de busca reversa e o *roving bug* (espécie de software malicioso que permite acessar e habilitar funcionalidades como câmera e microfone). MOURA, Maria Thereza Rocha de Assis e BARBOSA, Daniel Machionatti. *Dados digitais:* interceptação, busca e apreensão e requisição. In WOLKART, Erik Navarro, *et all*. *Direito, processo e tecnologia*. São Paulo: RT, 2020, p. 478.

analisadas abaixo duas das principais formas de acesso a dados digitais, a saber: a apreensão do suporte físico e o acesso oculto e remoto (mediante *hacking* governamental ou o uso do *malwares*).[53]

3.1. Apreensão do suporte físico

Embora usualmente realizadas na sequência uma da outra, a busca e a apreensão são, em verdade, medidas autônomas, que podem ocorrer separadamente.[54] A busca é meio de obtenção de prova que visa à localização de pessoas ou coisas. Segundo o Código de Processo Penal, pode haver busca domiciliar e busca pessoal.[55] A apreensão, por sua vez, constitui ato de apossamento de coisas, tornando-as indisponíveis, sob custódia do Estado, enquanto importarem à persecução penal. Trata-se de medida processual complexa, podendo ser utilizada como medida cautelar ou como meio coercitivo de prova, com objetivo assecuratório.[56] Pode haver busca com apreensão; busca sem apreensão, quando a busca é mal-sucedida; e apreensão sem busca, quando o bem é entregue independentemente de apreensão.

No cotejo com o mundo digital, convém destacar que as provas digitais não são percebidas a olho nu. Assim, as buscas somente são capazes de identificar os dispositivos informáticos em seus componentes externos, como os *smartphones*, *tablets*, computadores e *hard drives*. Isso significa que a autorização para a apreensão dos dispositivos é insuficiente para que os dados neles contidos sejam acessados.[57]

---

[53] A interceptação telemática não será objeto do presente estudo, porque já há ampla produção acadêmica sobre o tema. Por sua vez, a requisição a terceiros também não será analisada, porque o procedimento de requisição em si não é detalhado na Lei de Interceptações ou no Marco Civil da Internet, mas no Código de Processo Civil, que apresenta a forma mais próxima da requisição de exibição de coisa ou documento a terceiro, prevista nos artigos 380, II, e 401 a 404 do Código de Processo Civil. *Idem, ibidem,* p. 499.

[54] SMANIO, Gianluca Martins. *Vigilância policial em meio digital:* entre o garantismo e a eficiência. Curitiba: Juruá, 2022, p. 170-171.

[55] PITOMBO, Cleunice, *Op. cit.,* p. 123 (nota 30).

[56] PITOMBO, Cleunice, *Op. cit.,* p. 239 (nota 30).

[57] COSTA, Helena Regina Lobo da. LEONARDI, Maciel. Busca e apreensão e acesso remoto a dados em servidores. *Revista Brasileira de Ciências Criminais,* São Paulo, v. 19, n. 88, jan./fev. 2011, p. 213.

A autorização para o acesso aos dados em si deve ser fundamentada em elementos concretos que permitam concluir que (i) os vestígios digitais de um determinado crime encontram-se, de fato, em um sistema informático e (ii) que esses vestígios serão úteis e necessários para os fins da investigação. Do contrário, permitir-se-á que ocorra o levantamento de sigilos protegidos pela Constituição da República sem a devida e fundamentada autorização judicial.[58]

Ocorre que a ausência de parâmetros legais claros para a coleta de dados digitais presentes nos dispositivos informáticos apreendidos resulta em autorizações judiciais genéricas para o acesso a todo e qualquer conteúdo armazenado nesses dispositivos.[59]

Ricardo Gloeckner e Daniela Dora alertam que "o fato de que não há legislação específica sobre o acesso ao conteúdo do celular é diverso da afirmação de que se trata de um conteúdo de acesso 'livre' às autoridades públicas"[60]. A justaposição de aplicativos diversos, capazes de armazenar um sem-número de dados pessoais de naturezas distintas em apenas um dispositivo eletrônico reclama, no nosso entender, não apenas autorização judicial precisa, mas sim previsão legal anterior suficiente, com a indicação em lei capaz de conferir aos magistrados parâmetros mínimos para a tomada de decisão, e aos indivíduos preceitos objetivos para a impugnação de medidas abusivas.

A aplicação direta do artigo 240 e seguintes do Código de Processo Penal, que versam sobre busca e apreensão física, para o acesso a dados em dispositivos eletrônicos implica equiparação entre coisas materiais e dados, muito embora o grau de invasividade seja significativamente maior nos meios digitais – o que aumenta o potencial de afetação a direitos fundamentais. Assim, a utilização da mesma disciplina, com o mesmo

---

58 GLOECKNER, Ricardo Jacobsen; EILBERG, Daniela Dora. *Op. cit., passim* (nota 28).

59 AZEREDO. João Fábio. *Sigilo das comunicações eletrônicas diante do Marco Civil da Internet*. In: DE LUCCA, Newton. *Direito & Internet,* v. 3, tomo II. São Paulo: Quartier Latin, 2015, p. 222.

60 GLOECKNER, Ricardo Jacobsen; EILBERG, Daniela Dora. *Op. cit., passim* (nota 28).

grau de rigor, para situações que atingem a privacidade em diferentes níveis, tem como efeito a flexibilização de direitos.[61]

Diferentemente do mundo digital, a casa possui um espaço físico delimitado. A busca domiciliar que ali se realiza não é irrestrita e a autorização de ingresso não implica autorização para a devassa de todo o espaço.[62] Por outro lado, o desenvolvimento das tecnologias de armazenamento de dados permite que um dispositivo eletrônico mantenha grande quantidade de dados sobre uma pessoa, que podem ultrapassar, incomparavelmente, os limites do domicílio.

Destaca-se que, no caso dos dados digitais, a prática aponta para uma *inversão* dos institutos da busca e da apreensão. Enquanto no mundo físico, geralmente, se buscam e, depois, se apreendem os elementos relevantes para a investigação, no mundo digital, o que se vê é o acesso e a coleta generalizados de todo e qualquer conteúdo presente em um dispositivo, para, somente depois, selecionarem-se aqueles relevantes para a investigação, ocorrendo verdadeira devassa, em proporções muito maiores do que as medidas executadas no mundo físico.[63]

A elevada quantidade de dados e a expectativa de privacidade que recai sobre eles demanda, portanto, controle mais rígido para o acesso a dados digitais presentes em dispositivos eletrônicos, não sendo equiparável à mera busca e apreensão.

---

[61] WANDERLEY, Gisela Aguiar. Privacidade e cidadania: os limites jurídicos da atividade investigativa e a legalidade do acesso policial a aparelhos celulares. In: ANTONIALLI, Dennys; FRAGOSO, Nathalie (eds.). *Direitos fundamentais e processo penal na era digital:* doutrina e prática em debate, São Paulo: InternetLab, v. 2, 2019, p. 125-126.

[62] ZILLI, Marcos. *Op. cit.,* p. 89 (nota 31).

[63] Rafael Francisco França pondera que antes da apreensão formal e exame pericial, o conteúdo de um *smartphone* permanece desconhecido, nem sempre sendo possível definir o que poderá ser acessado para análise. Ainda assim, autorizações genéricas a todo o conteúdo podem constituir verdadeiras devassas à privacidade do usuário (implicando, inclusive, restrição ao direito à não incriminação em certos casos), sendo a solução mais racional, a princípio, a indicação dos tipos de dados que podem ser idôneos e necessários para o atingimento das finalidades da persecução. FRANÇA, Rafael Francisco. Balancing Self-Incrimination and Public Safety: A Comparative Analysis of Compelled Smartphone Unlocking in Brazilian and U.S. Legal Systems. *Revista Brasileira de Direito Processual Penal*, vol. 9, n. 3, set./dez. 2023, p. 1374.

Conforme avançam as tecnologias, os operadores do direito enfrentam o desafio de encontrar o sensível equilíbrio entre o direito à privacidade e a necessidade de investigação e efetividade da segurança pública por parte do Estado, especialmente em situações em que a apreensão e consequente acesso a *smartphones* e outros dispositivos informáticos pode levar ao conhecimento de uma extensa gama de dados pessoais sensíveis do usuário.

Entendemos que essas circunstâncias sublinham a importância do devido processo e da adesão a procedimentos legais na obtenção de provas digitais, onde a autorização judicial devidamente balizada por lei serve como um mecanismo crucial para equilibrar as necessidades investigativas com a proteção de direitos fundamentais.[64]

3.2. Acesso oculto e remoto

Além da apreensão do suporte físico nos quais os dados digitais estão armazenados, a evolução tecnológica permite, hoje, o acesso e apreensão desses dados de forma oculta e remota.

Diante do fortalecimento da criminalidade organizada e do aumento da ocorrência de crimes transnacionais, é natural que o Estado, com objetivo de maximizar seu potencial de investigação, tente valer-se de novas tecnologias, cada vez mais eficientes e invasivas, para acessar dispositivos e sistemas informáticos, buscando alcançar dados e informações que possam ter utilidade para a persecução criminal.[65]

Assim, tornou-se tecnologicamente viável que, de forma escamoteada, os agentes de persecução explorem vulnerabilidades dos sistemas-alvo para acessar informações, inclusive aquelas protegidas por sigilo, driblando mecanismos estabelecidos de criptografia.[66] Nesse contexto, duas medidas para obtenção de dados podem ser destacadas: o *hacking* estatal e a infiltração por *malware*[67].

---

[64] *Idem, ibidem*, p. 1410-1411.

[65] SMANIO, Gianluca. *Op. cit.,* p. 193 (nota 53).

[66] SMANIO, Gianluca. *Op. cit.,* p. 192 e 193 (nota 53).

[67] Sobre o tema, Carlos Hélder Mendes assinala: "Embora sejam metodologias similares em suas funcionalidades investigativas, o 'Hacking' e o uso de

Através do hackeamento estatal, os órgãos de investigação infiltram-se de forma oculta e remota em algum dispositivo e/ou sistema de interesse, valendo-se de falhas e aberturas previamente identificadas.[68] Essa prática depende, necessariamente, de conexão com a internet[69]. Um exemplo desta atuação é a quebra de uma senha de acesso, que permite o ingresso no dispositivo informático alvo de modo a viabilizar o acesso a arquivos protegidos.[70]

Os *malwares71*, por sua vez, são programas instalados[72] no sistema alvo, inseridos, evidentemente, sem autorização prévia do investigado.[73] Registra-se que a instalação desses *softwares* visa a promover a abertura de uma espécie de portal de acesso remoto, conhecido como "mecanismo de acesso excepcional"[74] ou *backdoor*.*75* A partir desta abertura, as informações podem ser acessadas e transmitidas.

Malware pelo Estado se diferenciam justamente pelo fato de que a primeira não se procede mediante a instalação de software em dispositivos informáticos, se tratando de um "acesso remoto não autorizado" possível e vinculado à utilização da internet. Por tal aspecto é limitado ao período de conexão, o que diferencia substancialmente as duas espécies". MENDES, Carlos Hélder C. Furtado. *Malware do Estado e processo penal:* a proteção de dados informáticos face à infiltração por software na investigação criminal. Dissertação (Mestrado em 2018) – PUCRS, Porto Alegre, 2018, p. 129.

68 SMANIO, Gianluca. *Op. cit.,* p. 193 (nota 53).

69 MENDES, Carlos Hélder C. Furtado. *Op. cit.,* p. 129 (nota 66).

70 SMANIO, Gianluca. *Op. cit.,* p. 193 (nota 53).

71 Uma completa diferenciação entre os tipos de *malwares* pode ser conferida em: RAMALHO, David Silva. *Métodos ocultos de investigação criminal em ambiente digital,* Coimbra: Almedina, 2017, p. 320 a 322.

72 As formas de instalação e o mecanismo de funcionamento dos *malwares* também são amplamente descritos por David Silva Ramalho. *Idem, ibidem,* p. 322 a 324.

73 MENDES, Carlos Hélder C. Furtado. *Op. cit.,* p. 129 (nota 66).

74 LIGUORI, Carlos. *Direito e criptografia:* direitos fundamentais, segurança da informação e os limites da regulação jurídica da tecnologia. São Paulo: Saraiva, 2022, p. 251.

75 Carlos Hélder Mendes explica que *backdoors* são "formas ocultas de acessar o sistema do computador infectado de maneira remota, enviando os mecanismos de autenticação existente, possibilitando assim, que o terceiro – investigador – acesse informações (como senhas e logins) ou monitore as atividades do usuário do sistema alvo infectado". MENDES, Carlos Hélder C. Furtado. *Op. cit.,* p. 130 (nota 66).

Essa instalação pode ocorrer a partir de um comportamento ativo do usuário (como clicar em um *link* malicioso, por exemplo) ou a partir da inserção de algum *hardware* no dispositivo alvo (acoplamento de um pen-drive, por exemplo). Fato é que, uma vez instalado, o *malware* independe de acesso constante à internet para execução de suas funcionalidades típicas.[76]

Dessa forma, mesmo sem internet, o *software* pode seguir executando suas funções até que, por exemplo, o computador-alvo restabeleça sua conexão com a internet, a fim de que os dados sejam, enfim, transmitidos.[77] Ainda, esses dados podem ser transmitidos por outras formas, como o *bluetooth*, ou a própria retirada de *hardware* (um HD, com informações coletadas, por exemplo).[78]

Ambas as práticas permitem o exercício de funcionalidades absolutamente invasivas, com a coleta massiva de dados do alvo, afetando, por isso, os direitos fundamentais à privacidade, à inviolabilidade do domicílio, à inviolabilidade das comunicações, à autodeterminação informativa e à integridade dos sistemas informáticos

A partir da utilização de *malwares*, por exemplo, os agentes de persecução penal podem executar diversas funcionalidades,[79] tais como: interceptar comunicações telemáticas (obtendo os dados na ponta, não em fluxo); efetuar buscas por dados armazenados ou produzidos; encetar captação ambiental, gravando áudio, pelo microfone do dispositivo, e vídeo, por sua *webcam*; estabelecer formas de vigilância *online*, acompanhando as atividades travadas pelo alvo em ambiente digital; realizar observação em tempo real mediante o monitoramento por vídeo; obter a geolocalização do investigado.[80]

---

[76] *Idem, ibidem,* p. 130.

[77] *Idem, ibidem,* p. 130.

[78] SMANIO, Gianluca. *Op. cit.,* p. 193 (nota 53).

[79] A relação entre as funcionalidades afetadas por cada tipo de software pode ser conferida em: RAMALHO, David Silva. *Op. cit.,* p. 320 a 322 (nota 70).

[80] SMANIO, Gianluca. *Op. cit.,* p. 194 a 198 (nota 53).

Quando comparados a outros meios de obtenção de prova legalmente previstos e disciplinados,[81] como a busca e a apreensão, e a interceptação telefônica e telemática, por exemplo, a diferença entre o grau de afetação dos direitos fundamentais e os procedimentos para recolhimento das informações de interesse demonstram a incapacidade de fundamentar a utilização de *hacking* e *malwares* de *lege lata*.

Por exemplo, na interceptação telemática tradicional, um agente externo, de forma passiva, acessa o fluxo das informações trocadas entre os participantes do processo comunicacional. Ao contrário, uma interceptação efetuada a partir de *malware* instalado no dispositivo ou mediante *hacking* pela quebra da senha do e-mail permitem que o investigador, de forma ativa, capte o dado na origem (antes mesmo do envio), ou no destino. Ainda, essa captação é direta e executada internamente ao sistema, corrompendo-o.[82]

Por isso, tendo em vista o grau de invasividade, a eventual utilização dessas técnicas depende de norma habilitadora expressa, que regule hipóteses, pressupostos, requisitos, forma de execução, tempo de duração e, sobretudo, que discipline a preservação da cadeia de custódia dos elementos, com demonstração dos procedimentos técnicos executados, com objetivo de assegurar a autenticidade e a confiabilidade dos elementos recolhidos.

De forma crítica, analisando a prática de *Online-Durchsuchung* na Alemanha e a possível aplicação de mecanismo semelhante no Brasil, Luís Greco e Orlandino Gleizer concluem que "se levarmos a sério a ideia de reserva de lei insculpida no art. 5, II, CF, basta verificar que inexiste dispositivo expresso que autorize a medida, para concluir que ela é inadmissível entre nós".[83]

Nessa linha, sob a ótica de uma sociedade politicamente organizada que regula seu processo judicial mediante valores basilares,

---

[81] Por todos, conferir: RIBEIRO, Gustavo Alves Magalhães; CORDEIRO, Pedro Ivo Rodrigues Velloso; FUMACH, Débora Moretti. O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. Revista Brasileira de Direito Processual Penal, v. 8, n. 3, 2022. https://doi.org/10.22197/rbdpp.v8i3.723

[82] SMANIO, Gianluca. *Op. cit.,* p. 195 (nota 53).

[83] GRECO, Luís; GLEIZER, Orlandino. *Op. cit.,* p. 1.497 (nota 45).

devemos ponderar os benefícios e os problemas decorrentes da utilização de técnicas como o *hacking* e o *malware*. De um lado, é inegável que essas tecnologias possibilitam um ganho epistêmico relevante: diante do elevado potencial de obtenção de informações que enriquecem o acervo probatório da persecução penal, práticas como as descritas ampliam exponencialmente as capacidades de investigação, sobretudo em face da criminalidade organizada e transfronteiriça.

De outro, precisamos estabelecer, de forma inequívoca, quais são as formas, limites e procedimentos aceitáveis. Afinal, existem problemas epistêmicos e processuais relevantes a partir da utilização dessas tecnologias. Por exemplo: uma vez acessado, o sistema alvo torna-se corrompido. Por isso, são necessárias formas de regulação que, diante das características das provas digitais, permitam assegurar a confiabilidade e autenticidade dos elementos obtidos.

4. Problematização

O desenvolvimento deste estudo permitiu identificar que, em razão das características peculiares das provas digitais, cuidados procedimentais particulares são necessários para que elas possam ser obtidas, admitidas, produzidas e valoradas. Nesta linha, Gustavo Badaró destaca que a integridade do elemento de prova digital relaciona-se, de forma direta e intransponível, com a força probatória desse elemento, influenciando seu potencial epistêmico para a reconstrução dos fatos. [84] Assim, por serem as provas digitais frágeis, voláteis e sujeitas às alterações e dissipações, voluntárias ou não, é imprescindível que o legislador estabeleça um regramento específico para as provas digitais, definindo de forma clara os procedimentos de obtenção, admissão, produção e valoração.[85]

Com relação às características das provas digitais, portanto, já surgem elementos a indicar a necessidade de uma disciplina particular.

---

[84] BADARÓ, Gustavo. *A cadeia de custódia da prova digital.* In: OSNA, Gustavo; SARLET, Ingo Wolfgang; MATIDA, Janaína Roland; REICHELT, Luis Alberto; JOBIM, Marco Félix; RAMOS, Vitor de Paula (org.). *Direito probatório.* Londrina: Editora Toth, 2023, p. 174-175 e 180.

[85] *Idem, ibidem,* p. 174-175 e 180.

Analisados os direitos fundamentais que são tensionados pela obtenção de dados digitais, depreendemos, em segundo lugar, que a ausência de regulamentação específica – apesar de, em abstrato, significar uma proibição absoluta de ingerência estatal nos direitos fundamentais –, que leve em conta as singularidades e o grau de tensionamento imposto aos direitos fundamentais, implica, em verdade, acessos desmedidos a dados pessoais armazenados. Apesar do gradual reconhecimento dos riscos causados pelo cruzamento massivo de dados, inexiste, hoje, lei infraconstitucional que regulamente as hipóteses, a forma e os limites para a obtenção e o tratamento de dados pessoais no âmbito das atividades de segurança pública e persecução penal.

A propósito, ainda que a aprovação da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados) represente um paradigma na proteção de dados pessoais no Brasil, estabelecendo ampla estrutura de proteção regulatória, com princípios e medidas de caráter organizacional, as operações de tratamento de dados para fins exclusivos de segurança pública e atividades de investigação e repressão de infrações penais foram excluídas do âmbito de aplicação da LGPD (artigo 4.º, III), estando pendentes os debates sobre a LGPD Penal,[86] que seria apta, em tese, a preencher tal lacuna.[87]

Finalmente, ao analisar em termos práticos duas formas de obtenção de dados digitais, o presente estudo identificou que (i) a ausência de parâmetros legais claros para a coleta de dados digitais presentes nos dispositivos informáticos apreendidos pode resultar em autorizações judiciais genéricas para o acesso a todo e qualquer conteúdo armazenado nesses dispositivos, com consequente violação dos direitos relacionados à privacidade e (ii) as formas de acesso oculto e remoto, como as práticas de *hacking* e a utilização de *malware* não encontram a mínima regulamentação.

---

[86] Acerca do Anteprojeto de Lei de Proteção de Dados Pessoais para Segurança Pública e Persecução Penal de 2020 e o Projeto de Lei nº 1.515/2022, ver: https://lapin.org.br/wp-content/uploads/2022/11/Nota-tecnica-Analise-comparativa-entre-o-anteprojeto-de-LGPD-Penal-e-o-PL-15152022-1.pdf.

[87] ABREU, Jacqueline de Souza. Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD. In: Bioni, Bruno; Doneda, Danilo *et all.* (Coord.) *Tratado de Proteção de Dados Pessoais*, 2ª ed., Rio de Janeiro: Editora Forense, 2021, p. 585-590.

Buscando soluções para a esses impasses, a doutrina já sugere o estabelecimento de *parâmetros procedimentais mínimos* a balizar a execução dos meios de obtenção de provas digitais.

Diogo Malan, por exemplo, se refere a um *roteiro normativo* para guiar a decisão judicial que autoriza o emprego dos métodos ocultos de investigação, que exija (i) a delimitação objetiva quanto ao fato naturalístico em apuração e (ii) a delimitação subjetiva quanto ao nome e qualificação das pessoas que suportarão os efeitos jurídicos, ao local de execução e ao meio técnico operacional a ser utilizado.[88]

Gilmar Mendes e Jurandi Pinheiro lecionam que se deve avançar não no sentido da previsão legal específica sobre cada nova tecnologia, mas da formulação de um *modelo de regulação* que estabeleça *requisitos mínimos* para o acesso aos dados, contendo (i) rol de crimes a autorizar as medidas e permitir elencá-las de acordo com a sua gravidade, oferecendo possível solução ao conflito de subsidiariedades;[89] (ii) prazo máximo de duração da medida; (iii) forma de registro dos dados obtidos; (iv) restrição na divulgação dos dados e (v) sistemas de acompanhamento do cumprimento desses requisitos.[90]

Ainda que não se possa olvidar as críticas doutrinárias no sentido de que legislações muito específicas podem ser tornar rapidamente

---

[88] Diogo Malan fez referência ao "roteiro normativo" em palestra apresentada ao InternetLab em 02.09.2020. Segundo o professor, a apresentação foi feita com base em texto de Enrique Bacigalupo e na jurisprudência do Tribunal Europeu de Direitos Humanos. MALAN, Diogo. Métodos ocultos, devido processo e o enfrentamento à criminalidade organizada. In: CRUZ, Francisco Brito; SIMÃO, Bárbara (org.). *Direitos fundamentais e processo penal na era digital:* doutrina e prática em debate. São Paulo: InternetLab, v. 4, 2021, p. 115-116.

[89] Gustavo Badaró leciona que como os meios de obtenção de provas só podem ser utilizados quando não houver outro meio menos gravoso para o atingimento dos objetivos da investigação, isso leva a uma "colisão de subsidiariedades". Essa questão pode ser solucionada a partir do grau de afetação que o meio de obtenção de prova causa aos direitos fundamentais ou a partir da previsão de crimes específicos a autorizar cada tipo de medida. BADARÓ, Gustavo. Hipóteses que autorizam o emprego de meios excepcionais de obtenção de prova. In: AMBOS, Kai; ROMERO, Eneas (Coord.). *Crime organizado:* análise da Lei 12.850/2013. São Paulo: Marcial Pons, 2017, p. 14.

[90] MENDES, Gilmar Ferreira; PINHEIRO, Jurandi Borges. *Op. cit.,* p. 250 (nota 35).

obsoletas com o avanço das tecnologias,[91] vale lembrar que a lei serve como salvaguarda de direitos fundamentais e como limitação à atividade dos agentes estatais, devendo conter limites materiais e procedimentais precisos à ingerência estatal, garantindo a observância de um rito racionalmente constituído, com maior segurança jurídica e confiança epistêmica da prova.

Considerações finais

O acesso a dados digitais inegavelmente afeta direitos fundamentais muito caros à liberdade individual e à convivência pacífica em uma sociedade democrática. A ausência de parâmetros específicos a regulamentar a obtenção das provas digitais propicia terreno fértil para a violação desses direitos. Assim, entendemos que o elevado volume de dados e a expectativa de privacidade que recai sobre eles exige controle mais rígido a ser definido, inescapavelmente, mediante lei específica. A previsão de parâmetros legais mínimos, mas claros, a balizar diferentes formas de acesso a dados digitais que representam diferentes graus de invasividade a direitos fundamentais garante o estabelecimento de um processo penal mais justo, com mais racionalidade, previsibilidade, segurança jurídica e limites às ingerências estatais. Conclui-se, portanto, que a obtenção de provas digitais demanda disciplina jurídica própria no processo penal.

Referências

ABREU, Jacqueline de Souza. Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD. In: Bioni, Bruno; Doneda, Danilo *et all*. (Coord.) *Tratado de Proteção de Dados Pessoais*, 2ª ed., Rio de Janeiro: Editora Forense, 2021.

AZEREDO. João Fábio. Sigilo das comunicações eletrônicas diante do Marco Civil da Internet. In: DE LUCCA, Newton. *Direito & Internet*. v. III, tomo II. São Paulo: Quartier Latin, 2015.

[91] LOUREIRO, João Carlos. Constituição, tecnologia e risco(s): entre medo(s) e esperança(s). In: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang. COELHO, Alexandre Zavaglia P. (coord.). *Direito, inovação e tecnologia*. São Paulo: Saraiva, 2015, v. 1, p. 68.

BADARÓ, Gustavo. A cadeia de custódia da prova digital. In: OSNA, Gustavo; SARLET, Ingo Wolfgang; MATIDA, Janaína Roland; REICHELT, Luis Alberto; JOBIM, Marco Félix; RAMOS, Vitor de Paula (org.). *Direito probatório*. Lodrina: Editora Toth, 2023.

BADARÓ, Gustavo Henrique. O debate constitucional sobre privacidade, intimidade e proteção de dados no Brasil. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). *Direitos fundamentais e processo penal na era digital:* doutrina e prática em debate. São Paulo: InternetLab, v. 4, 2021.

BADARÓ, Gustavo. Hipóteses que autorizam o emprego de meios excepcionais de obtenção de prova. In: AMBOS, Kai; ROMERO, Eneas (Coord.). *Crime organizado*: análise da Lei 12.850/2013. São Paulo: Marcial Pons, 2017.

BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. *Boletim IBCCRIM*, São Paulo, ano 29, n. 343, jun. 2021.

BADARÓ MASSENA, Caio. A propósito da cadeia de custódia das provas digitais no Processo Penal: breves notas sobre lógica da desconfiança, assimetria informacional e direito de defesa. *Boletim IBCCRIM*, São Paulo, v. 31, n. 368, 2023. Disponível em: <https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/506>. Acesso em: 17 jun. 2024.

BIONI, Bruno. *Xequemate*: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI/USP, 2015.

COSTA JÚNIOR, Paulo José da. *O direito de estar só*: tutela penal da intimidade. 4. ed. São Paulo: Revista dos Tribunais, 2011.

COSTA, Helena Regina Lobo da; LEONARDI, Maciel. Busca e apreensão e acesso remoto a dados em servidores. *Revista Brasileira de Ciências Criminais*. São Paulo, v. 19, n. 88, jan./fev. 2011.

DANIELE, Marcello. La prova digitale nel processo penale. *Rivista di Diritto Processuale,* v. 66, n. 2, 2011.

DELGADO MARTÍN, Joaquín. *La prueba digital*: concepto, clases, aportación al proceso y valoración. Diario La Ley, n. 6, Sección Ciberderecho, abr. 2017.Não paginado. Disponível em: <https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAAEAMtMSbF1CTEAAiMTUzMDI7Wy1KLizPw-8WyMDQ3MDE0NDkEBmWqVLfnJIZUGqbVpiTnGqWnJOamKRS2JJqnNiTm-peSmKRbUhRaSoAYE02pkwAAAA=WKE#I12>. Acesso em: 20 set. 2024.

DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. *Espaço Jurídico*, Joaçaba, v. 12, n. 2, jul./dez. 2011.

FERRAZ JÚNIOR, Tércio Sampaio. O alcance da proteção do sigilo das comunicações no Brasil. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). *Direitos fundamentais e processo penal na era digital:* doutrina e prática em debate. São Paulo: InternetLab, v. 4, 2021.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito da Universidade de São Paulo.* São Paulo, v. 88, jan./dez. 1993, p. 439-459. https://doi.org/10.11606/issn.2318-8235.v88i0p439-459

FERRER-BELTRÁN, Jordi. *Prova sem convicção*: standards de prova e devido processo. Tradução: Vitor de Paula Ramos. São Paulo: JusPodivm, 2022.

FRANÇA, Rafael Francisco. Balancing Self-Incrimination and Public Safety: A Comparative Analysis of Compelled Smartphone Unlocking in Brazilian and U.S. Legal Systems. *Revista Brasileira de Direito Processual Penal*, vol. 9, n. 3, p. 1371-1420, set./dez. 2023. https://doi.org/10.22197/rbdpp.v9i3.867

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. *O direito de proteção de dados no processo penal e na segurança pública.* São Paulo: Marcial Pons, 2021.

GLOECKNER, Ricardo Jacobsen; EILBERG, Daniela Dora. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. *Revista Brasileira de Ciências Criminais,* São Paulo, ano 27, v. 156, jun. 2019.

GOMES FILHO, Antonio Magalhães. Notas sobre a terminologia da prova (reflexos no processo penal brasileiro). In: YARSHELL, Flávio Luiz; DE MORAES, Zanoide (Coods.). *Estudos em Homenagem à Professora Ada Pellegrini Grinover*. São Paulo: Editora DPJ, 2005.

GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal: notícia sobre a experiência alemã. *Revista Brasileira de Direito Processual Penal,* v. 5, n. 3, pp. 1483–1518, 2019. https://doi.org/10.22197/rbdpp.v5i3.278

GRINOVER, Ada Pellegrini. *Liberdades públicas e processo penal*: as interceptações telefônicas. 2. ed. São Paulo: Malheiros, 1983.

KERR, Orin S. Digital *Evidence and the new Criminal Procedure*. Columbia Law Review. v. 105, pp. 279-318, 2005.https://doi.org/10.18574/nyu/9780814739334.003.0013

LIGUORI, Carlos. *Direito e criptografia*: direitos fundamentais, segurança da informação e os limites da regulação jurídica da tecnologia. São Paulo: Saraiva, 2022.

LOUREIRO, João Carlos. Constituição, tecnologia e risco(s): entre medo(s) e esperança(s). In: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang. COELHO, Alexandre Zavaglia P. (coord.). *Direito, inovação e tecnologia*. v. 1. São Paulo: Saraiva, 2015.

MALAN, Diogo. Métodos ocultos, devido processo e o enfrentamento à criminalidade organizada. In: CRUZ, Francisco Brito; SIMÃO, Bárbara (org.). *Direitos fundamentais e processo penal na era digital:* doutrina e prática em debate. São Paulo: InternetLab, v. 4, 2021.

MARTINS, Leonardo (org.). *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal alemão.* Montevideo: Konrad-Adenauer-Stiftung, 2005.

MENDES, Carlos Hélder C. Furtado. *Malware do Estado e processo penal*: *a proteção de dados informáticos face à infiltração por software na investigação criminal.* Dissertação (Mestrado em 2018) – PUCRS, Porto Alegre, 2018, p. 129.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de Direito Constitucional,* São Paulo: Editora Saraiva, 2011.

MENDES, Gilmar Ferreira; PINHEIRO, Jurandi Borges. Interceptações e privacidade: novas tecnologias e a Constituição. In: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (Coord.). *Direito, inovação e tecnologia*. São Paulo: Saraiva, v. 1, 2015.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. *Revista Pensar,* Fortaleza, v. 25, n. 4, out./dez. 2020. https://doi.org/10.5020/2317-2150.2020.10828

MENDES, Laura Schertel Ferreira. *Uso de softwares espiões pela polícia*: prática legal? Jota, publicado em 04/06/2015, atualizado em 07/06/2015. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espioes-pela-policia-pratica-legal-04062015>. Acesso em: 26 fev. 2023.

MOURA, Maria Thereza Rocha de Assis e BARBOSA, Daniel Machionatti. Dados digitais: interceptação, busca e apreensão e requisição. In: WOLKART, Erik Navarro, *et all*. *Direito, Processo e Tecnologia.* São Paulo: RT, 2020.

PINHEIRO, Patrícia Peck. *Proteção de dados pessoais: comentários à Lei n. 13.709/2018 - LGPD.* São Paulo: Saraiva, 2020.

PIOVESAN, Flavia. *Direitos Humanos e o Direito Constitucional Internacional*, 14ª Ed. São Paulo: Saraiva, 2013.

PITOMBO, Cleunice. *Da busca e da apreensão no processo penal.* 2. ed. São Paulo: Revista dos Tribunais, 2005.

QUITO, Carina. As quebras de sigilo telemático no processo penal e o paradoxo do acesso irrestrito às comunicações armazenadas. In: LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro; LAUX, Francisco de Mesquita; RAVAGNANI, Giovani dos Santos (Coord.). *Direito, processo e tecnologia.* São Paulo: Revista dos Tribunais, 2020.

RIBEIRO, Gustavo Alves Magalhães; CORDEIRO, Pedro Ivo Rodrigues Velloso; FUMACH, Débora Moretti. O *malware* como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. *Revista Brasileira de Direito Processual Penal,* v. 8, n. 3, 2022. https://doi.org/10.22197/rbdpp.v8i3.723

SIDI, Ricardo. *A Interceptação das comunicações telemáticas no processo penal*. Belo Horizonte: D'Plácido, 2016. https://doi.org/10.11606/D.2.2014.tde-04032015-082717

SILVA, José Afonso da. *Curso de direito constitucional positivo*. 11. ed. São Paulo, Malheiros, 1996.

SMANIO, Gianluca Martins. *Vigilância policial em meio digital*: entre o garantismo e a eficiência. Curitiba: Juruá, 2022.

VAZ, Denise Provasi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório.* Tese (Doutorado em 2012) – Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012. https://doi.org/10.11606/t.2.2012.tde-28052013-153123

WANDERLEY, Gisela Aguiar. Privacidade e cidadania: os limites jurídicos da atividade investigativa e a legalidade do acesso policial a aparelhos celulares. In: ANTONIALLI, Dennys; FRAGOSO, Nathalie (eds.). *Direitos fundamentais e processo penal na era digital*: doutrina e prática em debate, São Paulo. InternetLab, v. 2, 2019.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. *Harvard Law Review*, v. 4, n. 5, 1890, p. 193-220. https://doi.org/10.1080/10811680.2020.1805984

ZILLI, Marcos. A prisão em flagrante e o acesso de dados em dispositivos móveis. Nem utopia, nem distopia. Apenas a racionalidade. In: ANTONIALLI, Dennys; ABREU, Jacqueline de Souza. *Direitos fundamentais e processo penal na era digital*: doutrina e prática em debate, São Paulo: InternetLab, v. 1, 2018.

Authorship information

Marta Cristina Cury Saad Gimenes. PhD Professor of Criminal Procedural Law at the Faculty of Law of the University of São Paulo. PhD (2007) and Master (2002) in Criminal Procedural Law from the Faculty of Law of the University of São Paulo. Graduated in Law from the Faculty of Law of the University of São Paulo. Former President and former Advisor of the Brazilian Institute of Criminal Sciences (IBCCRIM). Former President of the Ibero-American Criminal Advocacy Network. Lawyer. martasaad@usp.br.

Helena Costa Rossi. Graduated in Law from the Faculty of Law of the University of São Paulo and a master's student in Criminal Procedural Law in the Postgraduate Program of the same institution, linked to the Department of Procedural Law. Attorney. helena.rossi@usp.br.

Pedro Henrique Partata. Graduated in Law from the Faculty of Law of the University of São Paulo and a master's student in Criminal Procedural Law in the Postgraduate Program of the same institution, linked to the Department of Procedural Law. Attorney. pedro.mortoza@usp.br.

Additional information and author's declaratations
(scientific integrity)

Acknowledgement: this article is the result of a research developed in the postgraduate activities of the postgraduate program at the Faculty of Law of the University of São Paulo. More specifically, it derives from the studies carried out in the subject: DPC5845 - Critical Study of the Means of Evidence and Obtaining Evidence in Criminal Procedure in 2023.

Conflict of interest declaration: the authors confirm that there are no conflicts of interest in conducting this research and writing this article.

Declaration of authorship: all and only researchers who comply with the authorship requirements of this article are listed as authors; all coauthors are fully responsible for this work in its entirety.

- *Marta Cristina Cury Saad Gimenes*: writing – review and editing, final version approval.
- *Helena Costa Rossi*: conceptualization, methodology, data curation, investigation, writing – original draft, validation, writing – review and editing, final version approval.
- *Pedro Henrique Partata*: conceptualization, methodology, data curation, investigation, writing – original draft, validation, writing – review and editing, final version approval.

Declaration of originality: the authors assure that the text here published has not been previously published in any other resource and that future republication will only take place with the express indication of the reference of this original publication; they also attest that there is no third party plagiarism or self-plagiarism.

Editorial process dates
(https://revista.ibraspp.com.br/RBDPP/about)

- Submission: 21/07/2024
- Desk review and plagiarism check: 30/07/2024
- Review 1: 07/08/2024
- Review 2: 26/08/2024
- Review 3: 01/09/2024
- Preliminary editorial decision: 06/09/2024
- Correction round return: 21/09/2024
- Final editorial decision: 29/09/2024

Editorial team

- Editor-in-chief: 1 (VGV)
- Reviewers: 3

How to cite (ABNT Brazil):

SAAD GIMENES, Marta C.; ROSSI, Helena C.; PARTATA, Pedro H.. A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais. *Revista Brasileira de Direito Processual Penal*, vol. 10, n. 3, e1071, set./dez. 2024. https://doi.org/10.22197/rbdpp.v10i3.1071