LUIZ FERNANDO BUGIGA REBELLATO

A análise constitucional do sigilo e da privacidade nas investigações criminais: o acesso a dados armazenados em aparelhos celulares

Dissertação de Mestrado

Orientador: Professor Doutor José Raul Gavião de Almeida

UNIVERSIDADE DE SÃO PAULO

FACULDADE DE DIREITO

São Paulo - SP

2020

LUIZ FERNANDO BUGIGA REBELLATO

A análise constitucional do sigilo e da privacidade nas investigações criminais: o acesso a dados armazenados em aparelhos celulares

Dissertação de Mestrado, apresentada à Banca Examinadora do Programa de Pós-Graduação em Direito, da Faculdade de Direito da Universidade de São Paulo, como exigência parcial para obtenção do título de Mestre em Direito, na área de concentração de Direito Processual, sob a orientação do Professor Doutor José Raul Gavião de Almeida.

UNIVERSIDADE DE SÃO PAULO
FACULDADE DE DIREITO
São Paulo - SP
2020

Catalogação da Publicação
Serviço de Biblioteca e Documentação
Faculdade de Direito da Universidade de São Paulo

Rebellato, Luiz Fernando Bugiga
A análise constitucional do sigilo e da privacidade nas investigações criminais: o acesso a dados armazenados em aparelhos celulares ; Luiz Fernando Bugiga Rebellato ; orientador José Raul Gavião de Almeida -- São Paulo, 2020.
305
Dissertação (Mestrado - Programa de Pós-Graduação em Direito Processual) - Faculdade de Direito, Universidade de São Paulo, 2020.

1. Acesso a dados armazenados em aparelhos celulares. 2. Formas de acesso aos dados armazenados. 3. Indispensabilidade de autorização judicial. 4. Procedimento legal. 5. Eficiência e garantismo. I. Almeida, José Raul Gavião de, orient. II. Título.

Nome: REBELLATO, Luiz Fernando Bugiga.

Título: A análise constitucional do sigilo e da privacidade nas investigações criminais: o acesso a dados armazenados em aparelhos celulares

Dissertação de Mestrado, apresentada à Banca Examinadora do Programa de Pós-Graduação em Direito, da Faculdade de Direito da Universidade de São Paulo, como exigência parcial para obtenção do título de Mestre em Direito, na área de concentração de Direito Processual, sob a orientação do Professor Dr. José Raul Gavião de Almeida.

Aprovado em

Banca Examinadora

Professor Doutor José Raul Gavião de Almeida – Orientador e Presidente
Faculdade de Direito da Universidade de São Paulo

1º examinador (a)

2º examinador (a)

3º examinador (a)

Agradecimentos

Primeiramente, agradeço a Deus por me acompanhar em cada desafio e a quem sempre recorro nos momentos de tribulação.

Ao Professor Doutor José Raul Gavião de Almeida, que me abriu as portas da prestigiosa Faculdade de Direito da Universidade de São Paulo e me concedeu a honra de tê-lo como orientador, demonstrando sempre, desde as primeiras aulas, uma inteligência invulgar, conhecimento ímpar e vasta experiência acadêmica e profissional.

A minha noiva Marianna, que sempre me demonstrou seu amor ao compartilhar dos meus sonhos e se alegrar com minhas conquistas. Ao longo deste período, mesmo separados fisicamente por duas jornadas durante seu aprimoramento acadêmico e profissional em Chicago e Tóquio, sempre tive a certeza de que a distância apenas serviu para reafirmar nosso compromisso de trilharmos, juntos, os caminhos desta vida. Inclusive, foi graças aos seus estudos em Chicago que tive a oportunidade de, por ao menos três vezes, fazer uso da biblioteca da Universidade de Chicago para complementar meus estudos.

Aos meus pais, José Angelo e Josiane, e a minha irmã, Isabella, verdadeiros exemplos de amor incondicional, ética, honestidade e caráter, sendo compreensivos quando, por vezes, deixei de compartilhar de momentos alegres e de união familiar para me desincumbir desta engrandecedora oportunidade acadêmica.

Ao amigo e colega Professor Doutor Fábio Ramazzini Bechara, que testemunhou os meus primeiros passos profissionais, estando presente no meu exame oral para o ingresso na carreira do Ministério Público, na minha banca de qualificação deste mestrado, além de ter me auxiliado quando, por circunstâncias do destino, assumi a titularidade da Promotoria de Justiça de Novo Horizonte, sua cidade natal. Seu exemplo de compromisso com o conhecimento e o estímulo para meu aperfeiçoamento profissional e acadêmico moveram-me para a conclusão de mais esta etapa.

RESUMO

REBELLATO, Luiz Fernando Bugiga. **A análise constitucional do sigilo e da privacidade nas investigações criminais: o acesso a dados armazenados em aparelhos celulares**. 2020. 305 f. Dissertação (Mestrado) – Faculdade de Direito, Universidade de São Paulo, 2020.

A revolução digital alterou significativamente as relações sociais e permitiram a ressignificação de conceitos clássicos, tais como a noção de privacidade. Nesta dinâmica, a criminalidade igualmente usufruiu destes novos recursos tecnológicos para o cometimento de crimes, o que exigiu a adoção de novos mecanismos de investigação criminal, dentre eles o acesso ao conteúdo de dados armazenados em aparelhos celulares, especialmente considerando que mecanismos de criptografia tornaram obsoletos os meios tradicionais de investigação disponíveis no ordenamento jurídico brasileiro. Em contrapartida, não houve evolução legislativa condizente com esta realidade digital, exigindo a busca de um ponto de equilíbrio na relação entre os direitos fundamentais à segurança e à liberdade, prestigiando-se a eficiência das atividades investigativas e, ao mesmo tempo, a proteção à privacidade e ao sigilo de dados, enquanto direitos fundamentais autônomos da personalidade. Neste contexto, amparados pelas referências a outros meios de obtenção de prova e mediante pesquisa nacional e internacional sobre o tema, buscou-se discorrer sobre os requisitos legais e procedimentais para o regular acesso ao conteúdo de *smartphones*, de maneira remota ou através de apreensão física do aparelho, tanto em um cenário de consentimento e voluntariedade do titular, quanto nas hipóteses em que, não havendo colaboração do acusado ou em razão da necessidade investigativa, a medida se revele imprescindível. Nestes casos, considerando a indefinição das Cortes quanto à necessidade de autorização judicial para o acesso aos dados em situações fáticas distintas, especialmente durante abordagens policiais em situação de flagrante delito, pretendeu-se adotar um modelo procedimental desde o acesso até a extração dos dados, o que motivou uma análise da cadeia de custódia da prova digital, atentando-se para suas particularidades, a fim de se preservar sua autenticidade e integridade da prova. Finalmente, avançou-se para o estudo das consequências jurídicas processuais em caso de descumprimento do referido modelo procedimental.

Palavras-chave: Acesso a dados armazenados em aparelhos celulares – Formas de acesso – Indispensabilidade de autorização judicial – Procedimento legal – Eficiência e garantismo

ABSTRACT

REBELLATO, Luiz Fernando Bugiga. **The constitutional analysis of secrecy and privacy in criminal investigations: access to data stored on cell phones.** 2020, 305 f. Dissertation (Master) - Law School, University of São Paulo, 2020.

The digital revolution has significantly altered social relations and allowed the re-signification of classic concepts, such as the concept of privacy. Within this dynamic, criminality also took advantage of these new technological resources to commit crimes, which required the adoption of new mechanisms for criminal investigation, including access to the data content stored on cell phones, especially considering that encryption mechanisms have made the traditional means of investigation, as available in the Brazilian legal system, obsolete. On the other hand, there was no legislative evolution in line with this digital reality, which led to the need to find a balance in the relationship between the fundamental rights to security and freedom, giving prestige to the efficiency of investigative activities and, at the same time, the protection of privacy and data confidentiality, as autonomous fundamental rights of the personality. In this context, supported by references to other means of obtaining evidence and through national and international research on the topic, we sought to discuss the legal and procedural requirements for regular access to smartphone's content, remotely or through physical apprehension of the device, both in a scenario of consent and voluntariness of the holder and also in the cases in which, in the absence of collaboration by the accused or due to the investigative need, the apprehension proves to be essential to the investigation. In these cases, considering Brazilian Courts lack of definition as to the need for judicial authorization for access to data in different factual situations, especially during police approaches in situations when an individual is caught committing the criminal act, the intention was to adopt a procedural model from access to data extraction, which motivated an analysis of the chain of custody of the digital proof, paying attention to its particularities, in order to preserve the authenticity and integrity of the criminal evidence. Finally, we proceeded to the study of the legal consequences for non-compliance of said procedural model.

Keywords: Access to data stored on mobile devices - Forms of access - Need for judicial authorization - Legal procedure - Efficiency and guarantee

SUMÁRIO

INTRODUÇÃO

O presente trabalho acadêmico tem, por objetivo, a análise da proteção constitucional ao sigilo e o acesso a dados armazenados em aparelhos celulares, dentro de uma perspectiva de equilíbrio na relação entre eficiência e garantismo[1].

A revolução digital e o avanço tecnológico permitiram que os telefones celulares, originariamente criados para servirem como mero instrumento de comunicação entre os cidadãos através da propagação de ondas eletromagnéticas de transmissão bidirecional de voz, evoluíssem a ponto de se transformar em dispositivos multifuncionais, reunindo-se em um mesmo recurso tecnológico ampla e diversificada gama de funcionalidades a serviço do usuário, tais como a de computador, câmera, loja de aplicativos variados, processador de texto, *e-mail*, comunicação digital instantânea por aplicativos (*v.g., WhatsApp*, etc.), geolocalização, acesso à *internet*, dentre outras.

Infere-se que uma plêiade de dados[2], intimamente relacionados à privacidade e intimidade das pessoas, foram alocados em um mesmo dispositivo, cujo acesso permitiria descortinar a vida íntima e particular de uma pessoa, expondo-a de maneira sensível.

É certo que esta mesma evolução tecnológica permitiu que a criminalidade moderna se valesse do telefone celular como instrumento para projetar as

---

[1] A análise percuciente do tema posto em discussão permitirá que se encontre uma solução equilibrada desta equação, bem sintetizada pelo Professor das Arcadas Antonio Scarance Fernandes: "(...) não é tarefa fácil realizar a justa ponderação entre o interesse público na realização da quebra para a consecução de prova e o interesse privado de quem é submetido à investigação ou ao processo criminal. Encontram-se normalmente vozes extremadas. De um lado, a dos que sustentam ardorosamente a necessidade de ampla permissividade no acesso aos sigilos pessoais para coibir a prática criminosa, e, de outro, a daquele que, em defesa da privacidade, apregoam a necessidade de serem os indivíduos intensamente protegidos contra as invasões em suas esferas íntimas e particulares, só sendo permitidas em casos extremos. Necessário, contudo, buscar o ponto de equilíbrio, de modo que se garanta a eficiência do sistema persecutório, mas, ao mesmo tempo, se preservem os direitos da pessoa investigada ou acusada (...)". (FERNANDES, Antonio Scarance. *O sigilo financeiro e a prova criminal.* In "Direito Penal, Processo Penal e Direitos Fundamentais. Uma visão Luso-brasileira", p.457/477, 2006, Quartier Latin. São Paulo).

[2] Conforme bem definido por Gregório Edoardo Raphael Selingardi, o "(...) dado digital constitui a informação de estrutura numérica e imaterial, processadas por sistemas computacionais, voltada a desempenhar uma função e representada em diversos formatos informativos (textos, imagens, áudio e vídeo) Denomina-se documento eletrônico o agrupamento de dados digitais gerados, transmitidos ou conservados por meio de computador ou rede telemática (...)" (GUARDIA, Gregório Edoardo Raphael Selingardi. Comunicações Eletrônicas e dados digitais no processo penal. Tese (Mestrado em Direito Processo Penal) – Faculdade de Direito, Universidade de São Paulo, 2016, p. 99).

ações delitivas e garantir o sucesso da empreitada infracional, o que revela a importância do acesso aos dados contidos em aparelhos celulares, como importante instrumento de investigação criminal.

Entretanto, as formas de acesso ao conteúdo dos dados armazenados e a necessidade de se buscar um equilibro entre a imprescindibilidade de uma investigação eficiente e o resguardo à proteção da privacidade e intimidade motivaram atuais e importantes discussões, especialmente em âmbito jurisprudencial, sobre a necessidade de autorização judicial para o acesso ao conteúdo e qual o marco legal e regulamentar a ser adotado para se assegurar a legalidade do acesso e preservar a integridade do seu conteúdo.

A guisa de exemplo, em campo jurisprudencial, a 2ª Turma do Supremo Tribunal Federal (STF), no julgamento do *Habeas Corpus* n.º 91.867/PA[3], decidiu que a análise do histórico de chamadas de um celular apreendido, após a prisão em flagrante, não violaria o sigilo das comunicações, previsto no artigo 5º, inciso XII, da Constituição Federal, sinalizando que, em situações de flagrante delito, o acesso ao conteúdo dos dados armazenados nos aparelhos celulares poderia ser feito sem a necessidade de uma ordem judicial autorizativa.

O Superior Tribunal de Justiça (STJ), em posicionamento distinto, registrou a imprescindibilidade da ordem judicial para acesso aos dados armazenados nos telefones celulares, conforme se verifica do *Recurso em Habeas Corpus* n.º 51.531/RO[4], que se tornou referência para o posicionamento atual daquela Corte[5].

O assunto ainda permanece sob discussão no Supremo Tribunal Federal (STF), em âmbito de Repercussão Geral no Recurso Extraordinário com Agravo n.º 1.042.075/RJ[6], cujo julgado já foi iniciado e, dos votos até então apresentados, infere-se a inexistência de unanimidade no posicionamento dos julgadores.

---

[3] STF, HC n.º 91.867/PA, 2ª Turma, Rel. Min. Gilmar Mendes, j. 24/04/2012, DJe 19/09/2012.

[4] "STJ, RHC n.º 51.531/RO, 6ª Turma, Rel. Nefi Cordeiro, julgado em 19 de abril de 2016, DJe 09/05/2016,

[5] Como exemplo, o Superior Tribunal de Justiça (STJ) tem mantido o posicionamento acerca da imprescindibilidade da ordem judicial para acesso aos dados, em decisão de suas duas turmas julgadoras em matéria criminal (STJ, RHC n.º 77.232/SC, 5ª Turma, Rel. Min. Felix Fischer, DJe 16/10/2017; STJ, HC n.º 372.762/MG, 5ª Turma, Rel. Ministro Felix Fischer, julgado em 3 de outubro de 2017, DJe 16/10/2017)

[6] STF, ARE n.º 1.042.075/RJ, Tribunal Pleno – Meio Eletrônico, Rel. Min. Dias Toffoli, julgado em 23/11/2017.

Portanto, a pesquisa pretende analisar quais as formas de acesso aos dados armazenados em aparelhos celulares, bem como se há necessidade de ordem judicial autorizativa para acesso aos dados armazenados em aparelhos celulares. Ainda, pretende-se identificar quais as balizas formais e procedimentais para que, da apreensão do aparelho celular até a extração dos dados, sejam resguardadas as garantias do processo justo e, ao mesmo tempo, assegure-se a eficiência da atividade investigativa.

Para tanto, a pesquisa estará dividida em 7 (sete) partes.

Na primeira parte, dentro da seara hermenêutica-constitucional, serão fixadas premissas conceituais e técnicas atinentes à privacidade, intimidade e vida privada (artigo 5º, inciso X, da Constituição Federal), bem como do sigilo de dados (artigo 5º, inciso XII, da Carta Política), além de se estabelecer uma análise histórica e evolutiva do conceito de "privacidade" e sua ressignificação, especialmente diante do advento de novas tecnologias, a exemplo dos modernos aparelhos celulares (*smartphones*).

Na segunda parte, o trabalho buscará realizar um sobrevoo sobre conceitos relacionados à prova digital, sua produção, bem como se discorrerá sobre os meio de obtenção e produção de provas atípicos e a necessidade do uso da analogia, de forma a se conferir um marco procedimental para o acesso a dados armazenados em aparelhos celulares.

Na terceira parte, será objeto de atenção as formas de acesso ao conteúdo do aparelho, mediante voluntário consentimento do acusado. Assim, serão estabelecidos os requisitos de validade para o consentimento, sem se olvidar de discussões bastante sensíveis relacionadas à possibilidade do consentimento do acusado preso e a (in)dispensabilidade do advogado como requisito de validade do ato. Neste mesmo capítulo, serão discutidas as formas de manifestação do consentimento e as hipóteses de cessão voluntária dos dados por terceiros.

Na quarta etapa, serão analisadas as formas de acesso aos dados armazenados quando não houver consentimento do titular, o que exigirá a adoção de medidas invasivas. Neste capítulo, dar-se-á destaque para as hipóteses de acesso remoto ao aparelho celular, com a adoção de medidas para busca, apreensão e interceptação dos dados sem a necessidade de apreensão do suporte eletrônico. Ainda, será analisada a possibilidade da

utilização de *malwares* como meios de investigação, além de outras ações encobertas em meio digital.

Na quinta etapa, novamente serão estudadas as formas de acesso não voluntário aos dados armazenados, mas desta vez mediante apreensão física do aparelho celular. Assim, o estudo se debruçará sobre os requisitos para a busca e apreensão dos dados digitais armazenados, bem como sobre a necessidade de ordem judicial para o acesso e a observância aos mandamentos da proporcionalidade, especialmente a partir do estudo das cláusulas constitucionais e legais de reserva de jurisdição.

A análise será estendida para o plano concreto, a partir de contextos fáticos distintos e da necessidade em se observar o princípio da inafastabilidade da jurisdição em cada situação apresentada: dentro de uma abordagem policial motivada por fundada suspeita, sem a caracterização do flagrante delito, bem como da busca de maneira incidental à prisão em flagrante delito. Finalmente, serão estabelecidas as consequências processuais relacionadas à inobservância formal e procedimental no acesso aos dados contidos nos telefones celulares, além das exceções relacionadas às teorias da fonte independente e da descoberta inevitável.

Na sexta parte, o trabalho avançará sob o prisma do direito comparado, buscando a formação de um modelo normativo processual a partir da experiência obtida com as iniciativas legislativas e jurisprudenciais de outros países.

Finalmente, na sétima e derradeira etapa, será objeto de estudo a cadeia de custódia da prova extraída a partir dos dados armazenados em aparelhos celulares, discorrendo-se sobre as etapas a serem percorridas e as consequências jurídicas para a violação da cadeia de custódia.

Desta forma, justificada a relevância e atualidade do tema, almeja-se contribuir na sistematização dos aspectos formais e procedimentais a serem adotados para acesso aos dados contidos em telefones celulares, como forma de se assegurar a eficiência investigativa e, ao mesmo tempo, prestigiar-se as garantias da privacidade e intimidade contempladas no texto constitucional.

1) PRIVACIDADE E SUA EVOLUÇÃO INTERPRETATIVA: A RELAÇÃO ENTRE EFICIÊNCIA E GARANTISMO

A Constituição Federal de 1988, cunhada após um longo período de ruptura institucional no país, redefiniu as bases democráticas e republicanas da nação e sedimentou valores que se cristalizaram ao longo da evolução social.

Ao mesmo tempo, ao inaugurar uma nova ordem jurídica no país e ao estabelecer um rol não taxativo de garantias processuais[7], a Constituição Federal passou a servir como filtro de validade e legitimidade dos demais diplomas infraconstitucionais existentes.

Assim, faz parte do núcleo das cláusulas pétreas constitucionais regras e princípios aplicáveis ao processo penal, notadamente a obrigação de se respeitar um devido processo legal para que a pessoa se veja privada de sua liberdade (artigo 5º, inciso LIV), a inadmissibilidade de provas produzidas por meios ilícitos (artigo 5º, inciso LVI), regras específicas sobre a prisão e identificação do responsável pelo ato constritivo (artigo 5º, incisos LXI e seguintes), bem como, especialmente na temática do presente trabalho, a inviolabilidade da intimidade, vida privada, imagem e honra das pessoas, do domicílio, bem como o sigilo da correspondência, comunicações telegráficas, dados e comunicações telefônicas, salvo para fins de investigação ou instrução criminal (artigo 5º, incisos X, XI e XII).

Portanto, ao estabelecer uma plêiade de direitos e garantias, a Constituição Republicana demandou que os demais diplomas infraconstitucionais, devotassem a ela integral submissão, inadmitindo-se que um processo penal que não se assentasse sobre bases democráticas e que observasse os valores e princípios insculpidos no texto constitucional,

---

[7] "(...) A conscientização sobre a importância das 'garantias processuais', como expressão desses valores fundamentais de civilidade que devem informar as atividades de aplicação jurisdicional de direito, representa talvez o traço mais saliente da cultura processual contemporânea, chegando-se mesmo a afirmar a fecunda e expressiva ideia de um 'jusnaturalismo processual'. Não se trata, porém, de simples orientação filosófica, visto que essa conscientização tem sido acompanhada pela progressiva 'positivação' e, mais precisamente, pela 'constitucionalização' do direito ao processo, com a correspondente explicitação, cada vez mais completa e analítica, das garantias do processo nos textos constitucionais (...)" (GOMES FILHO, Antônio Magalhães. *A Motivação das Decisões Penais*, 1ª edição, São Paulo: Editora Revista dos Tribunais, 2001, p. 31)

especialmente se considerarmos que a estrutura processual penal de uma nação constitui o verdadeiro termômetro dos elementos corporativos ou autoritários de sua Constituição[8].

De início, prima-se por se buscar uma delimitação conceitual sobre temas que serão tratados ao longo de todo o trabalho científico e que servirão de base estrutural para se responder as inquietações lançadas na parte introdutória.

1.1. Privacidade: evolução histórica

As primeiras noções relacionadas a um conceito de direito à privacidade foram desenhadas na célebre obra *"The right to privacy"*[9], de Samuel Dennis Warren e Louis Dembitz Brandeis, bem como no trabalho *"A Treatise on the Law of the Torts"*[10], em que o juiz Thomas Cooley utilizou a expressão *"right to be alone",* já em 1880.

Originariamente, a *"privacy"* assumiu uma concepção individualista, vinculada ao isolamento e à tranquilidade, garantindo-se a possibilidade de o indivíduo ser deixado só. Warren e Brandeis conciliaram as noções de privacidade (*"privacy"*) como sendo um direito ("*right"*) reconhecido dentro do panorama jurídico-normativo da *common law*[11], desenvolvendo a temática a partir de uma necessidade de proteção à integridade psicológica dos indivíduos, através do exercício do controle de informação que reflitam e, por vezes, afetem suas personalidades[12].

---

[8] GOLDSCHMIDT, James. *Problemas Jurídicos y Políticos del Proceso Penal*. Barcelona: Editora Bosch, 1935, p. 67. Citando H. Henkel, Jorge Figueiredo Dias relembra que o processo penal é o "verdadeiro direito constitucional aplicado" (FIGUEIREDO DIAS, Jorge. *Direito processual penal.* Coimbra: Editora Coimbra, 2004, p. 74). Ainda, Claus Roxin sustenta que o processo penal é o "sismógrafo da Constituição do Estado" (ROXIN, Claus. *Derecho Procesal Penal.* Buenos Aires: Editores del Puerto, 2003, p.10). Na mesma linha, Julio Maier aponta que o processo é o próprio "*Derecho constitucional reglamentado*" (MAIER, Julio B. J. *Derecho Procesal Penal.Tomo I: Fundamentos*. 3ª edição, Buenos Aires: Editores del Puerto, 2004, p. 162/163).

[9] WARREN, Samuel Dennis. BRANDEIS, Louis Dembitz. *The Right to Privacy*, Harvard Law Review, Vol. IV, n.º 5, 1890.

[10] COOLEY, Thomas McIntyre. *A treatise on the law of torts*. Chicago: Callaghan, 1880.

[11] Para uma análise detalhada da perspectiva norte-americana sobre a privacidade e os direitos à personalidade: ZANINI, Leonardo Estevam de Assis. *O surgimento e o desenvolvimento do right of privacy nos Estados Unidos*. Revista Brasileira de Direito Civil. Vol. 3, Jan/Março 2015.

[12] GLANCY, Doroth. *The invention of the right to privacy.* Arizona Law Review, v.21, n.1, p. 2 (1979).

Ainda que, originariamente, a proteção à privacidade guardasse relação com a proteção da integridade psicológica[13] dos indivíduos, que poderia ser violada diante da profusão difusa e indevida de determinadas informações, posteriormente se evoluiu a ponto de se concebê-lo como um direito autônomo e básico de todo e qualquer indivíduo diante das alterações transformações sociais e tecnológica da época[14], que aumentaram a possibilidade de exposição pessoal e, por conseguinte, reafirmaram a necessidade de se proteger o direito ao isolamento[15].

Diante da ausência de um direito formalmente reconhecido à privacidade, os autores recorreram a uma interpretação extensiva de outros direitos e valores consagrados na *First Amendment*[16], *Fourth Amendment*[17] e na *Fifth Amendment*[18], estendendo-se à privacidade as noções protetivas relacionadas à vida, liberdade e propriedade, bem como a proteção ao domicílio.

---

[13] Esta perspectiva psicológica e individual contrasta com as noções de privacidade atuais. Ao estabelecer um rol de direitos e garantias individuais relacionados à privacidade, estabeleceu-se a impossibilidade de sua violação ainda que, psicologicamente, o indivíduo não se veja abalado. Por exemplo, a interceptação ilegal de um telefonema constitui indefensável violação à privacidade, não sendo necessário perquirir se o cidadão, psicologicamente, se sentiu abalado com as informações amealhadas a partir da interceptação irregularmente realizada.

[14] Samuel Warren e Louis Brandeis apontam que *"(...)*The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat rom the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury (…)" (WARREN, Samuel Dennis. BRANDEIS, Louis Dembitz. *The Right to Privacy*, Harvard Law Review, Vol. IV, n.º 5, 1890, p. 196)

[15] Stefano Rodotà aponta que "(…) é de fato o fim da linha de um longo processo evolutivo experimentado pelo conceito de privacidade – de uma definição original como o direito de ser deixado em paz, até o direito de controle sobre as informações de alguém e determinar como a esfera privada deve ser construída" (...)" (RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. MORAES, Maia Celina Bodin de Moraes (org). Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 17).

[16] "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances".

[17] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized"

[18] "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation".

Assim, se a própria Constituição Estadunidense assegura a proteção à propriedade, à vida, à liberdade e ao domicílio, defende-se que, implicitamente, haveria um resguardo não expresso da própria privacidade, que passa a ser reconhecida como direito e valor constitutivo da pessoa humana, diante do desenvolvimento tecnológico e do engrandecimento do risco à violação dos direitos da personalidade do cidadão.

Posteriormente, as noções de *"right to privacy"* foram paulatinamente se desenvolvendo e sendo reconhecidas nas Cortes Norte-Americanas, sendo certo que, no caso *Griswold v. Cosmetitan, 381 U.S. 479 (1965)*[19], a Suprema Corte reconheceu que o direito estaria implicitamente albergado na Constituição Estadunidense.

No direito brasileiro, a proteção à privacidade evoluiu ao longo do tempo, até se cristalizar na proteção individual à intimidade e à honra previstos expressamente no artigo 5º, inciso X, da Carta Cidadã de 1988[20]: "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".

---

[19] Disponível em <https://supreme.justia.com/cases/federal/us/381/479/>. Acesso em: 20 de dezembro de 2020.

[20] De início, observou-se um esboço de proteção aos direitos à personalidade e, especialmente, a proteção à privacidade na Constituição Política do Império (1824), notadamente em seu artigo 179, incisos VII e XXVII , em que se estabeleceu uma proteção ao domicílio e ao sigilo de correspondências.
A proteção à inviolabilidade do domicílio e ao sigilo das correspondências foi mantido na Constituição da República de 1891, em seu artigo 72, parágrafos 11 e 18 , muito embora tenham ocorridas pequenas alterações no texto constitucional: estabeleceu-se a possibilidade de ingresso em domicílio durante a noite, para salvamento de vítimas de crimes ou para auxiliar em caso de desastres, bem como suprimiu-se a expressão "segredo", utilizada para se referir às correspondências na Constituição anterior, mantendo-se, todavia, a inviolabilidade anterior.
A Constituição da República de 1934, por sua vez, manteve a mesma tutela da inviolabilidade do domicílio (artigo 113, 16) e o sigilo das correspondências (artigo 113, 8), inclusive com redação quase idêntica à da Constituição da República de 1891.
Já a Carta Constitucional de 1937, cujo preâmbulo já revelou seu caráter de ruptura à ordem democrática e externou sua inclinação fascista e déspota, também tutelou a inviolabilidade de domicílio e o sigilo das correspondências, especialmente em seu artigo 122, 6º. Diferentemente das previsões contidas nos textos constitucionais precedentes, a Constituição de 1937 se aliou a uma tendência revelada nas Constituições europeias e condicionou a inviolabilidade do domicílio e o sigilo das comunicações às "exceções expressas em lei". Houve, portanto, um rebaixamento de proteção à privacidade, especialmente diante da possibilidade de previsões legais limitarem o pleno exercício de direitos que, sob a égide das Constituições anteriores, eram assegurados de forma plena e irrestrita.
Esta diminuição da esfera protetiva foi corrigida na Constituição Federal de 1946, que novamente retomou a inspiração democrática. Em seu artigo 141, parágrafos 6º e 15º, foi adotada uma redação similar àquela prevista na Constituição de 1934, assegurando-se novamente a inviolabilidade de domicílios e o sigilo de correspondências sem qualquer limitação ou condição infraconstitucional.
A Constituição Federal de 1967, em sua redação original, passou a acrescentar, ao lado da inviolabilidade da correspondência, a proteção ao sigilo das comunicações telegráficas e telefônicas (artigo 150, § 9º), bem como tornou a prever a inviolabilidade de domicílio (artigo 150, § 10º). Com o advento da Emenda Constitucional n.º 1 (1969), as mesmas previsões foram mantidas, porém no artigo 153, §§ 9º e 10º

Como se vê, a Constituição vigente reconheceu e positivou um direito autônomo à privacidade, expressada através dos conceitos de "*intimidade"* e *"vida privada",* bem como estabeleceu uma proteção concreta à honra e à imagem das pessoas, cuja violação seria passível de indenização.

Não bastasse, o resguardo constitucional da privacidade é assegurado sob outras formas, notadamente ao se garantir a inviolabilidade de domicílio (artigo 5º, inciso XI), bem como a proteção ao sigilo da correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas (artigo 5º, inciso XII, da Constituição Federal).

1.2. Privacidade, intimidade, vida privada e sigilo de dados: definições conceituais e históricas

Conforme ressaltado, apenas a partir da Constituição Federal de 1988 a privacidade deixou de assumir um papel meramente coadjuvante, vinculada à inviolabilidade de domicílio e ao sigilo da correspondência, para ser erigida à condição de direito autônomo integrante da personalidade do cidadão.

Mediante o emprego de expressões vagas[21] como "vida privada*"* e *"*intimidade*",* coube à doutrina e à jurisprudência buscar uma interpretação do alcance dos termos e, mais precisamente, sua definição conceitual, especialmente diante de sua ressignificação em razão da época, lugar e a forma em que inseridos[22].

---

[21] José Afonso da Silva, reconhecendo a indefinição conceitual, aponta que *"(...) de fato, a terminologia não é precisa. Por isso, preferimos usar a expressão direito à privacidade, num sentido genérico e amplo, de modo a abarcar todas essas manifestações da esfera íntima, privada e da personalidade, que o texto constitucional em exame consagrou* (...)" (SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. 29. edição, São Paulo: Editora Malheiros, 2007, p. 205).

[22] BASTOS, Celso Ribeiro. *Comentários à Constituição do Brasil: promulgada em 5 de outubro de 1988.* São Paulo: Editora Saraiva, 1988, p. 83. De igual sorte, David Gray aponta que *"(...)* privacy is a content neutral and context dependent. Nothing is inherently private or not private. Places, things, activities, and relationships are only private or not private to the extent that they lie on one side of a guarded boundary. Neither is there a necessary link between privacy and what is sensitive, embarrassing, or even illegal. In fact, much of what we regard as private is perfectly ordinary. Privacy is, instead, about agency, status and relationship *(...)"* (GRAY, David. *The Fourth Amendment in an Age of Surveillance.* Cambridge: Cambridge University Press, 2017, p. 7)

Entretanto, ainda que não haja consenso[23] com relação à definição de cada uma das expressões – especialmente diante da necessidade de interpretá-las a partir do contexto social, econômico e tecnológico em que inseridas –, há espaço para algumas noções conceituais sobre os institutos.

1.2.1. Privacidade

A expressão "privacidade" tem raiz latina, derivando do adjetivo *privatus*, o qual ganha o significado de "privado", "particular", "próprio"[24]. Enquanto direito autônomo, a privacidade está naturalmente relacionada à personalidade humana, como sendo zona de exclusão sob controle social do cidadão, como forma de assegurar sua individualidade e a autonomia privada[25].

A terminologia "privacidade" é objeto de inúmeras discussões quanto à sua definição conceitual, já que seu conceito é confundido com outras expressões relacionadas à tutela dos direitos da personalidade: "vida privada", "intimidade", "segredo", "sigilo", "privatividade", "privaticidade", fato que também ocorre na conceituação de "privacidade" em legislações de outros países[26].

A despeito desta impropriedade terminológica, é certo que ousou-se formular uma definição conceitual para "*privacidade",* tendo JOSÉ AFONSO DA SILVA a definido como "(...) o conjunto de informações acerca do indivíduo, que ele pode decidir

---

[23] LEONARDI, Marcel. *Tutela e Privacidade na Internet*. São Paulo: Editora Saraiva, 2012, p. 46.

[24] SAMPAIO, José Adércio Leite. *Direito à intimidade e à vida privada*. Belo Horizonte: Editora Del Rey, 1998. p. 268.

[25] Para Marcel Leonardi, a privacidade pode ser resumida em quatro perspectivas: a) o direito de ser deixado só; b) o resguardo contra interferências alheias; c) o segredo ou sigilo; d) o controle sobre informações e dados pessoais (LEONARDI, Marcel. *Tutela e Privacidade na Internet*. São Paulo: Editora Saraiva, 2012, p. 79). Esta última, propriamente, interessa ao presente trabalho científico.

[26] Conforme bem exposto por Danilo Doneda, "*(...)* a privacy norte-americana, o droit au secret de la vie privée ou simplesmente la protection de la vie privée na França; o diritto alla risevatezza (ou a segretezza) na Itália (ou mesmo a privacy, termo usado no país); a reserva da intimidade da vida privada (Portugal); o Derecho a la intimidad na Espanha; a noção da Die Privatsphäre, que divide a autonomia individual e a vida social, presente na doutrina da Alemanha; a integritet da Suécia, que compreende a noção pela qual as pessoas têm direito de serem julgadas de acordo com um perfil completo e fiel de sua personalidade; são algumas das designações utilizadas para se referir ao complexo de interesses que remetem ao termo privacidade (...)" (DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2ª ed. São Paulo: Editora RT, 2019, p. 98).

manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito (...)[27]".

Denota-se que a privacidade está relacionada à particular escolha do titular do direito, sobre o que será ou não submetido à exposição pública ou para um rol restrito de outras pessoas. Não se trata de uma obrigação estabelecida a cada cidadão, mas apenas uma alternativa a ele franqueada de, querendo, ter para si assegurado um campo de resguardo de informações que, por qualquer razão, não devam ser compartilhadas com terceiros.

Em verdade, a privacidade assume a característica de permitir controlar a informação referente a si mesmo, que poderá ser ou não compartilhada com outros, bem como a possibilidade de limitar a forma e a finalidade de uso desta informação.

Muito embora DAVID GRAY aponte que "(...) privacy is a complicated concept, and therefore resist reduction to a concise definition. Most accounts of privacy are tied to the ability to maintain boundaries and to limit access to the self (…)"[28], é certo que sua existência está relacionada à necessidade de se assegurar uma certa autonomia individual às pessoas para que desenvolvam sua criatividade e inovação, permitindo-se que floresça a liberdade intelectual, a liberdade de pensamento e de expressão[29], além de

---

[27] SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. 29. edição, São Paulo: Editora Malheiros, 2007, p. 206. Para Tércio Sampaio Ferraz Júnior, a *"(...)* privacidade, como direito, tem por conteúdo a faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é, das situações vitais que, por dizerem a ele só respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão *(...)",* apontando ainda que o objeto da privacidade seria a integridade moral do sujeito, sendo ainda a proteção inerente ao desenvolvimento da própria cidadania (FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado*. Revista da Faculdade de Direito, Universidade de São Paulo, São Paulo, v. 88, p. 440, jan. 1993. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67231/69841>. Acesso em: 20 de dezembro de 2020).

[28] Em tradução livre: "A privacidade é um conceito complicado e, portanto, resiste a uma concisa definição. A maioria dos relatos sobre privacidade estão vinculados à habilidade de se manterem fronteiras e limitar o acesso às pessoas" (GRAY, David. *The Fourth Amendment in an Age of Surveillance.* Cambridge: Cambridge University Press, 2017, p. 6). Igualmente, para RIGAUX, *"*La juridiction constitutionnelle a déduit du droit de la personnalité l'un de ses attributs, à savoir: « le pouvoir reconnu à l'individu et résultant de la notion d'auto-détermination, de décider en premier lieu lui-même quand et dans quelle mesure des faits relatifs à sa propre existence sont divulgués (…) Cet attribut du droit de la personnalité est appelé « droit à la maîtrise des données personnelles » (…) Il n'est toutefois pas sans limite. (…)" (RIGAUX, François. *La protection de la vie privée et des autres biens de la personnalité*. Bruylant: Bruxelles, 1990, p. 588-589, n.º 532).

[29] RICHARDS, Neil M. *The Dangers of Surveillance,* 126 Harvard Law Review, 2013, p. 1935.

assegurar que, por meio da exposição de ideias, se fomente a participação individual do cidadão no processo político-democrático de uma nação[30].

A proteção à privacidade[31], muito embora não tenha sido adotada explicitamente em algumas Constituições Federais, encontra previsão em diversos diplomas internacionais[32].

A partir do reconhecimento da privacidade como um direito inerente à própria personalidade, permitiu-se o desenvolvimento evolutivo no tratamento da tutela a dados pessoais, tais como se observa na: *a)* Convenção n.º 108/1981 do Conselho da Europa, para proteção de pessoas a respeito do tratamento automatizado de dados pessoais; e *b)* Diretivas n.º 95/46/CE e 2002/58/CE, ambas do Parlamento Europeu e do Conselho Europeu, relacionadas respectivamente à proteção das pessoas singulares no tratamento de dados pessoais e da livre circulação destes dados, bem como a proteção à privacidade no setor das comunicações eletrônicas; c) a Decisão-Quadro 2008/977/JAI, do Conselho da União Europeia, que regulamentou a proteção de dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal, posteriormente revogada e substituída pelo Regulamento Geral de Proteção de Dados na União Europeia (*General Data Protection Regulation*), conforme Diretiva (UE) 2016/680.

De igual sorte, a Carta dos Direitos Fundamentais da União Europeia, de 7 de dezembro de 2000, reconheceu em seu artigo 8º[33] a proteção dos dados de caráter

---

[30] A Corte Europeia de Direitos Humanos, no caso *"Amman v. Switzerland"* em 16 de fevereiro de 2000, definiu que a expressão "*(...)* "private life" must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings (…)" (Disponível em <https://www.legal-tools.org/doc/6e49ed/pdf/>, § 65º, Acesso em: 20 de dezembro de 2020).

[31] A privacidade, nesta perspectiva, será considerada em sua acepção interpretativa global, incluindo-se a vida privada e a intimidade, já que os ordenamentos jurídicos internacionais, via de regra, não seguiram a mesma divisão estabelecida na Constituição Federal de 1988.

[32] Com efeito, a Declaração Universal de Direitos Humanos de 1948 estabeleceu, em seu artigo 12, que "Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques a sua honra e reputação. Todo o homem tem direito à proteção da lei contra tais interferências ou ataques". De igual sorte, a privacidade foi objeto de expresso reconhecimento no artigo 8º da Convenção Europeia dos Direitos do Homem de 1950 , assim como no artigo 17 do Pacto Internacional de Direitos Civis e Político de 1966 , no artigo 11, n. 2, do Pacto de São José da Costa Rica de 1969 e no artigo 16, n. 1, da Convenção sobre os Direitos da Criança de 1990 .

[33] Artigo 8.º Proteção de dados pessoais
1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente

pessoal, bem como o Comitê de Direitos Humanos da Organização das Nações Unidas, em sua Recomendação n.º 16, disciplinou que os Estados deverão assegurar, sinteticamente, que informações a respeito da vida privada não estejam ao alcance de pessoas que não são autorizadas para recebê-las, processá-las ou utilizá-las.

Tanto em uma perspectiva internacional quanto convencional sobre a proteção à privacidade, sua tutela se dá sob o *nomen* de "vida privada", expressão que também foi contemplada no texto constitucional brasileiro, ao lado de "intimidade". Desta feita, tem-se apontado que a privacidade seria o gênero, dos quais a "intimidade" e a "vida privada" seriam espécies[34].

Ainda no que tange à privacidade, merece destaque a menção expressa pela Lei Geral de Proteção de Dados (artigo 2º, inciso II, da Lei n.º 13.709/2018) ao conceito de "autodeterminação informativa"[35], erigindo à condição de "fundamento" do referido diploma normativo.

Trata-se de noção extraída a partir da garantia da inviolabilidade do sigilo de dados, da intimidade e da vida privada (artigo 5º, incisos X e XII, da CF) e do princípio da dignidade da pessoa humana (artigo 1º, inciso III, da CF), sendo reconhecido como direito fundamento autônomo[36] conferido a cada cidadão de ter, sob seu controle, as

---

[34] CUNHA JÚNIOR, Dirley da. *Curso de Direito Constitucional*. 5ª edição, Salvador: Editora Juspodivm, 2011, p. 700. Luis Roberto Barroso identifica que "(...) a intimidade e a vida privada estariam representadas em esferas distintas, compreendidas no conceito mais amplo de direito de privacidade (...)" (BARROSO, Luís Roberto. *Temas de direito constitucional – tomo III*. Rio de Janeiro: Renovar, 2005. p. 96)

[35] As primeiras noções de "autodeterminação informativa" foram trazidas a partir do célebre julgamento, pelo Tribunal Constitucional Alemão, do caso BVerfGE 65, 1, "Recenseamento" (Volkszählung), versando sobre a Lei do Censo Alemã de 1983. Na ocasião, a Corte alemã reconheceu reconhecida a capacidade do indivíduo de autodeterminar seus dados pessoais enquanto parcela fundamental do direito de desenvolver sua privacidade, embora tenha destacado que o direito à autodeterminação informativa não é absoluto (MARTINS, Leonardo (org.) *Cinquenta anos de Jurisprudência do Tribunal Constitucional Federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005, p. 233-234). Sobre o tema, recomenda-se também: DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2ª ed. São Paulo: Editora RT, 2019, p. 165-172.

[36] Para Laura Mendes, o "(...) reconhecimento desse direito fundamental não é apenas uma possibilidade; trata-se de uma necessidade para tornar efetivos os fundamentos e princípios do Estado democrático de direito, na sociedade contemporânea da informação, conforme determina a Constituição Federal (...)" (MENDES, Laura Schertel Ferreira. *Habeas data e autodeterminação informativa: os dois lados da mesma moeda*. Direitos Fundamentais & Justiça, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018. p. 202).

A "autodeterminação informativa" foi expressamente reconhecida pelo Supremo Tribunal Federal (STF) como direito autônomo fundamental, tendo sido considerada como um dos fundamentos utilizados pela Corte ao suspender a eficácia de uma Medida Provisória que versava sobre o compartilhamento de dados por empresas de telecomunicação, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública decorrente da pandemia da COVID-19 (STF, ADI-MC Ref n.º 6.387-DF, Relatoria Min. Rosa Weber, julgado em 7 de maio de 2020, DJe 12/11/2020)

próprias informações; de determinar sobre a exibição e o uso de seus dados pessoais, delimitando-se o alcance do seu direito à privacidade; bem como de ter conhecimento sobre quem sabe e o que sabe sobre si, quando e em que ocasião.

1.2.2. Vida privada e intimidade

É certo que não há consenso doutrinário no tocante ao conceito e alcance das expressões "intimidade" e "vida privada"[37].

A "vida privada" tem sido interpretada como uma esfera de proteção que recai sobre as relações pessoais e profissionais que o indivíduo pretenda manter alheio ao conhecimento público. Trata-se de uma expressão que comporta um número elástico de situações jurídicas, abrangendo tanto as relações mais restritas (*v.g.*, as relações familiares e entre pessoas mais próximas) quanto as mais amplas, que importem em um grau natural de sociabilidade, mas que todos convencionem mantê-las afastadas do conhecimento público (*v.g.*, uma frequência a determinadas entidades religiosas ou clubes privados)[38].

---

[37] Manoel Gonçalves Ferreira Filho, por exemplo, não identifica diferença entre as expressões "vida privada" e "intimidade" (FERREIRA FILHO, Manoel Gonçalves. *Comentários à Constituição Brasileira de 1988.* São Paulo: Editora Saraiva, 1990, v. 1, p. 35). Já para Paulo José da Costa Júnior, em célebre obra sobre o tema: "em correspondência com a sua natural divisão em ser individual e ser social, o homem vive como personalidade em esferas diferentes: numa esfera individual e numa esfera privada. Assim, o homem como pessoa, procura satisfazer dois interesses fundamentais: como indivíduo, o interesse a uma livre existência; como coparticipe do consórcio humano, o interesse a um livre desenvolvimento na vida de relação. Enquanto os direitos que se destinam à proteção da 'esfera individual' servem para a preservação da personalidade dentro da vida pública, na proteção da 'esfera privada' cogita-se da inviolabilidade da personalidade dentro de seu retiro, necessário a ser desenvolvimento e evolução, em seu mundo particular, à margem da vida exterior (...) Contrapõe-se à esfera individual a esfera particular ou privada. Aqui, não se trata mais do cidadão do mundo, relacionado com os semelhantes, como na esfera individual. Trata-se, pelo contrário do cidadão na intimidade ou na sua reserva, no isolamento moral, convivendo com a própria individualidade (...)" (COSTA JÚNIOR, Paulo José da. *O direito de estar só: tutela penal da intimidade.* 2ª edição, São Paulo: Editora RT, 1995, p. 24-25). Na mesma linha, reconhecendo o conceito plurívoco da expressão "intimidade": MARÍN, Fernando Rodríguez. *Los delitos de escuchas ilegales y el derecho a la intimidad. Anuario de Derecho Penal y Ciencias Penales*, Madrid, t. XLIII, Fasc/Mes 1, 1990, págs. 197-240.

[38] Tércio Sampaio Ferraz Júnior reconhece que, "(...) no que diz respeito à 'vida privada', trata-se da informação de dados referentes às opções de convivência, como a escolha de amigos, a frequência a lugares, os relacionamentos civis e comerciais, ou seja, de dados que, embora digam respeito aos outros, não afetam (ainda que, no interior da própria convivência, possam vir a afetar) direitos de terceiros (exclusividade da convivência). Pelo sentido inexoravelmente comunicacional da convivência, a vida privada compõe, porém, um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos – como nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial, etc. -, condicionam o próprio intercâmbio humano em sociedade, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura (...)" (FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo bancário, a Constituição Federal e a Lei Complementar n. 105/2001, de dados: o direito à privacidade e os limites à função fiscalizadora do Estado*. In: Direito Constitucional: liberdade de fumar, privacidade, estado, direitos humanos e outros temas. Sampaio Ferraz Junior, Barueri: Editora Manole, 2007, p. 174-175).

Portanto, o conceito abrangeria sempre uma relação intersubjetiva, de diferentes graus de abrangência ou restrição[39], admitindo um conceito de proteção mais amplo do que a própria "intimidade".

A "intimidade", por sua vez, tem sido definida dentro de uma acepção mais exclusiva[40], relacionada ao direito de estar só e privar do conhecimento de terceiros, ainda que próximos, informações que deseja manter forma recôndita[41]. Neste contexto, a proteção à intimidade teria relação com a própria noção do direito de estar só ("right to be alone" ou "right of privacy"[42]).

Vale dizer, a "intimidade" estaria relacionada aos segredos mais íntimos do indivíduo, abrangendo seus pensamentos, desejos, convicções[43] e, por

---

[39] CUNHA JÚNIOR, Dirley da. *Curso de Direito Constitucional.* 5ª edição, Salvador: Juspodivm, 2011, p. 702.

[40] Para Tércio Sampaio Ferraz Júnior, no âmbito da privacidade, a "(...) intimidade é o mais exclusivo dos seus direitos (...) É o âmbito exclusivo que alguém reserva para si, sem nenhuma repercussão social, nem mesmo ao alcance de sua vida privada que, por mais isolada que seja, é sempre um viver entre os outros (na família, no trabalho, no lazer em comum). Não há um conceito absoluto de intimidade, embora se possa dizer que o seu atributo básico é o estar-só, não exclui o segredo e a autonomia. Nestes termos, é possível exemplifica-la: o direito íntimo, o segredo sob juramento, as próprias convicções, as situações indevassáveis de puder pessoal, o segredo íntimo cuja mínima publicidade constrange (...)" (FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado*. Revista da Faculdade de Direito, Universidade de São Paulo, São Paulo, v. 88, p. 439-459, jan. 1993. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67231/69841>. Acesso em: 20 de dezembro de 2020). Ainda, o autor aponta que "(...) trata-se da informação daqueles dados que a pessoa guarda para si e que dão consistência à sua personalidade, dados de foro íntimo, expressões de auto-estima, avaliações personalíssimas com respeito a outros, pudores, enfim, dados que, quando constantes de processos comunicativos, exigem do receptor extrema lealdade e alta confiança, e que, se devassados, desnudariam a personalidade, quebrariam a consistência psíquica, destruindo a integridade moral do sujeito. Seu correlato, em face de um eventual receptor, é o sigilo profissional (CF, art. 5º, XIV). Em termos do princípio da exclusividade, diríamos que ela é, nesses casos, de grau máximo (...)" (FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo bancário, a Constituição Federal e a Lei Complementar n. 105/2001, de dados: o direito à privacidade e os limites à função fiscalizadora do Estado.* Op. cit. p. 174). Para Cleunice Pitombo, "(...) é um valor e cada indivíduo guarda-lhe a medida, no encontro de si mesmo; ainda que imerso no mundo interior do próprio organismo, ou no exterior, ou dos outros. Diverso viés exibe a vida privada, posto que não privilegia a autoconsciência, mas a convivência (...)" (PITOMBO, Cleunice Valentim Bastos. *Da Busca e da Apreensão no Processo Penal*. São Paulo: Editora Revista dos Tribunais, 1999. p. 75).

[41] FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado.* Revista Da Faculdade De Direito, Universidade De São Paulo, 88, p. 439-459. Para Fernando Rodrígues Marin, "(...) el derecho a la intimidad se perfila como el derecho de todos los ciudadanos a mantener una determinada parte de sus vidas fuera del conocimiento inconsentido de los demás (esto es el resto de los particulares y sobre todo, el Gobierno) y, como consecuencia, de ejercer um controlo sobre la información relativa a la misma. Intimidad o privacy es la parte de la vida de las personas donde tiente lugar la toma de decisiones personalísimas y se ponen las bases para la consecución de la autorrealización personal (...)" (MARÍN, Fernando Rodríguez. *Los delitos de escuchas ilegales y el derecho a la intimidad. Anuario de Derecho Penal y Ciencias Penales*, Madrid, t. XLIII, Fasc/Mes 1, 1990, p. 197-240)

[42] WARREN, Samuel e BRANDEIS, Louis. *The right to privacy*. *Harvard Law Review*, n. 5, vol. 4, Dec. 1890.

[43] SILVA, José Afonso da, Curso de Direito Constitucional Positivo, 29ª edição, São Paulo: Editora Malheiros, 2007, p. 206-208.

conseguinte, excluiria[44] as relações intersubjetivas. O objeto da tutela seriam os desejos, valores e segredos inconfessáveis, que não se compartilham com terceiros, sendo ainda um aspecto relacionado à própria essência e à personalidade do indivíduo como, por exemplo, as memórias, confissões, opções sexuais, aspectos da vida conjugal etc.

1.2.3. Sigilo de dados

A expressão "sigilo" é trazida pelo texto constitucional em diversas previsões normativas, à exemplo do artigo 5º, incisos XII, XIV, XXXIII, XXXVIII, dentre outros dispositivos relacionados ao tema.

O sigilo pode ser definido como *"*aquilo que deve ficar acobertado e não deve chegar ao conhecimento ou à vista das pessoas"[45], sendo sinônimo da expressão "segredo". Extrai-se, portanto, que o constituinte buscou projetar a tutela à privacidade também com relação ao sigilo de correspondências e de comunicações telegráficas, de dados e telefônicas.

Especificamente no que toca à presente pesquisa, interessa-nos a análise do sigilo prevista pela Constituição Federal em seu artigo 5º, inciso XII, tutelando quatro formas de liberdades individuais: *a)* comunicação postal ou de correspondência; *b)* comunicação telegráfica; *c)* comunicação de dados; *d)* comunicação telefônica[46].

Entretanto, a controversa redação do dispositivo[47] e a inclusão da expressão "no último caso", utilizada para se referir à possibilidade de, para fins de

---

[44] Alexandre de Moraes sintetiza que "(...) 'intimidade' relaciona-se às relações subjetivas e de trato íntimo da pessoa, suas relações familiares e de amizade, enquanto 'vida privada' envolve todos os demais relacionamentos humanos, inclusive os objetivos, tais como relações comerciais, de trabalho, de estudo, etc (...)" (MORAES, Alexandre de. *Direito Constitucional*. 28ª edição, São Paulo: Editora Atlas, 2012, p. 54).

[45]Definição extraída a partir de pesquisa no dicionário eletrônico *Michaelis* (<https://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=sigilo>. Acesso em: 20 de dezembro de 2020).

[46] BADARÓ, Gustavo Henrique Righi Ivahy. *Processo Penal*, 8ª edição, São Paulo: Editora RT, 2020, p. 594.

[47] Ada Pellegrini Grinover aponta que "(...) foi a Comissão de Redação que, exorbitando de seus poderes, acrescentou ao texto as palavras "comunicações", "no último caso" e "penal", limitando consideravelmente o alcance da norma constitucional legitimamente aprovada em plenário. (...). No meu sentir, a redação restritiva do inciso XII do art. 5º da Constituição é formalmente inconstitucional, por vício de competência e afronta ao processo legislativo. (...) resta saber se o vício teria ficado superado pela promulgação. Tudo indica que não: assim como a sanção não sana o defeito de iniciativa, no tocante às normas infraconstitucionais, do mesmo modo parece-me que a promulgação, em bloco, não teve o condão de convalidar a norma, viciada pela competência e pela violação ao processo legislativo (votação em dois turnos). (...)" (GRINOVER, Ada

investigação criminal ou instrução processual penal, afastar-se o sigilo mediante autorização judicial e nas hipóteses legais, suscitou intensa discussão acadêmica e jurisprudencial sobre o alcance do dispositivo constitucional, surgindo-se ao menos quatro interpretações sobre o tema:

a) a primeira delas sustenta que, ao dispor sobre a expressão "no último caso", o constituinte permitiu apenas o afastamento do sigilo das comunicações telefônicas, impedindo-se qualquer restrição às demais formas de comunicação[48];

b) a segunda interpretação sustenta que a inviolabilidade somente seria aplicável apenas ao sigilo das correspondências, mas não às demais formas de comunicação telegráfica e telefônica, já que a expressão "no último caso" seria limitada a este segundo grupo[49];

c) a terceira interpretação, de forma bastante similar à anterior, considera que o inciso XII deve ser separado em dois grupos, sendo o primeiro composto pelo "o sigilo da correspondência e das comunicações telegráficas" e o segundo compreenderia o sigilo "de dados e das comunicações telefônicas", autorizando-se a quebra do sigilo apenas destes últimos (comunicação de dados e telefônica)[50];

Pellegrini. *"O regime brasileiro das interceptações telefônicas".* Revista de Direito Administrativo, n. 207, p. 21). Para maiores informações sobre a tramitação do projeto e as alterações posteriores na redação, bem como uma análise percuciente e à luz das diversas formas de interpretação sobre a matéria, confira-se: GUARDIA, Gregório Edoardo Raphael Selingardi. *Comunicações Eletrônicas e dados digitais no processo penal*. Tese (Mestrado em Direito Processo Penal) – Faculdade de Direito, Universidade de São Paulo, 2016, p. 75-77.

[48] GRECO FILHO, Vicente. *Interceptação telefônica (considerações sobre a lei nº 9.296 de 24 de julho de 1996)*. São Paulo: Editora Saraiva, 1996, p. 12/13; GRINOVER, Ada Pellegrini. *O regime brasileiro das interceptações telefônicas.* Revista de Direito Administrativo. Rio de Janeiro, 207, jan./mar. 1997, p. 25; PITOMBO, Sérgio Marcos de Moraes. *Sigilo nas comunicações. Aspecto processual penal.* Boletim IBCCrim, São Paulo, n. 49, p. 7-8. dez. 1996, p. 7.

[49] NERY JUNIOR, Nelson; NERY, Rosa Maria de Andrade. *Constituição Federal comentada e legislação constitucional.* 2ª edição, São Paulo: Editora RT, 2009, p. 176.

[50] Para Paulo Rangel, "(...) a expressão "último caso" açambarcaria dados e comunicações telefônicas, pois do contrário, o legislador deveria ter dito: "sigilo das correspondências, das comunicações telegráficas, de dados e das comunicações telefônicas onde a expressão "último caso" teria como ponto de apoio somente a expressão isolada pela disjuntiva 'e' (...)" (RANGEL, Paulo. *Breves considerações sobre a Lei n.º 9.296/1996: interceptação telefônica.* Revista Brasileira de Ciência Criminais, São Paulo, v. 7, n. 26, p.143-151, abr./jun. 1999, p. 143). No mesmo sentido: FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito, Universidade de São Paulo, São Paulo, jan. 1993, v. 88, p. 446. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67231/69841>. Acesso em: 20 de dezembro de 2020. Também foi a interpretação dada pelo Ministro Marco Aurélio Mello, ao interpretar que "(...) vejo o emprego de dois conectivos 'e' a revelar que temos, na verdade, não quatro casos, mas apenas dois: o primeiro, abrangendo a 'correspondência' e as 'comunicações telegráfica'; (...) o segundo a envolver 'dados' e 'comunicações telefônica'. Se estou certo neste enfoque, rechaço a possibilidade de se ter

d) a quarta aponta que a ressalva constitucional abrange todos os tipos de sigilos estabelecidos no dispositivo constitucional, os quais podem ser relativizados diante da falta de outras medidas invasivas[51].

Com relação à expressão "dados", trazida no texto constitucional, uma conceituação ampla e genérica permite concluir que esta abrange todo e qualquer tipo de informação que possa estar direta ou indiretamente relacionada a pessoas, coisas ou situações jurídicas, passíveis de serem veiculados por qualquer meio de comunicação[52].

Em verdade, a palavra "dados" foi inserida na Constituição Federal e, tal como visto, não encontra precedentes nos textos constitucionais anteriores. Sustentou-se que o dispositivo em questão estaria entrelaçado ao segredo das comunicações telefônicas[53] e seria uma medida de reforço à tutela da intimidade e da privacidade, desdobrando-se nas vertentes do segredo bancário e do segredo fiscal[54].

Deve ser destacada, ainda, a impropriedade na redação dada ao artigo 5º, inciso XII, da Constituição Federal, uma vez que, se interpretada em sentido literal, a

---

o sigilo relativo a 'dados' como inafastável (...)" (STF, PET n.º 577, QO/DF, Rel. Min. Carlos Velloso, julgado em 25 de março de 1992, DJ 23/04/1993, pp. 06918),

[51] Alexandre de Moraes reconhece que "(...) apesar de a exceção constitucional expressa referir-se somente à interceptação telefônica, entende-se que nenhuma liberdade individual é absoluta, sendo possível, respeitados certos parâmetros, a interceptação de correspondências e comunicações telegráficas e de dados sempre que as liberdades públicas estiverem sendo utilizadas como instrumento de salvaguarda de práticas ilícitas (...)" (MORAES, Alexandre de. Direito Constitucional. 28ª edição, São Paulo: Editora Atlas, 2012, p. 59). No mesmo sentido: STRECK, Lênio. *Sigilo de correspondência e comunicações*. Comentário ao art. 5º, XII, da CF. In: CANOTILHO, J.J.; MENDES, Gilmar; SARLET, Ingo; STRECK, Lênio (Coords.). Comentários à Constituição do Brasil. São Paulo: Saraiva/Almedina, 2013, p. 293.
O Supremo Tribunal Federal (STF) já reconheceu a possibilidade da interceptação de correspondência remetida por sentenciados, já que "(...)a cláusula tutelar da inviolabilidade do sigilo epistolar não pode constituir instrumento de salvaguarda de práticas ilícitas (...)" (STF, *Habeas Corpus* n.º 70.814-5/SP, Rel. Min. Celso de Mello, *Diário da Justiça*, Seção I, 24 de junho de 1994, p. 15.650 – RT 709/418; STF, Recurso em *Habeas Corpus* n.º 115.983/RJ, 2ª Turma, Rel. Min. Ricardo Lewandowski, julgado em 16 de abril de 2013, DJe 03/09/2013).

[52] A Lei Geral de Proteção de Dados (Lei n.º 13.709/2018) estabeleceu, em seu artigo 5º, incisos I a III, uma definição para os propósitos daquela normativa acerca do conceito de dado pessoal, dado pessoal sensível e dado anonimizado.

[53] Em sentido contrário, José Afonso da Silva reconhece que "(...) o sigilo de dados não se refere necessariamente aos dados das comunicações telefônicas (...) o que não nos parece conformar-se com um bom entendimento da norma é entender que o 'sigilo de dados' só se refere aos registros de uma comunicação telefônica que atestam sua existência, duração, destino, etc. Entendemos que 'sigilo de dados' se refere a cadastros de dados em geral, inclusive os utilizados pela ciência da informática e dados dos cadastros bancários (...)" (SILVA, José Afonso da. *Comentário contextual à Constituição*. São Paulo: Editora Malheiros, 2006, p. 105-106)

[54] BULOS, Uadi Lammêgo. *Constituição Federal Anotada.* São Paulo: Editora Saraiva, 2012, p. 147.

inviolabilidade alcançaria toda e qualquer forma de comunicação, uma vez que em todas elas o conteúdo versará, inevitavelmente, sobre determinados dados[55].

Impende destacar que, embora os dados possuam distintas natureza e forma (*v.g.*, dados pessoais, cadastrais, dados de conexão, dados de registro, etc.) e também sejam objeto de proteção jurídica por diversos dispositivos constitucionais e legais[56], tem prevalecido, ao menos em campo jurisprudencial, que a tutela assegurada por intermédio do artigo 5º, inciso XII, da Constituição Federal estaria circunscrita à comunicação destes dados, e não sobre seu conteúdo propriamente dito[57].

1.2.4. Teoria das três esferas

Ainda no que tange à proteção da "intimidade" e da "vida privada", desenvolveu-se na Alemanha, em 1935, a teoria dos círculos concêntricos da vida privada, também conhecida por "teoria das três esferas"[58], que seria composta por círculos concêntricos que compreenderiam, nesta ordem, a "vida privada", a "intimidade" e o "segredo", estando elas em grau crescente de proteção dada pela Constituição Federal.

---

[55] BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. *Comentários à Constituição do Brasil*. São Paulo: Editora Saraiva, 1989. v. 2, p. 73.

[56] Gregório Edoardo Raphael Selingardi aponta que "(...) a 'comunicação de dados' pode ser definida como o processo de fluxo de informações entre dois ou mais comunicantes por intermédio de um aparelho capacitado. Os 'dados' referem-se a todas as informações que indicam atributos específicos de pessoas, coisas ou eventos. Sobre o conceito de dados, já se aludiu que não se faz referência a quaisquer dados pessoais (protegidos pelo CF, art. 5º, inciso X), mas apenas aos dados constantes em aparelhos eletrônicos. O constituinte originário optou por tutelar a inviolabilidade da 'comunicação' por correspondências e telegrafia, bem como a 'comunicação' telefônica e os dados. Conforme entendimento da Excelsa Corte, esta proteção refere-se à comunicação de dados e não aos dados em si mesmos. No entanto, concluída a comunicação não cessa a necessidade de tutela jurisdicional para o conhecimento de seu conteúdo. Por esta razão, não há que diferenciar a proteção das comunicações e a proteção dos dados em si mesmos (...). Para a obtenção dos dados, em respeito ao princípio democrático insculpido no art. 1º da Constituição Federal, se faz imprescindível a determinação judicial, não podendo quedar ao livre alvedrio do Poder Executivo e de outros órgãos institucionais, a decisão sobre o conhecimento de informações caras à vida pessoa (...)" (GUARDIA, Gregório Edoardo Raphael Selingardi. *Comunicações Eletrônicas e dados digitais no processo penal*. Tese (Mestrado em Direito Processo Penal) – Faculdade de Direito, Universidade de São Paulo, 2016, p. 90).

[57] Por esta razão, Gustavo Badaró aponta que a proteção constitucional da liberdade das comunicações, insculpida no art. 5º, inciso XII, não inclui os dados do registro das ligações telefônicas (números discados e recebidos, horários das ligações, etc), já que tais dados ficariam registrados nas operadores dos serviços de telefonia e, por essa razão, seriam objeto de proteção pela cláusula da intimidade e vida privada (artigo 5º, inciso X, da Constituição Federal) (BADARÓ. Gustavo Henrique Righi Ivahy. *Interceptação de Comunicações Telefônicas e Telemáticas: limites ante o Avanço da Tecnologia*. Badaró Advogados, São Paulo: 2009. Disponível em: <http://badaroadvogados.com.br/interceptacao-de-comunicacoes-telefonicas-e-telematicas-limites-ante-oavanco-da-tecnologia.html>. Acesso em: 20 de dezembro de 2020).

[58] Para maiores informações sobre o tema, confira a obra de Paulo José da Costa Júnior (COSTA JÚNIOR, Paulo José da. *O direito de estar só: tutela penal da intimidade.* 2ª edição, São Paulo: Editora RT, 1995, p. 24-25), em que se aponta que a teoria teria sido idealizada por Heinrich Hubbmann e posteriormente desenvolvida e aperfeiçoada por Heinrich Henkel e Schmidt.

Na parte de mais externa da esfera – e, por conseguinte, de menor grau de proteção à tutela da informação – estaria alocada a noção de "vida privada" (*Privatsphäre*), que abrangeria as informações que não seriam propriamente de divulgação pública mas que, ao mesmo tempo, estariam ao alcance de um número indeterminado de pessoas. São comportamentos e acontecimentos que, embora compartilhados por diversas pessoas, ainda não são de domínio público.

Já na parte intermediária da referida esfera imaginária estaria localizada a "intimidade" (*Vertrauenssphäre*) ou da "confiança" (*Vertraulichkeitssphäre*), em que apenas um número restrito e limitado de pessoas, geralmente de elevada proximidade e familiaridade do indivíduo, poderia privar da informação.

Por derradeiro, no círculo mais restrito estaria o *"segredo"* (*Geheimsphäre*), que é caracterizado por compreender uma parcela da vida particular da pessoa que não é compartilhada ou divulgada, ainda que para membros da própria família. Trata-se de uma parcela absolutamente individual, em que o indivíduo não socializa a informação ou conteúdo restrito com ninguém[59], diante do seu elevado grau de importância para a proteção à privacidade do cidadão.

Esta distinção, embora de acepção teórica, vem sendo diluída a partir do intenso cruzamento de dados pessoais, permitindo-se o acesso a diversas camadas de privacidade sem, muitas vezes, contarem com a anuência do titular dos dados[60].

1.3. A privacidade e as relações sociais da era moderna e pós-moderna

O ponto de partida para o desenvolvimento da temática relacionada à extensão da proteção à privacidade e o acesso a dados armazenados em aparelhos celulares

[59] José Raul Gavião de Almeida acrescenta uma quarta esfera, relacionada à intimidade oculta, a qual abarcaria todos os segredos que não se deseja compartilhar, mas reservar à própria consciência. É nesta esfera que estaria incluído a "*reserva da própria mente*", inadmitindo-se métodos que eliminar a capacidade volitiva da pessoa, tal como o soro da verdade ou a hipnose (ALMEIDA, José Raul Gavião de. *Anotações acerca do direito à privacidade*. In: Jorge Miranda; Marco Antônio Marques da Silva. (Org.). Visão Luso-Brasileira da Dignidade Humana. 1ª edição, São Paulo: Editora Quartier Latin, 2008, v. 1, p. 677-684).

[60] SOARES, Paulo Vinícius de Carvalho. *A Diluição das Esferas de Privacidade e de Intimidade diante da Era dos Dados.* In: LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro. LAUX, Francisco de Mesquita; RAVAGNANI, Giovani dos Santos. *Direito, processo e tecnologia.* São Paulo: Editora RT, p. 571-572.

exige, necessariamente, uma análise evolutiva das noções sociais de privacidade ao longo do tempo.

Os valores que inspiraram a criação e reconhecimento de uma esfera íntima do cidadão, enquanto aspecto inerente à própria personalidade, transmudaram-se ao longo tempo[61], culminando-se na atual era moderna (ou pós-moderna), representada pela fluidez das relações sociais e familiares[62], com a crescente dinamização das interações intersubjetivas amparadas por um exponencial avanço tecnológico.

Não bastasse, típico destas relações mutantes e transitórias da vida cotidiana, adere-se a perspectiva de maximização das projeções individuais ("eu"), com a necessidade de dizer ao mundo quem se é e de colher a aprovação e reconhecimento dos demais[63].

Esta nova dinâmica é satisfatoriamente representada pelas redes sociais e as relações de comunicações instantâneas e massificadas travadas, em que há uma voluntária e, por vezes, inconsciente exposição da vida íntima e privada com terceiros, especialmente por parte de vulneráveis adolescentes[64].

---

[61] Zygmund Bauman aponta, em uma prognose realista, que "(...) perdemos a coragem, energia e sobretudo disposição de persistir na defesa desses direitos, esses tijolos insubstituíveis na construção da autonomia individual. Em nossos dias, o que nos assusta não é tanto a possibilidade de traição ou violação da privacidade, mas o oposto: o fechamento das saídas. A área da privacidade está se transformando num local de encarceramento (...)" (BAUMAN, Zygmunt. *Danos colaterais. Desigualdades sociais numa era global*. Tradução: Carlos Alberto Medeiros, Rio de Janeiro: Editora Zahar, 2013, p. 113-114).

[62] BAUMAN, Zygmunt. *Modernidade Líquida.* Tradução: Plínio Dentzien, Rio de Janeiro: Editora Zahar, 2000, p. 12.

[63] NIETZSCHE, Friedrich. *Ecce homo: como alguém se torna o que é*. Traduzido por Artur Morão. Covilhã: Editora Lusosofia, 2008. Disponível em: <http://www.lusosofia.net/textos/nietzsche_friedrich_ecce_homo.pdf>. Acesso em: 20 de dezembro de 2020.

[64] Susan B. Barnes aponta que "(…) according to three 2005 Pew Reports (Lenhart, 2005; Lenhart, et al., 2005; Lenhart and Madden, 2005), 87 percent of American teens aged 12–17 are using the *Internet*. Fifty–one percent of these teenagers state that they go online on a daily basis. Approximately four million teenagers or 19 percent say that they create their own weblogs (personal online journals) and 22 percent report that they maintain a personal Web page (Lenhart and Madden, 2005). In blogs and on personal Web sites, teenagers are providing so much personal information about themselves that it has become a concern. Today, content creation is not only sharing music and videos, it involves personal diaries (…)" (BARNES, Susan, *A privacy paradox: Social networking in the United States*, First Monday, volume 11, number 9, September 2006. Disponível em: <http://firstmonday.org/issues/issue11_9/barnes/index.html>. Acesso em: 20 de dezembro de 2020).

Ao mesmo tempo em que as redes sociais fomentaram esta superexposição, com o afrouxamento da proteção aos dados e informações compartilhadas[65], há uma preocupação generalizada dos usuários com a privacidade e seus contornos protetivos. Trata-se de um fenômeno conhecido como "paradoxo da privacidade", caracterizado pelo fato de o usuário esboçar uma preocupação com o resguardo à sua privacidade e, contraditoriamente, não adotar medidas preventivas para resguardá-la em seu comportamento diário[66].

Soma-se a esta nova concepção o crescente enfraquecimento da proteção à privacidade, em prol de uma tutela da segurança nacional[67] direcionada à produção preventiva e antecipada de informações.

Lastreada precipuamente no medo[68] de que novas ações criminosas venham a ocorrer e que ao Estado é atribuível o dever de se antecipar a estes atos, pretendeu-

---

[65] WINTER destaca que "(...) es cierto que a través de las redes sociales en internet o de 'reality shows' el valor de la privacidad está experimentando un cambio. Pero también es cierto, que esa perdida de privacidad es consentida (…)", bem como que "(…) el ámbito de protección de la esfera privada, en mi juicio, no se ve afectado por esa nueva concepción de la privacidad. El individuo tiene derecho a decidir qué parte de su privacidad desea compartir y tiene derecho, como regla, a saber si está siendo observado e con qué fines (…)" (BACHMAIER WINTER, Lorena. *Investigación criminal y protección de la privacidad en la doctrina del Tribunal Europeo de Derechos Humanos*. In: 2º Congresso de Investigação Criminal. Coordenação: Maria Fernanda Palma, Augusto Silva Dias e Paulo de Sousa Mendes. Lisboa: Almedina, 2010, p. 165).

[66] TADDICKEN, Monika. "*The 'Privacy Paradox'in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure*". Journal of Computer-Mediated Communication, 19 (2014) 248–273. Disponível em: < https://academic.oup.com/jcmc/article/19/2/248/4067550>. Acesso em: 20 de dezembro de 2020; BOYD, Dana; HARGITTAI, Eszter. *Facebook privacy settings: Who cares?*. 2010, First Monday, 15(8) <http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589>. Acesso em: 20 de dezembro de 2020.

[67] Para WINTER: "(...) los tres factores unidos: 1) stress emocional; 2) actuación preventiva; 3) calificación de la lucha como un estado de 'guerra', constituyen una importante amenazada para la proteccíon de los derechos fundamentales, dentro del marco de la investigación penal. Em primer lugar, porque el sentimiento de fuerte inseguridad hace que los ciudadanos tiendan a aceptar más injerencias en la esfera de sus derechos fundamentales a cambio de una mayor seguridad. En segundo lugar, porque las actuaciones de los servicios de inteligencia no están sometidas a los estrictos controles que prevén las leyes procesales. Y, em tercer lugar, porque, ante situaciones que pueden calificarse de emergencia o de execpción, los propios convenios internacionales em materia de derechos fundamentales, permiten la derogación de ciertos derechos, como prevé por ejemplo, el art. 15 del CEDCH (...)" (BACHMAIER WINTER, Lorena. *Investigación criminal y protección de la privacidad en la doctrina del Tribunal Europeo de Derechos Humanos*. Op. cit, p. 162-163). A título de exemplo, nos Estados Unidos foi editado, pouco após os atentados terroristas de 11 de setembro de 2001, o "The USA PATRIOT Act: Preserving Life and Liberty", um acrônimo para "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism", verdadeiro conjunto de atos que, a pretexto de reforçarem e fortalecerem a segurança nacional na prevenção de atentados e ações terroristas, acabaram por reduzir o espectro de proteção conferido aos cidadãos por intermédio da "Fourth Amendment".

[68] Como destaca Gustavo Torres Soares, "(...) quanto maior o medo, justificado ou não, sentido pelos cidadãos ante o fenômeno criminoso, maior é a disponibilidade de tais cidadãos para abrirem mão de parcelas de sua liberdade (do que decorre a aceitação social majoritária a, por exemplo, controles pessoais antes de embarques

se reduzir a esfera de interpretação sobre a abrangência da garantia constitucional insculpida na precitada Emenda Americana, em troca de uma promessa de segurança[69] comum a ser fornecida aos cidadãos.

Esta relação é pautada, sobretudo, na crença de que o recrudescimento das esferas de proteção às informações proporciona uma inevitável insegurança nacional. Sob essa premissa, em prol da segurança nacional e difusa, seria necessário se sacrificar parte das garantias individuais dos cidadãos, sendo uma delas a noção de privacidade[70]. WILLIAM STUNTZ, professor da Universidade de Harvard, conclui que, diante da desordem e das ameaças transnacionais, continuar-se falando em privacidade é uma "doença" que enfraquece e subverte a segurança pública e nacional[71].

Não bastasse, acrescenta-se a esta equação um ingrediente adicional: a difusão de uma concepção de que os cidadãos não deveriam se preocupar com a crescente vigilância estatal e a redução da proteção aos dados privativos, especialmente se nada interessassem a esconder[72]. Nesta linha, sob o prisma de uma visão individualista, a tutela

---

aéreos ou à edição de normas jurídicas fortemente cerceadoras, como interceptações das variadas formas de comunicação (...)" (SOARES, Gustavo Torres. *Investigação criminal e inovações técnicas e tecnológicas: perspectivas e limites.* Tese (Doutorado em Direito Processual Penal) - Faculdade de Direito da Universidade de São Paulo, 2014, p. 203-204).

[69] Richard Posner aponta que "(…) in an era of global terrorism and weapons of mass destruction, the government has a compelling need to gather, pool, sift, and search vast quantities of information, much of it personal (...)" (POSNER, Richard. A. *Not a Suicide Pact.* New York: Oxford University Press, 2006, p. 141).

[70] Stephen J. Schulhofer sustenta que *"*(...) a majority of Americans seem to assume that traditional Fourth Amendment safeguards must be relaxed, at least to some extent, in order to confront this threat and provide an extra margin of safety. Many who treasure the Bill of Rights see the sacrifice of some privacy as a small price to pay for preventing a catastrophic attack. Either they assume that constitutional rights must give way in an 'emergency', or they assume that the rights themselves expand or contract, accordion-like, as countervailing security needs fluctuate. That intuition has led Americans to accept a host of new laws weakening traditional constraints on the executive. The nations has also tolerated law enforcement actions that disregard limits supposedly still in force. Existing Fourth Amendment requirements, already weakened by decades of Supreme Court precedent, have come under further attack. Statutory remedies for flaws in pre-9/11 Supreme Court precedent never had the constitutional status they deserve, and many of them have been rolled back under the pressures of the moment. When it comes to international terrorism, most people seem to assume that individuals like themselves will not come under suspicion. And even if they think that their own privacy may be affected, in matters of national security they prefer not to take chance. As a result, restraints have eroded across the entire spectrum of search-and-seizure powers (…)" (SCHULHOFER, Stephen J. *More Essential Than Ever. The Fourth Amendment in the Twenty-first Century.* Oxford University Press, 2012. p. 146).

[71] "(…) Today, the danger that American democracy faces is not that rulers will know too much about those they rule, nor that too many decisions will be made without public scrutiny. Another danger looms larger: that effective, active government–government that innovates, that protects people who need protecting, that acts aggressively when action is needed–is dying. Privacy and transparency are the diseases. We need to find a vaccine, and soon (…)" (STUNTZ, William J. *Secret Service: Against Privacy and Transparency.* The New Republic, April 17, 2006, p. 12).

[72] SCHULHOFER, Stephen J. *More Essential Than Ever. The Fourth Amendment in the Twenty-first Century.* p. 5. Para David Gray "(…) a common refrain is that 'If you are not doing anything wrong, then you should

da privacidade somente interessaria àqueles que, envolvidos em ilegalidades, pretendam obstar a atuação estatal.

Esta visão distorcida desconsidera o fato de que a privacidade interessa a cada um dos cidadãos, enquanto necessidade para o desenvolvimento de nossa identidade pessoal e da personalidade humana[73]. Ainda que determinadas pessoas não se enveredem pelos tortuosos caminhos da ilegalidade, é inegável a necessidade de se estabelecer um mínimo espaço de controle sobre quais informações os cidadãos possam revelar e a quem, como projeção de sua individualidade.

Ademais, ao contrário do que se imagina, a garantia da privacidade não pretende impedir ou dificultar a atuação estatal no combate às ações criminosas, como bem destaca ADA PELLEGRINI GRINOVER, ao reconhecer que os direitos e garantias individuais "(...) tem sempre feitio e finalidade éticos, não podendo proteger abusos e nem acobertar violações (...)"[74].

Ao mesmo tempo, a proteção assegurada aos cidadãos cria um dever de responsabilidade ao Estado, impedindo-se que os agentes estatais devassem de maneira temerária e injustificável a vida privada daqueles que, justamente, nada teriam a esconder.

---

not care whos is watching'. In a similar vein, some maintain that, if our lives are uninteresting, then government authorities will not bother to watch. Others assert that they just do not care whether the government is watching what they make for breakfast. (…)" (GRAY, David. *The Fourth Amendment in an Age of Surveillance.* Cambridge University Press, 2017, p. 11). Em outra ponderação, Hans-Joerg Albrecht indica que *"(...)* secret surveillance and investigation techniques are then discussed in the context of public trust in the state and state institutions. In this respect it is argued that public opinion surveys provide for evidence that the public accepts secret surveillance as well as general surveillance of the public space ("someone to watch over me"). Acceptance, however, declines significantly if surveillance aims at the immediate environment of citizens as well as at intimate areas. But, not much is known about how trust in public institutions (incluing law enforcement) as a basic condition of democratic societies is related to the states capacity and practices of interfering with individual privacy *(...)"* (ALBRECHT, Hans-Joerg. *Secret Surveillance. Measures of Secret Investigation in the Criminal Process.* Revista Brasileira de Ciências Criminais, 92, p. 138).

[73] BELLOQUE, Juliana Garcia. *Sigilo Bancário: Análise Crítica da LC 102/2001.* São Paulo, Ed. Revista dos Tribunais: 2003, p. 21-22.

[74] GRINOVER, Ada P. *Liberdades públicas e processo penal – as interceptações telefônicas.* 2ª edição. São Paulo: Editora Saraiva, 1982, p. 306-307.

Em suma, a garantia desta privacidade assume um papel relevante em prol de uma sociedade democrática[75], especialmente como forma de se assegurar a liberdade de expressão, a possibilidade de discordâncias políticas e a proteção de todas as minorias[76].

1.4. A privacidade diante das novas tecnologias: os aparelhos celulares e sua evolução tecnológica

Neste contexto, a despeito das flexibilizações interpretativas por ação de seus próprios titulares ou em prol de uma "segurança nacional", a abrangência da tutela protetiva à privacidade se vê diante de um novo desafio, em razão do surgimento de novas tecnologias que dinamizaram as relações sociais, especialmente com a facilitação comunicativa e a criação de instrumentos de produção, captação e compartilhamento massificado de dados digitais.

Assim, ao mesmo tempo em que o avanço tecnológico se generalizou nas sociedades modernas, a criminalidade também se valeu destes instrumentos para a perpetração de novas e antigas condutas criminosas, especialmente diante da possibilidade do criminoso digital "anonimizar" seus rastros cibernéticos, o que torna atrativa a utilização da *internet* por grupos de criminalidade organizada e transnacional[77].

Esta realidade demandou uma mudança também nos mecanismos de investigação criminal[78]. Para além da aceitação de modernos meios de produção de provas

---

[75] VIANNA, Túlio Lima. *Transparência pública, opacidade privada: o Direito como instrumento de limitação do poder na sociedade de controle.* Tese (Doutorado em Direito) – Faculdade de Direito da Universidade Federal do Paraná, Curitiba, 2006, p. 84.

[76] Stephen J. Schulhofer registra, com absoluta precisão, que "(…) when unrestricted search and surveillance powers chill speech and religion, inhibit gossip, and dampen creativity, they undermine politics and impoverish social life for everyone (…) In this respect, as in the others just mentioned, an effective Fourth Amendment fosters the sense of personal security that is necessary for individual autonomy and political liberty in a free society (…)" (SCHULHOFER, Stephen J. *More Essential Than Ever. The Fourth Amendment in the Twenty-first Century.* p. 14-15)

[77] RODRIGUES, Benjamim Silva. *Das Escutas Telefónicas à Obtenção de Prova (Em Ambiente) Digital: a monotorização dos fluxos informais e comunicacionais*, Tomo II, Coimbra: Editora Coimbra, 2009, p. 505-506.

[78] Como bem salienta Miren J. Pérez Estrada, "(...) a utilização habitual das novas tecnologias torna necessária a obtenção de prova de tipo tecnológico que, embora contribua para aprimorar a eficácia estatal na persecução dos delitos, em igual medida aumentará o risco de lesividade ao direito fundamental à autodeterminação informativa das pessoas investigadas (...)" (PÉREZ ESTRADA, Miren J. *La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información.* Revista Brasileira de Direito Processual Penal, vol. 5, n. 3, set./dez. 2019, p. 1308, tradução livre)

digitais[79] e sua respectiva contextualização com as garantias constitucionais relacionadas à privacidade e ao sigilo de dados[80], vislumbrou-se a necessidade de se estabelecer a criação de agrupamentos policiais dotados de conhecimento forense informático-digital, sem prejuízo de uma possível adoção de "uniformidade legal internacional" em matéria de criminalidade global do risco informático e da informação[81].

Em suma, não há mais como se ignorar que a persecução criminal deva se ater à realidade do entorno digital[82], em que o meio tecnológico é alvo da conduta ou mera ferramenta para conseguir se obter a finalidade do delito, ainda que com alvo diverso do tecnológico[83].

Com efeito, parte dos delitos são advindos do próprio uso da informática, porquanto praticados necessariamente em espaços virtuais, sendo o recurso tecnológico um instrumento para a perpetração do próprio crime[84].

Nestes casos, o sistema informático e os dados seriam objeto do crime e o bem jurídico a ser tutelado, tal como o delito de invasão de computadores (artigo 154-A do Código Penal), o de inserção de dados falsos em sistema de informações (artigo 313-A

---

[79] VALENTE, Manuel M. G. *Editorial dossiê "Investigação preliminar, meios ocultos e novas tecnologias*. Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 3, n. 2, mai./ago. 2017, p. 473-482. Disponível em: https://doi.org/10.22197/rbdpp.v3i2.82. Acesso em: 20 de dezembro de 2020.

[80] GONZÁLEZ-CUÉLLAR SERRANO, Nicolás. *Garantías constitucionales de la persecución penal em el entorno digital.* In: GÓMEZ COLOMER, Juan Luis. Prueba y proceso penal (Análisis especial de la prueba prohibida em el sistema español y em el derecho comparado). Valencia: Tirant Le Blanch, 2008, p. 152.

[81] ROVIRA DEL CANTO, Enrique. *Delincuencia informática y fraudes informáticos.* Granada: Editora Comares, 2002, p. 86.

[82] Orin Kerr, em análise sobre a aplicabilidade da *Fourth Amendment* às relações estabelecidas por intermédio da *internet*, mas que é integralmente aplicável ao contexto das investigações digitais no Brasil, conclui que *"(...)* criminal investigations are increasingly moving from the physical world to computer networks. The Fourth Amendment will have to adopt new principles to maintain its longstanding function. The need for evolution is nothing new: the Fourth Amendment will adapt to how wrongdoers use the Internet just as it adapted to how wrongdoers started using postal letters, automobiles, and the telephone. At the same time, the future doctrines of Fourth Amendment law online are likely to be both more complex and more far-reaching than either the postal letter, automobile, or telephone precedents. Postal letters send and receive text from one person to another. Automobiles transport property in trunks and backseats. Telephones send and receive conversations. In contrast, computer networks are entire worlds of activity: they act as jukeboxes, libraries, stores, schools, concerts, private rooms, and hundreds of other services and virtual places. And computer networks seem to provide more and more: every passing year brings another new program, another new service, another new way in which our general-purpose computers add to the virtualization of our environments (…)" (KERR, Orin S., *Applying the Fourth Amendment to the Internet: A General Approach*. Vol. 62: 1005 Stanford Law Review, 2010, p. 1048).

[83] SYDOW, Spencer Toth. *Crimes informáticos e suas vítimas*. São Paulo: Editora Saraiva, 2015.

[84] CAMARGO, Coriolano Almeida; SANTOS, Cleórbete. *Crimes digitais no ordenamento brasileiro.* Revista de Direito e as Novas Tecnologias, vol. 2/2019, Jan-Mar/2019.

do Código Penal), a interceptação telemática (artigo 10 da Lei n.º 9.296/1996), dentre outros. Esta categoria é classificada[85] como delitos informáticos "próprios" ou "puros", em que o sistema informático é utilizado como meio e fim da conduta[86], consumando-se o delito também no espaço virtual.

Por sua vez, os delitos informáticos "impróprios" ou "impuros" seriam aqueles já tipificados no ordenamento jurídico pátrio em que, embora os dados digitais não sejam elementos relacionados e inerentes ao próprio tipo penal – que também são cometidos por meios "tradicionais" -, poderão servir como meio para a produção do resultado naturalístico, ofendendo bens jurídicos diversos da informática[87]. *Ad exemplum,* uma injúria praticada pelo meio informático; um tráfico de drogas cuja negociação seja operacionalizada através de mensagens enviadas e recebidas por aplicativos de comunicação instantânea[88], dentre outros.

1.4.1. Aparelhos celulares e *smartphones*

Dentro desta "sociedade de informação"[89] representada pela "datificação" dos aspectos que circundam a vida social e a personalidade humana e que, em

---

[85] Dentro da taxonomia classificatória, para além dos crimes informáticos puros e impuros (ou próprios e impróprios), há doutrinadores que vislumbram a categoria dos crimes informáticos mistos, em que "(...) crimes complexos em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa. São delitos derivados da invasão de dispositivo informático que ganharam status de crimes sui generes, dada a importância do bem jurídico protegido diverso da inviolabilidade dos dados informáticos (...)" (VIANNA, Túlio; MACHADO, Felipe. *Crimes informáticos*. Belo Horizonte: Editora Fórum, 2013, p. 35).

[86] SILVA, Rita de Cássia Lopes da. *Direito Penal e sistema informático*. Revista dos Tribunais. São Paulo, v.4, 2003, p. 60.

[87] ARAS, Vladimir. *Crimes de informática, uma nova criminalidade*. Jus Navegandi. Teresina, 1 de outubro de 2001. Disponível em: http://jus.com.br/artigos/2250/crimes-de-informatica&gt. Acesso em: 20 de dezembro de 2020).

[88] Parte da doutrina classifica estes delitos como "comuns", em que a prova digital seria instrumento de comprovação do delito (VAZ, Denise Provazi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório.* Tese (Doutorado em Direito) - Faculdade de Direito da Universidade de São Paulo, 2012, p. 33).

[89] Como bem define Scott Lash, "(…) en contraste com otros análisis, por ejemplo, los de Bell (1973), Touraine (1974) y Castells (1996), creo que debemos entender la sociedad de la información concentrandonós en las cualidades primarias de la propia información. Esta debe interpretarse aquí en marcada distinción de otras categorías socioculturales anteriores, como la narrativa, el discurso, el monumento o la instituición. Las cualidades primarias de la información son el fluijo, el desarraigo, la compresión espacial y temporal e las relaciones en tiempo real. En este sentido, no excluyente, pero sí fundamental, vivimos en una era de la información. (LASH, Scott. *Crítica de la información*. Buenos Aires: Editora Amorrortu, 2005, p. 22). No mesmo sentido: MONCAU, Luiz; LEMOS, Ronaldo; BOTTINO, Thiago. *Projeto de Lei de Cibercrimes: há outra alternativa para a internet brasileira?*. Revista de Direito Administrativo – RDA, Belo Horizonte, ano 2008, n. 249, set.-dez. 2008.

grande proporção, permitiu o avanço da criminalidade contemporânea, a *internet* assumiu um papel relevante de comunicação[90] e, em contrapartida, permitiu um significativo avanço na perda do direito à privacidade e ao sigilo.

O acesso à rede mundial de computadores se difundiu[91] por meio de diversos dispositivos portáteis, transformando-os em verdadeiros "microcomputadores" que permitem a conexão imediata e instantânea à *internet.*

Neste cenário, os aparelhos celulares deixaram de servir como mero instrumento de comunicação entre os cidadãos através da propagação de ondas eletromagnéticas de transmissão bidirecional de voz para, a partir da evolução tecnológica, ganharem natureza multifuncional, reunindo em um mesmo suporte tecnológico ampla e diversificada gama de funcionalidades a serviço do usuário[92].

Assim, convencionou-se adotar uma nova concepção para estes modernos aparelhos celulares, nominando-os de "smartphones*",* que se caracterizam por serem "(...) um celular com capacidade avançada, que executa um sistema operacional identificável permitindo aos usuários estenderem suas funcionalidades com aplicações terceiras que estão disponíveis em uma loja de aplicativos (...)" e que "(...)devem incluir um *hardware* sofisticado com: a) capacidade de processamento avançada (CPUs modernas, sensores) b) Capacidade de conexões múltiplas e rápidas (Wi-Fi, HSDPA) e c) tamanho de tela adequado e limitado. Além disso, seu Sistema Operacional deve ser claramente identificável, como Android, Blackberry, Windows Phone, Apple`s IOS, etc. (...)"[93].

---

[90] CASTELLS, Manuel. *A sociedade em rede: a era da informação: economia, sociedade e cultura*. Tradução Roneide Venancio Majer. 21. edição, São Paulo: Editora Paz e Terra, 2020, p. 19.

[91] Conforme recente pesquisa da Fundação Getúlio Vargas (FGV), o número de celulares em uso no Brasil e nos Estados Unidos já é superior ao da respectiva população, o que revela a disseminação do objeto (https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/fgvcia2020pesti-ppt_0.pdf. Acesso em: 20 de dezembro de 2020).

[92] Para uma análise evolutiva do aparelho celular até os atuais *smartphones*, bem como o padrão de uso do objeto no país, recomenda-se: COUTINHO, Gustavo Leuzinger. *A Era dos 'Smartphones: Um estudo exploratório sobre o uso dos 'smartphones' no Brasil.* Monografia. Universidade de Brasília (UNB), dezembro de 2014.

[93] THEOHARIDOU, Marianthi; MYLONAS, Alexios; GRITZALIS, Dimitris. *A Risk Assessment Method for Smartphones. 27th Information Security and Privacy Conference (SEC)*, Jun 2012, Heraklion, Crete, Greece, p.444-445, tradução livre. No mesmo sentido a definição de Ricardo Gloeckner e Daniel Eilberg, para quem os *smartphones* seriam"(...) plataforma tecnológica de integração entre múltiplos canais de comunicação, além de permitir, como dispositivo tecnológico, a utilização de aplicativos de trocas de mensagens (e.g. WhatsApp), de acesso e movimentação de contas bancárias, de aquisição e armazenamento de passagens aéreas, de verificação e utilização de e-mails registrados no dispositivo, de acesso às redes sociais como o Facebook. Portanto, evidentemente, o aparelho de telefone celular não se presta unicamente à comunicação por telefone,

Não bastasse, os *smartphones* ganharam ampla capacidade de memória, o que permitiu o armazenamento massivo de dados relacionados à personalidade dos seus titulares e de terceiros que com ele tenham interagido[94].

Diante de suas múltiplas funções que conjugam atividades comunicativas e informáticas, o moderno aparelho celular vem sendo utilizado como instrumento para o cometimento de crimes e, por conseguinte, se tornou relevante fonte de provas[95]. Ao mesmo tempo, o armazenamento de uma vasta quantidade de dados que biografam a personalidade de seus indivíduos e sua possível superexposição impede que o acesso ao conteúdo dos aparelhos[96] seja feito de forma indiscriminada e desproporcional, sob pena de se violar a proteção constitucional conferida à privacidade.

---

o que lhe rende uma terminologia enganosa. Apesar da nomenclatura "telefone celular", os atuais aparelhos (smartphones) são computadores móveis multifuncionais, capazes de servir, também, como instrumentos para ligações telefônicas (...)" (GLOECKNER, Ricardo Jacobsen. EILBERG, Daniela Dora. *Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos.* In: Revista Brasileira de Ciências Criminais, vol. 156/2019, Jun/2019, p. 353-393).

[94] Conforme recente pesquisa da Fundação Getúlio Vargas (FGV), o número de celulares em uso no Brasil e nos Estados Unidos já é superior ao da respectiva população, o que revela a disseminação do objeto (https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/fgvcia2020pesti-ppt_0.pdf. Acesso em: 20 de dezembro de 2020).

[95] As modernas técnicas de investigação criminal vêm sendo utilizadas para auxiliar a elucidação de delitos, sejam eles eminentemente digitais ou, ainda, aquelas tradicionais que necessitem, direta ou indiretamente, da prova informática ou digital. Para se assegurar a proteção ao núcleo fundamental da privacidade e intimidade, tem-se sustentado a necessidade de se estabelecer um rol taxativo de tipos penais que possam ser investigados por métodos de tecnologia da informação, além de preceitos e diretrizes para a busca, aquisição e preservação do material probatório.

Nesta linha, Carlos Hélder Furtado propõe uma equiparação entre o grau de lesividade do método de investigação tecnológica que incide nos direitos fundamentais do investigado e o grau de ligação entre o cometimento do ilícito investigado e o meio tecnológico, para delimitação de quais crimes poderiam compor este rol. Assim, nos dizeres do autor, "(...) não seria possível – porquanto que inapropriada e demasiadamente lesiva – a investigação por meios digitais ou informáticos de um homicídio ou de um roubo comum não relacionados aos meios tecnológicos. Não se poderia supor a utilização de tais mecanismos pela facilidade em determinar suspeitos ou busca uma 'fonte' de prova contra o indiciado ou acusado através de mecanismos que sirvam para identificar o lugar, o horário e o trajeto seguido pelo investigado na data do fato apurado. Quer-se dizer que não existindo liame entre o ilícito investigado e o meio digital, jamais se poderá falar em uma investigação que se utiliza prioritariamente ou exclusivamente de métodos tecnológicos, informáticos ou digitais, sob pena de serem demasiadamente lesivos a direitos como a privacidade, intimidade e personalidade (...)" (MENDES, Carlos Hélder Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software.* São Paulo: Ed. Juspodivm, 2020, p. 106). Grégório Guardia, por sua vez, aduz que a "(...) a pertinência do uso de novas tecnologias na investigação criminal é observável na quase totalidade dos ilícitos. Porém, mostra-se ainda mais proveitosa em certos delitos, como tráfico de drogas, oferta de conteúdos ilícitos através da 'internet', atentados contra a propriedade intelectual, crimes contra crianças e adolescentes, 'cyberstalking' e terrorismo (...)" (GUARDIA, Gregório Edoardo Raphael Selingardi. *Comunicações Eletrônicas e dados digitais no processo penal*. Op. cit., p. 120).

[96] Para fins do presente trabalho científico, as expressões "aparelhos celulares" e "*smartphones"* serão utilizados indistintamente e de maneira genérica, de modo que ambos serão interpretados como o instrumento portátil, com finalidade de comunicação, que conjuga múltiplas funções envolvendo também atividades informáticas, permitindo-se o armazenamento extensivo de uma quantidade relevante de dados.

1.4.2. A busca de um equilíbrio entre a eficiência e o garantismo

Se a evolução tecnológica alcançou a vida social de maneira inarredável, é certo que muito pouco se evoluiu, legislativa e doutrinariamente, para se fazer frente a esta nova realidade.

Com efeito, disposições relacionadas às interceptações telefônicas (Lei n.º 9.296/1996), a busca e apreensão (artigo 240 e seguintes do Código de Processo Penal) e a Lei do Marco Civil da *Internet* (Lei n.º 12.965/2014) são insuficientes para regularem, de forma direta e imediata, os aspectos procedimentais e legais na obtenção de provas digitais, especialmente a partir de dados comunicados e armazenados em aparelhos celulares.

Neste panorama, os dispositivos constitucionais relacionados à tutela da privacidade, direta e indiretamente, podem servir como ponto de equilíbrio para balizar as relações entre a eficiência na atividade investigativa com a proteção às garantias constitucionais.

Em verdade, ao mesmo tempo em que assegurou limites à atuação estatal, a Constituição Federal também impôs ao Estado o dever de proteger e tutelar o direito à vida e segurança (artigo 5º, *caput*). Não bastasse, reafirmando seu compromisso, o artigo 144, *caput*, da Constituição Federal[97] estabeleceu que a segurança pública é um dever do Estado, em busca da preservação da ordem pública e da incolumidade das pessoas e do patrimônio.

[97] De acordo com Sérgio Fernando Moro, "(...) talvez seja essa a norma mais categórica ao dispor sobre o dever do Estado em relação à segurança pública e ela mesmo como um direito do cidadão. O grau de abstração da norma, todavia, não permite conclusões óbvias acerca do nível de segurança pública que pode ser exigido do Estado. Interessante notar a inexistência de qualquer precedente do STF no qual o direito à segurança pública tenha sido invocado para a resolução de um caso concreto (...) a norma em questão permanece, em nossa jurisprudência, apenas como uma potencialidade a ser explorada, sem maiores reflexos no julgamento de casos (...)" (MORO, Sérgio Fernando. *Direito fundamental contra o crime*. In: CLÈVE, Clèmerson Merlin. *Direito Constitucional brasileiro: teoria da Constituição e direitos fundamentais*. São Paulo: Revista dos Tribunais, 2014, p. 559-581)

Assim, o direito processual penal é balizado pelo reconhecimento de dois valores igualmente importantes e que devem ser equilibrados: o direito à liberdade e o direito à segurança pública[98].

Reconhece-se, portanto, que ao Estado é imposto o dever de assegurar indistintamente a segurança pública, criando-se condições para o desenvolvimento da atividade investigativa e preventiva, além de estabelecer meios que propiciem uma resposta rápida e eficiente após o abalo social causado pelo crime. Em contrapartida[99], exsurge a obrigação de se respeitar e propiciar o exercício dos direitos e garantias fundamentais do cidadão, porquanto inerentes ao ser humano em razão de sua condição de titular, e não mero objeto de direitos[100].

O direito fundamental à segurança pública, em uma projeção endoprocessual, é reconhecido à medida que o processo penal será o instrumento para concretização das normas repressivas penais, como instrumento de punição àqueles que tenham violado a norma jurídica e ferido bens penalmente relevantes, bem como para se reafirmar os fundamentos de validade e eficácia da norma jurídica[101].

---

[98] Novamente, invoca-se aqui o professor Antônio Scarance Fernandes, em seu clássico artigo sobre a relação entre eficiência e garantismo: "(...) são dois direitos fundamentais do indivíduo que interessam especialmente ao processo criminal: o direito à liberdade e o direito à segurança, ambos previstos no art. 5º, 'caput', da CF/1988. Como decorrência desses dois direitos fundamentais, os indivíduos têm direito a que o Estado atue positivamente no sentido de estruturar órgãos e criar procedimentos que, ao mesmo tempo, lhes dêem segurança e lhes garantam a liberdade. Em outras palavras, têm direito a um sistema que faça atuar as normas do direito repressivo, necessárias para a concretização do direito fundamental à segurança, e atribua ao acusado todos os mecanismos essenciais para a defesa de sua liberdade. De forma resumida, um sistema que assegura 'eficiência' com 'garantismo' (...)" (FERNANDES, Antonio Scarance. *Equilíbrio entre a eficiência e o garantismo*. Revista Brasileira de Ciências Criminais n.º 70/229, jan-fev/2008, p. 744)

[99] Revela-se a possibilidade de se estabelecer, nesta perspectiva processual-penal, a aplicação de dois *status* mencionados por Georg Jellinek em sua obra *"As declarações de direitos do homem e Sistema de direitos públicos subjetivo",* que foram bem esmiuçados por Paulo Thadeu Gomes da Silva*:* o *status negativo,* que compreende que o indivíduo tem um espaço de liberdade com relação a intervenções dos poderes estatais; e o *status positivo,* em que o indivíduo pode demandar do Estado uma prestação. Assim, o direito à segurança poderia ser considerado uma expressão deste *status positivo,* já que o cidadão tem direito de exigir que o Estado lhe garanta e assegure a prestação de segurança, como forma de, ao se concentrar esta prerrogativa nas mãos do Estado, desencorajar-se a vingança pessoal. Ao mesmo tempo, o direito à liberdade constitui projeção do *status negativo,* já que os direitos e garantias individuais são instrumentos de limitação ao exercício da atividade perscrutatória estatal, impondo-se que o Estado não interfira indevidamente na esfera de liberdades do cidadão sem justo motivo e, sempre que o faça, deverá estrita obediência ao devido processo legal e às garantias legais e constitucionais aplicáveis à espécie. Vide: GOMES DA SILVA, Paulo Thadeu. *Direitos Fundamentais. Contribuição para uma teoria geral.* São Paulo: Editora Atlas, 2010, p. 99-102).

[100] SAAD, Marta. *O direito de defesa no inquérito policial*. São Paulo, Revista dos Tribunais, 2004, p. 206-206.

[101] A perspectiva dogmática-penal de que o Direito Penal teria a finalidade de estabilização do sistema social através de suas próprias normas sistemáticas, de modo que a punição estaria intrinsecamente relacionada ao descumprimento da norma enquanto frustração de uma expectativa social. Trata-se da concepção funcionalista sistêmica de Günther Jakobs (EIBE, Manuel José Arias. *Funcionalismo penal moderado o teleológico-*

Entretanto, se a eficiente resposta estatal servirá como forma de concretizar uma parcela deste dever de segurança pública, é certo que os direitos e garantias individuais, enquanto conquistas civilizatórias, não podem ser sobrepujados imotivadamente, em nome de um interesse social vago e difuso de "segurança".

Ainda que a sensação generalizada de insegurança ganhe contornos avassaladores, especialmente em um país com elevadas estatísticas de crimes graves e violentos, o exercício da atividade investigativa e persecutória não poderá flertar com o desrespeito à ordem jurídica preexistente e, especialmente, aos direitos e garantias insculpidos na própria Constituição Federal e nos instrumentos infraconstitucionais, que nela encontrem fundamento de validade.

Ao mesmo tempo, nesta equação composta por valores conciliáveis[102] de eficiência e garantismo, é necessário se estabelecer parâmetros legais, formais e procedimentais[103] que confiram a validade no acesso, apreensão, extração e integração dos dados armazenados em aparelhos celulares[104].

---

valorativo Versus Funcionalismo Normativo o Radical. Doxa: Cuadernos de Filosofia del Derecho, Alicante, n. 29, p. 439-453, 2006)

[102] GRINOVER, Ada Pellegrini. *Lineamentos gerais do novo processo penal na América Latina.* Revista de Processo. São Paulo, v. 15, n. 58, p. 134, 1990, *apud* FERNANDES, Antonio Scarance. *Equilíbrio entre a eficiência e o garantismo*. Revista Brasileira de Ciências Criminais n.º 70/229, jan-fev/2008, p. 745.

[103] O procedimento compreende a projeção externa por intermédio do qual o processo se instaura, desenvolve e termina, atingindo o fim predeterminado e visando a satisfação do interesse tutelado. Trata-se do meio pelo qual a lei determina como os atos devem se desenvolver, em seu conjunto, observando-se fórmulas predefinidas, numa relação de coordenação lógica antecedente através do qual os atos anteriores se relacionam como pressuposto para os atos subsequentes. Assim, para se obter uma decisão justa e adequada, o procedimento deve ser válido e justo, permitindo-se a participação das partes envolvidas e a possibilidade de, à sua medida, trazerem elementos de informação que possam auxiliar na formulação do convencimento do julgador (GRINOVER, Ada Pellegrini; FERNANDES, Antônio Scarance; GOMES FILHO, Antônio Magalhães. *As nulidades no processo penal*. 7.ed. São Paulo: Editora RT, 2001. p. 249-250). Especialmente no processo penal, o procedimento demanda a observância das formalidades prescritas em lei e, ainda, a obediência irrestrita aos princípios constitucionais e à garantia do devido processo legal (TUCCI, Rogério Lauria. *Direitos e garantias individuais no processo penal brasileiro*. São Paulo: Editora Saraiva, 1993. p. 91-94).

[104] Antônio Magalhães Gomes Filho reconhece o direito à prova como um direito subjetivo às partes, que teriam a possibilidade de participar de todas as fases do procedimento respectivo, influindo-se no convencimento do julgador. Ainda, reconhece que o direito à produção da prova percorrerá ao menos cinco etapas distintas: investigação; propositura; admissão; produção; e valoração (GOMES FILHO, Antônio Magalhães Gomes Filho, *Direito à prova no processo penal*, São Paulo: Editora RT, 1997, p. 84). Para Fernando Capez, a incorporação da prova demanda a superação de quatro etapas: proposição, admissão, produção e valoração (CAPEZ, Fernando. *Curso de Processo Penal*. 13ª edição, São Paulo: Editora Saraiva, 2006, p. 309-310). No tocante aos critérios lógicos de admissibilidade da prova e a pertinência e relevância para sua introdução, recomenda-se: BADARÓ, Gustavo Henrique Righi Ivahy. *Direito à prova e os limites lógicos de sua admissão: os conceitos de pertinência e relevância*. In: *Sistema penal e poder punitivo: estudos em homenagem ao prof. Aury Lopes Jr.*, p. 550; 2015; e BADARÓ, Gustavo Henrique Righi Ivahy. *Editorial dossiê "Prova*

A legalidade exigirá que o acesso aos dados armazenados seja realizado em consonância com as disposições processuais e os direitos e garantias individuais insculpidos na Carta Constitucional, dentro dos limites ali estabelecidos para a produção e integração processual da prova digital. Trata-se de elemento que assegura a licitude da atuação persecutória estatal, permitindo-se que, para determinadas finalidades investigativas, a esfera de proteção constitucional à privacidade do cidadão venha a ser mitigada em prol do interesse na prova a ser produzida.

Ainda, o acesso aos dados demandará a observância de uma forma legalmente predeterminada, a fim de que o conteúdo dos aparelhos celulares seja alcançado de forma remota ou mediante a apreensão do suporte eletrônico que armazena os precitados dados.

Finalmente, há de se estabelecer um procedimento para este acesso, enquanto verdadeira projeção da garantia do devido processo legal[105]. Exige-se, pois, que o acesso aos dados armazenados em aparelhos celulares obedeça a uma série de atos e requisitos predefinidos, notadamente com relação aos meios de busca e produção da prova, sob pena de tingir os elementos amealhados pelas cores da ilicitude e da inadmissibilidade.

Ao mesmo tempo, imprescindível se avançar na sistemática a ser observada para o acesso a estes dados armazenados, especialmente no tocante à imprescindibilidade de ordem judicial autorizativa, distinguindo-se também as situações fáticas relacionadas ao momento deste acesso, a fim de se constatar se, em todas elas, a chancela judicial se revela necessária.

---

penal: fundamentos epistemológicos e jurídicos". In: Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 4, n. 1, p. 43-80, jan.-abr. 2018.

[105] O "devido processo legal" constitui expressão com múltiplas definições, podendo ser entendido como o "(...) "conjunto de garantias constitucionais que, de um lado, asseguram as partes o exercício de suas faculdades e poderes processuais e, do outro, são indispensáveis ao correto exercício da jurisdição (...)" (CINTRA, Antônio Carlos de Araújo; GRINOVER, Ada Pellegrini; DINAMARCO, Candido Rangel. *Teoria Geral do Processo*. São Paulo: Malheiros, 2001, p. 89) e também, em sua faceta material, como elemento de controle quanto à racionalidade e razoabilidade dos atos normativos jurídicos emanados do poder público (BARROSO, Luís Roberto. *Interpretação e aplicação da Constituição: fundamentos de uma dogmática constitucional transformadora*, 4ª Edição, São Paulo: Saraiva, 2001, p. 214).

2. AS PROVAS E DOCUMENTOS DIGITAIS

2.1. Provas e documentos digitais: noções conceituais e características

Dentro desta nova realidade e lidando com um novo formato de provas, desta vez sob a via digital, avança-se para a necessidade de se debater sobre as características e a conceituação de *provas digitais*, bem como sobre aspectos relacionados aos meios de produção e de busca de prova digitais.

Com efeito, o conceito de *prova* é dotado de múltiplos e distintos significados no campo científico e jurídico[106], podendo inclusive transcender aspectos meramente técnicos para alcançar também fatores políticos, sociais e culturais[107].

Uma das definições clássicas sobre prova é trazida por ADA PELLEGRINI GRINOVER, ANTÔNIO CARLOS DE ARAÚJO CINTRA e CÂNDIDO RANGEL DINAMARCO, para quem prova é um *"instrumento por meio do qual se forma a convicção do juiz a respeito da ocorrência ou inocorrência dos fatos controvertidos no processo*"[108].

Avançando-se sobre a definição de *prova*, ANTÔNIO MAGALHÃES GOMES FILHO e MICHELE TARUFFO propõe uma divisão classificatória da prova, enquanto: (a) demonstração, quando tem a pretensão de "estabelecer a verdade sobre determinados fatos"; (b) experimentação, como "atividade ou procedimento destinado a verificar a correção de uma hipótese ou afirmação" e (c) desafio, como "obstáculo que deve ser superado como condição para se obter o reconhecimento de certas qualidades ou aptidões"[109].

---

[106] Tendo em vista que a pretensão do trabalho está circunscrita ao acesso aos dados e os meios de busca e de produção de prova a ele relacionados, opta-se por não se realizar uma avançada digressão histórica e conceitual sobre o tema.

[107] GOMES FILHO, Antônio Magalhães. *Direito à prova no processo penal.* São Paulo: Editora RT, 1997, p. 18.

[108] CINTRA, Antônio Carlos de Araújo; GRINOVER, Ada Pellegrini; DINAMARCO, Candido Rangel. *Teoria Geral do Processo*. São Paulo: Editora Malheiros, 2001, p. 349.

[109] GOMES FILHO, Antonio Magalhães. Notas sobre a terminologia da prova (reflexos no processo penal brasileiro). In YARSHELL, Flávio Luiz; MORAES, Maurício Zanoide de (coord.). *Estudos em homenagem à professora Ada Pellegrini Grinover*. São Paulo: DPJ, 2005, pp. 303-318; TARUFFO, Michele. La prova dei fatti giuridici. Milano, Giuffrè, 1992, p. 415.

Com o avanço tecnológico que promoveu sensível alteração na realidade social, tem-se tornado ainda mais necessário avançar sobre o estudo da prova digital, cujo conceito pode ser extraído a partir da expressão "digital evidence" (utilizada para definir "prova digital" na doutrina norte-americana). Para EOGHAN CASEY, a "digital evidence" pode ser definida como "(...) any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi (...)"[110].

Ainda tomando-se as lições de CASEY, outras definições podem ser estabelecidas para a expressão "digital evidence"*:* (i) todo dado que pode estabelecer que um crime foi cometido ou pode proporcionar uma ligação entre o crime e sua vítima ou entre o crime e seu autor; (ii) toda informação de valor probatório que é armazenado ou transmitido no formato digital[111]; (iii) a informação armazenada ou transmitida de forma binária que pode ser levada à apreciação da Corte Judicial[112]; (iv) a informação ou dado investigativo armazenado ou transmitido por intermédio de um computador[113]; (v) o dado digital que confirma ou refuta uma hipótese sobre eventos digitais ou o estado de dados digitais.

Para THAMAY e TAMER, a prova digital consiste no:

> instrumento jurídico vocacionado a demonstrar a ocorrência ou não de determinado fato e suas circunstâncias, tendo ele ocorrido total ou parcialmente em meios digitais ou, se fora deles, esses sirvam como instrumento para sua demonstração. A prova digital é o meio de demonstrar a ocorrência de um fato ocorrido em meio digital, o que tem no

---

[110] CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers and the internet.* 3th Edition, Ed. Elsevier, 2011, p. 7, a partir do conceito trazido por CHISUM, J. W. *Crime reconstruction and evidence dynamics*. 1999. Presented at the Academy of Behavioral Profiling Annual Meeting. Monterey, CA. A mesma definição, diante de sua relevância, é rememorada por Giovanni Ziccardi (ZICCARDI, Giovanni. *Informatica giuridica. 2: Privacy, sicurezza informatica, computer forensics e investigazioni digitali.* Milano: Ed. Giuffrè, 2008, p. 271).

[111] Definição trazida pela Standard Working Group on Digital Evidence (SWGDE), em *Proposed Standards for the Exchange of Digital Evidence Scientific Working Group on Digital Evidence (SWGDE)*, April 2000, vol. 2, n. 2, tradução livre.

[112] Definição da International Organization of Computer Evidence (IOCE) (ZICCARDI, Giovanni. *Informatica giuridica. 2: Privacy, sicurezza informatica, computer forensics e investigazioni digitali.* Op. cit. p. 272, tradução livre).

[113] Definição dada pela Association of Chief Police Officers (CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers and the internet.* Op. cit. 7, tradução livre).

> meio digital um instrumento de demonstração de determinado fato de seu conteúdo (THAMAY, Rennan; TAMER, Mauricio. *Provas no direito digital. Conceito da prova digital, procedimentos e provas digitais em espécie.* São Paulo: Editora RT, 2020, p. 33).

Destarte, seriam consideradas provas digitais tanto os fatos ocorridos por meios digitais (*v.g.*, a prova de um crime de invasão de dispositivo informático) quanto aqueles em que o meio digital sirva de instrumento para demonstrar a existência de um fato ocorrido em meio não digital (*v.g.*, por intermédio da prova digital é possível se identificar a localização de uma vítima sequestrada).

Todavia, esta concepção abrangente não é compartilhada por toda a doutrina, que vislumbra uma distinção técnica entre a prova digital e a prova eletrônica. Com efeito, a categoria de provas eletrônicas é gênero da qual se inclui a prova digital, pois compreenderia todo e qualquer documento acessível e interpretável por um equipamento eletrônico (*v.g.*, uma câmera fotográfica, uma filmadora, etc.)[114]. Não seria necessário, portanto, que o valor probatório tenha sido criado de forma digital, por intermédio de um computador.

Assim, um documento originalmente analógico que conserve essa formatação ou que venha a ser digitalizado pode ser considerado um documento eletrônico e, caso detenha relevante valor de interesse para comprovação ou refutação de uma hipótese fática debatida, é considerada uma prova eletrônica.

Já a prova digital, por sua vez, abrange os documentos eletrônicos de relevante valor probatório que sejam codificados em dígitos binários e acessado por instrumento computacional. Nesta ordem, todo documento digital é, ao mesmo tempo, um

---

[114] Na precisa definição de Joaquín Delgado Martín, "(...) por prueba electrónica cabe entender toda información de valor probatorio contenida em un medio electrónico o transmitida por dicho medio. En esta definición cabe destacar los siguientes elementos: se refiere a cualquier clase de información; que ha ser producida, almacenada o transmitida por medios electrónicos; y que pueda tener efectos para acreditar hechos en el proceso abierto para la investigación de todo tipo de infracciones penales, y no solamente para los denominados delitos informáticos. De esta manera, la fuente de la prueba radica en la información contenida o transmitida por medios electrónicos, mientras que el medio de prueba será la forma a través de la cual esa información entra en el proceso: normalmente como prueba documental o como prueba pericial, pero también incluso a través de la prueba testifical mediante el testimonio de la persona que ha tenido contacto con el dispositivo electrónico (...)" (DELGADO MARTÍN, Joaquín. *La prueba electrónica em el proceso penal.* Diario La Ley, Nº 8167, Sección Doctrina, 10 Oct. 2013, Año XXXIV, Editorial LA LEY, p. 1).

documento eletrônico, mas nem todo documento eletrônico assume a característica de digital.

Denota-se que o conceito de provas digitais não se dissocia da acepção terminológica de provas pelos meios convencionais. Com efeito, ambas se prestam a confirmar ou refutar um fato suscitado, contribuindo na formação do convencimento das partes e do julgador. Todavia, as provas digitais têm um propósito maior, podendo ser mais sensíveis em razão da vastidão de dados que contemplam, móvel e demandar a utilização de ferramentas e conhecimento tecnológico para lidar com seu formato[115].

Nas palavras de DENISE VAZ, as provas digitais são "(...) 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 (...)"[116].

As provas digitais gozam de algumas características que demandam a observância de certas peculiaridades no tocante à forma de acesso, extração, arquivamento e validação, dentre as quais se destacam sinteticamente:

a) *imaterialidade*: as provas digitais consistem em verdadeiros impulsos elétricos autônomos, não palpáveis, que se revelam a partir da utilização de um recurso tecnológico. Embora o suporte físico seja necessário para se revelar os contornos

---

[115] GOODISON, Sean E., DAVIS, Robert C., JACKSON, Brian A. *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*. Santa Monica, CA: RAND Corporation, 2015, p. 3. Disponível em <https://www.rand.org/pubs/research_reports/RR890.html>, Acesso em: 20 de dezembro de 2020.
Ainda no tocante à prova digital e a necessidade de preservação das fontes digitais, Guardia adverte que "(...) a complexidade técnica da investigação ou a urgência para assegurar fontes de provas não podem justificar a delegação à polícia de funções ligadas a faculdades judiciárias instrutoras. A pré-constituição probatória figura como intolerável fonte de fragilização da via judicial que converte o juiz em mero agente de convalidação de decisões previamente tomadas (...)" (GUARDIA, Gregório Edoardo Raphael Selingardi. *Comunicações Eletrônicas e dados digitais no processo penal*. Tese (Mestrado em Direito Processo Penal) – Faculdade de Direito, Universidade de São Paulo, 2016, p. 141).

[116] VAZ, Denise Provazi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório*. Tese (Doutorado em Processo Penal) - Faculdade de Direito da Universidade de São Paulo, 2012, p. 63. Citando *Eoghan Casey*, a autora estabelece uma distinção entre as provas digitais e as provas eletrônicas, sendo esta utilizada para se referir ao suporte físico onde os dados estariam armazenados (*v.g.*, o aparelho celular), ao passo que as provas digitais seriam efetivamente, o conteúdo dos dados extraídos da precitada base tecnológica. No mesmo sentido: DANIELE, Marcelo. *La prova digitale nel processo penale.* Rivista di Diritto Processuale Anno LXVI (Seconda Serie) – n. 2, Marzo – Aprile, 2011, p. 284.

existenciais da prova, não é condição de sua existência, porquanto os dados digitais podem ser transferidos livremente para outros dispositivos sem que perca sua forma ou essência[117];

b) *volatilidade:* trata-se de característica derivada da imaterialidade e consiste na variabilidade da prova digital, a qual não é perene e possui uma preocupante facilidade de desaparecimento. Um problema técnico irrecuperável em um *hardware,* a sobreposição de gravações e o desaparecimento de um arquivo temporário são exemplos de dificuldades técnicas que podem levar ao desaparecimento da prova produzida, comprometendo-a enquanto elemento valorativo[118];

c) *fragilidade:* a prova digital, para além de volúvel, é facilmente modificável, alterável ou manipulável por qualquer pessoa, não apenas pelo criador mas, sobretudo, por terceiros que tenham tido contato com a prova, inclusive os investigadores durante sua aquisição e análise[119]. A fragilidade do dado o torna refém de atitudes deliberadas para sua manipulação ou destruição ou, ainda, a meros erros procedimentais na escolha do método para extração do dado, o que pode comprometê-lo[120];

d) *intrusividade:* a busca da prova digital permitirá que, diante da sua forma de armazenamento, se tenha acesso a uma gama variada de dados que estejam relacionados à intimidade e privacidade do titular. Assim, especialmente considerando que a vasta e diversificada quantidade de dados armazenados em um mesmo suporte, é possível

---

[117] Marcelo Daniele reconhece que "(...) oggi nessuno dubita più del fatto che le prove digitali esistano indipendentemente dai supporti in cui si trovano, i quali sono solo involucri esterni di per sè processualmente irrilevanti. Spesso vi è, anzi, un'assoluta sproporzione tra le prove digitali ed i loro recipienti: un supporto di piccole dimensioni è in gradodi contenere una massa enorme di informazioni digitali (...) Dalla immaterialità discendono ulteriori caratteristiche delle prove digitali, che creano non pochi inconvenienti in rapporto alla loro acquisizione processuale.Si pensi, anzitutto, al rischio della loro dispersione. Molto più frequentemente delle prove tradizionali, le prove digitali di un reato si trovano dislocate in luoghidistanti tra loro: ad esempio in 'servers' e in 'personal computers' fisicamente moltolontani. Considerata l'estensione mondiale delle reti informatiche, potenzialmentela dispersione può riguardare l'intero globo terrestre (...)" (DANIELE, Marcelo. *La prova digitale nel processo penale*, op. cit. p. 285)

[118] Denise Vaz, todavia, ressalva que o dado digital poderá deixar de ser volátil, caso seja armazenado em suporte eletrônico e submetido a técnicas de armazenamento que assegurem a perenidade do dado (VAZ, Denise Provazi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório.* Op. cit. p. 67).

[119] Ministério Público Federal. *Roteiro de autuação: crimes cibernéticos,* 2. ed. rev. – Brasília: MPF/2ª CCR, 2013, p. 172

[120] Como bem menciona John. R. Vacca, "(...) digital evidence is the most easily lost evidence. There's nothing in criminal justice more easily damaged, corrupted, or erased. You need to be able to demonstrate that the evidence is what you say it is, came from where you say it did, and has not been modified in any way since you obtained it (…)" (VACCA, John. R. *Computer Forensics: Computer Crime Scene Investigation.* Second Edition, Charles River Media, p. 238).

que a violação à privacidade ocorra de maneira mais aguda do que na mera pesquisa de dados e elementos físicos[121];

e) *suscetibilidade de clonagem:* a prova digital é passível de ser reproduzida e replicada de forma fiel, mediante espelhamento, com absoluta identidade ao arquivo original. Ademais, as cópias poderão ser utilizadas como elemento de comparação com o arquivo original, a fim de se apurar eventual alteração ou modificação em seu conteúdo e, com isso, atestar-se a utilidade ou imprestabilidade do elemento probatório produzido;

f) *intermediação de equipamento para acesso:* a prova digital, embora de existência autônoma, é processada e disponibilizada por intermédio de equipamentos e ferramentas próprias, razão pela qual dele são dependentes para sua verificação.

2.1.1. A prova digital e sua produção por meio documental

A prova digital poderá ser documentada, ocasião em que será reconhecida na condição de "documento digital"[122], que são os atos, fatos ou dados juridicamente relevantes e que são incorporados em uma base material por meio de um

[121]PINTO PALACIOS, Fernando. PUJOL CAPILLA, Purificación. *La prueba en la era digital.* 1ª Edicion. Madrid: Editora Wolters Kluwer, 2017, p. 26-29. GUARDIA, Gregório Edoardo Raphael Selingardi. *Comunicações Eletrônicas e dados digitais no processo penal*. Op. cit., p. 123-126. Marcelo Daniele trata desta característica sob o nome de *promiscuità,* aduzindo que "(...) Queste prove possono trovarsi collocate in spazi virtuali enormi e pieni di dati di ogni tipo. Non è raro che siano mescolate ad informazioni irrilevanti rispetto al reato, e magari attinenti alla vita privata dell'indagato o di altre persone. Le indagini informatiche, dunque, sono sempre potenzialmente in grado di pregiudicare la riservatezza degli individui. La loro capacità lesiva della 'privacy' è addirittura superiore a quella delle intercettazioni; queste ultime si limitano a carpire le informazioni che la persona intercettata ha deciso di rivelaread altri, mentre l'analisi dei sistemi informatici e delle reti possono rivelare ilcontenuto di intere esistenze: abitudini, opinioni politiche, preferenze di ogni genere (...)" (DANIELE, Marcelo. *La prova digitale nel processo penale,* op. cit. p. 285)

[122] VAZ, Denise Provazi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório.* Op. cit. p. 66-76. Anote-se que, terminologicamente, tem-se tratado de maneira equivalente as provas digitais e os documentos digitais, reconhecendo-se a ambos as mesmas características. Entretanto, Denise Vaz reconhece a prova digital como uma categoria autônoma, razão pela qual não menciona a expressão documento digital ou eletrônico. Ao tratar a prova digital, a autora a distingue da prova documental em geral, por defender que a prova digital exiba um fato ou ideia de maneira mais ampla, possua desprendimento material – já que a prova digital poderia ser alterada ou destruída sem comprometer o seu suporte, o que não ocorreria no tocante ao documento –, bem como por não ser, necessariamente, um registro da representação de forma duradoura

método digital[123], produzidos sem contraditório prévio em sua formação, posteriormente introduzidos ao processo pela via do meio de prova documental.

Dispõe o artigo 232 do Código de Processo Penal que "consideram-se documentos quaisquer escritos, instrumentos ou papéis, públicos ou particulares", sendo certo que, no parágrafo único, o legislador reconheceu que *"*(...) à fotografia do documento, devidamente autenticada, se dará o mesmo valor do original (...)*"*.

Ao mesmo tempo, no artigo 479 do Código de Processo Penal, houve uma inequívoca extensão do conceito de documento. Com efeito, ao se referir aos "documentos" que não poderiam ser juntados antes do tríduo legal, na realização de julgamentos perante o Tribunal do Júri, o legislador reconheceu que *"*compreende-se na proibição deste artigo a leitura de jornais ou qualquer outro escrito, bem como a exibição de vídeos, gravações, fotografias, laudos, quadros, croqui ou qualquer outro meio assemelhado, cujo conteúdo versar sobre a matéria de fato submetida à apreciação e julgamento dos jurados".

A definição de uma concepção sobre documentos pode estar relacionada a uma definição mais restritiva ou ampliativa[124]. Todavia, seja qual a formatação que se pretenda adotar, não se pode ignorar o fato de que o "documento", verdadeiro meio de prova por intermédio do qual os dados são introduzidos no processo, deverá incluir novas formas representativas de fatos, diversas da mera escrita, inclusive em atenção à evolução e desenvolvimento tecnológico.

---

[123] MENDONÇA, Andrey Borges. *Prova documental no processo penal: aspectos relevantes e controvertidos.* In: SALGADO, Daniel Resende. KIRCHER, Luis Felipe Schneider. QUEIROZ, Ronaldo Pinheiro. *Altos Estudos sobre a prova no processo penal*. Ed. Juspodium, 2020, p. 508; TONINI, Paolo. *Manuale di Procedura Penale*, Undicesima edizione, Milano: Editora Giuffè: Milano, 2010, p. 350.

[124] Novamente invoca-se o magistério de Denise Vaz, que discorre com perfeição sob as mais distintas abordagens no tocante à concepção de "documentos", desde as mais restritivas – que enxergam como documento apenas os escritos em papel – até as mais ampliativas, que o tratam como qualquer representação de um fato ou ideia, bem como um objeto qualquer criado para fins probatórios. Ao final, a autora adota uma visão intermediária, para reconhecer os documentos como sendo o "(...) registro da representação de um fato ou ideia, pela intervenção humana, por meio de escrito, imagem ou som, em base material móvel, de maneira duradoura e realizado fora do processo (...)" (VAZ, Denise Provazi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório.* Op. cit. p. 72)

O documento, assim, é "prova histórica real" de fatos, composta por elementos comunicativos, que consistem na representação de um pensamento ou ocorrência; e certificante, com a demonstração de que a representação é exata e exprime a verdade[125].

A despeito de suas peculiaridades, os dados digitais se assemelham à prova documental[126], aplicando-se aos documentos digitais toda a disciplina relacionada à prova documental, com as devidas ressalvas decorrentes das particularidades inerentes às provas digitais.

Com efeito, em ambos são reconhecidos os elementos constitutivos[127] dos "documentos", a saber: um fato representado, que poderá ser um fato, pessoa ou coisa que venha a ser objeto de prova; a representação de um fato, por meios de imagens, palavras, gestos ou sons, a fim de se permitir que um fato se torne conhecido por outras pessoas; a incorporação, que consiste no meio pelo qual a representação é fixada em uma base material, através do registro do fato; e a base material, onde se incorpora a representação e poderá ser analógica ou digital.

Entretanto, os documentos digitais distinguem-se dos documentos tradicionais especialmente no tocante à sua forma de incorporação sobre uma base digital[128]. Em sendo obtido por intermédio de um dispositivo eletrônico ou durante sua transmissão, os dados extraídos são incorporados sobre este formato de base digital, distinta da tradicionalmente analógica[129].

---

[125] BADARÓ, Gustavo Henrique Righi Ivahy. *Processo Penal*, 8ª edição, São Paulo: Editora RT, 2020, p. 573.

[126] Refoge ao propósito do presente trabalho científico a análise da prova documental no processo penal. Assim, o subtópico limitou-se a apontar as semelhanças e distinções relativas à prova documental digital e a prova documental pelo formato "tradicional". Para aprofundamento com relação ao tema da prova documental, suas características e elementos, a forma de produção, o procedimento a ser seguido, seu valor e os limites probatórios de cada um dos meios, recomenda-se: DEZEM, Guilherme Madeira. *Curso de processo penal*. 6. ed., Op. cit, p. 666-696 e 761-766. BADARÓ, Gustavo Henrique Righi Ivahy. *Processo Penal*, Op. cit., p. 497-511 e 571-576; NUCCI, Guilherme de Souza. *Curso de processo penal.* 17ª Edição, São Paulo: Gen/Forense, 2020, p. 446-469 e 548-555; MENDONÇA, Andrey Borges. *Prova documental no processo penal: aspectos relevantes e controvertidos.* In: *Altos Estudos sobre a prova no processo penal*. Ed. Juspodium, 2020, p. 430-523.

[127] TONINI, Paolo. *Manuale di Procedura Penale.* Op. cit. p. 349-352.

[128] Denise Vaz reconhece que as principais precauções relacionadas às provas digitais, quando cotejadas com a análise dos documentos tradicionais, diz respeito à autenticidade, identificação de autoria e consequente valor probatório, além do acesso aos sujeitos processuais à fonte de prova (VAZ, Denise Provazi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório.* Op. cit. p. 114).

[129] Marcelo Daniele reconhece que "(...) oggi nessuno dubita più del fatto che le prove digitali esistano indipendentemente dai supporti in cui si trovano, i quali sono solo involucri esterni di per sè processualmente

Extrai-se, pois, a importância do suporte eletrônico que armazenam as informações, haja vista que, como bem destacam MARINONI e ARENHART, "(...) a confiabilidade da prova documental – e a importância singular que os ordenamentos processuais lhe emprestam – assenta-se, exatamente, na estabilidade do suporte em que a informação é registrada (...)"[130].

Algumas peculiaridades, próprias das características dos documentos digitais, merecem atenção especialmente no que se refere no tocante à obtenção da prova e sua correspondente valoração.

Especialmente em razão de sua volatilidade, a produção e captura do documento digital deve ser dar de forma rápida, com o fito de se assegurar a preservação do máximo de elementos que guarneçam e integrem a prova, especialmente diante dos dados em tráfego. Ao mesmo tempo, tão logo o documento seja produzido, há necessidade de sua fixação em uma base material acessível no futuro, reduzindo-se sobremaneira as chances de alterabilidade e preservando-se a integralidade e autenticidade da prova produzida[131].

Outrossim, para fins práticos e com o claro intuito de se direcionar o documento à representação do fato ou ideia que se pretenda comprovar, há necessidade de organização e filtragem destes documentos digitais, geralmente abundantes em razão da enorme capacidade de armazenagem dos dispositivos eletrônicos que os contém[132].

Por derradeiro, a documentação da prova digital é considerada válida por expressa disposição do artigo 11 da Lei n.º 11.419/2006, desde que assegurados dois elementos essenciais: autenticidade e integridade, que demandarão a observação da cadeia de custódia[133].

---

irrilevanti. Spesso vi è, anzi, un'assoluta sproporzione tra le prove digitali ed i loro recipienti: un supporto di piccole dimensioni è in gradodi contenere una massa enorme di informazioni digita (DANIELE, Marcelo. *La prova digitale nel processo penale,* op. cit. p. 285)

[130] MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. *Prova*. 2ª edição, São Paulo: Editora RT, 2011, p. 563-564.

[131] MENDONÇA, Andrey Borges. *Prova documental no processo penal: aspectos relevantes e controvertidos.* Op. cit. p. 511.

[132] VAZ, Denise Provazi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório.* Op. cit. p. 78.

[133] Vide Capítulo 7.

A autenticação é o processo estabelecido para se garantir que o elemento probatório é, exatamente, o que ele se propõe a ser. Assim, compete à parte que apresentou a prova digital comprovar sua veracidade e genuinidade, especialmente de forma a se identificar o autor do documento. Assim, *ad exemplum,* o órgão acusatório deverá demonstrar que uma mensagem supostamente encaminhada pelo investigado a um terceiro foi, efetivamente, emitida e enviada pelo dispositivo eletrônico pertencente ao investigado.

A autenticidade do documento, no ordenamento jurídico brasileiro, pode se dar através da assinatura eletrônica de documentos (artigo 411 do Código de Processo Civil), emitidos geralmente pela certificação digital. Entretanto, os documentos digitais não providos de uma certificação que lhes permita reconhecer a autenticidade podem ser comprovados por intermédio de outras formas digitais, tais como o registro de acesso a páginas, o *Internet Protocol (IP),* os dados cadastrais utilizados no aplicativo por intermédio do qual a mensagem foi enviada, dentre outros meios[134].

Ainda, a higidez do documento é essencial, como forma de se garantir que a prova não fora alterada indevidamente. Para tanto, extrai-se a imprescindibilidade de se observar a cadeia de custódia da prova, a fim de assegurar que o documento apresentado em Juízo é exatamente o mesmo que fora apreendido no aparelho celular do investigado e não sofreu qualquer alteração ou supressão.

Diante destas características e, especialmente, das peculiaridades da prova digital com relação à sua introdução no processo na qualidade de prova documental ou pericial, é inegável reconhecer que a busca e produção da prova digital exige novas

---

[134] Importante destacar que, no cenário americano, a *Federal Rules of Evidence,* adotada em alguns Estados como regras elementares para se assegurar a validade e eficácia da prova, permite que a autenticação se dê pela via testemunhal, tal como, *verbi gratia,* o depoimento do agente público que efetuou a busca no celular ou no computador e pode testemunhar onde e como os arquivos e dados foram apreendidos. Ademais, um aspecto importante relacionado às provas digitais é a sua confiabilidade, o que poderá ser atestada por intermédio de métodos científicos confiáveis pela comunidade científica, o que vem causando grandes adversidades diante das novas formas de tecnologia. Sobre o tema, confira-se: GOODISON, Sean E., DAVIS, Robert C., JACKSON, Brian A. *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*. Santa Monica, CA: RAND Corporation, 2015, p. 11-12, Disponível em <https://www.rand.org/pubs/research_reports/RR890.html>. Acesso em 20 de dezembro de 2020).

formas, métodos e ferramentas que permitam assegurar a credibilidade e confiabilidade da prova[135].

2.1.2. A prova digital e sua produção por meio pericial

Após a introdução no processo, a prova documental digital poderá vir a ser submetida a exame pericial, cuja disciplina encontra-se inserida nos artigos 158 a 164 do Código de Processo Penal. A perícia consiste em um exame que demanda a invocação de conhecimentos técnicos, científicos, jurídicos e artísticos, subministrando fundamentos ao julgador e as partes que estariam fora da órbita do saber ordinário[136].

A natureza jurídica da prova pericial é controversa: ao mesmo tempo em que pode ser considerada meio de prova[137], no âmbito de inquéritos policiais ou

---

[135] Como bem aponta Armando Ramos, a evidência digital "(...) não se compraz com os velhos métodos de busca que se realizavam (e continuam a realizar) na descoberta de provas de outros tipos de criminalidade. Ela exige novas formas, novos métodos e ferramentas informáticas específicas conducentes a uma recolha de prova digital que possam ser indubitáveis e credíveis em sede de audiência e julgamento (...)" (RAMOS, Armando Dias. *A prova digital em processo penal: o correio eletrônico*. Lisboa: Ed. Chiado, 2014, cap. 2.3, p. 103-105)

[136] LOPES JR., Aury. *Direito Processual Penal.* São Paulo: Saraiva, 2020, p. 469.

[137] BADARÓ, Gustavo Henrique Righi Ivahy. *Processo Penal*, Op. cit., p. 434; TONINI, Paolo. *Manuale di Procedura Penale*. Op. cit. p. 327.

Impende estabelecer uma distinção classificatória entre os "meios de prova" e os "meios de produção ou obtenção de prova". Com efeito, os meios de provas são os "instrumentos e atividades" (GOMES FILHO, Antonio Magalhães. *Notas sobre a terminologia da prova (reflexos no processo penal brasileiro)*. Op. cit, p. 308), que servem de liame introdutório dos elementos de prova ao processo, visando sua produção a partir das fontes de provas, com o objetivo de se chegar ao resultado da prova. Para Cândido Rangel Dinamarco, são as "*técnicas destinadas a atuar sobre fontes e delas se extrair o conhecimento dos fatos relevantes para a causa*" (DINAMARCO, Cândido Rangel. *Instituições de Direito Processual Civil*. São Paulo: Malheiros, 2001, vol. III, p. 47). Seriam "(...) todos los elementos que pueden servir para producir el convencimento judicial (...)" (ROMERO COLOMA, Aurelio. *Estudios de la prueba procesal*, Madrid, Colex, 1986, p. 39), vale dizer, "(...) todo aquello que permite conocer los hechos relevantes de la causa; es decir, lo que 'permite formular o verificar' enunciados asertivos que sirven para reconstruir esos hechos (...)" (GASCÓN ABELLÁN, MARINA, *Los hechos en el Derecho. Bases argumentales de la prueba*, Marcial Pons, 1ª edic., Madrid, 1999, pp. 83-86).

Os meios de prova, todavia, não se confundem se distinguem de outro conceito semelhante, consistente nos meios de pesquisa (também chamados de meios de investigação e meios de busca da prova), uma distinção conceitual que fora objeto de expressão previsão no Código de Processo Penal Italiano, mas que não se repetiu no ordenamento processual pátrio. Sobre o tema, confira-se: TONINI, Paolo. CONTI, Carlotta. *Il diritto delle prove penali*. 1ª *edizione aggiornata*, Ed. Giuffrè, 2011, 379-380.

Assim, enquanto os meios de prova se referem a "(...) uma atividade endoprocessual que se desenvolve perante o juiz, com o conhecimento e participação das partes, visando a introdução e a fixação de dados probatórios no processo (...)", os meios de pesquisa ou investigação estão relacionados aos procedimentos, geralmente anteriores à formação da relação jurídica processual, com "(...) o objetivo de conseguir provas materiais, e que podem ser realizados por outros funcionários (...)" (GOMES FILHO, Antonio Magalhães. *Notas sobre a terminologia da prova*. Op. cit. p. 309-310). A utilidade da definição terminológica se extrai no tocante à análise de possíveis repercussões das irregularidades verificadas em relação a ambos, haja vista que, em vícios apresentados com relação ao meio de prova, a consequência seria a nulidade dos elementos da prova produzida, ao passo que as irregularidades nos meios de pesquisa acarretarão a inadmissibilidade da prova, por violação às regras atinentes à Para Marcos Alexandre Coelho Zilli, os meios de prova constituem os instrumentos que

procedimentos ministeriais próprios, visando a formação de *opinio delicti*, pode também assumir a condição de meio de investigação e de prova[138]. Ainda, alguns a situam em um patamar distinto, revelando-a como instrumento de auxílio valorativo ao convencimento do julgador, situando-se em um local autônomo entre a prova e a sentença[139].

Embora seja inegável o grande relevo probatório conferido à prova pericial, especialmente diante de seu cunho eminentemente técnico, é de grande valia a advertência de AURY LOPES JR., para quem, rememorando-se a exposição de motivos do Código de Processo Penal, sustenta que todas as provas são relativas e nenhuma delas terá, *ex vi*, valor decisivo ou prestígio superior a outras[140], especialmente em um sistema pautado pelo livre convencimento motivado, o que afasta qualquer prévia vinculação do julgador a uma ou outra prova.

Para TONINI, a prova pericial tem o objetivo de *a)* realizar investigações para adquirir dados probatórios; *b)* adquirir os mesmos dados, selecionando e interpretando-os; *c)* realizar avalições sobre os dados já adquiridos[141].

Especificamente com relação à prova digital, bem destaca VAZ, a prova pericial poderá ser necessária para a pesquisa da prova, nas hipóteses de apreensão remota dos dados; para a captação da prova e a realização de procedimentos técnicos para a interceptação de dados ou para cópia de um dispositivo; para a análise dos dados apreendidos e sua separação; e também para a constatação da autenticidade dos dados e eventuais modificações da prova[142], destacando ainda que, nas duas primeiras hipóteses, o trabalho

---

"(...) levam ao conhecimento dos sujeitos processuais os fatos (...)" ao passo que os meios de "busca de prova" (expressão utilizada pelo autor) são as "(...) próprias medidas tendentes à busca, à coleta, à obtenção, enfim, de provas (...)" para posterior instrumentalização e transporte até o processo (ZILLI, Marcos Alexandre Coelho. *A iniciativa instrutória do juiz no processo penal.* São Paulo: RT, 2003).
Ainda, os meios de pesquisa, busca ou investigação da prova, via de regra, seriam realizados sem o conhecimento da parte investigada – sob pena de se comprometer a obtenção das fontes materiais de prova – e não constituem efetivas fontes de conhecimento, mas mero instrumento para se chegar às fontes de provas, por meio das quais a Polícia e o Ministério Público poderão requerer a produção dos elementos de prova.

138 SOARES, Gustavo Torres. *Investigação criminal e inovações técnicas e tecnológicas: perspectivas e limites.* Op. cit., p. 235-236.

139 TORNAGHI, Hélio. *Curso de processo penal*. 7ª. Ed. São Paulo: Saraiva, 1990, p. 313.

140 LOPES JR., Aury. *Direito Processual Penal.* Op. cit, p. 470.

141 TONINI, Paolo. *Manuale di Procedura Penale.* Op. cit. p. 327.

142 VAZ, Denise Provazi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório.* Op. cit., p. 116.

pericial auxiliará na captação da prova digital, ao passo que as etapas finais seriam, propriamente ditas, o meio de prova pericial.

De igual sorte, a prova pericial poderá ser capaz de afiançar a integralidade e autenticidade da prova, mormente considerando que as provas digitais, em razão de suas características peculiares, são imateriais, frágeis e voláteis, de modo que a ausência de padrões seguros para a busca, identificação, captação, análise e documentação dos dados poderá comprometer sobremaneira seu grau de convencimento ou, ainda, prejudicar sua própria admissibilidade[143].

2.2. Meios de obtenção e produção de prova atípicos

O legislador processual, ainda que de forma não expressa, optou por se desvincular de um sistema rígido de taxatividade dos meios de prova, admitindo-se analogicamente (artigo 3º do Código de Processo Penal) a liberdade na produção da prova[144], nos termos do artigo 369 do Código de Processo Civil. Assim, o ordenamento jurídico admite a utilização de meios de produção de provas atípico[145].

Entretanto, esta liberdade probatória não é irrestrita. Com efeito, os meios de prova atípicos, para serem admissíveis, estão condicionados[146] à licitude da prova

---

[143] Para os propósitos específicos do presente trabalho científico, especialmente no que tange à localização, captação, extração e produção da prova dos dados armazenados em aparelhos celular, o tema será melhor explorado no capítulo pertinente à "cadeia de custódia".

[144] SCARANCE FERNANDES, Antonio. *Tipicidade e sucedâneos de prova*. In: SCARANCE FERNANDES, Antonio; GAVIÃO DE ALMEIDA, José Raul; ZANOIDE DE MORAES, Maurício (coord.). *Provas no Processo Penal: estudo comparado*. São Paulo: Saraiva, 2011. p. 28-29*;* DEZEM, Guilherme Madeira. Curso de processo penal. 6ª edição, São Paulo: Revista dos Tribunais, 2020, p. 600-601.

[145] Para Aury Lopes Jr., "(...) como regra, somente podem ser admitidas as provas tipificadas no CPP. Excepcionalmente, podem ser admitidas provas atípicas ou inominadas, desde que não constituam subversão da forma estabelecida para uma prova nominada e, ainda, guardem estrita conformidade com as regras constitucionais e processuais atinentes à prova penal (...)" (LOPES JR., Aury. *Direito Processual Penal.* Op. cit. p. 425-426). A livre produção de provas também é princípio adotado pela legislação francesa. Conforme leciona Michèle-Laure Rassat, "(...) on sait que la question des différents modes de preuve utilisable dans un procès pénal est régie par deux principes fondamentaux et apparemment contradictoires déjà énoncés : le principle de la liberté de la preuve que autorise le recours à n'importe quel mode de preuve et le principle de la légalité de la preuve qui ne permet d'utiliser celle-ci qu'autanto qu'elle n'est pas proscrite et a été recueille et présentée selon les modes procéduraux qui lui sont propres, compte tenu de sa nature et du stade de la procédura auquel on se trouve. Il y a, en effet, un lien étroit entre chaque type de preuve et une procédure de rassemblement et de production spécifiques (...) " (RASSAT, Michèle-Laure. *Procédure pénale,* 3e édition : Ellipses, 2017, p. 284).

[146] DEZEM, Guilherme Madeira. *Da prova penal: tipo processual, provas típicas e atípicas (Atualizado de acordo com as Lei 11.689/08, 11.690/08 e 11.719/08).* Campinas: Ed. Millenium, 2008, p. 275 e ss.

a ser produzida, em observância ao disposto no artigo 5º, inciso LVI, da Constituição Federal e artigo 157, *caput*, do Código de Processo Penal.

Assim, não se admite que o meio atípico constitua afronta a qualquer direito fundamental, bem como às regras de proibição de prova[147], devendo ainda respeitar o direito de defesa e os valores da dignidade da pessoa humana[148], além de serem idôneos à produção de um resultado útil ao processo.

De igual sorte, a legislação processual não contempla um procedimento padrão a ser utilizado em situações de meios atípicos. Torna-se necessária, pois, a prévia existência de um meio de prova típico, com procedimento probatório definido em lei, que possa ser aplicado em analogia ao meio de prova atípico pretendido[149], respeitadas suas peculiaridades[150].

Outrossim, a utilização da prova atípica exige a comprovação de que nenhum outro meio de prova típico, com procedimento positivado em lei, alcance o mesmo resultado pretendido, sob pena de se produzir inadvertidamente a prova anômala[151].

---

[147] DEZEM, Guilherme Madeira. *Curso de processo penal*. Op. cit. p. 777.

[148] MARQUES, José Frederico. *Elementos de Direito Processual Penal.* 3ª Atualização, vol. II, Campinas: Millenium Editora, 2009, p. 270-271.

[149] GOMES FILHO, Antonio Magalhães; BADARÓ, Gustavo. *Prova e sucedâneos da prova no processo penal brasileiro*. Revista Brasileira de Ciências Criminais, São Paulo, v. 15, n. 65, p. 175-208, mar./abr., 2007, p. 185. Como salienta Antônio Scarance Fernandes, *"(...) em geral, não se prevê procedimento probatório-tipo que pudesse, em linhas gerais, servir para a obtenção ou a produção de toda prova atípica, sendo difícil essa solução porque o rito a ser adotado depende de particularidades inerentes à forma de colheita da prova atípica. Mais usual é a remissão ao rito de um meio de prova similar (...)"* (FERNANDES, Antônio Scarance. *Tipicidade e sucedâneos de prova*. Op. cit. p. 29). Para Guilherme Madeira Dezem, para o uso da analogia, deve se considerar como semelhantes as provas quando o verbo da conduta for similar (DEZEM, Guilherme Madeira. *Curso de processo penal*. Op. cit. p. 770).

[150] Como bem define Guilherme Madeira Dezem, as regras a serem observadas para a produção da prova atípica são, necessariamente, "(...) a) a prova, como regra, deve ser praticada em juízo, sob o pálio do contraditório. Somente se admite sua produção fora dele quando a natureza do meio de prova o exigir; b) somente se admite a produção da prova atípica no inquérito policial quando houver cautelaridade a justificar tal medida ou quando a própria lei indica esta possibilidade; c) a vontade pode atuar no meio de prova quando for elemento diretamente a ele ligado; d) somente se afastar a parte da produção da prova quando houver cautelaridade a justificar esta medida ou, então, quando a ciência da parte for contrária à medida, tornando-a ineficaz. Nesta situação, não haverá naturalmente a incidência da regra de discussão com as partes do modelo probatório a ser seguido (...)" (DEZEM, Guilherme Madeira. *Curso de processo penal*. Op. cit., p. 779). O autor defender, ainda, a necessidade de as partes serem consultadas acerca do procedimento de produção de prova a ser observado, em homenagem ao contraditório, ainda que não haja previsão legal expressa.

[151] Com relação às provas, há uma classificação decorrente da tipicidade da prova e a existência de um procedimento a ser observado para se assegurar a genuinidade e a capacidade demonstrativa do referido meio (BADARÓ, Gustavo Henrique Righi Ivahy. *Direito Processual Penal. Tomo I.* Rio de Janeiro: Ed. Elsevier, 2008, p. 200). Destarte, se há um procedimento a ser observado para a execução do meio de prova, este deve ser fielmente seguido, não se podendo ignorá-lo ou, ainda, se valer de outra ritualística procedimental para, sob o manto livre admissão da prova atípica, se adotar o regramento que parecer mais conveniente. Nestes casos,

Não há dúvidas de que a prova atípica, de acordo com SCARANCE FERNANDES "(...) deve estar sujeita a critérios mais rígidos e ser marcada pela excepcionalidade, e, por isso, deve obedecer a parâmetros de validade mais exigentes do que os das provas tipificadas (...)"[152].

Entretanto, importante destacar que a diferenciação qualitativa das provas típicas e atípicas se dá no tocante à sua admissibilidade, não se projetando para aspectos relacionados ao valor de convencimento da prova.

Alcançados estes padrões mais rigorosos relacionados à admissão da prova atípica, é certo que seu valor probatório para ratificar ou refutar os fatos deve ser pleno, sujeitando-se a padrões de avaliação exclusivamente racionais em cada caso concreto[153], com supedâneo na motivação das decisões como garantia de regular e racional aplicação da prova.

No tocante ao "meio de busca de provas atípico", o tema enfrenta maiores resistências[154], já que se poderia cogitar na violação ao princípio da legalidade, à

surge a figura da prova anômala e da prova irritual. A prova irritual é aquela em que a lei estabeleceu um rito processual a ser seguido, mas no momento da produção da prova pretendida este procedimento não é cumprido (BADARÓ, Gustavo Henrique Righi Ivahy. *Provas atípicas e provas anômalas: inadmissibilidade da substituição da prova testemunhal pela juntada de declarações escritas de quem poderia ser testemunha*. In: Yarshell, Flávio Luiz; Moraes, Maurício Zanoide (coords.). *Estudos em homenagem à professora Ada Pellegrini Grinover*. São Paulo: DPJ, 2005, p. 344).
Nota-se que não há a utilização, a reboque, de outro procedimento, mas apenas a inobservância ritual das normas procedimentais aplicáveis àquele meio probatório. A prova anômala tem uma semelhança com a prova irritual, à medida que, novamente, a ritualística processual prevista não é observada. Todavia, diferentemente da prova irritual, a prova anômala ocorre quando se adota, de maneira equivocada, um outro rito processual previsto tipicamente para outra espécie de meio de investigação ou meio de prova. As noções de irritualidade ou anomalia da prova são indistintamente aplicáveis ao meio de pesquisa e ao meio de prova propriamente dito.

[152] FERNANDES, Antônio Scarance. *Tipicidade e sucedâneos de prova*. Op. cit. p. 28.

[153] RICCI, Gian Franco. *Le Prove atipiche.* Milano: Giuffrè, 1999, p. 650-651; LOMBARDO, Luigi, *Profili delle prove civile atipiche*, Rivista trimestrale di diritto e procedura civile, Milano, A. LXIII, n.º 4, Diciembre 2009, p. 1464-1465.

[154] Na mesma linha, sustenta Scarance Fernandes que "(...) o problema da ilicitude coloca-se mais em relação aos meios de investigação ou de obtenção de prova. Como, quase sempre, eles importam restrição ou ameaça de restrição a direitos individuais, a regra deve ser a tipicidade, dependendo a obtenção da fonte de prova de lei que indique as hipóteses em que a restrição será possível e os limites em que será permitida. Somente quando o meio de investigação atípico não interfira em direito individual será possível a sua utilização (...)" (FERNANDES, Antônio Scarance. *Tipicidade e sucedâneos de prova*. Op. cit. p. 28-29).

medida que os meios de busca de prova impõem restrições a direitos e garantias fundamentais, o que exige a presença de requisitos, pressupostos e limites para sua adoção[155].

O artigo 189 do Código de Processo Penal Italiano[156] admite a utilização de meios atípicos, conquanto idôneos para assegurar a veracidade dos fatos discutidos, desde que não infrinjam a liberdade moral da pessoa e permitam a realização do contraditório para admissibilidade do referido meio atípico.

Entretanto, diferentemente do sistema italiano, ordenamento jurídico brasileiro não estabeleceu regra expressa quanto à admissibilidade de "meios de produção e de busca" de provas atípico, embora tenha, em alguns dispositivos legais, estabelecido "meios de produção" sem o correspondente procedimento probatório.

Considerando que a garantia do contraditório é necessária para a admissibilidade dos "meios de busca de prova atípicos*",* estabeleceram-se três correntes acerca do tema[157].

A primeira delas admitiria a existência de meio de busca de prova atípicos, desde que assegurado o contraditório previamente à execução do meio probatório. Portanto, o contraditório seria fator preexistente à produção da prova, sem a qual sua admissibilidade padeceria de vício na origem.

Entretanto, a exigência prévia do contraditório poderá trazer dificuldades práticas. Sem embargos, há meios de busca de prova que exigem, para sua efetividade, a implementação sem o necessário conhecimento prévio da parte contrária, por exigirem um caráter de surpresa a fim de não se frustrar os propósitos investigativos da

---

[155] MORAES, Maurício Zanoide de. *Presunção de inocência no processo penal brasileiro: análise de sua estrutura normativa para elaboração legislativa e para a decisão judicial.* Rio de Janeiro: Editora Lumen Juris, 2012, p. 315-316.

[156] Art. 189.
Prove non disciplinate dalla legge.
1. Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova.

[157] O tema é tratado exaustivamente em: ARANTES FILHO, Márcio Geraldo Britto. *A interceptação de comunicação entre pessoas presentes como meio de investigação de prova no processo penal brasileiro.* Dissertação (Mestrado em Direito Processual Penal) - Faculdade de Direito da Universidade de São Paulo, 2011, p. 63-68.

atividade. Trata-se, em regra, das fontes materiais de prova que estão à disposição do investigado e que ele poderá facilmente inutilizá-las, caso saiba da diligência vindoura, tal como a busca e apreensão.

Todavia, outros meios de busca de prova permitiriam, em tese, a realização do contraditório antecipado, sem que isso acarretasse qualquer prejuízo à diligência. *Ad exemplum*, uma quebra de sigilo bancário não traria prejuízos práticos com a realização prévia do contraditório[158], já que as fontes de prova estariam em poder de terceiros e insuscetíveis de alteração por parte do investigado.

Uma segunda corrente, atenta às peculiaridades da surpresa de alguns meios de busca de provas, vem admitindo que o contraditório poderá ser realizado *a posteriori*, tão logo executado o procedimento de busca das fontes materiais de provas. Ocorreria, nesta hipótese, um contraditório prévio ou diferido, conforme o caso, a fim de se compatibilizar as garantias do acusado com a efetividade da investigação desenvolvida[159].

Finalmente, uma terceira vertente interpretativa militaria pela inadmissibilidade dos meios de busca de prova atípicos.

---

[158] Para Juliana Belloque, os "(...) meios de obtenção de prova, levados a cabo, normalmente, ainda em fase preliminar da persecução penal, têm como traço fundamental o elemento surpresa, para que possam prestar-se à sua finalidade assecuratória. Deste modo, não já que se falar em prévia intimação do defensor do investigado (...)" (BELLOQUE, Juliana Garcia. *Sigilo Bancário: Análise Crítica da LC 102/2001*. São Paulo, Ed. Revista dos Tribunais: 2003, p. 89). Já para Marcus Alan Melo Gomes,"(...) o contraditório no pedido de quebra dos sigilos financeiro, bancário e fiscal há de ser 'prévio', ou seja, anterior à decisão judicial que autoriza ou não o referido meio de obtenção de prova. E deve abranger tanto a matéria de direito quanto de fato, para que se faculte ao investigado ou réu a oportunidade de se contrapor à fundamentação jurídica do pedido – a necessidade ou excepcionalidade da medida podem ser questionadas – bem como de se manifestar sobre os fatos alegados e sua comprovação (...)" (GOMES, Marcus Alan de Melo. *Breve crítica ao afastamento dos sigilos financeiro, bancário e fiscal na Lei nº 12.850/2013*. In: AMBOS, Kai; ROMERO, Eneas (Orgs.). Crime organizado: análise da Lei 12.850/2013. 1ª edição, São Paulo: Editora Marcial Pons, 2017, p. 211).

[159] Paolo Tonini, em sua obra, aponta para a aplicabilidade indistinta aos meios de produção e de busca de provas: "(...) a. Si discute se siano configurabili 'mezzi di ricerca della prova atipici'. L'orientamento minoritario, che nega tale categoria, fa leva sul fatto che i mezzi di ricerca della prova sono posti in essere prevalentemente nel corso delle indagini preliminari, senza previo contraddittorio con la difesa (es. perquisizione o intercettazione). Pertanto, si afferma, sarebbe impossibile dare attuazione all'art. 189 c.p.p. nella parte in cui impone che il giudice senta le parti sulle modalità di assunzione della prova prima di decidere con ordinanza sulla richiesta di ammissione. Tuttavia, la dottrina maggioritaria e, di recente, le Sezioni unite della Cassazione hanno affermato che è ben possibile configurare mezzi di ricerca della prova atipici, come ad esempio le video-riprese di immagini in luoghi diversi dal domicilio. A tal fine, occorre procedere ad una interpretazione adeguatrice dell'art. 189 c.p.p. Qualora si tratti di mezzi di ricerca della prova atipici, anziché configurare un contraddittorio anticipato sulla ammissione nel corso delle indagini, si potrà svolgere un contraddittorio successivo sulla utilizzabilità degli elementi acquisiti (...)" (TONINI, Paolo. *Manuale di Procedura Penale*, Ed. Giuffè: Milano, Undicesima edizione, p. 265).

No cenário brasileiro, parte da doutrina tem inadmitido a utilização de meio de busca de prova atípicos, por ausência de prévia disposição legal[160]. Sustentam, para tanto, a necessidade de uma interpretação restritiva do artigo 369 do Código de Processo Civil, aduzindo que, diferentemente dos meios de produção de prova – em que a produção se dá em Juízo, com prévio controle judicial e contraditório na formação da prova –, os meios de busca de prova seriam realizados, via de regra, sem a possibilidade de um contraditório prévio, com potencial violação a direitos e garantias fundamentais, tais como a inviolabilidade de domicílio, a privacidade e intimidade, dentre outros[161].

Entretanto, não nos parece que a simples atipicidade de meios de busca ou obtenção de provas configure impeditivo absoluto para sua admissibilidade. Neste sentido, valioso o ensinamento de GUSTAVO SOARES, que destaca não ser possível confundir a inovação na seara dos meios investigativos criminais como sinônimo de irritualidade, atipicidade ou extralegalidade, já que as inovações investigativas, ainda que legalmente inominadas e desprovidas de regulamentação, poderão ser validadas judicialmente em juízo de ponderação entre as potencialidades reconstrutivas de cada veículo investigativo, em cotejo com os direitos fundamentais comprimidos e as normas já existentes sobre os temas correlatos, sempre submetidas a um controle jurídico especialmente quanto às condutas adequadas e suas respectivas fundamentações[162].

Entretanto, o autor adverte que a existência de normas procedimentais sobre determinado meio de investigação não pode levar a seu descumprimento ou burla, sob pena de se caracterizar irritualidade, nem tampouco se admitir a utilização de meios investigativos *contra legem* ou *extra legem*, em completa desconexão com a lei ou sem pontos suficientes de extensão ou analogia com outros meios já adequadamente regulamentados[163]. Nestes casos, o meio de investigação ou obtenção de provas seria ilegal.

---

[160] CASTILHOS, Guilherme Machado. POLL, Roberta Eggert. *"E se a sua geladeira pudesse depor contra você no tribunal?": internet das coisas e provas no processo penal brasileiro".* Revista Brasileira de Ciências Criminais, vol. 163/2020, p. 363-391, Jan/2020.

[161] LOPES, Anderson Bezerra. *Os conhecimentos fortuitos de prova no direito processual penal.* Dissertação (Mestrado em Direito Processual Penal) - Faculdade de Direito da Universidade de São Paulo, 2013, p. 119; ARANTES FILHO, Márcio Geraldo Britto. *A interceptação de comunicação entre pessoas presentes como meio de investigação de prova no processo penal brasileiro.* Op. cit. p. 68.

[162] SOARES, Gustavo Torres. *Investigação criminal e inovações técnicas e tecnológicas: perspectivas e limites.* Op. cit., p. 263.

[163] Idem, p. 264.

Ao menos em alguns precedentes jurisprudenciais e acompanhando entendimento doutrinário neste sentido[164], já se admitiu a utilização de meios de busca ou obtenção de provas atípicos. *Ad exemplum,* o Supremo Tribunal Federal (STF), em apreciação à validade das escutas ambientais do revogado artigo 2º, inciso IV, da Lei n.º 9.034/1995, incluída pela Lei nº 10.217/01, julgou ser legítima a utilização do precitado meio de busca mesmo sem a existência de procedimento legal prévio que, à época, o regulamentasse[165].

2.2.1. A ausência de disciplina procedimental para a prova digital e as iniciativas estrangeiras

A *prova digital* não possui disciplina procedimental previamente regulamentada no Código de Processo Penal, sendo considerado verdadeiro meio atípico de obtenção e produção de prova[166]. Muito embora a legislação faça menção aos documentos eletrônicos e digitais e tangencie aspectos relacionados à sua validade quando produzidos eletronicamente ou armazenados nestas formas de suporte – conforme se verifica do artigo 11, *caput,* da Lei n.º 11.419/2006 e artigo 2º-A, § 2º, da Lei n.º 12.682/2012 –, não há regulamentação probatória dos meios de prova e de produção de provas[167].

A ausência de uma previsão relativa aos meios de obtenção de provas digitais conduz à sua absoluta inadmissão. Entretanto, a falta de uma regulamentação própria quanto aos meios de obtenção e produção gera inevitável segurança e potencial afronta a

---

[164] GOMES FILHO, Antônio Magalhães; BADARÓ, Gustavo. *Prova e sucedâneos da prova no processo penal brasileiro*. Op. cit. p. 180-183; FERNANDES, Antônio Scarance. *Tipicidade e sucedâneos de prova*. Op. cit. p. 28-29.

[165] STF, Inquérito n.º 2424, Rel. Min. Cezar Peluso, julgado em 26 de março de 2009, DJe 25/03/2010. Destaque-se que, com o advento da Lei n.º 13.964/2019, foi incluído o artigo 8º-A na Lei n.º 9.296/1996, que passou a regulamentar o precitado meio de prova.

[166] VAZ, Denise Provazi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório.* Op. cit. p. 60 e 80.

[167] Como sustenta Carlos Hélder Carvalho Furtado Mendes, "(...) em um salto de uma década o legislador brasileiro se mantém negligente. A atenção legislativa se volta ao emprego do meio eletrônico na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais conforme a Lei n.º 11.419/06. Todavia, não se avança quanto à temática relativa às provas penais eletrônica, informática ou digital, exceto quando da inclusão de conteúdos probatórios via documentação digital de atos processuais (...)" (MENDES, Carlos Hélder Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software.* São Paulo: Editora Jospodivm, 2020, p. 115).

direitos e garantias fundamentais, por não se estabelecer limites e marcos aceitáveis para utilização destas novas tecnologias[168].

Esta insuficiência legislativa não é uma realidade unicamente brasileira e ganha contornos globais[169]. Nos Estados Unidos, berço da primazia tecnológica e precursor das amplas liberdades individuais, reconhece-se as dificuldades relativas à adaptação desta nova tecnologia ao conteúdo protetivo das emendas constitucionais assecuratórias de direitos e garantias individuais, conforme expõe ORIN S. KERR:

> The problem of digital evidence should inspire the creation of a new criminal procedure, a set of rules that both builds upon and expands from traditional solutions to embrace new and creative mechanisms for regulating evidence collection and use. We should also recognize that the problem of digital evidence extends beyond our borders, and that helpful solutions and insights may be found there. Every industrial country is undergoing the same shifts from physical evidence and eyewitness testimony to digital evidence that is occurring in the United States. We all use the same networks, the same hardware, and the same software. Although different countries have different constitutional traditions and protect different values, all are facing the same basic questions of how to regulate third-party evidence collection, prospective surveillance, and the computer forensics process. By looking broadly for new institutional arrangements and approaches to regulate digital evidence collection, we can open ourselves to the best ideas abroad to supplement the solutions generated from within our constitutional traditions (KERR, Orin S. *Digital Evidence and The New Criminal Procedure*. *Digital Evidence and the New Criminal Procedure.* 105 Columbia Law Review 279 (2005). Disponível

[168] Gustavo E. L Garibaldi reconhece que "(...) la peor actitud frente a tal estado de cosas es la renuncia a toda regulacion, y reconocer el fenómeno como ilimitable em función de sua velocidad de diversificación. Legitimar simplemente certa realidade y renunciar a toda fijación de limites y marcos aceptables de utilización sería uma claudificación inaceptable del Estado de derecho (...)" (GARIBALDO, Gustavo E. L. *Las modernas tecnologias de control y de investigación del delito: su incidência em el derecho penal y los princípios constitucionales.* 1ª Ed. Buenos Aires: Ad-Hoc, 2010, p. 103, *apud* MENDES, Carlos Hélder Furtado. Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software, p. 109).

[169] Daniela Dupuy, analisando-se as perspectivas do direito argentino – mas que são igualmente aplicáveis ao direito processual penal brasileiro -, aponta os desafios a serem enfrentados para investigação de delitos informáticos digitais, dentre eles a adaptação e reforma das normas processuais, adaptando-as inclusive à Convenção de Budapeste, sem prejuízo do fortalecimento dos mecanismos de cooperação internacional e o estreitamento de laços com provedores de *internet*.

em https://ssrn.com/abstract=594101. Acesso em: 20 de dezembro de 2020)[170].

Visando fazer frente a esta insuficiência legislativa, um primeiro passo foi dado com a Convenção sobre *cybercrime*, conhecida por "Convenção de Budapeste". O documento, celebrado em 23 de novembro de 2001 e em vigor desde 1º de julho de 2004, buscou estabelecer uma harmônica política criminal entre os Estados-parte signatários, mediante uma sucessiva alteração do ordenamento jurídico interno a fim de que, no âmbito penal e processual, todos se comprometessem a adaptar a legislação local para investigar e combater, de forma eficiente, a referida criminalidade.

Na Convenção, foram estabelecidas definições conceituais e terminológicas comuns, bem como alinhavadas medidas para se garantir uma relação equilibrada na tutela penal e processual dos delitos informáticos, sempre com a observância aos direitos e garantias fundamentais da liberdade de expressão e privacidade[171].

No espectro penal, por intermédio dos Títulos 1 a 4 da referida Convenção, os Estados-partes se comprometeram a editar medidas legislativas incriminadoras visando zelar pela confidencialidade, integridade e disponibilidade dos sistemas e dados informáticos, a falsidade e a burla perpetradas por meio igualmente

---

[170] Em tradução livre: "O problema da prova digital deve inspirar a criação de um novo procedimento criminal, um conjunto de regras que se baseia e se expande das soluções tradicionais para adotar mecanismos novos e criativos para regulamentar a coleta e o uso de provas. Também devemos reconhecer que o problema da evidência digital se estende além de nossas fronteiras e que soluções e ideias úteis podem ser encontradas lá. Todo país industrial está passando pelas mesmas mudanças de provas físicas e testemunhas oculares para provas digitais, que é o que está ocorrendo nos Estados Unidos. Todos usamos as mesmas redes, o mesmo hardware e o mesmo software. Embora países diferentes possuam tradições constitucionais diferentes e protejam valores igualmente distintos, todos enfrentam as mesmas questões básicas de como regular a coleta de provas em poder de terceiros, a vigilância prospectiva e o processo forense de computadores. Ao procurar amplamente novos arranjos e abordagens institucionais para regular a coleta de evidências digitais, podemos nos abrir para as melhores ideias no exterior para complementar as soluções geradas dentro de nossas tradições constitucionais (...)".

[171] Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;
Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (...)

informático, além do combate à pornografia infantil e à violação aos direitos autorais e conexos.

No âmbito processual e à guisa de exemplo, a Convenção de Budapeste estabeleceu, em seu artigo 19[172], a obrigação dos Estados-partes de adotarem meios legislativos para permitir que as autoridades façam a regular apreensão e coleta de dados armazenados em dispositivos informáticos, além de dispor sobre medidas para preservação da integridade do dado.

O artigo 19.3 dispõe sobre as medidas relacionadas à preservação da integridade da prova, com a subsequente apreensão do próprio suporte físico informático, a cópia e conservação dos dados e o seu armazenamento, visando assegurar sua integridade e evitar desaparecimento e eliminação dos dados informáticos do sistema acessado. Por sua vez, o artigo 19.4 preconiza a necessidade de os Estados promoverem a capacitação das autoridades competentes, para que tenham imersão no sistema informático e saibam adotar medidas para proteção e conservação do conteúdo buscado e apreendido.

Embora a Convenção tenha sido proposta pelo Conselho da Europa, sua participação não se limitou a países europeus, à medida que Japão, África do Sul, Canadá e Estados Unidos também subscreveram os termos do acordo. O Brasil, por sua vez, não

---

[172] Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory.
2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.
3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
a seize or similarly secure a computer system or part of it or a computer-data storage medium;
b make and retain a copy of those computer data;
c maintain the integrity of the relevant stored computer data;
d render inaccessible or remove those computer data in the accessed computer system.
4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15”

figurou como um dos países signatários da Convenção, sendo certo que as recentes medidas penas e processuais são, ainda, verdadeiramente incipientes.

2.2.2. O uso da analogia e os meios de busca e de produção de provas digitais

Como destaca SOARES, a vagarosidade da produção legislativa contrasta com as frequentes alterações da vida em sociedade, de modo que as normas processuais deveriam ser dinâmicas a ponto de alcançar e reger os fenômenos sociais relevantes e contemporâneos. Daí, surgiria a necessidade de o direito processual se valer de instrumentos integradores para a construção de soluções judiciais amoldadas às especificidades de cada caso[173].

Este vácuo legislativo procedimental, por sua vez, vem sendo suplantado pela obtenção e incorporação destas provas mediante a utilização de analogia[174] com outros meios de produção probatória tradicionais[175].

A utilização da analogia não constitui meio de prova anômala ou irritual, haja vista que estas espécies de provas inadmissíveis pressupõem a existência de um procedimento que venha a ser descumprido ou substituído por outro. Como já mencionado, não há procedimento probatório legalmente atribuído às provas digitais.

O sistema normativo processual penal admite, em regra, a utilização da analogia, salvo em hipótese previamente excepcionadas por expressa reserva legal[176]. Portanto, aplicar-se a analogia nos casos admitidos é, em última análise, assegurar-se a aplicação da Lei de Introdução às Normas do Direito Brasileiro e, portanto, prestigiar-se o princípio da legalidade.

---

[173] SOARES, Gustavo Torres. *Investigação criminal e inovações técnicas e tecnológicas: perspectivas e limites.* Op. cit., p. 253.

[174] A analogia é um dos meios de integração jurídica previstos no artigo 4º da Lei de Introdução às Normas do Direito Brasileiro, utilizado para se suprir uma lacuna decorrente da ausência de regulamentação específica, ocasião em que poderá ser utilizada uma regulamentação aplicável a uma situação análoga (DEZEM, Guilherme Madeira. *Curso de processo penal*, op. cit. p. 81).

[175] SALT, Marcos G. *Tecnología informática: um nuevo desafio para el Derecho Procesal Penal?* 1ª ed. Bueno Aires: Ad-hoc, 2017, p. 7, *apud* MENDES, Carlos Hélder Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software*, p. 109.

[176] *Verbi gratia*, a analogia não poderá ser utilizada para se admitir a criação de um crime ou interpretação em desfavor do réu (analogia *in malam partem*), diante do princípio da reserva legal assegurado no tocante à definição de crimes e penas (artigo 5º, inciso XXXIX, da Constituição Federal)

Desta forma, a liberdade probatória e a analogia poderão ser utilizadas para se assegurar a obtenção e produção de novos meios de provas que surjam a partir das mudanças oriundas do dinamismo social e tecnológico, como bem pontua GISELA AGUIAR WANDERLEY:

> a evolução tecnológica impede a normatização precisa de todo e qualquer meio de obtenção de prova. Quebras de sigilo e acesso a dados armazenados em computador, em correio eletrônico ou aparelhos celulares são exemplos de meios de obtenção de prova cuja regulamentação não foi exaurida por meio de lei, mas que ostentam extrema relevância para a investigação penal. Em tal contexto, não é adequado inviabilizar a atividade de persecução penal ao simplesmente cominar de nulo qualquer meio de obtenção de prova ainda não regulamentado em lei específica. Ao revés, é preciso examinar, diante das novas tecnologias existentes, quais critérios, procedimentos e limites devem ser impostos de forma a compatibilizá-las às diretrizes do Estado de Direito. Assim, na ausência de lei específica, o desafio de estabelecer tais requisitos de validade recai sobre o Poder Judiciário e sobre os demais atores do processo penal, inclusive e sobretudo na fase de investigação preliminar (WANDERLEY, Gisela Aguiar. *Privacidade e Cidadania: os limites jurídicos da atividade investigativa e a legalidade do acesso policial a aparelhos celulares*, Disponível em <https://www.internetlab.org.br/wp-content/uploads/2019/08/InternetLabCongressoII_simples.pdf>. Acesso em: 20 de dezembro de 2020).

Por óbvio, a analogia exige o respeito às garantias individuais, especialmente aquelas contempladas no texto constitucional, bem como a utilização dos parâmetros procedimentais de outros meios de obtenção de prova típicos. Seria impensável se cogitar em analogia diante de outros meios atípicos, sob pena de se conceber flagrante desrespeito ao princípio da legalidade.

Conclui-se, desta forma, que o meio de busca de provas atípico é admissível, especialmente diante das características assumidas pelas provas de natureza

digital[177], desde que não se constante ofensa aos direitos e garantias fundamentais, à eficiência do processo e, principalmente, à autenticidade e integridade da prova produzida.

Entretanto, esta atipicidade dos meios de busca não regulamentados os conduz à utilização em cunho excepcional e subsidiário, relegando-a às situações fáticas em que, diante da forma em que o delito tenha se aperfeiçoado (*v.g.*, nos casos de delitos puramente informáticos) ou em razão de suas peculiares características, a veiculação de outros meios típicos seja inaplicável ou comprovadamente insuficiente para os propósitos técnico-investigativos almejados[178].

Como se verá adiante, a busca de dados armazenados em modernos aparelhos celulares constitui verdadeiro meio atípico de busca e obtenção de provas[179], cuja admissibilidade exigirá a analogia para com outros meios típicos de busca de provas, à exemplo da busca e apreensão (artigo 240 e seguintes do CPP), da interceptação telefônica e telemática (Lei n.º 9.296/1996), dentre outros.

---

[177] VAZ, Denise Provazi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório.* Op. cit. p. 77-79.
[178] MENDES, Carlos Hélder Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software,* p. 214-215.
[179] ZILLI, Marcos Alexandre Coelho. ZILLI, Marcos Alexandre Coelho. *A prisão em flagrante e o acesso de dados em dispositivos móveis. Nem utopia, nem distopia. Apenas a racionalidade.* In: ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (eds.). *Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate*. Vol. I. São Paulo. InternetLab, 2018, p. 90.

3. FORMAS DE ACESSO AOS DADOS ARMAZENADOS EM APARELHOS CELULARES: A VOLUNTARIEDADE COMO ELEMENTO DE VALIDADE DO ACESSO

Reconhecida a analogia como meio para se permitir a obtenção e a integração de provas digitais, especialmente aquelas armazenadas em aparelhos celular, é necessário se avançar para o estudo quanto às formas pelas quais os referidos dados poderão ser acessados.

Assim, de maneira sintética, admitem-se ao menos três formas pelas quais o conteúdo dos dados armazenados poderá ser acessado:

a) cessão voluntária dos dados, mediante consentimento e colaboração livre e desimpedida do seu titular[180];

b) cessão dos dados comunicados, por um dos interlocutores, independentemente de autorização judicial;

c) utilização de medidas invasivas para acesso, apreensão e extração dos dados, por meio físico ou remoto, notadamente: *c.1.)* apreensão remota dos dados contidos em aparelhos celulares, sem a necessidade de apreensão do objeto fisicamente, o que se dá por diversas formas; *c.2)* mediante apreensão material do suporte eletrônico que armazena os dados a ser acessados por intermédio da diligência realizada.

Torna-se imprescindível se debruçar sobre as hipóteses aventadas, a fim de aferir a legalidade de cada uma das formas tecnologicamente viáveis para o precitado acesso, analisando-as sob a perspectiva constitucional da proteção à privacidade e intimidade, além de verificar sua conformidade com os dispositivos processuais penais aplicáveis analogicamente ao tema.

---

[180] Tendo em vista que a privacidade e intimidade são esferas individuais relacionadas à personalidade humana, tem-se como possível que o seu titular, em situações específicas, possa delas dispor, em exercício propriamente dito ou na medida da sua extensão. Especialmente no tocante ao consentimento e sua validade, o tema será desenvolvido em tópico próprio.

3.1. Cessão voluntária dos dados pelo titular

A cessão dos dados que interessam à investigação poderá ser feita pelo próprio acusado[181], enquanto titular do seu conteúdo, que escolherá livremente entregá-los, total ou parcialmente, às autoridades investigativas.

Trata-se de hipótese que, em regra, dispensa a intervenção judicial para acesso, captação e extração dos dados de interesse da investigação. Para tanto, pressupõe-se a voluntariedade do ato, enquanto elemento de proteção à vontade do indivíduo em franquear o acesso aos dados.

A expressão da vontade pode se dar através de um ato de iniciativa própria do acusado, que voluntariamente entrega o aparelho celular para ser examinado[182] ou, ainda, mediante consentimento[183], a partir do momento em que o suporte eletrônico já está em poder do Estado. Nesta hipótese, o indivíduo, por iniciativa autônoma ou mediante influência de terceiros, concorda com o acesso aos dados de seu aparelho pelo órgão estatal, especialmente nas hipóteses em que se exige uma autorização judicial.

3.1.1. Requisitos de validade para o consentimento no acesso a dados armazenados em aparelhos celulares

Dispõe o artigo 5º, inciso XII, da Lei n.º 13.709/2018 que o consentimento pode ser definido como a *"*manifestação livre, informada e inequívoca pela

---

[181] Para fins do presente trabalho científico, será adotado o conceito de "acusado" em sentido amplo, que abrange o suspeito, o indiciado, o investigado, o increpado, o imputado, o acusado propriamente dito, enfim "(...) todas as formas de acusados, formais e informais, incluindo-se aí o sujeito investigado no inquérito policial (...)" (SAAD, Marta Cristina Cury. *Defesa no inquérito policial.* Revista de Direito de Polícia Judiciária, Brasília, ano 2, n. 4, p. 67, jul-dez de 2018). Na mesma linha, reconhecendo-se que ao suspeito devem ser assegurados todos os direitos reconhecidos: *Caso Vélez Loor v. Panama*, julgado pela Corte Intermaricana de Direitos Humanos, disponível em < https://www.corteidh.or.cr/docs/casos/articulos/resumen_218_esp.pdf>. Acesso em: 20 de dezembro de 2020.

[182] Via de regra, a utilidade e eficácia na busca de elementos de provas está relacionada às hipóteses de consentimento em que a apreensão do objeto se deu em situações repentinas, completamente inesperadas por parte do acusado. Vale dizer, nas hipóteses de cessão espontânea do aparelho celular por parte do investigado, há grandes chances de os elementos de prova pretendidos estarem comprometidos.

[183] Nos dizeres do português Manoel da Costa Andrade, o consentimento aparece *"invariavelmente como via de legitimação dos correspondentes meios de prova"* (COSTA ANDRADE, Manoel. *Sobre as Proibições de Prova em Processo Penal*, Coimbra: Editora Coimbra, 1992, p. 50). Para Dario José Kist, o consentimento deve ser "(...) completo, voluntário e manifestado por agente capaz e sem deficiências; tendo estas características, ele supre a necessidade de ordem judicial (...)" (KIST, Dario José. *Prova digital no processo penal.* Leme: Editora JHMizuno, 2019, p. 399).

qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"[184].

De igual sorte, o artigo 7º, inciso VII, da Lei n.º 12.965/2014, prevê que os dados pessoais, registros de conexão e acesso a aplicações de *internet* somente poderiam ser concedidas mediante "consentimento livre, expresso e informado ou nas hipóteses previstas em lei"[185].

Os conceitos legais, embora direcionado para os fins específicos da Lei Geral de Proteção de Dados e do Marco Civil da *Internet*, podem ser tomados por empréstimo[186] para se explorar os requisitos mínimos para validade do ato de consentimento. Assim, é pressuposto natural do consentimento que este seja prestado de maneira livre, de maneira inequívoca e destinada a uma finalidade específica, conforme se verá nos tópicos seguintes.

Por ora, é relevante voltar-se os olhos para o direito estrangeiro, especialmente a experiência espanhola com a *Ley de Enjuiciamiento Criminal*, em que se disciplinou, no Título VIII, "las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución[187]".

---

[184] Sobre o tema, na ótica do direito privado, recomenda-se: BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento.* 2ª ed. Rio de Janeiro: Ed. Forense, 2019, p. 179-190.

[185] Para Renato Leite Monteiro, o "(...)o consentimento livre, expresso e informado, será aquele em que o usuário não é forçado a concordar com os termos do contrato, e as cláusulas que discorrem sobre qualquer tipo de tratamento de dados – inclusive fornecimento a terceiros – deverão ser redigidas de forma destacada, e se possível, separadas das demais (...)" (MONTEIRO, Renato Leite. *Da Proteção aos Registros, aos dados pessoais e às comunicações privadas*. In: MASSO, Fabiano del et al. (Coord.). Marco Civil da *Internet*. São Paulo: Revista dos Tribunais, 2014. p. 146). A previsão normativa contida na Lei do Marco Civil da *Internet* (Lei n.º 12.965/2014) e que posteriormente foi repetida na Lei Geral de Proteção de Dados (Lei n.º 13.709/2018) tem clara inspiração na normativa europeia de proteção de dados, que dá ênfase e tratamento prioritário ao consentimento livre do usuário na tutela de seus dados – em detrimento à tratativa anterior, que estabelecia uma espécie de consentimento forçado no tratamento de dados, para além do necessário no funcionamento de determinada atividade ou serviço –, bem como estabelece expressamente que "(...) consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (…)" (art. 4º, (11), da General Data Protection Regulation (GDPR)

[186] Importante ressaltar que os diplomas normativos mencionados possuem especificidades relacionadas ao consentimento. Todavia, não há como se aplicar todas as suas previsões normativas, muitas delas específicas para cada legislação, de forma geral e abrangente para os atos de consentimento na esfera penal e civil, conforme será explicitado ao longo do trabalho.

[187] Artículo 18.

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

Com efeito, o artigo 18, item 1, da Constituição Espanhola, disciplina o dever de se garantir o direito à honra, à intimidade pessoal e familiar e à própria imagem, em redação bastante similar àquela contida no artigo 5º, inciso X, da Constituição Federal. Infere-se que a Constituição Espanhola, à semelhança da Constituição Federal brasileira, não exigiu expressamente a necessidade de autorização judicial ou a reserva de lei.

Interpretando-se o dispositivo em questão, a Corte Suprema Espanhola reconheceu que o direito à intimidade pessoal deriva da dignidade da pessoa humana (art. 10.1 da Constituição Espanhola) e implica o reconhecimento de âmbito próprio e reservado do indivíduo, em anteparo à ação e conhecimento dos demais, como forma de se manter uma mínima qualidade de vida[188], vedando-se a terceiros – particulares ou ao próprio poder público –, a intromissão e decisão sobre os limites a este espaço pessoal.

Haveria, assim, um direito conferido ao cidadão para impor a terceiros o dever de se absterem de toda intromissão à esfera íntima e a proibição de fazer uso do que ali for conhecido[189], salvo nas situações em que se verificar a necessidade de se preservar outros direitos fundamentais e bens jurídicos constitucionalmente protegidos – dentre os quais estaria a necessidade de persecução e apuração de um fato criminoso –, em análise balizada pela proporcionalidade[190].

Especialmente no que tange ao consentimento, a Corte Suprema Espanhola já reconheceu que esta é uma das formas pelas quais o particular poderá autorizar que terceiros se imiscuam em seu direito à intimidade, salientando-se que este consentimento poderá ser revogado a qualquer tempo[191].

---

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos

[188] SSTC 207/1996, de 16 de diciembre, FJ 3; 186/2000, de 10 de julio, FJ 5; 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 4; y 159/2009, de 29 de junio, FJ 3.

[189] SSTC 127/2003, de 30 de junio, FJ 7 y 89/2006, de 27 de marzo, FJ 5 e SSTC 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 5; y 70/2009, de 23 de marzo, FJ 2.

[190] SSTC 98/2000, de 10 de abril, FJ 5; 156/2001, de 2 de julio, FJ 4; 70/2009, de 23 de marzo, FJ 3; SSTC 25/2005, de 14 de febrero, FJ 6 y 206/2007, de 24 de septiembre, FJ 6; y SSTC 127/2000, de 16 de mayo, FJ 3 a) y 292/2000, de 30 de noviembre, FJ 9.

[191] SSTC 83/2002, de 22 de abril, FJ 5 y 196/2006, de 3 de julio, FJ 5; STC 159/2009, de 29 de junio, FJ 3.

Já o artigo 18, item 2, da Constituição Espanhola, dispõe que o domicílio é considerado inviolável, de modo que nenhuma entrada ou registro poderá ser feito sem o consentimento do titular ou determinação judicial, salvo nos casos de flagrante delito. Trata-se de previsão similar a do artigo 5º, inciso XI, da Constituição Federal e também autoriza a entrada em domicílio mediante consentimento do titular do imóvel, acrescentando-se a possibilidade do ingresso também para prestar socorro ou em caso de desastre.

Ao regulamentar o artigo 18 da Constituição Espanhola, a *Ley de Enjuiciamiento Criminal* estabeleceu, em seus artigos 545 a 572, as "medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución".

Dentro deste capítulo, ao tratar das hipóteses de ingresso mediante consentimento, a *Ley de Enjuiciamiento Criminal* disciplinou, em seu artigo 551, que "se entenderá que presta su consentimiento aquel que, requerido por quien hubiere de efectuar la entrada y registro para que los permita, ejecuta por su parte los actos necesarios que de él dependan para que puedan tener efecto, sin invocar la inviolabilidad que reconoce al domicilio el artículo 6.º de la Constitución del Estado"[192].

Como se vê, o legislador espanhol estabeleceu que o consentimento se dará quando o titular do domicílio realizar atos necessários para que se permita o ingresso no imóvel, sem invocar a garantia da inviolabilidade do domicílio.

A norma trazida, por ser bastante genérica, foi objeto de interpretação jurisprudencial pelas Cortes Espanholas. Especialmente no julgamento do STS 4761/2013 e invocando outros precedentes jurisprudenciais (SSTS. 1803/2002 de 4.11, 261/2006 de 14.3 y 922/2010 de 28.10), a Suprema Corte Espanhola, em voto de seu relator Juan Ramon Berdugo Gómez de la Torre, definiu quais seriam os requisitos para se ter como válido o consentimento de um cidadão com relação ao ingresso em seu domicílio[193].

---

[192] O artigo 6º da Constitución del Estado corresponde, atualmente, ao art. 18.2 da Carta Constitucional Espanhola.

[193] Diante da primazia da análise, vale transcrever o trecho do voto em que se estabeleceu, expressamente, os requisitos legais: "(...) a) Otorgado por persona capaz; esto es mayor de edad, y sin restricción alguna en su capacidad de obrar. En supuestos de minusvalía psíquica aparente, esté o no declarada judicialmente, no puede considerarse válidamente prestado el consentimiento, todo ello en base al art. 25 del Código penal: "a los efectos de este Código se considera incapaz a toda persona, haya sido o no declarada su incapacitación, que

Em breve síntese, reconheceu-se que o consentimento somente será válido caso prestado por pessoa capaz, maior, com pleno gozo das faculdades mentais, de forma livre e consciente. Ainda, de acordo com a jurisprudência espanhola, o consentimento poderá ser prestado de forma verbal ou escrita, mas deverá ser documentado posteriormente, devendo ainda ser outorgado expressamente, ainda que o artigo 551 da *Ley de Enjuiciamiento Criminal* permita o consentimento presumido.

Finalmente, o consentimento deverá ser outorgado para uma finalidade específica, da qual aquele que consente tenha conhecimento, sem poder ser utilizado para outras finalidades distintas[194].

Ainda que os requisitos tenham sido estabelecidos à luz da legislação processual espanhola, é possível que, dada a similitude das previsões constitucionais, se possa transplantá-los para a legislação processual brasileira. Especificamente no que

---

padezca uma enfermedad de carácter persistente que le impida gobernar su persona o bienes por sí misma". b) Otorgado consciente y libremente. Lo cual requiere: a?) que no esté invalidado por error, violencia o intimidación de cualquier clase; b?) que no se condicione a circunstancia alguna periférica, como promesas de cualquier actuación policial, del signo que sean; c?) que si el que va a conceder el consentimiento se encuentra detenido, no puede válidamente prestar tal consentimento si no es con asistencia de Letrado, lo que así se hará constar por diligencia policial. "El consentimiento a la realización de la diligencia, uno de los supuestos que permiten la injerencia en el derecho fundamental a la inviolabilidad del domicilio, requiere que ha de ser prestado ante un letrado que le asista y ello porque esa manifestación de carácter personal que realiza el detenido puede afectar, indudablemente, a su derecho a la inviolabilidad y también a su derecho de defensa, a la articulación de su defensa en el proceso penal, para lo que ha de estar asesorado sobre el contenido y alcance del acto de naturaleza procesal que realiza" (STS 2-12-1998). Si la asistencia de letrado es necesaria para que éste preste declaración estando detenido, también le es necesaria para asesorarle si se encuentra en la misma situación para la prestación de dicho consentimiento, justificándose esta doctrina en que no puede considerarse plenamente libre el consentimento así prestado en atención a lo que se ha venido denominándose "la intimidación ambiental" o "la coacción que la presencia de los agentes de la actividad representan (STS. 831/2000 de 16.5). c) Puede prestarse oralmente o por escrito, pero siempre se reflejará documentalmente para su constância indeleble.d) Debe otorgarse expresamente, si bien la Ley de Enjuiciamiento Criminal en su art. 551 autoriza el consentimiento presunto. Este articulo ha de interpretarse restrictivamente, pues el consentimiento tácito ha de constar de modo inequívoco mediante actos propios tanto de no oposición cuanto, y sobre todo, de colaboración, pues la duda sobre el consentimiento presunto hay que resolverla en favor de la no autorización, en virtud del principio in dubio libertas y el criterio declarado por el Tribunal Constitucional de interpretar siempre las normas en el sentido mas favorable a los derechos fundamentales de la persona, en este caso del titular de la morada. El silencia puede interpretarse como consentimiento: "Qui siluit cum loqui debuit, et notint, consentire de videtur" (SS. 7.3 y 18.12.97), pues consiente el que soporta, permite, tolera y otorga, inequívocamente" que entre y registre y registre (S. 23.1.98).e) Debe ser otorgado por el titular del domicilio, titularidad que puede provenir de cualquier título legítimo civilmente, sin que sea necesaria la titularidad dominical. En caso de que varias personas tengan su domicilio en el mismo lugar no es necesario el consentimiento de todos ellos, bastando el de uno de los cotitulares, salvo los casos de intereses contrapuestos (STS. 779/2006 de 12.7).f) El consentimiento debe ser otorgado para un asunto concreto, del que tenga conocimiento quien lo presta, sin que se pueda aprovechar para otros fines distintos (Sentencia de 6 de junio de 2001).g) No son necesarias en ese caso las formalidades recogidas en el art. 569 de la Ley de Enjuiciamiento Criminal, respecto de la presencia del Secretario Judicial (...)"

[194] SSTC 196/2004, de 15/11, FJ 2; 206/2007, de 24/09, FJ 5; y 70/2009, de 23/03, FJ 2.

concerne ao acesso aos dados armazenados em aparelhos celulares, AURY LOPES JR. e ALEXANDRE MORAIS DA ROSA enumeram quais seriam os requisitos para o consentimento, já adaptados à normativa processual penal brasileira:

> 1) outorga por pessoa capaz, maior de idade e no exercício de seus direitos; 2) outorga consciente e livre, a qual requer: a) que não esteja invalidade por erro, violência ou intimidação de qualquer modo; b) que não seja condicionada a alguma circunstância periférica, como promessas de qualquer atuação policial; c) que se o consentimento for de pessoa que estiver presa/conduzida, não pode validamente prestar o consentimento se não tiver antes a assistência de um defensor, do que constará da diligência policial (STS 2-12-1998). Isso porque, se a assistência de defensor é necessária para que o conduzido preste declarações, dado o prejuízo aos seus direitos, o consentimento também o será, dada a "intimidação ambiental" ou "a coação que a presença dos agentes da atividade representa" (STS. 831/2000). 3) pode ser prestada oral ou por escrito, porém sempre vertida documentalmente; 4) deve ser outorgada expressamente, não servindo o silêncio como consentimento tácito, em face do princípio in dubio pro liberdade (SS. 7.3 y 18.12.97 e S. 23.1.98). 5) o consentimento deve ser outorgado para um caso concreto, sem que seja usado para fins distintos, ou seja, vigora a especialidade da busca (STS, sentença de 6 de junho de 2001). Desta feita, ainda que se considere a existência de anuência pelo investigado para vasculhar seu celular, tem-se que, com a intimidação ambiental e constrangimento que a prisão proporciona, não é possível validar tal manifestação da vontade, salvo se acompanhado por defensor e advertido formal e documentalmente dos direitos renunciados, nas forma dos critérios acima" [195] (LOPES JR. Aury. MORAIS DA ROSA, Alexandre. *Critérios de validade para vasculhar o celular (WhatsApp) do preso*. Disponível em

[195] Os requisitos delineados pela jurisprudência espanhola já foram utilizados como fundamento decisório pelo Superior Tribunal de Justiça, ao apreciar a legalidade de buscas domiciliares. Na ocasião, o relator Ministro Rogério Schietti Cruz criticou que *"(...) esses requisitos, evidentemente, não têm sido sequer ventilados pela jurisprudência pátria, muito menos por leis de nosso país ou, ainda, por regramentos administrativos, mas refletem uma orientação que poderia ser adotada, na medida do possível, com vistas a minimizar a praxe, tão comum em comunidades de baixa renda, em que casas são ocasionalmente invadidas sem o amparo do Direito (...)"* (STJ, Recurso Especial n.º 1.574.681/RS, 6ª Turma, Rel. Min. Rogério Schietti Cruz, julgado em 20/04/2017, DJe 30/05/2017)

<https://www.conjur.com.br/2018-mai-25/limite-penal-criterios-validade-vasculhar-celular-whatsapp-preso>. Acesso em 20 de dezembro de 2020).

Importa notar que, estabelecidas algumas ressalvas que serão melhor tratadas oportunamente[196], os requisitos indicados pela jurisprudência espanhola e posteriormente adaptados à normativa brasileira amoldam-se à previsão normativa do artigo 5º, inciso XII, da Lei n.º 13.709/2018, ao tratar do consentimento[197].

Assim, revela-se necessário esmiuçar os requisitos essenciais para a existência, validade e eficácia do consentimento.

3.1.1.1. Capacidade ativa

O primeiro requisito para o consentimento está relacionado à capacidade do agente, que consiste no pleno entendimento para o exercício de vontade, com a devida aptidão para a prática de atos na seara processual. Trata-se de requisito essencial para a celebração de todo e qualquer negócio jurídico (artigo 104, inciso I, do Código Civil).

Considerando que a legislação processual penal é aplicada, de forma direta, àqueles que possam vir a ser sujeitos ativos de uma infração penal, é certo que, ao menos no campo biológico, o consentimento somente será válido se prestado por pessoa maior de 18 (dezoito) anos, conforme dispõe o artigo 27 do Código Penal e artigo 228 da Constituição Federal. Ressalte-se que, para os que estão sujeitos à responsabilização por atos infracionais (artigos 103 a 105 da Lei n.º 8.069/1990), o consentimento poderá ser obtido na presença e mediante ratificação de um familiar ou responsável legal, a fim de se preservar a validade do ato.

No mais, o consentimento exige que a pessoa esteja no exercício regular de seus direitos e tenha plena capacidade de entendimento e determinação, não se admitindo a validade do consentimento prestado por aquele não demonstrar capacidade para

[196] A nosso sentir, o consentimento do indivíduo preso é válido, ainda que desacompanhado de um advogado ou defensor público, conforme será melhor explorado oportunamente.
[197] Para Kist, a livre manifestação de vontade abrange alguns aspectos, dentre eles o agir do agente por impulso, sem refletir os riscos da decisão adotada; a coerção, enquanto pressão externa que impediria a liberdade nas decisões, os distúrbios e incapacidade de ordem psicológica e o erro sobre os fatos, provocado ou não (KIST, Dario José. *Prova digital no processo penal.* Op. cit. p. 399-400).

entendimento do ato e conhecimento de suas consequências jurídicas. Nestas situações, se verificadas demonstrações que sugiram a incapacidade do agente, deverá o órgão estatal se abster de colher o ato de consentimento[198].

3.1.1.2 Manifestação livre: a formação do processo da vontade e os vícios de consentimento

O consentimento exige que o ato de outorga seja realizado de forma consciente e livre, de modo que o acusado deva possuir plena liberdade de escolha para decidir se irá franquear o acesso a seus dados.

O processo de formação da vontade, em razão do caráter reflexivo próprio dos indivíduos, estaria projetado em desejos de primeira e segunda ordem, naturalmente a declaração da vontade e a vontade efetiva do agente[199].

Ainda, a noção de "vontade" está relacionada à capacidade de autodeterminação dos indivíduos, notadamente o livre-arbítrio. Consiste na possibilidade íntima do indivíduo de, entre duas ou mais opções que lhe são apresentadas, optar por uma delas que lhe pareça mais razoável. Trata-se, pois, da "liberdade interna", a qual deve ser conjugada com a "liberdade externa", o que exige o fornecimento de condições objetivas para que o indivíduo exerça suas opções, livre de qualquer pressão, coação ou constrangimento.

---

[198] A Suprema Corte Espanhola, no julgamento do STS n.º 7291/2002, Sala de lo Penal, Ponente Julian Artemio Sanchez Melgar, recurso n.º 236/2002, julgado em 04/11/2002, reconheceu que *"(...)* en supuestos de minusvalía psíquica aparente, esté o no declarada judicialmente, no puede considerarse válidamente prestado el consentimiento, todo ello en base al art. 25 del Código penal : "a los efectos de este Código se considera incapaz a toda persona, haya sido o no declarada su incapacitación, que padezca una enfermedad de carácter persistente que le impida gobernar su persona o bienes por sí misma (...)"

[199] Em obra sobre a "delação premiada", Leonardo Dantas Costa sustenta, citando Harry Gordon Frankfurt, a existência de "(...) desejos de primeira ordem e desejos de segunda ordem. Os desejos de primeira ordem correspondem à forma mais comum à qual a vontade é referida, ou seja, o "desejo de algo" (na colaboração premiada, o desejo de se defender colaborando com a Justiça). Já os desejos de segunda ordem são mais complexos, pois dizem respeito ao "desejo de desejar algo" (o "desejo de desejar colaborar com a justiça"). Tais desejos de segunda ordem são derivados de uma característica exclusiva do ser humano, qual seja, sua capacidade de autodeterminação e avaliação reflexiva sobre aquilo que quer (...)". Assim, "(...) devido à confluência de motivos, razões e sentimentos, a aferição precisa da vontade humana deve passar pela identificação de seu desejo de segunda ordem, ou seja, aquele a partir do qual a pessoa é motivada a querer realizar a ação. Dessa forma, a determinação da vontade efetiva do agente está ligada à identificação do processo de formação de seu desejo de agir, e não da exteriorização pontual deste desejo (...)" (COSTA, Leonardo Dantas. *Delação Premiada,* Paraná: Editora Juruá, 2017, p. 154-155 e 160).

Desta feita, todo e qualquer constrangimento ou coação ilegais que maculem a livre expressão da vontade do ser humano ofendem, a um só tempo, a dignidade da pessoa humana, bem como sua autonomia e liberdade[200] neste processo decisório.

É certo que, para a cessão voluntária dos dados, bastaria tão somente a expressão da vontade do acusado na concessão dos dados digitais armazenados em seu aparelho celular (voluntariedade), sendo irrelevante que esta iniciativa parta dele mesmo (espontaneidade) ou por sugestão de terceiro. Em verdade, a espontaneidade somente é exigida quando há expressa previsão de sua necessidade[201], à exemplo do artigo 65, inciso III, alínea *d*, do Código Penal.

Assim, considerando que o consentimento do indivíduo é ato precário e desprovido de qualquer requisito formal, bem como não está relacionado a motivos íntimos, sejam éticos ou egoísticos, é despiciendo investigar se fora fruto de uma iniciativa própria refletida ou de conselhos ou coações externas por terceiros[202], inclusive da própria autoridade investigativa. Basta, pois, que seja assegurada margem de liberdade do indivíduo para agir e escolher[203].

Esta liberdade de agir, porém não está relacionada à liberdade física propriamente dita, mas sim à capacidade de realizar suas escolhas sem qualquer evento externo, de ordem física ou psicológica[204], que macule ou venha a influenciar negativamente o processo de formação da vontade.

Algumas hipóteses de atuação de má-fé, por parte de terceiros, poderão macular a autonomia e liberdade do acusado, fazendo com que sua vontade exista,

---

[200] COSTA, Leonardo Dantas. *Delação Premiada.* Op. cit. p. 164.
[201] PANNAIN, Remo. *Manuale di diritto penale: parte generale*. Torino: 1967, p. 649. *Apud* COSTA, Álvaro Mayrink. Direito penal: parte geral. v. 1., tomo II. 6ª ed. Rio de Janeiro: Forense, 1998, p. 1296.
[202] GOMES, Luiz Flávio; CERVINI, Raúl. *Crime organizado: enfoques criminológicos, jurídico (Lei 9.034/1995) e político-criminal*. São Paulo: Editora RT, 1995, p. 168; FRANCO, Alberto Silva, LIRA, Rafael, FELIX, Yuri. *Crimes hediondos*. 7ª ed. São Paulo: Editora Revista dos Tribunais, 2011, p. 530-531.
[203] AZEVEDO, David Teixeira de. *Delação premiada e direito de defesa*. Boletim IBCCRIM, São Paulo, IBCCRIM, v. 22, n. 265, p. 4, 2014.
[204] MENDONÇA, Andrey Borges. *Os benefícios possíveis na colaboração premiada: entre a legalidade e a autonomia da vontade*. In: MOURA, Maria Thereza de Assis; BOTTINI, Pierpaolo Cruz (Coord.). Colaboração premiada. São Paulo: Editora Revista dos Tribunais, 2017, p. 53-104.

mas internamente esteja contaminada por vícios no processo volitivo[205]. Trazendo-se a análise dos vícios no consentimento[206] para o plano processual penal, faz-se necessário que o ato de entrega do aparelho celular não decorra de dolo, coação ou violência das autoridades investigativas.

A coação ou violência físicas ou psicológicas são exemplos de cerceamento à liberdade de escolha do indivíduo. Não há liberdade e tampouco escolha do acusado quando este decide entregar seu aparelho celular às autoridades após sofrer ameaças concretas de prisão ou morte, torturas ou constrangimentos físicos lançadas ao próprio indivíduo ou a seus familiares.

Traçando-se um paralelo com a legislação estrangeira, o Código de Processo Penal Português foi expresso ao estabelecer, em seu artigo 126, os "métodos proibidos de prova", impondo-se a nulidade às provas obtidas mediante tortura, coação ou ofensa à integridade física ou moral das pessoas. O precitado dispositivo legal, nos itens 1 e 2[207], previu as hipóteses de nulidade da prova obtida mediante tortura, coação ou ofensa à integridade física ou moral das pessoas.

Trata-se de hipóteses em que, ainda que sob o consentimento do acusado, a prova não poderá ser produzida, por haver uma presunção absoluta de que a

---

[205] A propósito, o artigo 8º, § 3º, da Lei n.º 13.709/2018, estabelece expressamente que, no âmbito da proteção aos dados pessoais, estes não podem ser objeto de tratamento mediante vício de consentimento.

[206] O Código Civil de 2002, ao tratar sobre os defeitos do negócio jurídico em seu capítulo IV, estabeleceu um rol de vícios que contaminariam o negócio celebrado, tornando-os passíveis de anulabilidade e/ou nulidade por tisnarem a vontade do agente. Estabelece a legislação civil que são vícios do consentimento o erro, dolo, a coação, o estado de perigo, a lesão e a fraude contra credores. Embora todos estejam relacionados à perspectiva dos negócios jurídicos, parte destes vícios de consentimento se aplicaria à voluntariedade do agente no processo penal, especialmente sob a perspectiva do consentimento. Na perspectiva de Washington de Barros Monteiro, "(...) pode acontecer ainda que a vontade tenha existido; o interessado desejou realmente praticar o ato questionado; mas sua vontade estava contaminada por algum dos vícios do consentimento, erro ou ignorância, dolo e coação ou violência, estado de perigo ou lesão. Sendo o negócio jurídico pura emanação da vontade, efeito em relação à causa, é claro que ele se ressentirá dos mesmos vícios que a esta originariamente maculavam. A consequência natural será a ineficácia do ato eivado por qualquer daqueles vícios (...)" (MONTEIRO, Washington de Barros. *Curso de Direito Civil – Parte Geral.* 39ª Edição, São Paulo: Editora Saraiva, 2003, p. 219).

[207] 1 - São nulas, não podendo ser utilizadas, as provas obtidas mediante tortura, coacção ou, em geral, ofensa da integridade física ou moral das pessoas; 2. São ofensivas da integridade física ou moral das pessoas as provas obtidas, mesmo que com consentimento delas, mediante: a) Perturbação da liberdade de vontade ou de decisão através de maus tratos, ofensas corporais, administração de meios de qualquer natureza, hipnose ou utilização de meios cruéis ou enganosos; b) Perturbação, por qualquer meio, da capacidade de memória ou de avaliação; c) Utilização da força, fora dos casos e dos limites permitidos pela lei; d) Ameaça com medida legalmente inadmissível e, bem assim, com denegação ou condicionamento da obtenção de benefício legalmente previsto; e) Promessa de vantagem legalmente inadmissível".

concordância fora contaminada por vícios que afastaram qualquer liberdade de escolha. A nulidade da prova seria insanável, porquanto haveria clara violação à integridade física e moral do imputado.

O mesmo dispositivo legal, em seu item 3[208], estabelece a nulidade da prova obtida mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações, sem o consentimento do respectivo titular. Entretanto, nesta hipótese, o vício da nulidade seria sanável, mediante o consentimento do titular do direito violado, antes ou após a produção da prova[209].

Como se vê, portanto, a legislação portuguesa é expressa ao admitir o consentimento como forma de se permitir a produção de provas que afrontem o direito à privacidade, vedando-se, todavia, as provas obtidas mediante violação à integridade física e moral do indivíduo, ainda que de forma consentida.

Na mesma linha, o *Codice di Procedura Penale* italiano, em seu artigo 188, estabelece que "non possono essere utilizzati, neppure con il consenso della persona interessata, metodi o tecniche idonei a influire sulla libertà di autodeterminazione o ad alterare la capacità di ricordare e di valutare i fatti", evidenciando-se que, no campo probatório, não serão admitidos a utilização de métodos ou técnicas que possam influenciar a liberdade de autodeterminação ou alterar a capacidade de se recordar ou valor um fato, ainda que o consentimento do acusado [210].

De igual sorte, a fim de que se garanta a correta informação e conhecimento ao acusado, devem ser repelidos todo e qualquer meio enganoso, decorrente

---

[208] 3 - Ressalvados os casos previstos na lei, são igualmente nulas, não podendo ser utilizadas, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respectivo titular".

[209] Supremo Tribunal de Justiça, Processo n.º 149/07.9 JELSB.E1.S1, 3ª Secção, Rel. Raul Borges, julgado em 14 de julho de 2010. Na mesma linha a posição de Manuel Simas Santos e Manuel Leal Henrique, distinguindo-se as hipóteses de métodos proibidos de prova de caráter absoluto e relativos (SIMAS SANTOS, Manoel. LEAL HENRIQUE, Manuel. *Código de Processo Penal Anotado*, 3.ª edição, 2008, volume I, pág. 832, *apud* Supremo Tribunal de Justiça, Processo n.º 149/07.9 JELSB.E1.S1, 3ª Secção, Rel. Raul Borges, julgado em 14 de julho de 2010).

[210] TONINI, Paolo. *Manuale di Procedura Penale,* undicesima edición, Milano: Editora Giuffè, 2010, p. 267.

de promessas ilegais[211] ou dolosamente inexequíveis, a fim de se colher o consentimento do titular dos dados.

O dolo, enquanto vício de consentimento, consiste no erro provocado intencionalmente, por meio do qual a vontade passa a ser viciada. Trata-se do expediente astucioso, utilizado para se induzir alguém à prática de um ato que o prejudica, especialmente considerando, por vezes, o desconhecimento do agente quanto à possibilidade de resistir a esta pretensão. Portanto, pode-se entender que há dolo quando a autoridade investigativa promete um benefício sem qualquer amparo legal, para convencer o titular dos dados a fornecê-los voluntariamente.

3.1.1.2.1 O consentimento do preso e sua voluntariedade

Voltando-se à legislação nacional, um aspecto que desperta grande discussão está relacionado à voluntariedade em situações nas quais a liberdade ambulatória do acusado esteja cerceada. Perquire-se se há voluntariedade e plena capacidade de autodeterminação em um indivíduo que esteja, momentaneamente, privado de sua liberdade.

O tema ganhou campo fértil no âmbito das colaborações premiadas, em que se pretendia abordar se a prisão cautelar constitui uma forma de coação absoluta que suprime a vontade individual para a realização do negócio jurídico processual.

Parte da doutrina sustentou que a prisão do acusado suprimiria a autonomia da vontade e, por conseguinte, inviabilizaria o pressuposto de validade da voluntariedade na celebração da colaboração premiada. Dentre os argumentos lançados apontaram que a custódia cautelar seria uma clássica hipótese de coação ou estado de perigo, previstas no artigo 171, incisos I e II, do Código Civil, o que viciaria a declaração de vontade do encarcerado[212], bem como que a carga emocional e opressiva do ambiente prisional,

[211] Novamente invocando o artigo 126, item 2, alínea *e*, do Código de Processo Penal, são consideradas nulas as provas obtidas mediante promessas de vantagens legalmente inadmissíveis, ainda que consentidas. Sobre o tema, recomenda-se: ANDRADE, Manoel da Costa. *Sobre as Proibições de Prova em Processo Penal*, Coimbra: Editora Coimbra, 2006, p. 209 e ss.

[212] LEMOS, Bruno Espiñeira; CALDEIRA, Felipe Machado. *Delação premiada de acusado preso*. In: LEMOS, Bruno Espiñeira; CALDEIRA, Felipe Machado (Org.). *Delação premiada: estudos em homenagem ao ministro Marco Aurélio de Mello*. Belo Horizonte: Editora D´Plácido, 2016, p. 75-89. No mesmo sentido: BADARÓ, Gustavo Henrique Righi Ivahy. *Quem está preso pode delatar?* Jota, 23 jun. 2015. Disponível em: <http://jota.uol.com.br/quem-esta-preso-pode-delatar>. Acesso em: 20 de dezembro de 2020.

aliado à "vergonha" da cadeia, a superlotação carcerária e às sevícias físicas e sexuais formariam uma pressão psicológica no indivíduo, a ponto de ter suprimida sua liberdade de escolha[213].

Versando sobre o consentimento dado nas hipóteses de ingresso em domicílio desprovido da ordem judicial respectiva, tem-se apontado que o consentimento dado por alguém que está cautelarmente preso ou em flagrante seria insuficiente para se aperfeiçoar a validade do ato, especialmente considerando a intimidação ambiental ou situacional a que estaria submetido o agente[214]. Não bastasse, aponta-se que o consentimento jamais poderia ser prestado perante agentes de Estado, quaisquer que estes sejam, pois estes deveriam obter, previamente, o mandado judicial[215].

Todavia, em contraposição a este entendimento, parte da doutrina reconhece que a constrição física do acusado não retira sua possibilidade de escolha, sendo certo que deixar-se de conceder ao preso a possibilidade de colaborar constituiria afronta ao princípio da isonomia e da ampla defesa, especialmente por se negar ao acusado preso e, portanto, em situação mais gravosa, a concessão de um benefício legal oferecido àquele que está em situação mais vantajosa, por se encontrar em liberdade[216].

Ademais, a decretação da prisão do acusado é medida amparada por lei, sempre que respeitados seus pressupostos e requisitos legais, de modo que seria inconcebível se cogitar em coação psicológica irresistível no exercício regular de um direito por parte do Estado, dotado de amparo legal[217].

---

[213] D'URSO, Luiz Flávio Borges. *Delação premiada – Proibição para quem está preso. Migalhas*, 28 de julho de 2015, Disponível em: <https://www.migalhas.com.br/depeso/224179/delacao-premiada-proibicao-para-quem-esta-preso>. Acesso em: 20 de dezembro de 2020.
[214] LOPES JR., Aury. *Direito Processual Penal.* Op. cit, p. 561.
[215] TJRS, Apelação Criminal n.º 70058172628, 3ª Câmara Criminal, Relatoria Desembargador Diógenes V. Hassan Ribeiro, Porto Alegre, julgado em 15 de maio de 2014.
[216] CAPEZ, Rodrigo. *Pressupostos de admissibilidade e requisitos de validade da colaboração premiada: critérios para orientar a proposta e o controle da justiça criminal negocial*. In: *Colaboração Premiada*. Org. Maria Thereza de Assis Moura e Pierpaolo Cruz Bottini, São Paulo: Editora Revista dos Tribunais, p. 127-161.
[217] GRANDIS, Rodrigo de. *Prisão não invalida a delação premiada.* Jota, 5 de agosto de 2015, Disponível em: <http://jota.uol.com.br/quem-esta-preso-pode-delatar>. Acesso em: 20 de dezembro de 2020.

O Supremo Tribunal Federal (STF) encampou este posicionamento no bojo do *Habeas Corpus* n.º 127.483/PR[218], reconhecendo que a liberdade psíquica, relacionada à autodeterminação, não está condicionada necessariamente à liberdade física, de modo que, mesmo preso, é possível que o acusado preserve sua capacidade de escolha.

No mesmo julgamento, o Supremo Tribunal Federal (STF) consignou que as prisões e as demais medidas cautelares somente podem ser impostas nas hipóteses previstas na legislação processual, sendo *ilegítimas*[219] quando se constata um propósito claramente utilitarista, servindo-se como odioso instrumento para se obter confissão ou a colaboração premiada, em clara violação ao princípio do *nemu tenetur se detegere.*

Com a aprovação da Lei n.º 13.964/2019, foram estabelecidas reformas parciais na Lei n.º 12.850/2013, especialmente na temática relacionada à colaboração premiada. Assim, de forma expressa, o legislador impôs ao juiz que, quando da homologação do acordo de colaboração premiada, deverá analisar a voluntariedade das declarações do colaborador na presença de seu advogado, "especialmente nos casos em que o colaborador está ou esteve sob efeito de medidas cautelares" (artigo 4º, § 7º, inciso IV, da Lei n.º 12.850/2013).

Desta forma, evidencia-se a intenção do legislador em não impedir a celebração do negócio jurídico processual aos indivíduos presos, mas assegurando-se que a voluntariedade será observada de forma minuciosa quando o colaborador está ou esteve sob efeito de medidas cautelares.

Observadas as peculiaridades da colaboração premiada, é legítimo se estabelecer uma correlação entre a voluntariedade exigida para a celebração do acordo e para a concessão do acesso aos dados armazenados em aparelhos celulares.

---

[218] STF, *Habeas Corpus* n.º 127.483/PR, Rel. Min. Dias Toffoli, julgado em 27 de agosto de 2015, DJe 03/02/2016.

[219] CAPEZ, Rodrigo. *Pressupostos de admissibilidade e requisitos de validade da colaboração premiada: critérios para orientar a proposta e o controle da justiça criminal negocial*. *Op. cit.* p. 127-161; BORRI, Luiz Antonio. *Delação premiada do investigado/acusado preso cautelarmente: quando o Estado se transfigura em criminoso para extorquir a prova do investigado*. Boletim IBCCRIM, São Paulo, v. 24, n. 285, p. 6-8, ago. 2016.

Em verdade, não há razão para se vedar que o acusado preso decida colaborar com a investigação, fornecendo-se voluntariamente o acesso ao conteúdo do seu aparelho celular. Com efeito, desde que o seu consentimento seja dado de forma voluntária e expressa, sem qualquer tipo de coação direta ou indireta, as invocações de intimidação ambiental não seriam razoáveis para, isoladamente, justificarem a nulidade do consentimento dado. É necessário um elemento objetivo adicional, notadamente uma coação, erro ou outro vício de vontade que tenha o condão de macular o consentimento outorgado e, com isso, afaste sua validade[220].

Sem embargos, conclui-se que há inequívoca preservação da voluntariedade dos indivíduos presos ou sob medidas cautelares diversas da prisão, porquanto a liberdade psíquica e a capacidade de autodeterminação não são comprometidas em razão da momentânea restrição à liberdade física[221].

3.1.1.2.2. A (in)dispensabilidade do advogado como requisito de validade do ato

Conforme já exposto anteriormente, há entendimento doutrinário de que o ato somente seria válido caso o acusado, preso ou solto, esteja acompanhado de um advogado, invocando-se dois precedentes jurisprudenciais das Cortes Espanholas[222].

---

[220] Ademais, se adotada esta premissa da intimidação ambiental, não se poderia sequer se tomar por válida uma confissão do acusado na Delegacia de Polícia, após sua prisão em flagrante, porquanto o ambiente seria supostamente hostil e intimidador. Esta concepção, porém, traz consigo uma injustificável pecha de que todo o ato perpetrado em ambiente policial seja cerceador da autonomia da vontade do outorgante, o que é incongruente com o fato de o Delegado de Polícia, enquanto servidor público dotado da presunção de legalidade e veracidade de seus atos, exercer relevante função de assegurar os direitos e garantias fundamentais do acusado, podendo deixar de lavrar o flagrante quando ausentes as hipóteses do artigo 302 do Código de Processo Penal e até mesmo aplicar a fiança, nos termos do artigo 322 do mesmo Diploma Legal. A concepção chegaria ao paradoxo de, após cientificado de seu direito constitucional ao silêncio, admitir-se apenas a validade das alegações exculpatórias do acusado quanto ao cometimento do delito ou sua intenção de permanecer em silêncio, tomando-se a confissão como ato viciado em razão do ambiente em que prestado. Ignora-se, inclusive, que por vezes a confissão é uma medida de interesse processual do próprio acusado, haja vista que pode servir como estratégia processual para sinalizar ao Ministério Público a intenção de celebrar um acordo de não persecução penal (artigo 28-A do Código de Processo Penal), que posteriormente será firmado na presença de seu advogado.

[221] Não há como se invocar, todavia, o princípio da isonomia na presente hipótese. Com efeito, diferentemente da colaboração premiada, em que há um benefício ao agente que decide colaborar, o livre fornecimento de dados armazenados em aparelhos celulares não traz qualquer benefício direto ou indireto, senão uma análise mais rápida do conteúdo do aparelho e sua liberação de forma ágil. Ainda assim, justifica-se a possibilidade da cessão voluntária dos dados, porquanto não se verifica qualquer coação ilegal que tenha suprimido a margem de escolha do imputado.

[222] LOPES JR. Aury. MORAIS DA ROSA, Alexandre. *Critérios de validade para vasculhar o celular (WhatsApp) do preso*. Disponível em <https://www.conjur.com.br/2018-mai-25/limite-penal-criterios-validade-vasculhar-celular-whatsapp-preso>. Acesso em 20 de dezembro de 2020. Os autores aponta, ainda, a

Entretanto, conquanto a presença do advogado seja relevante e recomendável para o ato de consentimento, não nos parece que o ordenamento jurídico brasileiro reconheça sua indispensabilidade enquanto condição de validade do ato praticado, ao contrário do que fez a legislação espanhola para os acusados presos ou conduzidos pelas autoridades.

A Constituição Espanhola, em seu artigo 17.3[223], assegura que a pessoa detida será informada, de forma imediata e compreensível, dos direitos e razões de sua detenção, bem como será garantida a presença de advogado nas diligências policiais e judiciais, nos termos estabelecidos pela lei.

De igual sorte, o artigo 520 da *Ley de Enjuiciamiento Criminal* assegura uma plêiade de direitos assegurados à pessoa presa. Especialmente no tocante ao indivíduo preso, os artigos 520.2.c, 520.5 e 520.6.b e 520.6.c[224] conferem o direito ao preso

---

necessidade da presença do advogado para os indivíduos soltos que desejem fornecer voluntariamente o acesso aos dados armazenados no aparelho celular, ao sustentar que "(...) o investigado solto que se dirige ao estabelecimento policial e autoriza, juntamente e na presença de seu advogado, o acesso às mensagens, realiza ato cooperativo e desprovido de pressões das mais variadas formas. Nessa hipótese, o investigado pode franquear, devendo a diligência ficar registrada, bem assim o material extraído (eficácia da cadeia de custódia) (...)".

[223] Artículo 17.

3. Toda persona detenida debe ser informada de forma inmediata, y de modo que le sea comprensible, de sus derechos y de las razones de su detención, no pudiendo ser obligada a declarar. Se garantiza la asistencia de abogado al detenido en las diligencias policiales y judiciales, en los términos que la ley establezca

[224] Artículo 520.

2. Toda persona detenida o presa será informada por escrito, en un lenguaje sencillo y accesible, en una lengua que comprenda y de forma inmediata, de los hechos que se le atribuyan y las razones motivadoras de su privación de libertad, así como de los derechos que le asisten y especialmente de los siguientes:

(...)

c) Derecho a designar abogado, sin perjuicio de lo dispuesto en el apartado 1.a) del artículo 527 y a ser asistido por él sin demora injustificada. En caso de que, debido a la lejanía geográfica no sea posible de inmediato la asistencia de letrado, se facilitará al detenido comunicación telefónica o por videoconferencia con aquél, salvo que dicha comunicación sea imposible.

5. El detenido designará libremente abogado y si no lo hace será asistido por un abogado de oficio. Ninguna autoridad o agente le efectuará recomendación alguna sobre el abogado a designar más allá de informarle de su derecho.

La autoridad que tenga bajo su custodia al detenido comunicará inmediatamente al Colegio de Abogados el nombre del designado por el detenido para asistirle a los efectos de su localización y transmisión del encargo profesional o, en su caso, le comunicará la petición de nombramiento de abogado de oficio.

Si el detenido no hubiere designado abogado, o el elegido rehusare el encargo o no fuere hallado, el Colegio de Abogados procederá de inmediato al nombramiento de un abogado del turno de oficio.

El abogado designado acudirá al centro de detención con la máxima premura, siempre dentro del plazo máximo de tres horas desde la recepción del encargo. Si en dicho plazo no compareciera, el Colegio de Abogados designará un nuevo abogado del turno de oficio que deberá comparecer a la mayor brevedad y siempre dentro del plazo indicado, sin perjuicio de la exigencia de la responsabilidad disciplinaria en que haya podido incurrir el incompareciente.

6. La asistencia del abogado consistirá en:

(...)

de escolher e designar um advogado, bem como que, caso não o possua, que lhe seja nomeado um profissional para acompanhar seu depoimento, assegurando-se o contato pessoal, telefônico ou por videoconferência. Ainda, os dispositivos legais apontam ser direito do advogado intervir nas declarações a serem prestadas, além de informar ao detido as consequências da prestação ou denegação de consentimento para as práticas das diligências que a exigirem.

Ademais, o artigo 767 da *Ley de Enjuiciamiento Criminal*[225], a partir da reforma legislativa de 2002, também passou a dispor sobre a imprescindibilidade de se designar um advogado ("*letrado*"), desde a detenção de uma pessoa ou a partir do momento em que as atuações policiais resultarem na imputação de um delito a pessoa certa e determinada. Portanto, *ex vi* o disposto na legislação processual penal espanhola, é imprescindível a nomeação de um advogado ao acusado (*detenido*), especialmente quando ele decide prestar suas declarações ou conferir seu consentimento para a prática de determinado ato ou diligência. Idêntica previsão, todavia, não seria extensível ao acusado que está solto[226].

---

b) Intervenir en las diligencias de declaración del detenido, en las diligencias de reconocimiento de que sea objeto y en las de reconstrucción de los hechos en que participe el detenido. El abogado podrá solicitar al juez o funcionario que hubiesen practicado la diligencia en la que haya intervenido, una vez terminada ésta, la declaración o ampliación de los extremos que considere convenientes, así como la consignación en el acta de cualquier incidencia que haya tenido lugar durante su práctica.

c) Informar al detenido de las consecuencias de la prestación o denegación de consentimiento a la práctica de diligencias que se le soliciten.

[225] Artículo 767.

Desde la detención o desde que de las actuaciones resultare la imputación de un delito contra persona determinada será necesaria la asistencia letrada. La Policía Judicial, el Ministerio Fiscal o la autoridad judicial recabarán de inmediato del Colegio de Abogados la designación de un abogado de oficio, si no lo hubiere nombrado ya el interesado.

Registre-se, por oportuno, que a Instrucción 12/2007, da "Secretaria de Estado de Seguridad" sobre los comportamientos exigidos a los miembros de las fuerzas y cuerpos de seguridad del estado para garantizar los derechos de las personas detenidas o bajo custodia policial, também assegura, como *derechos del detenido*, o de "(...) 5.- Se pondrá especial empeño en garantizar que el derecho a la asistencia jurídica se preste de acuerdo con lo previsto en el ordenamiento jurídico, utilizando los medios disponibles para hacer efectiva la presencia del abogado a la mayor brevedad posible. Para ello, la solicitud de asistencia letrada se cursará de forma inmediata al abogado designado por el detenido o. en su defecto, al Colegio de Abogados. reiterando la misma, si transcurridas tres horas de la primera comunicación, no se hubiera personado el letrado. En el libro de telefonemas se anotará siempre la llamada o llamadas al letrado o Colegio de Abogados y todas las incidencias que pudieran producirse (imposibilidad de establecer comunicación, falta de respuesta etc) (...)".

[226] Luis M. Uriarte Valiente e Tomás Farto Piay, reconhecem que o direito é assegurado apenas àquele que estiver detido, não se aplicando extensivamente ao imputado solto. Sustentam os autores, baseados em precedentes jurisprudenciais, que "(...) el artículo 17 de la Constitución Española y el artículo 520 de la Ley de Enjuiciamiento Criminal, reconocen como derecho fundamental la asistencia de Letrado en las declaraciones, pero ambos preceptos se refieren única y exclusivamente al detenido, por lo que no cabe extender la previsión en ellos contenida al imputado que no se encuentra detenido; la prohibición de indefensión que recoge al artículo 24 de la Constitución Española, se satisface con la simple información al imputado no detenido de su derecho a ser asistido por un Letrado, no produciéndose por tanto indefensión, si el declarante no se acoge a

Lastreando-se nas previsões legislativas expressas acerca da indispensabilidade do *letrado* ao indivíduo preso, especialmente por se tratar de direito fundamental a ele assegurado, a Suprema Corte Espanhola interpretou que o ato de consentimento, para que seja válido, também deveria ser acompanhado de um advogado[227].

Como se verifica, há expressa previsão do auxílio de advogado ao indivíduo preso, especialmente para o ato de consentimento, sendo uma peculiaridade da legislação ibérica que, em verdade, não possui idêntica previsão e correlação no ordenamento jurídico brasileiro, salvo nos casos expressos em lei.

Em verdade, especialmente no que tange aos acusados presos em flagrante delito, a lavratura do auto, oitiva de testemunhas, interrogatório do imputado, entrega de nota de culpa e demais formalidades inerentes ao ato poderão ser realizadas sem a presença do advogado[228], o qual será obrigatoriamente comunicado no prazo de 24 (vinte

---

tal derecho y presta declaración voluntariamente sin dicha asistencia, como así proclama la sentencia del Tribunal Supremo de 20 de enero de 1995, argumentando además y por lo que al procedimiento abreviado se refiere, que es éste, y conforme a lo previsto en el artículo 784.1 de la Ley de Enjuiciamiento Criminal, la designación de Letrado sólo es obligatoria al abrirse el período de plenário (...)" (VALIENTE, Luis M. PIAY, Tomás Farto. *El proceso penal español: jurisprudencia sistematizada.* Madrid: Editora La Ley, 2007, p. 372-373). Na mesma linha a decisão do Tribunal Supremo Espanhol, na sentença n.º 1498/1998: "(...) aduce la vulneración de la asistencia letrada porque en su declaración ante la Guardia Civil no contó con ella, pero al no estar detenido, ni imputado, tal presencia de Abogado resultaba innecesaria - artículo 17.3 de la Constitución Española y 520.2 de la Ley de Enjuiciamiento Criminal - mas cuando en calidad de imputado comparece ante el Juzgado de Instrucción, se el asiste de Letrado y se le hicieron todas las advertencias legales previas a tal declaración, como constan documentadas en la causa (...)".
A Corte Suprema Espanhola, no bojo do julgamento STS 863/2002, de 11 de fevereiro de 2002, admitiu ser válido o consentimento e, por conseguinte, a realização de exame radiográfico de pessoa suspeita de ter ingerido porções de entorpecentes, porquanto a situação não seria equiparável a uma detenção ou declaração autocriminatória, o que afastaria a necessidade de acompanhamento por advogado e a formal cientificação de seus direitos legais: "(...) La sumisión de una persona a examen radiográfico, si presta su consentimiento, se ha considerado diligencia de investigación válida, que no exige ninguna información de derechos, ni asistencia de letrado, por entenderse que no es equiparable a una detención, ni a una declaración autoinculpatoria. A esta conclusión llegó esta Sala en el Pleno de 5 de febrero de 1999, y la doctrina se ratificó por la jurisprudencia, así entre otras, en las sentencias 1910/2000 de 13.12, y en las 29.1 y 23 y 26.11.2001 (...)".

[227] No julgado STS n.º 2032/2001, de 5 de novembro de 2001, a Suprema Corte reconheceu a necessidade de assistência letrada para que um indivíduo detido possa manifestar seu consentimento para a entrada e registro em seu domicilio, sem a correspondente autorização judicial. Na ocasião, argumentou-se que "(...) as razones…sobre el alcance de la asistencia letrada en las diligencias policiales son perfectamente extensibles al caso que nos ocupa, ya que tal autorización o consentimiento es igual o incluso más trascendente que la propia declaración (...)". De igual sorte, no julgamento STS n.º 1061/1999 (29 de junho de 1999), a Corte Suprema apontou que "(...) l consentimiento prestado por el detenido, se halla viciado al no gozar de las necesarias notas de libertad y autonomía que concurren cuando se dan circunstancias de signo distinto… la asistencia de Letrado es, en todo caso, decisiva para la validez de una toma de postura del detenido, que afecte a sus derechos fundamentales y que pueda comprometer seriamente su defensa (...)".

[228] STJ, HC n.º 442.334/RS, 5ª Turma, Rel. Min. Reynaldo Soares da Fonseca, julgado em 21 de junho de 2018, DJe 29/06/2018.

e quatro) horas após a realização da prisão, na forma do artigo 306, § 1º, do Código de Processo Penal.

Ao que se vê, diferentemente dos precedentes espanhóis, a legislação processual penal prevê que a comunicação se dá *a posteriori*, sendo perfeitamente válido o ato praticado desacompanhado do advogado nomeado ou defensor público[229]. Em verdade, o artigo 185 do Código de Processo Penal se refere à obrigatória presença de advogado durante o interrogatório judicial, o que não alcançaria o inquérito policial, que assume características eminentemente inquisitoriais.

Ademais, quando o legislador entendeu ser imprescindível a presença do advogado, ele o fez expressamente. Por força de expressa previsão legal contida no artigo 3º-C, §§ 1º e 7º da Lei n.º 12.850/2013, a colaboração premiada exige a presença de advogado ou defensor público em todas as tratativas relacionadas ao tema, bem como durante o ato judicial destinado a colher sua voluntariedade, estando o indivíduo com sua liberdade física restringida ou não.

Infere-se que a indispensável presença de um advogado é uma garantia conferida ao indivíduo que pretenda celebrar a colaboração premiada, a fim de que ele, amparado pelo auxílio de um profissional técnico, tenha integral conhecimento das informações existentes no processo, das consequências de sua decisão e, assim, forme seu convencimento no intuito de escolher realizar a colaboração. Não bastasse, a presença do advogado também salvaguarda a integridade da manifestação de vontade do indivíduo, de forma a rechaçar toda e qualquer coação física ou psicológica que possa influenciar na sua liberdade de escolha.

Assim, poder-se-ia cogitar na mesma obrigatoriedade, especialmente em se tratando de acusados presos que, eventualmente, venham a consentir com o acesso aos

[229] Guilherme Madeira Dezem aponta que a inexistência de comunicação ao advogado indicado ou à Defensoria Pública poderia ensejar nulidade, diante da necessidade de proteção de direitos e garantias fundamentais, sendo importante que a concretização, para além do plano teórico, seja feita pela prática diárias nos processos e inquéritos em todo o país (DEZEM, Guilherme Madeira. *Curso de processo penal*. 6ª edição, São Paulo: Editora Revista dos Tribunais, p. 931). Entretanto, o Superior Tribunal de Justiça (STJ) decidiu pela não ocorrência de nulidade diante da ausência de comunicação do auto de prisão em flagrante à Defensoria Pública no prazo estabelecido em lei, em razão da ausência da instituição na localidade ou nas proximidades: STJ, HC n.º 186.456/MG, 5ª Turma, Rel. Min. Jorge Mussi, julgado em 11 de outubro de 2011, DJe 19/10/2011.

dados armazenados em seu aparelho celular. Entretanto, não nos parece que a presença do advogado ou defensor público, conquanto recomendada, seja requisito imprescindível para a validade do ato de consentimento.

Cumpre destacar que a colaboração premiada traz consequências gravosas ao colaborador, por se tratar de ato que, necessariamente, exige a confissão e a necessidade de produzir os resultados especificamente trazidos pela Lei n.º 12.850/2013, sob pena de não receber o prêmio assegurado pelo seu ato colaborativo. Ademais, trata-se de verdadeiro negócio jurídico processual[230] complexo em que, dentro dos limites contemplados na lei, há uma ampla margem de negociação entre os órgãos estatais (Ministério Público e Polícia Judiciária) e o colaborador, especialmente no tocante aos benefícios, prazos e condições que podem ser pactuadas.

Portanto, são essas peculiaridades que justificam a imprescindibilidade do amparo técnico-jurídico, a ser realizado pelo advogado ou defensor público. Ainda que o advogado sirva, também, como garantidor da livre manifestação de vontade do colaborador, não nos parece que essa seja a razão de sua obrigatoriedade.

Com efeito, basta ver que a Lei n.º 12.850/2013 exige a presença de advogado ou defensor público para todo indivíduo que pretenda realizar a colaboração, estando preso ou não. Assim, revela-se que não é o fato de estar preso que atrai a necessidade da atuação do profissional, mas sim a complexidade jurídica do ato e a grande liberdade conferida às partes para celebração dos termos do acordo de colaboração, o que demanda a habilidade técnica para se assegurar uma posição favorável ao colaborador[231].

Com relação ao consentimento para o acesso aos dados armazenados no aparelho celular, é necessário salientar que o ato não detém qualquer dificuldade técnica que demande o auspício de profissional habilitado, senão a ciência do acusado quanto às consequências de seu consentimento, bem como sequer exige qualquer capacidade, habilidade técnica ou arte negocial de seus termos e condições.

---

[230] Artigo 3º-A da Lei n.º 12.850/2013.

[231] Trata-se de uma "dupla garantia", indicando que o procedimento só é aperfeiçoado quando haja um consenso do colaborador e do advogado, principalmente para que o colaborador tenha consciência das implicações penais, processuais e pessoas do ato de colaboração (FERNANDES, Antônio Scarance. *Teoria geral do procedimento e o procedimento no processo penal*. São Paulo: Editora RT, 2005, p. 283)

A figura do "consentimento" aparta-se da ideia negocial insinuada pela colaboração premiada, amoldando-se mais à noção trazida pelo artigo 5º, inciso XII, da Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018), que a tem como ato de disposição do titular, em exercício de sua autodeterminação na esfera das escolhas pessoais, que poderá legitimar a utilização destes dados por outra pessoa ou instituição[232].

Desta feita, se para a realização de um ato de prisão em *flagrante,* que avança em relevante densidade no espectro de direitos e garantias fundamentais do cidadão, a presença do advogado é considerada prescindível para a formalização e validade do ato, não há como se estabelecer raciocínio distinto com relação aos atos de consentimento e cessão voluntária do acesso aos dados contidos em aparelhos celulares, mormente considerando que o ato se dá, via de regra, no momento da prisão.

Ainda que se reconheça que a presença do profissional contribua para se dar ainda mais lisura à voluntariedade do ato de consentimento, não há previsão legal que indique a imprescindibilidade da sua presença como condição de validade e eficácia. Caso o advogado esteja presente, é recomendável que o profissional seja convidado a assinar o termo de consentimento juntamente com o titular dos dados armazenados no aparelho celular, especialmente em situações de acusados presos, para se afastar eventuais alegações de coações psicológicas em razão da constrição física de sua liberdade.

É também de bom alvitre que o ato de consentimento, oralmente prestado, seja ratificado por escrito ou corroborado por outros meios de provas, notadamente depoimentos de testemunhas, filmagens autorizadas pelo acusado ou outros meios lícitos, para se garantir que o ato foi desprovido de qualquer vício que o inquine e que o consentimento fora efetivamente prestado pelo outorgante, a fim de se assegurar a validade das provas decorrentes do ato de consentimento perpetrado.

---

[232] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* 2ª ed. São Paulo: Editora RT, 2019, p. 302.

3.1.1.3 Manifestação informada e inequívoca: as formas de manifestação do consentimento

Avançando-se na tarefa de delimitar os requisitos para a validade do ato de consentimento, dessume-se a necessidade de se analisar dois requisitos essenciais para o ato consentido: o conhecimento do outorgante e a forma de manifestação do consentimento.

3.1.1.3.1 Conhecimento e informação: o direito de não se autoincriminar

É certo que o titular dos dados armazenados no aparelho celular possui uma legítima expectativa de privacidade quanto ao conteúdo das informações ali armazenadas. Assim, para que se permita a completa captação da vontade efetiva do outorgante do conhecimento, é necessário que ele detenha um mínimo de conhecimento das consequências do ato[233] para que, assim, reflita sobre seu desejo efetivo de colaborar[234].

Portanto, não basta que a autoridade investigativa conceda ao acusado informações sobre os fatos investigados, o que é elementar àquele que poderá fornecer uma fonte de prova aos órgãos estatais. É necessário que o outorgante seja informado de que os dados contidos no aparelho poderão ser utilizados na investigação, bem como que ele não tem obrigação legal de cedê-los voluntariamente, diante da possibilidade de não desejar produzir provas contra si mesmo[235].

---

[233] O valor do conhecimento claro e inequívoco para o consentimento é objeto de expressa previsão no artigo 9º, § 1º, da Lei n.º 13.709/2018, que impõe, na hipótese em que o consentimento é requerido, sua nulidade caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

[234] Interpretando-se a regra do consentimento nas hipóteses de busca domiciliar, Bottini registra que "(...) maior relevo tem a questão do grau de esclarecimento do morador que consentiu na realização da busca e apreensão. Para que se solucione o conflito de interesses — busca da verdade para realização da justiça e inviolabilidade do domicílio — por via consensual, é necessário que aquele que consente tenha pleno conhecimento das circunstâncias e consequências da realização da busca domiciliar, bem como que isso seja documentado. No ponto, não há previsão legal. Contudo, tratando-se de medida que pode implicar a produção de prova contra o próprio morador que consente com a busca, para que ele decida de forma justa e válida se franqueará a entrada em sua residência, necessário que no mínimo lhe sejam esclarecidos seus direitos e o alcance da inviolabilidade do domicílio, bem como as consequências da realização da busca domiciliar. A mesma lógica e o mesmo cuidado são observados nos procedimentos de interrogatórios, tanto judicial quanto policial, a fim de garantir o direito da pessoa de não produzir prova contra si (deriva das previsões constitucionais — artigo 5º, LVII e LXII — e consagrado do Pacto de São José da Costa Rica, artigo 8º) (...)" (BOTTINI, Pierpaolo Cruz. *Buscas policiais sem mandado judicial parecem ter se normatizado*. Disponível em <https://www.conjur.com.br/2014-nov-11/direito-defesa-buscas-policiais-mandado-parecem-normatizado#_edn7>. Acesso em: 20 de dezembro de 2020).

[235] A previsão de que o réu não é obrigado a produzir provas contra si mesmo encontra respaldo no artigo 8º, 2, *g*, do Pacto de San José da Costa Rica, bem como tutelados também pelo artigo 5º, incisos LVII e LXII, da

O conhecimento da informação pelo acusado, a fim de que possa fazer sua escolha livre e desimpedida, tem relação direta com o direito ao silêncio assegurado na *Fifth Amendment*, bem explorada na clássica decisão da Suprema Corte Norte-Americana no caso *Miranda v. Arizona, 384 U.S. 436 (1966)*[236], em que se concluiu que o direito ao silêncio é garantido a partir da custódia e detenção do acusado.

O Supremo Tribunal Federal já reconheceu, em situações análogas[237], que antes de um interrogatório formal ou entrevista com propósitos investigativos, o acusado deve ser cientificado quanto ao direito de permanecer em silêncio e de ter, se assim desejar, o auxílio de um advogado (art. 7º, XXI, da Lei n.º 8.906/1994), sob pena de ilicitude da prova produzida.

A partir destes fundamentos, é indiscutível que qualquer renúncia a direito assegurado deve ser objeto de prévio conhecimento e informação ao outorgante[238]. Desta feita, é fundamental que o outorgante do consentimento, para além de não ser coagido física ou psicologicamente para a realização do ato de consentimento com o acesso aos

---

Constituição Federal. Não é o propósito do presente trabalho científico, ao analisar as hipóteses de acesso a dados armazenados em aparelhos celulares, imiscuir-se no estudo avançado sobre a aplicação do princípio do princípio do *nemo tenetur se detegere*. Para uma compreensão sobre o tema, recomenda-se: AZEVEDO, David Teixeira. *O interrogatório do réu e o direito ao silêncio.* Revista dos Tribunais, São Paulo, v. 682, ago. 1992; CÓRDOBA, Gabriela E. *Nemo tenetur se ipsum accusare: ¿principio de pasividad?.* Estudios sobre Justicia Penal: Homenaje al Profesor Julio B. J. Maier, Buenos Aures: Editores del Puerto, 2005, p. 279-299; QUEIJO, Maria Elizabeth. *O direito de não produzir prova contra si mesmo*. São Paulo: Editora Saraiva, 2003; SAAD, Marta. *O direito de defesa no inquérito policial.* São Paulo: Revista dos Tribunais, 2004.

[236] Disponível em <https://supreme.justia.com/cases/federal/us/384/436/>. Acesso em 20 de dezembro de 2020. A própria jurisprudência norte-americana tem excepcionado o mandamento da advertência prevista no caso *Miranda v. Arizona*, especialmente em situações de "segurança pública" (*New York v. Quarles*, 467 U.S. 649. Disponível em <https://supreme.justia.com/cases/federal/us/467/649/>. Acesso em 20 de dezembro de 2020; e *People of the State of New York v. Scott F. Doll*, October 17, 2013, disponível em <http://www.courts.state.ny.us/Reporter/3dseries/2013/2013_06726.htm>) ou nas hipóteses de questionamentos e indagações feitas por autoridades policiais, em situações em que o indivíduo não teria sua liberdade de ir e vir cerceada, especialmente se o indivíduo foi voluntariamente à Delegacia de Polícia (Oregon v. Mathiason, 429 U.S. 492 (1977). No caso *Schneckloth v. Bustamonte*, 412 U.S. 218 (1973), a Suprema Corte sustentou que as buscas consentidas são constitucionais e que cabe ao órgão governamental comprovar que o consentimento fora efetivamente prestado. Todavia, decidiu-se que, muito embora o conhecimento da pessoa do direito de recusar o consentimento deva ser levado em consideração, o Estado não precisa provar que aquele que deu permissão para a busca sabia que ele tinha o direito de negar seu consentimento. Disponível em <https://supreme.justia.com/cases/federal/us/412/218/>. Acessos em: 20 de dezembro de 2020).

[237] STF, HC*s* n.º 80.949/RJ, 1ª Turma, Rel. Sepúlveda Pertence, julgado em 30 de outubro de 2001, DJ 14/12/2001; STF, Reclamação n.º 33.711/SP, 2ª Turma, Rel. Min. Gilmar Mendes, julgado em 11 de junho de 2019, DJe 22/08/2019.

[238] O Superior Tribunal de Justiça (STJ) reconheceu expressamente que, nas hipóteses de autorização dada pelo investigado para acesso aos dados armazenados em seu aparelho celular, há necessidade de se garantir que lhe tenha sido assegurado o direito de não produzir provas contra si mesmo (STJ, Recurso Especial n.º 1.744.974-MT, 6ª Turma, Rel. Min. Laurita Vaz, julgado em 12 de março de 2019, DJe 29/03/2019)

dados, tenha pleno conhecimento quanto à não obrigatoriedade de fornecê-los e que os dados contidos no aparelho poderão ser utilizados na investigação.

3.1.1.3.2 Formas de consentimento

Ainda no estudo do consentimento, é necessário averiguar de qual forma o consentimento pode ser prestado, a fim de que se assegure sua validade.

No âmbito do ordenamento jurídico brasileiro, até o advento da Lei Geral de Proteção de Dados (Lei n.º 13.709/2018) e da Lei do Marco Civil da *Internet* (Lei n.º 12.965/2014), não havia um regramento específico sobre o tema.

Assim, a doutrina vinha adotando interpretação semelhante àquela conferida pela jurisprudência espanhola no tocante às buscas domiciliares[239], exigindo-se o consentimento de forma expressa, ao menos que a autorização tácita tenha se dado de maneira bastante ostensiva e indubitável quanto à intenção do outorgante, mediante atos de colaboração ou evidente ausência de obstrução ao acesso. Ademais, toda e qualquer dúvida quanto à efetiva anuência deveria ser interpretada como se não houvesse existido[240].

Todavia, com o advento da Lei Geral de Proteção de Dados (Lei n.º 13.709/2018), estabeleceu-se no artigo 8º, *caput*, que o consentimento para fins de tratamento de dados pessoais deverá ser fornecido por escrito ou por outro meio que demonstra a manifestação de vontade do titular.

---

[239] Como visto, o artigo 551 da *Ley de Enjuiciamiento Criminal* espanhola permitiu que o consentimento seja prestado de forma expressa ou tácita. Todavia, a jurisprudência espanhola (Suprema Corte Espanhola, no julgamento do STS n.º 6328/2006, Sala de lo Penal, Ponente Juan Ramon Berdugo Gomez de La Torre, recurso n.º 1396/2005, julgado em 14/03/2006) tem interpretado o postulado legal de maneira restritiva, apontando que o consentimento tácito deve ser demonstrado de forma inequívoca, mediante atos próprios de não oposição e, sobretudo, de colaboração. Ademais, a dúvida sobre a realização do consentimento deve ser resolvida em favor da não autorização, como forma de se assegurar uma interpretação mais favorável aos direitos fundamentais do cidadão. Ainda em uma perspectiva de legislação comparada, impende destacar que nos Estados Unidos da América, o consentimento permite a realização de busca de um objeto ou um local sem uma autorização judicial e tampouco uma *probable cause*, que consiste em um conceito jurídico vago relacionado a um *standart* probatório mínimo para determinado ato, que representa mais do que a mera suspeita (SALTZBURG, Stephen A, SCHLUETER, David A. *Federal Criminal Procedure Litigation Manual*, Huntington, New York: Editora Juris, 2015, p. 10). Na França, o artigo 76 do *Code de procédure pénale* também estabelece, de forma expressa, que o consentimento deve ser outorgado de forma expressa e documentada por escrito.

[240] PITOMBO, Cleunice Valentim Bastos. *Da Busca e da Apreensão no Processo Penal*. São Paulo: Editora Revista dos Tribunais, 1999, p. 118.

De igual sorte, a Lei do Marco Civil da *Internet* (Lei n.º 12.965/2014), em seu artigo 7º, inciso VII e IX, estabeleceu ser direito do usuário da *internet* que seu consentimento, para tratamento de dados pessoais na rede mundial de computadores, seja expresso e informado.

Denota-se, pois, que as legislações recentes dispuseram que o consentimento deverá se dar de forma inequívoca, mas não o revestiram de qualquer formalidade, permitindo-se que seja fornecido de forma escrita ou por outro meio de manifestação da vontade. Trata-se, em verdade, de uma clara demonstração da intenção do legislador em resguardar a proteção aos dados pessoais e somente permitir seu tratamento pelo Poder Público, mediante manifestação inequívoca de seu titular.

Adotando-se esta premissa interpretativa, pode-se concluir por silogismo que, se os dados pessoais somente podem ser objeto de tratamento de forma inequívoca e expressa e os dados armazenados em aparelhos celulares são, no mais das vezes, eminentemente pessoais, o consentimento para acesso aos dados armazenados também deve se dar de forma inequívoca.

Não se ignora a previsão contida no artigo 4º, inciso III, alínea *d*, da Lei n.º 13.709/2018, que excluiu a incidência da Lei Geral de Proteção de Dados Pessoais (LGPD) ao tratamento de dados pessoais realizado para fins exclusivo de atividades de investigação e repressão de infrações penais. Todavia, a própria Lei n.º 13.709/2018 estabeleceu, no artigo 4º, § 1º, que o tratamento de dados pessoais para fins de atividades de investigação e repressão de infrações penais deverão ser regidos por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na legislação.

Ainda que o investigado não necessite concordar com a coleta, armazenamento e processamento de seus dados no contexto de uma investigação penal[241], é inegável que, nas hipóteses em que este consentimento for exercido – *v.g.*, para acesso ao

[241] Ministério Público Federal. *Roteiro de autuação: sistema brasileiro de proteção e acesso a dados pessoais: análise de dispositivos da lei de acesso à informação, da lei de identificação civil, da lei do marco civil da internet e da lei nacional de proteção de dados* – Brasília: MPF/3ª CCR, 2019, p. 76-81.

conteúdo dos dados armazenados em seu aparelho celular –, as balizas estabelecidas pela Lei Geral de Proteção de Dados Pessoais (LGPD) podem servir como referência para lastrear a forma e os requisitos do ato, diante de sua recente edição e inovação no tratamento do tema.

Sendo o consentimento um ato voluntário de plena dispensa da proteção constitucional à privacidade, intimidade e vida privada, bem como um inequívoco ato de disposição de dados pessoais, reforça-se a conclusão de que este consentimento deva ser dado de forma expressa[242].

Finalmente, não havendo qualquer formalidade especial predeterminada, é lícito que o consentimento seja proferido de maneira livre, inclusive de forma verbal ou por gestos, como o fornecimento voluntário das senhas de acesso ao aparelho celular por parte do acusado[243].

Embora seja recomendável a colheita de um registro formal do consentimento por parte do acusado, não nos parece que seja elemento necessário para validade do ato. Com efeito, por não haver prévia exigência legal da documentação posterior do consentimento como elemento para validade do ato – à exemplo do que expressamente optou a legislação portuguesa[244] –, o registro escrito posterior é juridicamente dispensável, se outros meios de prova puderem comprovar a voluntariedade da outorga concedida.

---

[242] BOTTINI, Pierpaolo Cruz. *Buscas policiais sem mandado judicial parecem ter se normatizado*. Disponível em <https://www.conjur.com.br/2014-nov-11/direito-defesa-buscas-policiais-mandado-parecem-normatizado#_edn7>. Acesso em: 20 de dezembro de 2020; LOPES JR., Aury. *Direito Processual Penal.* Op. cit., p. 560.

[243] Jennifer Badaró aponta que "(...) a garantia à intimidade, embora seja assegurada constitucionalmente, dela pode abrir mão o próprio sujeito. No caso de uma prisão em flagrante, em que a autoridade policial apreende o celular do preso e este fornece sua senha, está autorizado que o agente tenha acesso a todos os dados constantes do aparelho, inclusive seus e-mails e conversas de WhatsApp e Facebook. As provas obtidas poderão ser utilizadas no procedimento criminal e não serão consideradas ilícitas (...)" (BADARÓ, Jennifer Falk. *Produção de provas: WhatsApp, Facebook, e-mail.* AASP Boletim, Edição n.º 3096, Dezembro/2019).

[244] O Código de Processo Penal Português, especialmente em seu artigo 174, n.º 5, alínea b , consigna como exceção à necessidade de ordem judicial autorizativa o consentimento do "visado" na realização das buscas, desde que sua manifestação de vontade seja, de qualquer forma, documentada. Como se vê, o ordenamento jurídico português não prevê qualquer forma especial para a manifestação do consentimento, o qual pode ser verbal ou escrito, bastando que seja documentado, ainda que a posteriori.

Trata-se de inegável ônus[245] imposto ao órgão estatal acusador, que tem o dever de atestar, por qualquer elemento de prova (inclusive depoimentos testemunhais[246] e filmagens autorizadas), que o consentimento fora prestado lícita e inequivocamente pelo outorgante.

3.1.1.4. Finalidade certa e determinada

Dentre os requisitos enumerados para a validade do consentimento manifestado pelo seu legítimo titular, é relevante destacar a necessidade de que este seja prestado para um caso concreto e determinado, sem que o ato de vontade expressado seja indicativo de que o acusado dispôs, genericamente, de toda e qualquer proteção assegurada à sua privacidade e intimidade[247].

---

[245] Nesta linha, o Superior Tribunal de Justiça decidiu que "(...) a afirmação do Juízo sentenciante de que a defesa não comprovou a ausência de consentimento do réu para a submissão de seu aparelho celular a exame pericial constitui indevida inversão do ônus da prova e, por esse motivo, deve ser desconsiderada (...)" (STJ, RHC n.º 89.395/SP, 6ª Turma, Rel. Min. Rogério Schietti Cruz, julgado em 16 de agosto de 2018, DJe 28/08/2018)

[246] O Superior Tribunal de Justiça (STJ) reconheceu que os depoimentos testemunhais de policiais militares que participaram da diligência podem comprovar a validade do consentimento prestado pelo investigado ,quanto ao acesso aos dados armazenados em seu aparelho celular, bem como a inexistência de coação no ato de outorga (STJ, AgRg no REsp n.º 1.770.301, 6ª Turma, Rel. Min. Nefi Cordeiro, julgado em 18 de junho de 2019, DJE 28/06/2019). Outrossim, o Superior Tribunal de Justiça (STJ) admitiu que a quebra do sigilo de dados pode ser realizada mediante prévia autorização do investigado (STJ, RHC n.º 101.585/MG, 5ª Turma, Rel. Ministro Reynaldo Soares da Fonseca, julgado em 18 de outubro de 2018, DJe 26/10/2018). De igual sorte, em outro julgamento acerca do consentimento prestado pelo investigado quanto ao acesso aos dados armazenados, o Superior Tribunal de Justiça (STJ) deu guarida ao depoimento policial e decidiu que "(...) apesar de o impetrante afirmar que o paciente não teria autorizado os policiais a vasculharem seu aparelho celular, não há nas peças processuais quaisquer documentos que demonstrem que a medida teria sido forçada, notadamente porque o acusado, ao ser interrogado extrajudicialmente, manteve-se em silêncio (e-STJ fl. 69). Ademais, em consulta à página eletrônica do Tribunal de origem, constatou-se que já foi proferida sentença condenatória em desfavor do réu, ocasião em que o magistrado, após analisar toda a prova colhida no curso do feito consignou que "não há que se falar que acesso ao conteúdo de aparelho celular e do aplicativo whatsapp são ilícitos", pois "em seu interrogatório, o acusado admitiu que tinha imagens de diversas placas de motos e sequer mencionou que foi forçado a fornecer a senha de seu aparelho aos policiais", tendo o miliciano, por sua vez, assegurado que "foi autorizado por HUMBERTO a ver o conteúdo do aparelho que estava com ele (...)" (STJ, HC n.º 512.693/SP, 5ª Turma, Rel. Min. Jorge Mussi, julgado em 15 de agosto de 2019, DJe 22/08/2019). No mesmo sentido: STJ, AgRg no RHC n.º 116.792/SP, 5ª Turma, Rel. Min. Leopoldo de Arruda Raposo, julgado em 20 de fevereiro de 2020, DJe 03/03/2020; STJ, HC n.º 537.274/MG, 5ª Turma, Rel. Min. Leopoldo de Arruda Raposo, julgado em 19 de novembro de 2019, DJe 26/11/2019.

[247] A Lei Geral de Proteção de Dados Pessoais dispõe expressamente que o consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas (artigo 8º, § 4º, da Lei n.º 13.709/2018). Como sustenta Giorgio Resta, "(...) quem consente não exprime propriamente a ausência de interesse na proteção, nem a ela renuncia, porém lança mão de um verdadeiro ato de exercício do direito de autodeterminação na esfera das escolhas pessoais (...)" (RESTA, Giorgio. *Revoca del consenso ed interesse al tratamento nella legge sulla protezione dei dati personali,* In: Rivista Critica del Diritto Privado, 200, p. 307, *apud* DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 2ª ed. São Paulo: Editora. RT, 2019, p. 302).

O artigo 5º, inciso XII, da Lei n.º 13.709/2018, estabelece expressamente que a concordância do titular dos dados se dá para uma finalidade determinada, que confere os limites objetivos para a atuação estatal. Assim, diante da pluralidade de dados armazenados em um aparelho celular, é possível que, em situações peculiares, o consentimento seja dado para acesso a determinados dados, sem englobar os demais previamente ressalvados pelo outorgante.

Cuida-se, pois, da mesma linha lógica adotada com relação ao consentimento do morador, na esfera da proteção constitucional conferida ao domicílio (artigo 5º, inciso XI, da Constituição Federal). Nestas hipóteses, é plenamente admissível que o responsável autorize o ingresso de policiais a determinados cômodos específicos, mas não a outros[248].

Assim, há de se reconhecer que poderá o acusado, de forma expressa, consignar que o consentimento voluntário é conferido para acesso a determinados dados previamente individualizados, tais como fotografias e anotações, mas não para as mensagens de texto trocadas em aplicativos de comunicação instantânea. Nestas hipóteses, caso os órgãos persecutórios estatais manifestem disposição em investigar o inteiro conteúdo do aparelho, para além dos limites consentidos expostos pelo outorgante, deverão adotar a cautela de postular autorização judicial para tanto, sob pena de ilicitude da prova produzida.

[248] Nos Estados Unidos da América, um raciocínio similar é desenvolvido a partir do *scope of consent*, que está relacionado aos limites impostos pelo outorgante à busca desprovida de uma autorização judicial. Os Tribunais Americanos têm analisado o *scope of consent* de forma casuística, a fim de constatar se as circunstâncias particulares do caso evidenciaram que o consentimento prestado, implícita ou explicitamente, limitou a busca a um determinado objeto específico. Caso se infira que os propósitos da busca ultrapassaram os propósitos regulares do consentimento conferido pelo outorgante, a prova amealhada deve ser suprimida. Sobre o tema, recomenda-se o manual para busca e apreensão em computadores e dispositivos eletrônicos, elaborado pelo Departamento de Justiça dos Estados Unidos: *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. Disponível em: <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf>. Acesso em 20 de dezembro de 2020.

Nesta senda, o consentimento para o acesso aos dados armazenados no aparelho celular deve ser vinculado ao propósito investigativo que o motivou[249], nos exatos limites da finalidade expressamente especificada[250].

Ainda, a autorização dada pelo seu titular jamais poderá ser interpretada como um ato de livre disposição de toda e qualquer forma de tutela de seu direito à privacidade e intimidade. Portanto, a autorização dada para acesso a dados armazenados em seu aparelho celular, em determinada investigação, não configura uma renúncia ao direito à privacidade e intimidade de dados armazenados em outros suportes informáticos (*v.g.,* computadores, *tablets* ou outros dispositivos móveis). Caso se faça necessário ter acesso ao conteúdo destes outros dispositivos, os órgãos de investigação deverão buscar, por regra, a via não consensual, com a correspondente prévia e fundamentada autorização judicial.

---

[249] Na Suprema Corte Canadense, já se reconheceu que o consentimento para a realização de busca e apreensão, especialmente a obtenção de amostra de sangue para um propósito específico, não necessariamente permite a intrusão à privacidade alheia para outros propósitos distintos. Entretanto, se nenhum limite específico é oposto pela polícia ou pela parte que consentiu com a utilização, pode não haver expectativa razoável de privacidade na utilização do elementos para um investigação posterior que não foi e não poderia ter sido antecipada pela polícia no momento em que o elemento foi coletado poderia não foram razoavelmente antecipados pela polícia no momento em que a amostra foi coletada (R. v. Borden, [1994] 3 S.C.R. 145, disponível em <https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1174/index.do>; R. v. Arp, [1998] 3 S.C.R. 339, disponível em <https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1664/index.do>. Acessos realizados em 20 de dezembro de 2020). De igual sorte, na Espanha, o precedente que definiu a necessidade de um objeto concreto e determinado para o consentimento foi fixado a partir do julgamento pelo Tribunal Supremo Espanhol do STS n.º 4770/2001, Sala de lo Penal, Ponente Joaquin Gimenez Garcia, recurso n.º 3315/1999, julgado em 06/06/2001. Na ocasião, o ingresso de agentes estatais em um domicílio havia sido autorizado pela proprietária, sob alegação de que buscavam apurar um suposto delito de maus tratos contra seu filho. Todavia, em razão de investigações independentes e aproveitando-se que a porta estava aberta, policiais do grupo de investigação a entorpecentes foram ao local e, sem colher o consentimento da moradora, passaram a diligenciar no imóvel e localizaram entorpecentes nas dependências do apartamento, resultando em um processo criminal contra o marido da proprietária. Assim, concluiu a Corte Espanhola pela "(...) nulidad de la entrada en el domicilio de los funcionarios policiales del Grupo de Estupefacientes al no existir autorización de la cotitular del piso para permitirles la entrada conocedora de la concreta investigación relativa al sobre recibido que les había llevado a dicha vivienda. Es claro que la autorización dada por la cotitular de una vivienda para permitir el acceso a la misma de la policía con una finalidad concreta no puede extenderse, ni por tanto cubre la entrada de otros policías por otra investigación independiente de la primera, la autorización dada lo fue en el marco y con la finalidad para la que fue solicitada --las gestiones con el hijo menor de la pareja, no fue un cheque em blanco-- ahí agotó toda su potencialidad legitimadora de la entrada. La subsiguiente entrada de los agentes de la Brigada de Estupefacientes, hubiera exigido de nueva y cumplida autorización de la cotitular del piso a sabiendas de la nueva investigación, o en su caso autorización judicial, al no existir aquella, ni solicitarse esta, es claro que dicha entrada vulneró el derecho a la inviolabilidad de domicilio reconocida como derecho fundamental en el art. 18-2º de la Constitución, pues resulta patente que no se está en el supuesto de flagrante delito, al no existir certeza de que por el solo hecho de proceder el sobre de Colombia, necesariamente debía contener droga en su interior (...)".

[250] MENDES, Carlos Hélder Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software,* p. 212.

Importa destacar, todavia, que a finalidade certa e determinada da autorização não impede a descoberta fortuita de provas, também chamada de "serendipidade" e "crime achado"[251], que consiste na localização de elementos probatórios de um novo crime ou de um novo autor, no âmbito de uma diligência investigativa previamente autorizada para um propósito específico[252].

Assim, considerando que o consentimento, observados os seus requisitos de validade, é uma forma lícita de autorização para o acesso aos dados contidos em aparelhos celular, não há como se afastar a possibilidade de que, durante as buscas realizadas para apurar um propósito específico, se identifiquem novas provas de outras infrações penais[253].

Entretanto, a validade das provas encontradas deve estar condicionada e circunscrita à forma em que a diligência foi realizada, a fim de se impedir que, em casos de abuso de autoridade ou desvio de finalidade, a prova fortuitamente encontrada venha a ser considerada lícita, legitimando-se o procedimento ilegal encetado[254].

---

[251] A previsão do encontro fortuito de provas é tratada expressamente pelo United States Code, em 18 U.S Code § 2517, 5: "(5)When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable". A *Ley de Enjuiciamiento Criminal* também trata das hipóteses de encontro fortuito, especialmente em seu *Artículo 579 bis.*

[252] BADARÓ, Gustavo Henrique Righi Ivahy. *Processo Penal*. Op. cit., p. 602. Com relação à "serendipidade", paira uma controvérsia relacionada à validade da prova fortuitamente encontrada. Em verdade, não há unanimidade no campo doutrinário: parte da doutrina sustenta sua inadmissibilidade enquanto prova (LOPES JR., Aury. *Direito Processual Penal.* Op. cit., p. 432); um segundo entendimento reconhece a legitimidade da prova fortuitamente encontrada, sem qualquer ressalva, condicionada à restrição lícita da intimidade e privacidade do indivíduo na medida efetivada (DEZEM, Guilherme Madeira. *Curso de processo penal*. Op. cit. p. 802); finalmente, uma terceira interpretação admite a utilização da prova encontrada por acaso, desde que tenha conexão com o fato investigado. No âmbito jurisprudencial, embora as Cortes tenham se inclinado a adotar o entendimento quanto à necessidade da conexão dos fatos investigados com a prova fortuitamente localizada, é certo que o Superior Tribunal de Justiça (STJ) e o Supremo Tribunal Federal (STF) alteraram o posicionamento rumo à admissibilidade da validade da prova, independentemente da conexão com os fatos previamente investigados: STJ, ROC em HC n.º 117.113/MG, 5ª Turma, Rel. Min. Ribeiro Dantas, julgado em 26 de novembro de 2019, DJe 05/12/2019; STF, Habeas Corpus n.º 129.678/SP, 1ª Turma, Rel. Min. Alexandre de Moraes, julgado em 13 de junho de 2017, DJe 17/08/2017.

[253] Deliberando sobre uma hipótese de consentimento para ingresso em domicílio em horário noturno, o Tribunal de Justiça do Distrito Federal e Territórios considerou legítima a localização fortuita de outros elementos probatórios na residência do investigado (TJDFT, Apelação n.º 0007055-40.2017.8.07.0000, 1ª Turma Criminal, Rel. Desembargadora Ana Maria Amarante, julgado em 12 de abril de 2018).

[254] LIMA, Renato Brasileiro. *Manual de Processo Penal.* São Paulo: Editora Juspodivm, 2020, p. 699; PACELLI, Eugenio. *Curso de processo penal*. 19. ed. rev. atual. São Paulo: Atlas, 2015, p. 367.

Conclui-se, nesta ordem, que caso seja dado consentimento para uma finalidade específica, tem-se como legítima a localização de elementos probatórios fortuitamente localizados, ainda que não conexos, desde que inserida na linha dos desdobramentos investigativos propostos, bem como que configurem fatos novos e até então desconhecidos, sob pena de se incorrer na hipótese de extensão indevida do acesso anteriormente conferido.

3.2 Cessão voluntária dos dados por terceiros

Ainda na perspectiva da cessão voluntária de dados, que prescinde de autorização judicial, reconhece-se a possibilidade do acesso ao conteúdo de um aparelho celular mediante consentimento de um terceiro indivíduo que mantenha contato com o acusado e venha a fornecer os dados comunicados e compartilhados. Desta feita, é possível que se tenha acesso, por via indireta, a uma grande quantidade de dados[255] que foram objeto de interação entre o terceiro e a pessoa que se pretenda investigar[256], tais como as mensagens de aplicativos, SMS, fotografias, *e-mails,* e outros dados compartilhados.

O Código de Processo Civil, verdadeiro diploma supletivo ao processual, prevê expressamente em seu artigo 422 a possibilidade de reprodução mecânica como meio apto para fazer prova dos fatos ou das coisas representadas. Ademais, a autenticidade pode ser reconhecida mediante certificação ou pela simples ausência de impugnação da parte *ex adversa,* conforme prevê o artigo 411 da Lei Adjetiva Civil.

Nesta linha, o registro das conversas mantidas pelo próprio interlocutor, ainda que sem o conhecimento da parte contrária, não deixa de ser considerada uma reprodução mecânica com finalidade probatória, que poderá ser contestada a seu tempo e modo pela parte diretamente atingida.

---

[255] Há inegável limitação quanto ao conteúdo a ser acessado, haja vista que apenas os dados confidenciados e expostos perante o terceiro cedente poderão ser obtidos.

[256] Jennifer Badaró salienta que "(...) também não são consideradas ilícitas pelos tribunais as provas fornecidas pelo destinatário das mensagens. Situação comum atualmente se verifica em acordos de colaboração premiada, em que o réu colaborador fornece à autoridade policial ou ao Ministério Público e-mails e mensagens trocadas com o réu delatado. Tais provas têm sido admitidas no processo e utilizadas para condenação (...)" (BADARÓ, Jennifer Falk. *Produção de provas: WhatsApp, Facebook, e-mail.* AASP Boletim, Edição n.º 3096, Dezembro/2019).

3.2.1. Gravação clandestina: conceito legal

A divulgação de arquivos de comunicação compartilhados entre um terceiro indivíduo e a pessoa investigada, mediante consentimento daquele, não encontra expressa regulamentação no Código de Processo Penal, embora guarde simetria com as hipóteses de "gravação telefônica" e "gravação ambiental", verdadeiras espécies do gênero "gravação unilateral" ou "gravação clandestina".

A "gravação unilateral" consiste, nos dizeres de ALEXANDRE DE MORAES, "(...) a captação e gravação da conversa pessoal, ambiental ou telefônica se dão no mesmo momento em que a conversa se realiza, feita por um dos interlocutores, ou por terceira pessoa com seu consentimento, sem que haja conhecimento dos demais interlocutores (...)"[257].

O envio de mensagens de texto ou voz, enviadas e recebidas via SMS ou por intermédio de outros aplicativos de comunicação instantânea, constituem hipótese de gravação clandestina telefônica, que consiste na captação de uma "comunicação telefônica" por um dos interlocutores, sem o conhecimento do outro, o que incluiria, nos dizeres de LUIZ FLÁVIO GOMES e RAÚL CERVINI, "(...) não apenas a conversa por telefone, mas também a transmissão, emissão ou receptação de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza, por meio de telefonia, estática ou móvel (celular) (...)"[258].

Ainda que a conversa seja materializada digitalmente, sob a forma escrita ou sonora (áudio), bem como encaminhada por intermédio de aplicativos de comunicação instantânea, não se perderá a essência de uma comunicação mantida entre duas pessoas e gravada por uma delas, sem o consentimento de outro, o que justificaria a incidência das disposições relativas à gravação clandestina[259].

---

[257] MORAES, Alexandre de. *Direito Constitucional*. São Paulo: Ed. Atlas, 28ª Edição, 2012. p. 67.

[258] GOMES, Luiz Flávio CERVINI, Raúl. *Interceptação Telefônica*: Lei 9.296, de 24.07.96, São Paulo, Revista dos Tribunais, 1997, p. 100; LIMA, Renato Brasileiro. *Manual de Processo Penal.* Op. cit. p. 818. Este posicionamento não é unânime: para Vicente Greco Filho, a comunicação telefônica se caracteriza pela transmissão de voz entre os interlocutores (GRECO FILHO, Vicente. *Interceptação Telefônica*. São Paulo: Editora Saraiva, 1996, p. 17-20).

[259] A conversa gravada por uma das partes, após troca de mensagens via *Whatsapp*, consistiria na hipótese de "gravação clandestina", seja ela "telefônica" – a partir do conceito doutrinário de comunicação telefônica – ou "ambiental", tal como reconhecido por parte da jurisprudência, em que a captura da conversa entre presentes,

A gravação telefônica e ambiental, sem qualquer dissonância doutrinária ou jurisprudencial, está fora do âmbito de proteção assegurada no artigo 5º, inciso XII, da Constituição Federal e tampouco da Lei n.º 9.296/1996, bem como não fora objeto de regulamentação normativa. Entretanto, tal condição não a afasta da submissão à regra geral de proteção à privacidade, intimidade e vida privada, delineadas no artigo 5º, inciso X, da Constituição Federal.

Com efeito, a gravação clandestina vem ganhando relevo como meio atípico de produção de provas, especialmente considerando que o desenvolvimento tecnológico permitiu a criação e aperfeiçoamento de recursos que permitem a gravação, por voz ou texto, de uma conversa mantida entre duas pessoas. A recorrente utilização da gravação unilateral despertou uma intensa discussão relacionada à licitude de tais provas, diante da possível violação aos direitos da personalidade do interlocutor gravado.

Uma primeira linha interpretativa rechaça a admissibilidade da prova. Para LUIZ FLÁVIO GOMES[260], ainda que o ato de gravar não constitua um ilícito penal, é inegável que sua perpetração não deixa de ser uma medida de afronta direta à intimidade

---

por um dos interlocutores, sem o conhecimento do outro: *"*APELAÇÃO CRIMINAL - CONVERSAS VIA WHATSAPP – GRAVAÇÃO DOS DIÁLOGOS ENTRE A PRÓPRIA VÍTIMA E O RÉU - PROVA LÍCITA - ARTIGO 217-A DO CP - SUFICIÊNCIA DE PROVAS - TEMOR REVERENCIAL - ABSOLVIÇÃO DO CRIME DO ARTIGO 213 DO CP - PERSONALIDADE E CONDUTA SOCIAL - DECOTE - CONSEQUÊNCIAS - MANUTENÇÃO DA MODULADORA - AGRAVANTE DO ARTIGO 61, INCISO II, ALÍNEA F, DO CP VERSUS CAUSA DE AUMENTO DO ARTIGO 226, INCISO II, DO MESMO DIPLOMA LEGAL - MESMO FUNDAMENTO - CONTINUIDADE DELITIVA - FRAÇÃO MÁXIMA - DANOS MORAIS - REPARAÇÃO AFASTADA.1. A troca de mensagens pelo aplicativo WhatsApp é forma de comunicação escrita e imediata entre os interlocutores. O acesso aos dados sem autorização judicial prévia configura interceptação vedada. Entretanto, parte das mensagens foram escritas pela própria vítima e pelo réu. O acesso aos diálogos entre a ofendida e o acusado equivale à gravação ambiental, permitida pelas Cortes Superiores.
(...)IX. Parcial provimento ao apelo para redimensionar a pena e decotar a reparação por danos morais" (TJDFT Apelação Criminal n.º 20160610018836APR - Acórdão nº 1038895, Relatora: Sandra De Santis, 1ª Turma Criminal, Data de Julgamento: 10/08/2017). Ainda que, conceitualmente, as hipóteses sejam distintas, as consequências jurídicas são idênticas para ambos os institutos, o que torna a discussão estéril, ao menos para fins de (i)licitude probatória. O Tribunal de Justiça do Estado de São Paulo encampou o mesmo entendimento, ocasião em que o relator Guilherme G. Strenger consignou expressamente que "(...) Com efeito, o que não se admite é a devassa por terceiros da comunicação das partes, mas pode uma delas fornecer o material para comprovar suas alegações, pois equivale a gravação ambiental. Ademais, trata-se de prova indiciária, suficiente para a deflagração da ação penal, que deve ser corroborada pela prova colhida sob o crivo do contraditório (...)" (TJSP, Apelação Criminal n.º 0027534-44.2017.8.26.0576, julgado em 8 de maio de 2019). Também o Tribunal Superior Eleitoral entendeu que o fornecimento voluntário de trechos de conversas mantidas pelo aplicativo *"whatsapp",* por intermédio de um dos interlocutores da conversa travada, não exige autorização judicial (TSE, Recurso Especial Eleitoral n.º 455-02.2016.6.16.0114, Classe 32 (Serranópolis do Iguaçu – PR), julgado em 4 de abril de 2019).

[260] GOMES, Luiz Flávio CERVINI, Raúl. *Interceptação Telefônica*: Op. cit., p. 106-111. Na mesma linha a posição de ARANHA, Adalberto José Q. T. de Camargo: *Da prova no processo penal.* 7ª ed., São Paulo: Editora Saraiva, 2006, p. 58

alheia da pessoa gravada e, por tal razão, a prova merece ser considerada inadmissível, diante da expressa disposição do artigo 5º, inciso LVI, da Constituição Federal. Assim, a surpresa no ato de gravar torna a conduta moralmente reprovável, porquanto haveria uma quebra da confiança[261] entre os interlocutores[262], à medida que, possivelmente, não se manifestariam livremente caso imaginassem que a gravação fosse chegar ao conhecimento de terceiros.

Ainda, aponta-se que a inexistência de uma lei que discipline a gravação telefônica ou ambiental impediria que direitos fundamentais assegurados venham a ser restringidos, prevalecendo-se seu sentido mais extenso. Entretanto, os partidários da inadmissibilidade da prova admitem, em homenagem ao princípio da proporcionalidade, a licitude da gravação utilizada como meio de defesa para se comprovar a inocência do acusado[263] ou, ainda, para se rechaçar uma investida criminosa perpetrada por um dos interlocutores, tais como a gravação realizada pela vítima em situações de extorsões, concussões ou ameaças feitas por intermédio do telefone[264].

Já para uma segunda linha interpretativa, a gravação telefônica poderia ser considerada lícita, a depender dos fundamentos que justificaram sua divulgação.

---

[261] Nos Estados Unidos da América, a gravação ambiental é considerada ilícita em ao menos 12 (doze) estados, que exigem o consentimento de todas as partes (*all parties consent*) para se admitir a validade da gravação empregada (TEBET, Diogo. *Inadmissibilidade da gravação telefônica e ambiental clandestina: da necessária revisão da jurisprudência do Supremo Tribunal Federal* In. SIDI, Ricardo, LOPES, Anderson Bezerra (orgs.) Temas atuais da investigação preliminar no processo penal. Belo Horizonte, Editora D' Plácido, 2017, p. 221). O autor aponta as quatro razões pelas quais a gravação deve ser considerada inadmissível: a violação ao direito à intimidade por violação à *reasonable expectation of privacy;* a violação ao direito à autoincriminação da parte gravada; a vedação à utilização de meios sub-reptícios, ocultos e enganosos como meios de prova; inexistência de lei regulamentadora do referido meio de obtenção de provas.

[262] Para Manoel da Costa Andrade, "(...) as gravações de conversas entre presentes são mais gravosas e invasivas do que as escutas telefônicas. Já porque frustram uma expectativa mais consistente de confidencialidade e segredo; já porque não oferecem as mesas possibilidades e os mesmos estímulos de autotutela. Quem confia as suas mensagens aos serviços de telecomunicações sabe que perde o domínio e o controlo das coisas, partindo com expectativas de reserva mais baixa do que quem fala cara-a-cara, num ambiente que fundadamente se presume asséptico e imune a intromissões (...)" (ANDRADE, Manoel da Costa. *Métodos ocultos de investigações (plädoyer para uma teoria geral).* In: MONTE, Mário Ferreira et ali (org.). Que futuro para o direito processual penal? Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do código de processo penal português. Coimbra: Editora Coimbra, 2009, p. 538).

[263] O Superior Tribunal de Justiça (STJ) já considerou lícita a gravação realizada inclusive nas situações em que haveria um dever de sigilo imposto às partes, se a medida foi tomada em defesa de direito próprio. Nestes casos, já se admitiu a gravação da conversa, pelo cliente, com seu advogado (STJ, RHC n.º 48.397/RJ, Rel.Min. Nefi Cordeiro, 6ª Turma, julgado em 6 de setembro de 2016, DJe 16/09/2016) e entre a psicóloga da vítima e a mãe desta (STJ, RMS n.º 49.277/SP, Rel. Min. Nefi Cordeiro, 6ª Turma, julgado em 7 de abril de 2016, DJe 26/04/2016)

[264] STF, HC n.º 75.388/RJ, Rel. Min. Nelson Jobim, julgado em 11 de março de 1998, DJ 25/09/1998; STF, RE n.º 212-081/RO, Rel. Min. Octavio Gallotti, julgado em 5 de dezembro de 1997; STF, HC nº 75.261, Rel. Min. Octávio Gallotti, DJ de 22.08.97; STF, HC n.º 87.341/PR, 1ª Turma, Rel. Min. Eros Grau, julgado em 7 de fevereiro de 2006, DJ 03/03/2006.

LUIZ FRANCISCO TORQUATO AVOLIO aponta que eventual nulidade se projetaria para um segundo momento, relacionada à divulgação sem justa causa[265] da própria gravação realizada, o que poderia inclusive trazer a questão às barras da ilicitude penal (artigo 153 do Código Penal).

Outrossim, a inexistência de regulamentação legal quanto à gravação ambiental não nos parece que seja impeditivo da utilização do referido meio de obtenção de provas. Conforme já reportado, o sistema processual penal brasileiro adotou a liberdade nos meios de obtenção de prova, desde que não haja ofensa a afronta a qualquer direito fundamental individual, ao direito de defesa e aos valores da dignidade da pessoa humana.

Assim, seria reconhecível o direito à gravação da própria conversa e sua divulgação para a produção de provas, em juízo ou inquérito, em favor de quem as gravou, salvo nas hipóteses em que houver clara e patente violação a direitos e garantias fundamentais, especialmente nos casos de sigilo ou reserva legal.

Na esfera jurisprudencial, houve uma primeira inclinação do Supremo Tribunal Federal (STF) pela inadmissibilidade da prova obtida mediante gravação telefônica realizada por um dos interlocutores, sem o conhecimento do outro interlocutor[266]. A posição não vingou e, em outros precedentes, o Supremo Tribunal Federal (STF) e o Superior Tribunal de Justiça (STJ) consolidaram entendimento reconhecendo a licitude da gravação telefônica ou ambiental, desprovida de prévia autorização judicial, salvo se houver sigilo ou reserva legal[267].

---

[265] AVOLIO, Luiz Francisco Torquato. *Provas Ilícitas Interceptações telefônicas e gravações clandestinas*, 7ª ed., São Paulo: Editora Revista dos Tribunais, 2019, p. 156-157. Prossegue o autor que a "justa causa" seria "(...) a chave para se perquirir a licitude da gravação clandestina. E, dentro das excludentes possíveis, é de se afastar – frise-se – o direito à prova. Os interesses remanescentes devem ser suficientemente relevantes para ensejar o sacrifício da privacy. Assim, por exemplo, a vida, a integridade física, a liberdade, o próprio direito à intimidade e, sobretudo, o direito de defesa, que se insere entre as garantias fundamentais. Ocorrendo, pois, conflito de valores dessa ordem, a gravação clandestina é de se reputa lícita, tanto no processo criminal como no civil, independentemente do fato de a exceção à regra da inviolabilidade das comunicações haver sido regulamentada (...)"

[266] No julgamento da ação penal envolvendo Fernando Collor de Mello e outros réus, a Suprema Corte sustentou que a gravação da conversa com terceiros não poderia ser utilizada pelo Estado em juízo, já que se trataria de meio sub-reptício que envolve a quebra evidente de privacidade, a macular a eficácia jurídica da prova coligida por este meio (STF, AP n.º 307/DF, Rel. Min. Ilmar Galvão, julgado em 13 de dezembro de 1994, DJ 13/10/1995).

[267] STF, RE 583.937 QO-RG / RJ, Repercussão Geral na Questão de Ordem no Recurso Extraordinário, Rel. Min. Cezar Peluso, DJe 17-12-2009; STF, RE-AgR nº 402.035, Rel. Min. Ellen Gracie, DJ de 06.02.2004; STF, AgRg no RE n. 933.530, Segunda Turma, Rel. Min. Carmen Lúcia, DJe 15/03/2016; STF, RE n. 630.944 AgR, Segunda Turma, Rel. Min. Ayres Britto, DJe de 19/12/2011; STF, RE 402.717, Rel: Min. Cezar Peluso,

Finalmente, importante registrar que, diante de episódios recentes de grandes investigações relacionadas à macrocriminalidade[268], a colaboração premiada exsurgiu como instrumento de defesa por parte de alguns envolvidos. Assim, durante os procedimentos para obtenção da vantagem premial, parte dos agentes colaboradores se valeram de gravações telefônicas e ambientais como forma de corroborar as alegações prestadas perante os órgãos perscrutatórios. A medida tem gerado grande debate doutrinário[269], embora já tenha sido chancelada monocraticamente pelo Supremo Tribunal Federal (STF)[270].

3.2.2. Cessão dos dados por terceiros: a entrega pelo proprietário do aparelho celular

Na perspectiva das relações empresariais, é comum que o aparelho celular corporativo seja utilizado por um funcionário, mediante termo de anuência e consentimento do empregador. Nas hipóteses em que se faz necessário o acesso ao conteúdo dos dados, discute-se a possibilidade da cessão realizada por parte dos empregadores, enquanto proprietários dos suportes eletrônicos.

Com relação ao tema, põe-se a discussão se seria lícito o consentimento de acesso aos dados prestado por terceiros, para a localização, apreensão e extração de dados que possam estar relacionados à pessoa investigada.

De início, impende destacar que não se aplicariam, aqui, as disposições relativas às gravações clandestinas, haja vista que o proprietário do aparelho não

---

Segunda Turma, j. 02.12.2008, DJe 13.02.2009; STF, AGR/AI 578.858/RS, Rel. Min. Ellen Gracie, Segunda Turma, DJe 27.8.2009, STF, Inq. 4483-DF, Rel. Min. Edson Fachin, decisão monocrática DJe 12/09/2017; STF, HC n.º 84.203/RS, 2ª Turma, Rel. Min. Celso de Mello, j. 19/10/2004; STJ, AgRg no HC n.º 549.821/MG, 5ª Turma, Rel. Min. Jorge Mussi, j. 17/12/2019; STJ AgRg no AREsp 1301191/SP, 5ª Turma, Rel. Ministro Ribeiro Dantas, j. 19/03/2019, DJe 25/03/2019; STJ, AgRg no AREsp 754.861/PR, 6ª Turma, Rel. Ministro Sebastião Reis, j. 04/02/2016, DJe 23/02/2016; STJ, APn 644/BA, Ministra Eliana Calmon, Corte Especial, DJe 15/2/2012.

[268] ZILLI, Marcos Alexandre Coelho. *Resquícios Inquisitórios na Lei 9.034/ 1998*. *In*: Revista Brasileira de Ciências Criminais. Bimestral, ano 12 n° 46, jan-fev 2004, p. 174-176.

[269] A extensão do tema transborda os limites do presente trabalho investigativo. Recomenda-se, para aprofundamento: CASTRO, Pedro Machado de Almeida. *Operação Lava Jato e gravações clandestinas.* In. SIDI, Ricardo, LOPES, Anderson Bezerra (orgs.) Temas atuais da investigação preliminar no processo penal. Belo Horizonte, Editora D' Plácido, 2017, p. 415-425; TEBET, Diogo. *Inadmissibilidade da gravação telefônica e ambiental clandestina: da necessária revisão da jurisprudência do Supremo Tribunal Federal.* Op. cit. p. 213-225 AVOLIO, Luiz Francisco Torquato; REBELLATO, Luiz Fernando Bugiga. *Provas ilícitas*. In: Contraponto jurídico. Posicionamentos divergentes sobre grandes temas do Direito. São Paulo: Editora RT, 2018, p. 905.

[270] STF, Inq. 4483-DF, Rel. Min. Edson Fachin, decisão monocrática DJe 12/09/2017.

é interlocutor da conversa mantida, mas mero titular do objeto. Todavia, considerando que a veiculação da conversa teria se dado mediante utilização de um instrumento privado e pertencente a terceiro, perquire-se se o consentimento do proprietário do aparelho é suficiente para se reconhecer a licitude da prova ou se, ao revés, far-se-ia necessária uma ordem judicial para se avaliar o conflito entre o direito à privacidade e intimidade do acusado e a necessidade de se produzir elementos de prova relacionados a uma investigação.

A propósito do tema, nos Estados Unidos desenvolveu-se a doutrina da *third-party consent*, relacionada à possibilidade de um indivíduo consentir com a realização de uma busca ou com o acesso a um computador ou bem de uso comum e compartilhado[271].

A partir do caso *United States v. Matlock 415 US 164 (1974)*[272], a Suprema Corte entendeu que não haveria violação à *Fourth Amendment* quando a polícia obtém o consentimento voluntário de uma terceira pessoa que possui autoridade comum[273] sobre o estabelecimento ou o objeto a ser perscrutado. Posteriormente, no julgamento do caso *Georgia v. Randolph, 547 U.S. 103 (2006)*[274], a Suprema Corte decidiu serem inadmissíveis as provas obtidas a partir de busca consentida quando um dos proprietários autoriza a diligência e o outro, presente no local, a rejeita expressamente. A conclusão poderia ser distinta se, a despeito da ausência de consentimento da parte investigada, vislumbrar-se a possível situação de destruição de provas, de um crime estar sendo praticado no momento ou de abuso doméstico.

---

[271] Registre-se que, no Canadá, a jurisprudência não tem admitido a utilização da *third party consent* (R. v. Cole, 2012 SCC 53, [2012] 3 S.C.R. 34, at. P. 75-79. Disponível em https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/12615/index.do. Acesso em: 20 de dezembro de 2020).

[272] https://supreme.justia.com/cases/federal/us/415/164/. Acesso em: 20 de dezembro de 2020. A Suprema Corte fixou entendimento de que a autoridade comum, que estabelece o direito de consentimento de terceiros, exige *"(...) mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched (...)"*

[273] No precedente *Illinois v. Rodriguez, 497 U.S. 177 (1990)*, a Suprema Corte entendeu que, quando o consentimento para a busca é dado por terceiro que acreditava-se razoavelmente ter autoridade comum sobre o bem e, posteriormente, constata-se que não podia dele dispor, a busca é considerada válida, pois os policiais, ainda que tenham ingressado no local sem dispor de uma ordem judicial para tanto, estavam imbuídos de boa-fé por acreditarem que o consentimento prestado fora razoável e válido. Assim, não haveria ilicitude da prova, já que a *Fourth Amendment* pretende evitar buscas irrazoáveis ("unreasonable"). Disponível em: <https://supreme.justia.com/cases/federal/us/497/177/>. Acesso em: 20 de dezembro de 2020.

[274] Disponível em: <https://supreme.justia.com/cases/federal/us/547/103/>. Acesso em: 20 de dezembro de 2020.

Finalmente, no julgamento de *Fernandez v. California 571 U.S. 292 (2014)*[275], novamente a Suprema Corte voltou a discutir os limites da *third-party consent.* Na ocasião, reafirmando os dois precedentes já citados, firmou-se o entendimento de que a busca seria válida caso a pessoa que denegou o consentimento venha a ser detida por um outro crime ou seja removida do local por alguma infração. Nestes casos, o consentimento dispensado pelo proprietário remanescente é válido para a realização de buscas no local.

No ordenamento jurídico nacional, embora não haja qualquer regulamentação legal sobre o tema, o estudo dos precedentes norte-americanos pode auxiliar na análise quanto à licitude do consentimento prestado por terceiro.

Em verdade, embora o consentimento em objetos compartilhados entre dois ou mais proprietários possa, geralmente, ser dado por qualquer um deles, impende analisar se os dados buscados são comuns ou pertencem a apenas um dos coproprietários.

Deve-se reconhecer, portanto, que o consentimento para fornecimento voluntário dos dados somente poderá ser conferido pelo destinatário da proteção constitucional conferida ao sigilo e à intimidade dos dados. Estabelece-se, neste passo, um paralelo com o consentimento para ingresso em domicílio: ainda que o proprietário e titular do imóvel consinta com o ingresso nas dependências físicas do bem, é inegável que há espaços reservados, dentro da construção física, que pertencem a outras pessoas diferentes daquele que consentiu para com a entrada no imóvel.

Portanto, caso se pretenda realizar uma busca nestes espaços intramuros e exclusivos, que não sejam de uso comum[276], é necessário que se obtenha o

---

[275] Disponível em: <https://supreme.justia.com/cases/federal/us/571/292/>. Acesso em: 20 de dezembro de 2020. Ainda sobre o tema, recomenda-se: KERR, Orin. *Fernandez v. California and the problem of third-party consent*. 2013, Disponível em: <https://www.scotusblog.com/2013/11/fernandez-v-california-and-the-problem-of-third-party-consent/> . Acesso em: 20 de dezembro de 2020.

[276] Walter Nunes da Silva Júnior esclarece que o empregado, residente no local, tem o direito de negar o ingresso no espaço territorial definido para a sua privacidade, sendo pertinente a oposição contra outros moradores de casa e, até mesmo, contra seu patrão (SILVA JÚNIOR, Walter Nunes. *Curso de direito processual penal: teoria (constitucional) do processo penal.* Rio de Janeiro: Editora Renovar, 2008, p. 654/655, *apud* LIMA, Renato Brasileiro. Manual de Processo Penal. São Paulo: Editora Juspodivm, 2020, p. 804).

consentimento dos seus respectivos titulares[277], conforme vem destacando a jurisprudência portuguesa[278].

Pela mesma ordem de ideias, ainda que o aparelho celular seja de propriedade de terceiros, a outorga do consentimento somente será válida caso prestada pelo titular dos dados ali armazenados[279], sob pena de ilicitude da prova produzida[280].

Conquanto o aparelho celular seja uma *fonte de prova,* é certo que ele é um mero aparato tecnológico que armazena e reproduz os dados. Não há que se confundir a titularidade do objeto com a dos dados nele contidos, ainda que a sua extração dependa, por vezes, da apreensão física do próprio aparelho celular[281].

---

[277] A jurisprudência espanhola já assentou que *"(...) cada uno de los cónyuges o miembros de una pareja de hecho está legitimado para prestar el consentimiento respecto de la entrada de un tercero en el domicilio, sin que sea necesario recabar el del otro, pues la convivencia implica la aceptación de entradas consentidas por otros convivientes (...)"* (STC 22/2003, de 10/02, FJ 7)

[278] Interpretando-se o artigo 174, 5, b, do Código de Processo Penal, o Tribunal de Relação de Lisboa apreciou uma busca domiciliar realizada mediante autorização do morador e fixou algumas premissas: a) o consentimento não seria válido se outorgado por uma pessoa comprovadamente analfabeta; b) o consentimento permitiria a realização de diligências em espaços comuns da casa e nas dependências pessoais do outorgante, não se autorizando o ingresso nas dependências reservadas de outras pessoas maiores e capazes, a quem caberia conferir o consentimento para a diligência; c) o consentimento está relacionado ao direito à privacidade e não guarda relação com a tutela da propriedade, do domínio ou da titularidade do domicílio; d) o consentimento deve ser realizado antes do ato, não se confundindo com a ratificação posterior; e) não se autorizaria o consentimento de menor de 21 (vinte e um) anos de idade, salvo se ele estivesse acompanhado de um defensor (Recurso Penal n.º 6945/2008-3, rel. Carlos Almeida, j. 22 de outubro de 2008, por maioria).

[279] Interpretando-se o artigo 174, 5, b, do Código de Processo Penal, o Tribunal de Relação de Lisboa apreciou uma busca domiciliar realizada mediante autorização do morador e fixou algumas premissas: a) o consentimento não seria válido se outorgado por uma pessoa comprovadamente analfabeta; b) o consentimento permitiria a realização de diligências em espaços comuns da casa e nas dependências pessoais do outorgante, não se autorizando o ingresso nas dependências reservadas de outras pessoas maiores e capazes, a quem caberia conferir o consentimento para a diligência; c) o consentimento está relacionado ao direito à privacidade e não guarda relação com a tutela da propriedade, do domínio ou da titularidade do domicílio; d) o consentimento deve ser realizado antes do ato, não se confundindo com a ratificação posterior; e) não se autorizaria o consentimento de menor de 21 (vinte e um) anos de idade, salvo se ele estivesse acompanhado de um defensor (Recurso Penal n.º 6945/2008-3, rel. Carlos Almeida, j. 22 de outubro de 2008, por maioria). De igual sorte, Walter Nunes da Silva Júnior esclarece que o empregado, residente no local, tem o direito de negar o ingresso no espaço territorial definido para a sua privacidade, sendo pertinente a oposição contra outros moradores de casa e, até mesmo, contra seu patrão (SILVA JÚNIOR, Walter Nunes. *Curso de direito processual penal: teoria (constitucional) do processo penal.* Rio de Janeiro: Renovar, 2008, p. 654/655, *apud* LIMA, Renato Brasileiro. *Manual de Processo Penal.* São Paulo: Juspodivm, 2020, p. 804).

[280] Para Guardia, "(...) o consentimento para o oferecimento dos dados às autoridades competentes não pode ser prestado por terceiro. Nem mesmo o uso inadequado dos meios de comunicação – v.g., em violação dos horários de funcionamento de uma empresa ou sem a permissão do proprietário do computador ou aparato tecnológico – excepciona o necessário consentimento (...)", reconhecendo que "(...) é necessária autorização judicial para a coleta dos dados. E sempre o juízo de proporcionalidade guiará a excepcionalidade na determinação destas infegerências (...)" (GUARDIA, Gregório Edoardo Raphael Selingardi. *Comunicações Eletrônicas e dados digitais no processo penal*. Op. cit., p. 190)

[281] Sobre o tema, merece destaque o voto da Ministra Rosa Weber no julgamento do Recurso em *Habeas Corpus* n.º 132.062/RS, ocasião em que, analisando o tema à luz de precedentes internacionais, reconheceu a distinção entre a titularidade da base física e dos dados, apontando que "(...) a expectativa de privacidade

Importante destacar que, dentre os dados armazenados no aparelho, é possível que parte deles sejam de titularidade do proprietário do aparelho celular e outros pertençam exclusivamente ao usuário e possuidor legítimo do objeto. *Ad exemplum,* em um *smartphone* corporativo pertencente à empresa em que o acusado trabalha e que a ele fora fornecido enquanto instrumento de trabalho, é possível que haja dados de cunho eminentemente pessoal e outros que digam respeito à própria atividade laboral.

Nestes casos, ainda que seja informado ao acusado que os instrumentos e ferramentas de trabalho devam ser utilizados dentro dos limites estabelecidos no contrato de trabalho, os dados estritamente pessoais e particulares (*v.g.,* mensagem particular com a esposa do acusado, relacionada aos filhos do casal; fotografias de cunho eminentemente familiar, etc.), mantidos pelo acusado, somente poderão ser cedidos voluntariamente mediante seu expresso consentimento e anuência.

De outra banda, os dados pertencentes à empresa poderão ser livremente disponibilizados por seus responsáveis legais, ainda que estes dados sejam produzidos digitalmente pelo próprio acusado (*v.g.,* uma mensagem de *WhatsApp* enviada para terceiros em que se solicita ilicitamente uma quantia em dinheiro para beneficiar um contratante; o envio e recebimento, via de regra, de mensagens de cunho profissional no *e-mail* corporativo, etc.)[282].

---

protege os bens de uso especial integrantes dos gabinetes funcionais de órgãos públicos, inclusive os computadores e respectivos dados neles armazenados. Desimportante, a meu compreender, que o maquinário, a base física dos dados (HD, hardware) pertença à administração pública, pois a proteção, diz com o sigilo e à privacidade – 'ruptura da esfera de intimidade de quem se acha sob investigação' (MS 23452, Rel. Ministro Celso de Mello) – não com o direito de propriedade vinculado ao serviço público (...)", concluindo-se que "(...) estabeleço, portanto, a premissa de que os dados armazenados nos computadores de órgãos públicos estão sujeitos à proteção constitucional do artigo 5º, X, da CF, indiferente o maquinário, a base física dos dados, pertencer ao patrimônio público (...)" (STF, RHC n.º 132.062/RS, 1ª Turma, Rel. Min. Marco Aurélio Mello, Rel. p/ acórdão Min. Edson Fachin, julgado em 29 de novembro de 2016).

[282] No julgamento do caso *"Libert vs. France",* o Tribunal Europeu de Direitos Humanos (TEDH) foi chamado a analisar a regularidade da busca realizada pelo empregador ao computador de um funcionário da empresa ferroviária nacional francesa (SNCF), sem o consentimento de seu usuário, ocasião em que foram encontrados arquivos e materiais de cunho pornográfico. O funcionário fora demitido e contestou a legalidade da decisão, sendo que o Tribunal Europeu de Direitos Humanos reconheceu a inexistência de violação ao artigo 8º da Convenção Europeia de Direitos Humanos, haja vista que a consulta dos arquivos pelo empregador do requerente tinha buscado um objetivo legítimo de proteger os direitos dos empregadores, que podem legitimamente desejar garantir que seus funcionários estavam usando as instalações de computador em conformidade com as suas obrigações contratuais e as normas aplicáveis. Ainda, a Corte observou que a lei francesa inclui um mecanismo de proteção de privacidade que permite que empregadores abram arquivos profissionais, embora não pudessem acessar, clandestinamente, arquivos identificado como sendo pessoal. No caso, os arquivos não estavam identificados como sendo "privados", o que não impediu a ação dos empregadores e, por conseguinte, a legitimidade da demissão perpetrada (Disponível em:

Não se ignora a dificuldade prática de, em alguns casos, se distinguir a natureza dos dados a serem encontrados. Com efeito, o acesso à conta do *WhatsApp* permitirá a identificação de mensagens de caráter pessoal e, também, profissional. Nestas hipóteses, a possibilidade abstrata de se ter acesso a dados de conteúdo íntimo e pessoal não pode obstaculizar o acesso ao conteúdo das conversas. Entretanto, o consentimento do empregador legitimará a utilização processual apenas dos dados de natureza profissional.

Portanto, ainda que o aparelho celular pertença a terceiros, deve ser resguardado o direito à intimidade e privacidade do seu usuário, além do sigilo das comunicações e seus dados pessoais[283].

O Superior Tribunal de Justiça (STJ), em situação semelhante envolvendo o uso de e-mail corporativo, aplicou a mesma *ratio decidendi* adotada na resolução de questões relacionadas à iniciativa privada[284] e decidiu que "(...) não configura prova ilícita a obtenção de informações constantes de e-mail corporativo utilizado pelo servidor público, quando atinentes a aspectos não pessoais, mas de interesse da Administração Pública e da própria coletividade; sobretudo quando há expressa menção, nas disposições normativas acerca do seu uso, da sua destinação somente para assuntos e matérias afetas ao serviço, bem como advertência sobre monitoramento e acesso ao conteúdo das comunicações dos usuários para fins de cumprir disposições legais ou instruir procedimento administrativo (...)"[285].

<https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-6014614-7713110%22]}.> Acesso em 20 de dezembro de 2020)

[283] O Tribunal Superior do Trabalho (TST) reconheceu que o poder diretivo do empregador decorre do direito de propriedade (art.5º, XXII, da CF). Todavia, este poder não é absoluto, encontra limitações no direito à intimidade do empregado (art.5º, X, da CF), bem como na inviolabilidade do sigilo de correspondência, comunicações telegráficas, de dados e telefonemas(art.5º, XII, da CF), igualmente garantias constitucionais, das quais decorre o direito de resistência a verificação de sua troca de dados e navegação eletrônica. Nestes casos, deverá haver ponderação entre os valores envolvidos para se verificar se houve abuso do empregador (TST, Recurso de Revista n.º 183240-61.2003.5.05.0021, 2ª Turma, Relator Ministro Renato de Lacerda Paiva, DEJT 14/09/2012). No mesmo sentido: TST-Agravo de instrumento no Recurso de Revista n.º 1.542/2005-055-02-40.4, Rel. Min. Ives Gandra, 7ª Turma, DJ de 06/06/08.

[284] O Tribunal Superior do Trabalho (TST) concluiu ser lícita a utilização de um *e-mail* corporativo como forma de se justificar uma demissão por justa causa (TST, Recurso de Revista n.º 61300-23.2000.5.10.0013,1ª Turma, Rel. Min. João Oreste Dalazen, julgado em 18 de maio de 2005, DJe 10/6/2005). Na mesma linha, confira-se: Ag-AIRR-820-70.2012.5.07.0004, 2ª Turma, Relatora Ministra Delaíde Miranda Arantes, DEJT 30/08/2019.

[285] STJ, ROC em MS n.º 48.665/SP, 2ª Turma, Rel. Min. Og Fernandes, julgado em 15 de setembro de 2015, DJe 5 de fevereiro de 2016.

Com relação à exigência de autorização judicial para acesso ao conteúdo de aparelhos celulares funcionais[286], usados por agentes públicos mas que pertençam à Administração Pública, o tema é bastante discutível, embora o Supremo Tribunal Federal (STF) já tenha reconhecido que, em razão do princípio da publicidade administrativa, os dados não estariam protegidos pelo sigilo telefônico ou telemático, haja vista que "(...) o sigilo de informações necessárias para a preservação da intimidade é relativizado quando se está diante do interesse da sociedade de se conhecer o destino dos recursos públicos (...)"[287].

Entretanto, em outro procedente, a Suprema Corte já estendeu as garantias de privacidade e intimidade aos dados pertencentes a servidores públicos, em razão da expectativa de privacidade relacionada aos gabinetes funcionais, na parte privativa ao servidor[288], mas legitimou a apreensão dos computadores em razão da existência de uma ordem judicial posterior que autorizou a medida, o que teria convalidado a ilicitude[289].

---

[286] Para Victor Quintieri e Humberto Moura, "(...)não há que se falar em ato ilícito praticado na hipótese de se ter acesso ao conteúdo disponível no WhatsApp se o aparelho é de propriedade pública ou do empregador, pois em caso como tais, a polícia estaria legitimado a verificar o celular funcional do empregado, desde que autorizada pelo seu proprietário, com fulcro na excludente de ilicitude do exercício regular do direito prevista no art. 23, III do CP (...)" (QUINTIERI, Victor Minervino; MOURA, Humberto Fernandes de. *As (i)legalidades no processo penal: breve reflexão a respeito do 'whatsapp' a partir da lei 9.296/1996 – um estudo de caso*. In: FREITAS FILHO, Roberto; VELOSO FILHO, José Carlos (org.). Cadernos jurídicos temáticos. Direito do Consumidor e Direito Penal. Brasília: UNICEUB, 2016, p. 153 e seguintes).

[287] STF, MS n.º 33.340/DF, 1ª Turma, Rel. Min. Luiz Fux, julgado em 26 de maio de 2015, DJe 31/07/2015.

[288] A Suprema Corte Norte-Americana, no julgamento do caso *O'Connor v. Ortega, 480 U.S. 709 (1987),* reconheceu a existência de uma expectativa de privacidade aplicável também aos servidores que trabalham para o governo (Disponível em: <https://supreme.justia.com/cases/federal/us/480/709/>. Acesso em 20 de dezembro de 2020).

[289] STF, RHC n.º 132.062/RS, 1ª Turma, Relatoria Ministro Marco Aurélio, redator do acórdão Min. Edson Fachin, julgado em 22 de novembro de 2016, DJe 24 de outubro de 2017.

4. FORMAS DE ACESSO AOS DADOS ARMAZENADOS EM APARELHOS CELULARES: A AUSÊNCIA DE VOLUNTARIEDADE E A ADOÇÃO DE MEDIDAS INVASIVAS MEDIANTE ACESSO REMOTO AO APARELHO CELULAR

4.1. Adoção de medidas invasivas para aquisição dos dados

No capítulo precedente, avançou-se no estudo das formas de acesso aos dados armazenados em aparelho celular, de forma direta e indireta, mediante consentimento do próprio titular ou por intermédio da ação de terceiros, o que dispensaria a autorização judicial.

Entretanto, a atividade investigativa estatal não pode condicionar sua atuação à voluntariedade e assentimento do acusado ou de terceiros. Durante as diligências investigativas, a adoção de meios de busca de provas exige, no mais das vezes, uma atuação de surpresa[290], a fim de não se frustrar os propósitos investigativos da diligência.

O avanço tecnológico permitiu que a obtenção dos dados armazenados nos aparelhos celulares se dê pela via remota ou física, sendo a primeira operacionalizada à distância, mediante acesso virtual aos dados mantidos no aparelho, ao passo que a segunda consiste no acesso através da própria apreensão física do suporte eletrônico em que os dados são guardados, permitindo-se sua extração.

Fato é que, seja qual a forma de acesso utilizada no desenvolvimento da atividade investigativa, é certo que em todas elas haverá a necessidade de se afastar, momentânea e circunstancialmente, o exercício de direitos e garantias fundamentais relacionados ao sigilo de dados e à privacidade e intimidade.

Como já dito, dados armazenados em aparelhos celulares são reveladores da privacidade e intimidade do cidadão, de modo que seu acesso somente pode

[290] Com efeito, uma interceptação telefônica ou telemática e a busca e apreensão são medidas que, por sua natureza, exigem que a parte acusada não tenha conhecimento prévio de sua adoção, sob pena de se tornar inócua toda e qualquer investigação.

ser assegurado quando, em uma análise da relação entre a proteção constitucional aos direitos da personalidade (“garantista”) e a necessidade de se investigar um fato criminoso suspeito (“eficiência”), ponderar-se pela necessidade de se relativizar a proteção constitucional em prol da necessidade de se admitir a pesquisa da fonte de prova.

Nos próximos tópicos, mister se debruçar sobre as formas de acesso aos dados armazenados em aparelhos celulares, investindo-se em algumas de suas particularidades e culminando no estudo da imprescindibilidade da autorização judicial em determinadas situações.

4.2. O acesso remoto a dados digitais

O acesso remoto a dados digitais, armazenados ou comunicados mediante a utilização de aparelho celulares, dispensa a apreensão física do próprio objeto, mediante providências discretas que, por vezes, passam ao largo do conhecimento do titular dos dados.

A utilização da via remota pressupõe que os dados estejam localizados em um sistema informático distinto, situado em local geograficamente diverso daquele onde se realizou a pesquisa das fontes de prova. Nesta ordem, por intermédio das conexões em rede e interligação de sistemas informáticos, torna-se possível acessá-los.

Dentre as formas de acesso remoto aos dados armazenados em aparelhos celulares, sem apreensão física do suporte eletrônico, destacam-se:

a) aquisição de dados por servidores remotos e mediante apreensão de arquivos eletrônicos em *cloud computing*;

b) requisição de dados em poder de provedores ou de serviços de *internet*, com base na Lei do Marco Civil da *Internet* (Lei n.º 12.965/2014);

c) infiltração clandestina, através da utilização de *malwares* para se permitir a interceptação, busca, monitoramento e apreensão dos dados, inclusive em tempo real, além da geolocalização dos dispositivos;

d) ações encobertas em meio digital, prevista no ordenamento jurídico brasileiro sob a forma de infiltração de agentes de polícia para investigação de determinados crimes.

Sem pretender avançar detalhadamente em cada uma destas formas de acesso, será dada ênfase nos meios de acesso remoto previstos no ordenamento jurídico brasileiro, sem prejuízo de, quanto às demais formas, estabelecer-se uma análise comparativa com a previsão legal conferida aos institutos pelo ordenamento jurídico de outros países.

4.2.1. Aquisição de dados por servidores remotos e mediante apreensão de arquivos eletrônicos em *cloud computing*

O acesso a dados telemáticos, pela via remota, consiste na possibilidade de, sem a necessidade de se ter contato físico e direto com o suporte eletrônico que guarnece as informações desejadas, ingressar em uma plataforma de dados armazenadas em um servidor que, muitas vezes, não se encontra geograficamente localizado no local da diligência.

Em verdade, a expressão "servidores", no contexto informático, é composta pelo computador ou outro objeto que, inseridos numa rede, fornecem serviços e informações e administram os recursos da própria rede, a serem usufruídos pelos usuários-clientes, podendo armazenar arquivos dos usuários, enviar e receber mensagens, dentre outras funcionalidades[291].

A evolução tecnológica e o expansionismo na quantidade de dados produzidos permitiram o desenvolvimento de tecnologias para armazenamento e processamento de dados em ambiente remoto, denominado *cloud storage*, que são disponibilizados e acessados por provedores de recursos de *cloud computing*[292].

---

[291] CARVALHO, Manuel da Cunha. *O conceito de servidor em informática e suas implicações jurídicas.* In: Revista de Direito do Consumidor n.º 39/158 – São Paulo: Editora RT; COSTA, Helena Regina Lobo da; LEONARDI, Marcel. *Busca e apreensão e acesso remoto a dados em servidores.* In: Revista Brasileira de Ciências Criminais, São Paulo, v. 19, n. 88, p. 203-223, jan.fev/2011, p. 203.

[292] *Cloud computing* corresponde ao armazenamento e acesso a dados e programas através do uso da *internet*, sem a necessidade de se recorrer ao acesso físico de dados guardados no disco rígido de um computador. Já o *cloud storage* consiste no armazenamento "em nuvem" destas informações, através de um servidor seguro que

Nesta forma de armazenamento, os arquivos de interesse do usuário permanecem consolidados em servidores mantidos por provedores de serviço, que são terceiros alheios à investigação[293] e que oferecem o serviço de guarda e proteção dos dados, à exemplo do *Google Drive* e *Icloud Apple.*

Esta nova perspectiva alterou significativamente as relações sociais e profissionais, pondo fim à necessidade de que os dados somente fossem acessíveis mediante contato direto com o suporte eletrônico que os contém.

As vantagens do armazenamento de dados em servidores remotos (seja em uma outro dispositivo informático ou em "nuvens") são indiscutíveis: redução do custo operacional diante da desnecessidade de aquisição de diversos dispositivos informáticos para armazenarem os dados; mobilidade no acesso ao conteúdo, permitindo-se o compartilhamento e acesso dos objetos em qualquer lugar, bastando a disponibilização de um ponto de conexão com a *internet*; aumento à segurança dos dados, colocando-os sob a proteção de uma criptografia que impede o acesso a pessoas não autorizadas; assegurar a longevidade dos dados, evitando-se que o furto, perda ou deterioração de um suporte eletrônico pudesse comprometer os dados nele contidos.

De igual sorte, este movimento iniciado a partir dos avanços tecnológicos determinou uma releitura na perspectiva da investigação criminal. A anacrônica busca e apreensão dos suportes eletrônicos, conquanto extensivamente utilizada, vem sendo substituída pelo acesso remoto a dados armazenados em servidores, especialmente diante das dificuldades oriundas decorrentes da apreensão física do servidor e dos suportes eletrônicos.

é disponibilizado por um provedor de recursos. Toda e qualquer alteração nos dados deste servidor é automaticamente propagada para outros dispositivos que estejam sincronizados a esta mesma fonte de armazenamento.

[293] Leonardo Peret diferencia o servidor remoto, de propriedade da empresa ou da pessoa investigada, do serviço de armazenamento em "nuvem", à medida que, naqueles, os servidores pertenceriam aos respectivos investigados, ao passo que, no *cloud computing*, os arquivos digitais ficariam armazenados em servidores de uma empresa, estranha à investigação, que oferece o serviço (ANTUNES, Leonardo Leal Peret. *(Re)pensando a busca e apreensão no processo penal*. Rio de Janeiro: Editora Lumen Juris, 2016, p. 205). Dario Kist também diferencia a titularidade do servidor e dos dados buscados, ao indicar que *"(...) não há que se confundir estas pessoas, que são 'titulares' dos dados buscados, com o proprietário do sistema informático ou do suporte de armazenamento em que os dados estão, que poderá ser um terceiro; bastae pensar na 'nuvem', que é de propriedade da empresa que disponibiliza essa forma de armazenamento de dados, mas ela não será o alvo da busca, entendido este como a pessoa cujos dados informáticos são visados pela investigação (...)"* (KIST, Dario José. *Prova digital no processo penal.* Op. cit. p. 161).

Assim, inegável que o acesso a estes servidores remotos é de inquestionável relevo em investigações que envolvam empresas e outros conglomerados econômicos, especialmente pelo fato de que, por razões de facilidade organizacional, segurança ou dinamismo nas relações profissionais, as empresas preferem condensar o conteúdo das informações que dispõem em um ou diversos servidores de sua propriedade.

Portanto, a eficiência da medida de busca e apreensão é assegurada pelo acesso à vastidão dos dados contidos nestes servidores remotos, sendo igualmente proveitosa já que o acesso direto ao servidor permitirá o contato com ampla gama de dados que, por vezes, não estariam armazenados individualmente em cada um dos suportes eletrônicos diligenciados.

Com efeito, a realização da busca e apreensão remota dos arquivos armazenados em "nuvens" ou em servidores físicos, mantidos em local distinto do endereço diligenciado, obedece ao mesmo caminho procedimental fixado no marco legal para as buscas e apreensões "tradicionais"[294], conforme dispõe o artigo 240 e seguintes do Código de Processo Penal[295]. Portanto, independentemente da localização física destes servidores, é imprescindível a prévia autorização judicial, a partir da comprovação de "fundadas razões" para a execução da medida (artigo 240, § 1º e artigo 241, ambos do Código de Processo Penal).

A pesquisa de dados informáticos, realizada pela forma remota[296], é prevista expressamente na legislação portuguesa em seu artigo 15, n.º 5, da *Lei do Cybercrime* (Lei n.º 109/2009), como medida a ser desenvolvida quando, após uma busca tradicionalmente realizada, houver indicativos de que os dados estejam armazenados em outros sistemas informáticos, tais como, *verbi gratia,* em uma "nuvem".

---

[294] DOMINGOS, Fernanda Teixeira Souza. *As provas digitais nos delitos de pornografia infantil na Internet*. In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro de (Org.). A prova no enfrentamento à macrocriminalidade. Salvador: Editora JusPodivm, 2019, cap. 7, p. 205.

[295] O estudo relativo à busca e apreensão será realizado oportunamente, quando versarmos sobre o acesso aos dados mediante contato direto com o suporte eletrônico que os armazena. Optou-se por tratar do tema da busca e apreensão em servidores remotos neste tópico em razão da segmentação metodológica proposta para o presente trabalho científico, que enfatiza a forma de acesso aos dados, ainda que o tema guarde relação com o procedimento geral de busca e apreensão a ser oportunamente explorado.

[296] Artigo 15. "Pesquisa de dados informáticos (...) 5 - Quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente, nos termos dos n.os 1 e 2. (...)".

Nestas hipóteses, é necessária uma nova ordem judicial para a busca, salvo se a entrega dos dados for voluntariamente consentida, em ato devidamente documentado, por quem tiver disponibilidade e controle desses dados ou, ainda, nas hipóteses de terrorismo, criminalidade violenta ou altamente organizada, quando houve fundados indícios da prática iminente de crime que ponha em grave risco à vida ou a integridade de qualquer pessoa.

Igualmente, a legislação espanhola estabeleceu, em seu *articulo* 588 *sexies,* 3.c[297], da *Ley de Enjuiciamento Criminal,* que sempre que houver motivos razoáveis para considerar que os dados procurados estejam armazenados em outro sistema informático ou em parte dele, a busca e apreensão pode ser estendida, desde que os dados sejam legalmente acessíveis pelo sistema inicial ou estejam disponíveis. Na mesma linha da previsão normativa portuguesa, o dispositivo legal espanhol exige, ainda, uma nova decisão judicial autorizativa, salvo se a ordem anterior já autorizava a medida, salvo em situações de urgência.

Já no Brasil, considerando que os servidores guardam informações relevantes e sensíveis - muitas vezes relacionadas ao próprio exercício da atividade econômica do acusado ou da empresa investigada e, por isso, protegidas por métodos criptográficos[298] -, tem-se exigido que as ordens de busca e apreensão expedidas contenham expressa menção à possibilidade do acesso remoto aos dados contidos nestes servidores[299].

---

[297] Artículo 588 sexies c. Autorización judicial. (...) 3. Cuando quienes lleven a cabo el registro o tengan acceso al sistema de información o a una parte del mismo conforme a lo dispuesto en este capítulo, tengan razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático o en una parte de él, podrán ampliar el registro, siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este. Esta ampliación del registro deberá ser autorizada por el juez, salvo que ya lo hubiera sido en la autorización inicial. En caso de urgencia, la Policía Judicial o el fiscal podrán llevarlo a cabo, informando al juez inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, de la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la interceptación".

[298] Leonardo Peret assume que, se o sistema de acesso ao servidor, físico ou em "nuvem", estiver protegido por senha, o acusado não é obrigado a fornecê-lo, em homenagem à proibição de se compelir o investigado a produzir provas contra sua vontade. Todavia, isto não impede que os agentes estatais busquem, por meios lícitos, acessar os arquivos mantidos em "nuvem" ou, ainda, se permita que, por ordem judicial, a senha de acesso seja requisitada e fornecida diretamente pelo servidor responsável pela manutenção dos dados (ANTUNES, Leonardo Leal Peret. *(Re)pensando a busca e apreensão no processo penal*. Op. cit. p. 202-204).

[299] COSTA, Helena Regina Lobo da; LEONARDI, Marcel. *Busca e apreensão e acesso remoto a dados em servidores,* Op. cit. p. 203; DOMINGOS, Fernanda Teixeira Souza. *As provas digitais nos delitos de pornografia infantil na Internet*. Op. cit. p. 204; VAZ, Denise Provazi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório.* Op. cit., p. 149.

Saliente-se que o acesso aos dados armazenados remotamente deve ser feito de maneira a se evitar prospectivos transtornos indesejáveis[300] ao acusado ou a terceiros, durante o cumprimento da busca e apreensão. Assim, no tocante aos servidores físicos, possibilita-se que o mandado judicial expedido autorize a realização de uma simples cópia[301] dos documentos acessados[302], ao invés da apreensão de dispositivos informáticos, o que poderia comprometer sobremaneira o desenvolvimento de atividades profissionais de um acusado ou de uma empresa.

Ao mesmo tempo, o acesso a dados armazenados em sistemas de "*clouds"* traz algumas peculiaridades que geram dificuldades no tratamento dos dados, especialmente no uso de tecnologia para reconstituição e obtenção das provas digitais buscadas.

Em verdade, o armazenamento em nuvem permite que dados de diferentes titulares sejam alocados no mesmo sistema de depósito, o que dificulta a busca sem que se atinja a privacidade de outras pessoas, bem como tendo em vista a dificuldade de se apartar e examinar apenas os dados que sejam de interesse da investigação ou guardem relação com o acusado, o que não ocorreria caso apenas o computador de sua titularidade fosse apreendido. Outrossim, os sistemas de armazenamento remoto dificultam a própria realização da cadeia de custódia dos dados obtidos, especialmente considerando que, muitas vezes, não se tem notícias sequer de onde o servidor remoto está localizado[303].

---

[300] Conforme dispõe o artigo 203 da Lei n.º 9.279/1996, "tratando-se de estabelecimentos industriais ou comerciais legalmente organizados e que estejam funcionando publicamente, as diligências preliminares limitar-se-ão à vistoria e apreensão dos produtos, quando ordenadas pelo juiz, não podendo ser paralisada a sua atividade licitamente exercida".

[301] A cópia dos dados é uma medida expressamente admitida pela legislação portuguesa, expressamente em seu artigo 16, n.º 7, *b*, da Lei n.º 109/2009. Da mesma forma, a *Ley de Enjuiciamiento Criminal*, em seu artigo 588 *sexies 2.c*, prioriza a realização da cópia ao invés da própria apreensão do dispositivo físico. Finalmente, o artigo 254-bis e o artigo 260,2, do *Codice di procedura penale* italiano também permite que se determine a realização de uma cópia dos dados informáticos em suporte adequado, como medida de preservação de seu conteúdo original.

[302] O artigo 3º da Portaria n.º 1287/2005, do Ministério da Justiça, indicava expressamente que "não se fará a apreensão de suportes eletrônicos, computadores, discos rígidos, bases de dados ou quaisquer outros repositórios de informação que, sem prejuízo para as investigações, possam ser analisados por cópia (back-up) efetuada por perito criminal federal especializado". Entretanto, a precitada portaria foi revogada por outro ato normativo editado pelo Ministério da Justiça (Portaria n.º 759/2009)

[303] ZAWOAD, Shams; HASAN, Ragib. *Digital forensics in the cloud*. CrossTalk. The Journal of Defense Software Engineering, September/October 2013.

4.2.2. Requisição de dados em poder de provedores ou de serviços de *internet:* Lei n.º 12.965/2014

A Lei n.º 12.965/2014, conhecida por "Marco Civil da *Internet"*[304], buscou disciplinar os princípios, garantias, direitos e deveres no ambiente virtual, sendo pioneira como forma de se regulamentar as diretrizes para atuação do Estado, as relações em ambiente virtual e a disciplina da *internet* no Brasil[305].

Trata-se de uma legislação edificada sobre três bases sólidas, notadamente a neutralidade da rede, a liberdade de expressão e a privacidade do usuário[306], bem como objetivou oferecer uma tutela sobre dados pessoais e regramentos sobre seu consentimento, em alinhamento com as diretrizes europeias de proteção aos dados pessoais[307].

Em seu artigo 5º, a Lei do Marco Civil da *Internet* estabeleceu definições terminológicas de temas inerentes ao ambiente virtual, notadamente a abrangência do conceito de registro de conexão (inciso VI), aplicações de *internet* (inciso VII) e registros de acesso a aplicações de *internet*[308] (inciso VIII), que são relevantes na tratativa dedicada aos meios de provas digitais.

---

[304] Ultrapassa os propósitos do presente trabalho científico a análise minuciosa da Lei do Marco Civil da *Internet*, limitando-nos a apresentar medidas gerais de acesso aos dados de forma remota e ao estudo quanto à necessidade de se exigir, com base nesta lei, autorização judicial para acesso aos dados armazenados em aparelhos celulares.

[305] TEIXEIRA, TARCÍSIO. *Curso de direito e processo eletrônico: doutrina, jurisprudência e prática*. 3ª edição. São Paulo: Editora Saraiva, 2015, p. 89.

[306] CARDOZO, José Eduardo Martins. *Prefácio*. In: LEITE. George Salomão; LEMOS, Ronaldo. (Coord.). Marco Civil da *Internet*. São Paulo: Editora Atlas, 2014.

[307] Embora a legislação tenha sido inovativa ao trazer definições conceituais sobre o ambiente da rede mundial de computadores e pretender oferecer proteção à privacidade dos usuários, é relevante a crítica lançada por Letícia Tavares e Bruna Alvarez, para quem "(...) a despeito do avanço decorrente da elaboração do Marco Civil da *Internet*, é possível afirmar que a lei é falha e obscura em diversos aspectos relativos à proteção de dados pessoais, não sendo suficiente à ampla proteção do direito fundamental à vida privada, no que se inclui o direito à proteção dos dados pessoais. Em verdade, contraditoriamente, o quadro legislativo atual não permite ao Brasil sequer dar cumprimento ao estabelecido no artigo 4º da Resolução n. 68/167, proposta pelo próprio País à ONU. Assim sendo, o simples conceito alargado de privacidade somado a uma legislação esparsa e lacunosa sobre o assunto não se mostra suficiente para evitar abusos e nem supre a expectativa dos brasileiros em relação à proteção de seus dados pessoais (...)" (TAVARES, Letícia Antunes; ALVAREZ, Bruna Acosta. *Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil*. In: ONODERA, Marcus Vinicius Kiyoshi; FILLIPO, Thiago Baldani Gomes de. (Org.). Brasil e EUA: Temas de Direito Comparado. 1ª edição. São Paulo: Escola Paulista da Magistratura, 2017, p. 157-205)

[308] São exemplos de "aplicações de *internet"* os aplicativos, de qualquer natureza, obtidos mediante acesso a lojas *online,* tais como *Apple Store, Google Play*, dentre outras.

É inegável que os *smartphones* conjugaram atribuições informáticas e telefônicas em um mesmo objeto, permitindo-se ainda a utilização da *internet* para acesso a diversos aplicativos que, naturalmente, são instrumentos de produção de dados. O caminho para este acesso pode prescindir da apreensão física do próprio aparelho, de modo que, mediante requisição judicial nas hipóteses estabelecidas pela Lei n.º 12.865/2014, é possível se obter os registros de conexão, o acesso a aplicações de *internet* as comunicações privadas armazenadas, que constituem verdadeiros elementos de prova de notório interesse investigativo[309].

Diante da importância das informações obtidas por intermédio destes registros e das comunicações privadas, o artigo 10º da Lei do Marco Civil da *Internet* estabeleceu que os provedores[310] responsáveis pela guarda dos registros de conexão e acesso a aplicações de *internet*, bem como de dados pessoais e do conteúdo de comunicações privadas, devem zelar pela preservação da intimidade, vida privada, honra e imagem das partes direta ou indiretamente envolvidas, disponibilizando-se seu conteúdo apenas mediante ordem judicial (artigo 10, §§ 1º e 2º), salvo no tocante aos dados cadastrais, que poderão ser acessados pelas autoridades administrativas que disponham e competência legal para sua requisição (artigo 10, § 3º)[311].

---

[309] Bruno Ricardo Bioni salientar que, "(...) com tais dados, obtém-se possivelmente a posição única e inequívoca de um computador conectado à *Internet* e, em tese, do seu usuário. Essa é a razão para o regime legal de retenção dos chamados 'logs' de conexão e aplicação, a fim de identificar a autoria dos atos praticados na *Internet* por seus usuários (...)" (BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento.* 2ª edição, Rio de Janeiro: Editora Forense, 2019, p. 210).

[310] A expressão "provedores de serviço" abrange as hipóteses de "provedor de *backbone",* "provedor de acesso", "provedor de correio eletrônico" e "provedor de conteúdo". O "provedor de *backbone"* é o responsável por disponibilizar o acesso à infraestrutura na qual os dados trafegam, sem exercer controle sobre o conteúdo. Trata-se de um conceito não tratado na Lei do Marco Civil da *Internet*, já que o usuário final da *internet* dificilmente terá alguma relação com ele. Os "provedores de acesso" ou de "conexão" são os responsáveis por disponibilizar a conexão à *internet* para os usuários, sem monitorar as informações trafegadas. O "provedor de correio eletrônico" é o responsável por disponibilizar um nome e senha para envio e recebimento de mensagens (*e-mails*), além de armazená-las. O "provedor de hospedagem" é o responsável por prestar serviço de armazenagem de dados em servidores próprios de acesso, permitindo-se que terceiros acessem tais dados nas condições definitivas com o contratante. Finalmente, o "provedor de conteúdo" é o responsável por disponibilizar informações na *internet*, seja de sua própria autoria ou de terceiros, que são produzidas pelo "provedor de informação", que é o efetivo autor da informação a ser disponibilizada (LEONARDI, Marcel. *Responsabilidade Civil dos Provedores de Serviços de Internet*. São Paulo: Editora Juarez de Oliveira, 2005, p. 155-171)

[311] O dispositivo legal guarda similitude com a previsão dos artigos 15 a 17 da Lei n.º 12.850/2013, que também permitem que os dados cadastrais do investigado, notadamente qualificação pessoal, a filiação e o endereço mantidos pela Justiça Federal, empresas telefônicas, instituições financeiras, provedores de *internet* e administradoras de cartão de crédito, além de dados de reservas e registros de viagens mantidos por empresas de transporte, sejam informados ao Delegado de Polícia e ao Ministério Público independentemente de autorização judicial.

De igual sorte, com o intuito de preservar os registros de conexão e acesso a aplicações de *Internet*, a legislação estabeleceu nos artigos 13 a 15 que os registros de conexão sejam guardados e mantidos pelo administrador do sistema autônomo pelo prazo de 1 (um) ano, ao passo que os registros de acesso a aplicações de *internet* devem ser guardados pelo respectivo provedor de aplicações pelo prazo de 6 (seis) meses, sendo que o prazo poderá ser estendido mediante requerimento formulado pela autoridade policial, administrativa ou pelo Ministério Público[312].

No que concerne aos meios de obtenção de provas digitais, o artigo 22 da Lei n.º 12.865/2014 dispôs que os referidos registros de conexão ou acesso a aplicações de *internet* poderão ser fornecidos para formação de conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, mediante requerimento formulado pela parte interessado ao julgador, que deverá ser instruído com fundados indícios da ocorrência do ilícito, justificativa motivada da utilidade dos registros solicitadas para fins de investigação ou instrução probatório e o período ao qual se referem os registros (artigo 22, parágrafo único, incisos I a III).

Cumpre destacar que, por se tratar de uma requisição judicial, o servidor demandado deverá colaborar com o envio das informações demandadas[313], sob pena de, caso negue indevidamente o acesso ao conteúdo, vir a ser responsabilizado pelo delito de desobediência (artigo 330 do Código Penal), sem prejuízo da adoção de outras medidas excepcionais para apreensão dos dados em poder do servidor.

---

[312] Na Alemanha, a Suprema Corte apreciou a constitucionalidade de previsão normativa que permite aos fornecedores de serviços de telecomunicações que coletem e armazenem dados telefônicos (rede fixa, comunicações móveis, fac, SMS, MMS) sem motivação prévia, por um período de seis meses. No julgamento, a Corte assentou que "(...) precautionary storage of telecommunications traffic data without cause for six months by private service providers as provided by Directive 2006/24/EC of the European Parliament and the Council of 15 March 2006 (OJ L 105 of 13 April 2006, p. 54; hereinafter: Directive 2006/24/EC) is not in itself incompatible with Article 10 of the Basic Law (Grundgesetz – GG); any potential priority of the Directive is therefore not relevant to the decision (…)", bem como disciplinou a responsabilidade pela segurança dos dados e a restrição de sua utilização, permitindo-a apenas em situações proporcionais, tais como, na seara criminal "(…) this requires the suspicion of a serious criminal offence based on specific facts. For warding off danger and for performing the duties of the intelligence services, they may only be permitted if there is actual evidence of a concrete danger to the life, limb or freedom of a person, to the existence or the security of the Federation or of a Land or to ward off a danger to public safety (…)" (1BvR 256/08,1BvR 586/08, 1BvR263/08– Vorratsdatenspeicherung. Disponível em: <http://www.bverfg.de/e/rs20100302_1bvr025608en.html>. Acesso em 20 de dezembro de 2020).

[313] STJ, REsp n.º 1.622.483/SP, Rel. Ministro Paulo de Tarso Sanseverino, Terceira Turma, julgado em 15 de maio de 2018, DJe 18.05.2018; STJ, REsp n.º 1.560.976, Rel. Ministro Luis Felipe Salomão, julgado em 30 de maio de 2019, DJe 01/07/2019.

Os dados de registro devem ser requisitados sempre mediante autorização judicial, conforme previsão taxativa do artigo 10, § 1º e artigo 22, ambos da Lei n.º 12.965/2014.

Com relação aos dados pessoais autônomos, a legislação foi omissa, porquanto há menção expressa apenas aos dados cadastrais e aos dados de registro. Todavia, em uma interpretação do artigo 10, § 1º, da Lei n.º 12.965/2014, que prevê expressamente a possibilidade de que a disponibilização dos registros seja acompanhada dos dados pessoais ou outras informações que possam contribuir com a identificação do usuário ou do terminal, não se pode afastar a possibilidade da requisição de dados pessoais autônomos aos provedores de serviços e de aplicação de *internet*, com a observância dos requisitos previstos no artigo 22 do mesmo Diploma Legal.

Infere-se que a Lei n.º 12.865/2014 disciplinou a possibilidade de obtenção de prova digital e determinou sua preservação, mediante imposição de conservação[314] dos registros de conexão e acesso a aplicações de *internet*, além de ter regulamentado que o acesso aos dados deverá ser concedido[315] pelos referidos provedores, quando o material for de interesse no âmbito de um processo criminal, sempre mediante ordem judicial.

O artigo 7º, incisos II e III, da Lei n.º 12.965/2014, estabeleceu como direito do usuário da *internet* a "II - inviolabilidade e sigilo do fluxo de suas comunicações pela *internet*, salvo por ordem judicial, na forma da lei" e a "III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial[316]". De igual forma, no

---

[314] A conservação expedita de dados armazenados em dispositivos informáticos, colocando-os a salvo de supressões e modificações que comprometam seu conteúdo, é uma das medidas estabelecida na Convenção de Budapeste, especialmente no já mencionado artigo 16. Nota-se que, embora não seja signatário da referida Convenção, o Brasil acabou por disciplinar a medida para os provedores de conexão e aplicação de *internet* (KIST, Dario José. *Prova digital no processo penal.* Op. cit. p. 137-138). Previsão similar foi adotada pela legislação portuguesa, ao determinar a conservação de dados (artigo 12 da Lei n.º 109/2009)

[315] A apresentação dos dados e a concessão do acesso, mediante requisição judicial, também é objeto de disciplina pela Convenção de Budapeste, especialmente no artigo 18. Trata-se de medida adotada em substituição ao emprego da busca e apreensão propriamente dita, sempre que as pessoas e fornecedores de serviços apresentarem os dados a partir da ordem expedida. Igualmente, o artigo 14 da Lei Portuguesa n.º 109/2009 também disciplinou a medida, chamada de "injunção para apresentação ou concessão do acesso a dados".

[316] A previsão trazida na Lei n.º 12.965/2014 é bastante similar àquela contemplada no artigo 3º, inciso V, da Lei n.º 9.472/1997, que prevê expressamente como sendo direito do usuário dos serviços de telecomunicação a "à inviolabilidade e ao segredo de sua comunicação, salvo nas hipóteses e condições constitucional e legalmente previstas". Trata-se de uma forma de se estender a mesma previsão contida no campo dos serviços

artigo 10, § 2º, preconizou-se que "o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º".

Constata-se que a Lei do Marco Civil da *Internet* assegurou ao usuário a garantia do sigilo do fluxo de suas comunicações e a inviolabilidade e sigilo das comunicações privadas armazenadas, que somente poderão ser franqueadas mediante ordem judicial, nas hipóteses e na forma que a lei vier a estabelecer.

Denota-se que, ao se referir expressamente às "comunicação privadas armazenadas", a legislação se ateve unicamente aos dados privados "comunicados", vale dizer, aqueles que foram produzidos e repassados a terceiros, não se aplicando, *in thesis*, aos dados produzidos e armazenados localmente que, por qualquer razão, não tenham sido objeto de compartilhamento para com terceiros. Em relação a eles, aplicar-se-iam unicamente as disposições constitucionais do artigo 5º, inciso X, da Constituição Federal, mas não propriamente a regulação contida na Lei n.º 12.965/2014.

Extrai-se do parágrafo 2º do artigo 10 que houve um aprofundamento no nível de abrangência das informações a serem fornecidas. Impôs-se uma obrigação aos provedores de acesso e aplicações de *internet* de franquear não apenas os registros, mas também o próprio conteúdo das comunicações privadas armazenadas de que disponham legitimamente.

Como se vê, o grau de adensamento das informações é substancialmente maior, já não se está a demandar apenas informações periféricas e menos custosas à privacidade e intimidade[317], tais como os registros de conexão e de acesso a aplicação de *internet* (artigo 10, § 1º, da Lei do Marco Civil da *Internet*) [318], os quais

---

de telecomunicação aos usuários da *internet*, com as observâncias referentes às peculiaridades de cada serviço prestado.

[317] MOURA, Maria Thereza Rocha de Assis; BARBOSA, Daniel Marchionatti. *Dados digitais: interceptação, busca e apreensão e requisição.* In: LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro. LAUX, Francisco de Mesquita; RAVAGNANI, Giovani dos Santos. *Direito, processo e tecnologia.* São Paulo: Editora RT, 2020, p. 498.

[318] A previsão ao acesso a registros de conexão e dados encontra previsão no *Communications Data Act* de Israel, editado em 27 de junho de 2008, que permitiu que autoridades investigativas israelenses de obter dados de telecomunicação, sem, contudo, terem acesso propriamente ao conteúdo da conversa mantida, o que somente seria possível nas hipóteses trazidas pela *Secret Monitoring Act.*

permitem apenas a identificação do usuário do serviço, o início e término de uma conexão, as informações de data e hora de determinado aplicativo, o número do IP utilizado para o acesso, etc.

4.2.2.1. Obtenção de dados de geolocalização

Os dados relacionados à geolocalização ganham destaque em investigações criminais, especialmente nos casos em que os meios tradicionais de provas se revelem insuficientes para se descortinar a autoria de um delito. Por intermédio da aplicação de *Global Positioning System* (GPS) do sistema informático ou de dispositivos móveis (*v.g.*, *smartphones*) ou da distribuição territorial do sinal de telefonia móvel (Estação Rádio Base[319]), é possível relacionar o suspeito à cena do crime ou afastar sua participação.

A utilização de instrumentos investigativos para a geolocalização de pessoas vem sendo alvo de intensos debates no cenário jurisprudencial norte-americano. Em *United States vs. Jones 565 U.S. 400 (2012)*, a Suprema Corte julgou que a instalação de um

---

O referido Ato prevê, em sua Seção 3, que "(a) The court may, upon a motion by a police officer authorized by the Inspector General, or by a representative of another investigatory authority (in this section referred to as "the motion"), permit by order the Police or the other investigatory authority to obtain communications data from the database of a telecommunications licensee as prescribed in the order, if it is satisfied it is necessary for any of the purposes specified below, provided that obtaining such communications data does not infringe any person's privacy beyond that necessary: (1) To save or to protect human life; (2) To detect, investigate or prevent offenses; (3) To detect and prosecute offenders; (4) To lawfully confiscate property". De igual sorte, a Seção 4 do Ato prevê, em casos urgentes, a possibilidade de as informações serem obtidas sem a respectiva ordem judicial autorizativa. Os dispositivos legais foram objeto de questionamento judicial pela Associação pelos Direitos Civis de Israel e pela Ordem dos Advogados Israelita, que alegaram a suposta violação à privacidade e à proporcionalidade das previsões normativas contidas nos atos. A Suprema Corte de Israel, por unanimidade, afastou as alegações trazidas pelas autoras, mas estabeleceu parâmetros proporcionais e interpretativos do ato, a fim de amoldá-lo ao respeito à privacidade e, ao mesmo tempo, à necessidade de investigação. (Disponível em <https://versa.cardozo.yu.edu/sites/default/files/upload/opinions/Association%20for%20Civil%20Rights%20in%20Israel%20v.%20Israel%20Police.pdf>. Acesso em: 20 de dezembro de 2020).

[319] OLIVER, Nancy K. *Location, Location, Location: Balancing Crime Fighting Needs and Privacy Rights*, University of Baltimore Law Review: Vol. 42: Iss. 3, Article 5, 2013, p. 487-488. Disponível em: http://scholarworks.law.ubalt.edu/ublr/vol42/iss3/5. Acesso em: 20 de dezembro de 2020. Como bem sintetiza LIMA, "(...) por meio da estação rádio base (ERB), é possível saber a localização aproximada de qualquer aparelho celular ligado, desde que este esteja em uso, seja enviando ou recebendo uma ligação, e, consequentemente, de seu usuário. Grosso modo, as ERB's são as antenas ou estações fixas utilizadas pelos aparelhos móveis para se comunicar. Utilizando seus dados, é possível saber o local aproximado onde se encontra o referido aparelho. Ademais, muitos celulares possuem GPS, o que permite encontra-los em determinado momento ou saber, posteriormente, por onde seus proprietários estiveram. Tais informações podem ser extremamente úteis em determinadas investigações, não apenas como indício de que determinado agente estava nas proximidades do local do crime no exato momento em que o delito foi executado, mas também como contra-indício para informar a validade de eventual álibi apresentado pelo acusado no sentido de que estava em local diverso à época do delito (...)" (LIMA, Renato Brasileiro. *Legislação especial comentada.* São Paulo: Ed. Juspodivm, 8ª edição, 2020, p. 523)

dispositivo de *Global Positioning System* (GPS) em um veículo de um suspeito, a fim de monitorar seus deslocamentos, constituiria uma modalidade de *"search and seizure"* protegida pela *Fourth Amendment*, o que exigiria uma prévia autorização judicial para a utilização do referido meio de produção de prova[320].

Em *United States vs. Carpenter, 585 U.S. ___ (2018)*[321], a Suprema Corte reconheceu, por apertada maioria, a necessidade de ordem judicial lastreado em "probable cause", para a aquisição de dados digitais atinentes à movimentação das pessoas, através dos registros das torres de chamadas dos aparelhos celulares, não sendo aplicável a extensão da *"third party doctrine"* quanto aos registros mantidos pela operadora de telefonia celular.

---

[320] *Harvard Law Review*, Vol. 126:176-2012, p. 226-236. Disponível em: https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_united_states_v_jones.pdf, Acesso em: 20 de dezembro de 2020.

[321] No caso apreciado, a Suprema Corte foi instada a decidir se a obtenção do histórico de registros de dados contendo a localização do aparelho, sem uma ordem judicial específica, configuraria uma violação à expectativa de privacidade do acusado. Entre 2010 e 2011, policiais passaram a investigar uma sequência de roubos violentos praticados em lojas da região de Michigan e Ohio. Em abril de 2011, quatro dos acusados foram capturados e presos, tendo um deles confessado a prática do crime e entregado o telefone para os agentes do FBI pudessem revisar as ligações feitas pelo telefone na época dos assaltos. O FBI, com base na *Stored Comumunication Act, 18 U.S.Code, 2703 (d)*, solicitou e obteve uma autorização judicial para que as operadores de telefonia móvel fornecessem os registros históricos dos aparelhos investigados e, com isso, pudessem obter a *Cell Site Location Information (CSLI)*, notadamente a relação de comunicação dos aparelho celular de Carpenter com torres de telefonia. A partir de então, concluiu-se que Carpenter estava num raio de duas milhas de 4 (quatro) assaltos praticados, o que motivo uma acusação em face dele. Carpenter veio a ser condenado em julgamento perante um júri e, recorrendo à Suprema Corte, questionou a licitude da prova produzida, sob alegação de que, apesar de ter sido obtida uma ordem judicial, os requisitos para o acesso aos registros perante as operadoras (*Stored Comumunication Act*) são mais brandos do que aqueles necessários para um mandado judicial de busca e apreensão ("*warrant*" em "*search and seizure*"), que demandariam a comprovação de uma *probable cause*. Nota-se que não se desafiou, propriamente, a existência de uma ordem judicial, a qual já havia sido obtida pelo FBI, mas sim um mandado de busca e apreensão específico, cujos requisitos para a concessão são mais qualificados do que aqueles necessários para a obtenção do conteúdo perante as operadoras. Em verdade, o questionamento levado a efeito por Carpenter consistiu no fato de que a autorização judicial emitida foi baseada na requisição de dados perante terceiros (*third party doctrine*), que não demanda elevado rigor probatório para sua concessão, bastando a existência de "reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation". Ao revés, caso a medida consistisse em uma "search and seizure" nos moldes contidos na *Fourth Amendment*, o padrão de *standart* probatório é substancialmente elevado, de requisitos mais complexos, cabendo aos órgãos investigativos comprovar a existência de uma "probable cause" , mediante afirmação ou juramento, além de descrição pormenorizada do local da busca, de pessoas e coisas a serem localizadas. Cotejando-se a situação trazida com outros precedentes relacionados ao tema, a Suprema Corte reconheceu que, embora o cidadão esteja ciente de que os registros são mantidos pela sua operadora de telefonia celular, isso acontece sem nenhum ato afirmativo da parte do usuário. Portanto, a Suprema Corte reconheceu a necessidade de um mandado judicial para acesso aos dados de localização do acusado, equiparando a situação às hipóteses de *search and seizure* sob o regime jurídico protetivo da *Fourth Amendment* (Disponível em: <https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf>. Acesso em 20 de dezembro de 2020).

Trazendo a discussão para o cenário nacional, o artigo 13-B do Código de Processo Penal versou sobre o tema. Para tanto, dispôs o legislador sobre a possibilidade de se requisitar às empresas prestadoras de serviço de telecomunicações e/ou telemática, mediante autorização judicial, a disponibilização de meios técnicos adequados para localização da vítima ou de suspeitos de um delito de tráfico de pessoas, que esteja em curso.

Dessume-se que a intenção legislativa foi a de, para prevenção e repressão dos crimes relacionados ao tráfico de pessoas, permitir-se uma rápida e eficaz localização da vítima ou dos suspeitos do crime em curso. Importante destacar, porém, que o fornecimento de sinais, informações e outros elementos técnicos se limitam a questões georreferenciais, atinentes à cobertura, setorização e radiofrequência (artigo 13-B, § 1º, do CPP), não compreendendo o acesso ao conteúdo da comunicação propriamente dita, o que dependeria de autorização judicial (artigo 13-B, § 2º, inciso I, do mesmo Diploma Legal).

Analisando-se o dispositivo legal em sua inteireza e reconhecendo-se a boa intenção legislativa, não se pode deixar de criticar sua questionável técnica legislativa, o que põe em dúvida a necessidade de autorização judicial para obtenção dos referidos dados.

Inicialmente, denota-se que o artigo 13-B, *caput,* é expresso ao impor que a requisição poderá ser feita pelo Ministério Público ou o Delegado de Polícia, mediante autorização judicial. Infere-se que há expressa indicação da imprescindibilidade da chancela judicial para a diligência. Entretanto, de maneira inadvertida e contraditória, o legislador se vale da expressão "requisitar", que tem natureza mandamental, enquanto ordem a ser conferida pelos referidos órgãos investigativos e, por conseguinte, tornaria dispensável a prévia autorização judicial para obtenção das informações e dados pretendidos[322].

De igual sorte, o artigo 13-B, § 2º, incisos II e III, estabelece que a prestadora de telefonia móvel celular deverá fornecer o sinal por período não superior a 30 (trinta) dias, renovável por uma única vez, por igual período e, caso haja renovação por prazo superior, será necessária a apresentação de ordem judicial.

[322] Tourinho Filho aduz que "(...) requisição é exigência legal. Requisitar é exigir. Já a palavra requerimento traduz a ideia de solicitação de algo permitido por lei (...)" (TOURINHO FILHO, Fernando da Costa. *Processo Penal.* 33ª edição. São Paulo: Editora Saraiva, 2011, v. 1, p. 224).

Mais uma vez a redação é imprecisa. Se toda e qualquer "requisição" somente pode ser feita mediante ordem judicial – como dispõe o *caput* do artigo 13-B do Código de Processo Penal –, é irrazoável que o legislador tenha apontado a imprescindibilidade da ordem judicial apenas para a obtenção de sinais por prazo superior a 60 (sessenta) dias, o que compreende os 30 (trinta) dias iniciais renováveis por uma única vez. Portanto, remanesce a dúvida se a ordem judicial seria necessária para toda e qualquer "requisição" (como dispõe o artigo 13-B, *caput*) ou apenas para os casos em que houver a necessidade de fornecimento de sinais por prazo superior a 60 (sessenta) dias, nos termos do artigo 13-B, § 2º, incisos II e III, do Código de Processo Penal[323].

O arremate da incoerência legiferante decorre do artigo 13-B, § 4º, do Código de Processo Penal, o qual dispõe que, caso não haja manifestação judicial no prazo de 12 (doze) horas, a autoridade competente requisitará o fornecimento dos meios técnicos identificados no *caput*, comunicando-se imediatamente o juiz. A bem da verdade, se o fornecimento do sinal representa uma informação com potencial de atingir a privacidade, intimidade e vida privada do cidadão e, por isso, demanda uma chancela judicial para se compatibilizar o interesse investigativo com os direitos e garantias individuais constitucionalmente assegurados, a fixação de prazo de 12 (doze) horas fere qualquer razoabilidade.

Em verdade, para além de se tratar de prazo exíguo, inferior a outros estabelecidos na legislação processual que envolvem valores igualmente relevantes (*v.g.*, o prazo conferido ao julgador para apreciação do pedido de prisão temporária é de 24 horas, conforme artigo 2º, § 2º, da Lei n.º 7.960/1989), a possibilidade de se requisitar diretamente o sinal e meios técnicos para localização da vítima ou dos suspeitos equivaleria dizer que os referidos direitos constitucionais das pessoas atingidas, nos casos de tráfico de pessoas em curso, vigeriam por apenas 12 (doze) horas.

---

[323] Para Aury Lopes Júnior, "(...) as informações serão prestadas durante um prazo máximo de 30 dias, renováveis uma única vez, por igual período. Dois pontos precisam ser sublinhados: 1) Considerando o disposto no art. 13-B, § 2º, III, do CPP, qualquer prorrogação deverá ser precedida de autorização judicial. 2) A requisição direta não se aplica à prorrogação, que sempre deverá ser judicialmente autorizada. A urgência justifica a primeira intervenção nas comunicações por requisição direta, para rápida implementação (já que, passadas 12 horas do pedido, não houve decisão judicial), ainda que sem autorização judicial, mas não legitima a prorrogação (...)" (LOPES JR., Aury. *Direito Processual Penal.* São Paulo: Saraiva, 2020, p. 189).

Ademais, os crimes de tráfico de pessoas são geralmente complexos e demandam uma extensa análise de elementos de informação angariados, muitas vezes de cunho transnacional, o que revela ser contraproducente estabelecer um prazo tão ínfimo ao julgador para apreciação da medida. Diante das diversas incoerências legislativas – que suscitam alegações de inconstitucionalidade[324]–, é duvidosa a necessidade de ordem judicial para o fornecimento dos referidos dados[325], tendo já sido admitida a desnecessidade da ordem judicial[326], em julgamento realizado antes do advento do artigo 13-B do Código de Processo Penal.

Outrossim, embora o dispositivo legal seja aplicável unicamente às hipóteses de crimes relacionados a tráfico de pessoas, não se afasta a possibilidade da quebra de sigilo de dados de localização, por ordem judicial, na apuração de outros delitos igualmente graves e por intermédio de técnicas distintas, inclusive a "reverse location search"[327].

---

[324] CUNHA, Rogério Sanches; PINTO, Ronaldo Batista. *Código de Processo Penal e Lei de Execução Penal Comentados.* 2ª ed. São Paulo: Editora Juspodivm, 2018, p. 76-77. Para Guilherme Dezem, não haveria inconstitucionalidade no texto do artigo 13-B, § 4º, do Código de Processo Penal, já que não haveria restrição do direito aquém de seu conteúdo essencial (DEZEM, Guilherme Madeira. *Curso de processo penal*. Op. cit., p. 257).

[325] Reconhecendo-se a necessidade de autorização judicial: LIMA, Renato Brasileiro. *Legislação especial comentada*, op. cit. p. 525.

[326] STJ, HC n.º 247.331/RS, rel. Min. Maria Thereza Moura, julgado em 21 de agosto de 2014, DJe 03/09/2014.

[327] Ainda com relação à geolocalização, discute-se a admissibilidade da utilização da técnica "reverse location search", pela qual se requisitam os dados de todos os usuários que estiveram logados em determinado local e hora e, partir de então, procede-se à mineração dos dados para se identificar o perpetrador do delito. Trata-se de uma técnica bastante utilizada nos Estados Unidos, para identificação da autoria de crimes graves (Disponível em <https://slate.com/technology/2019/02/reverse-location-search-warrants-google-police.html>. Acesso em 20 de dezembro de 2020). A técnica tem sido utilizada em investigações sobre crimes graves, tais como, *ad exemplum,* nas investigações relacionadas ao assassinato da vereadora Marielle Franco, no Rio de Janeiro. Matéria com acesso em 28 de junho de 2020 e disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2019/03/13/como-os-celulares-ajudaram-a-achar-o- assassino-de-marielle-franco.htm>. Acesso em 20 de dezembro de 2020.
O Tribunal de Justiça do Estado de São Paulo, por intermédio da sua 4ª Câmara de Direito Criminal, no Mandado de Segurança n.º 2219862-80.2016.8.26.0000, autorizou a concessão de dados coletivos por usuários das aplicações da plataforma *Google*, mas houve por bem inadmitir a extensão para um raio de até 500m (quinhentos metros), o que causaria inevitável violação a privacidade de uma gama indefinida de usuários, bem como obstou o fornecimento de senhas dos serviços, sem a identificação precisa das pessoas envolvidas. Em pedido de tutela provisória ao Superior Tribunal de Justiça (STJ), foi concedido efeito suspensivo ao Recurso em Mandado de Segurança n.º 54.133/SP, até o julgamento da decisão final (STJ, Tutela Provisória n.º 292/SP, Rel. Ministro Antônio Saldanha Palheiro, julgado em 24 de fevereiro de 2017, DJe 03/03/2017). Sobre o tema, recomenda-se a sequência de artigos jurídicos disponibilizados em: <https://www.jota.info/especiais/juizes-ordenam-quebra-coletiva-de-sigilo-de-dados-com-base-em-localizacao-27052019>. Acesso em: 20 de dezembro de 2020. Em campo doutrinário, Maria Thereza Rocha de Assis Moura e Daniel Barbosa Marchionatti defendem a medida, desde que usada com moderação e quando se revelar indispensável para apuração de crimes graves, descartando-se os dados de terceiros (MOURA, Maria Thereza Rocha de Assis; BARBOSA, Daniel Marchionatti. *Dados digitais: interceptação, busca e apreensão e requisição.* Op. cit., p. 498).

4.2.3. Infiltração clandestina: a utilização de *malwares* para interceptação, busca, monitoramento e apreensão de dados

Dentre as formas de acesso remoto a dados contidos em aparelhos celulares, vem ganhando destaque, especialmente no cenário internacional, a utilização de meios e técnicas sub-reptícias e ocultas que possibilitariam a realização de infiltrações verdadeiramente clandestinas, geralmente por intermédio da utilização de *malwares*.

Malware constitui um conceito genérico que abrange uma gama de produtos (*software*) maliciosos que são instalados discreta e clandestinamente em um sistema de processamento de dados, sem o consentimento do usuário, oferecendo risco às informações ali contidas, à confiabilidade dos dados e à disponibilidade do sistema[328].

Por intermédio de um *malware*, um usuário externo e estranho ao padrão de usuários do sistema informático invadido passa a ter acesso e controle de todo o conteúdo armazenado, sem que o usuário legítimo tenha conhecimento desta ação[329]. Compreendem, para tanto, os vírus, *computer worms*, *trojan horses*[330], *ransomware*, *spyware*, *adware*, dentre outros programas instalados que promovam alterações, modificações e remoções na plataforma de dados do sistema invadido.

A inoculação de um *malware* pode se dar mediante acesso físico ao sistema informático pretendido, mediante utilização de um *pendrive*, *CD*, ou outro meio correlato, bem como por intermédio da *internet*, mediante envio *online* de um arquivo sub-reptício ao alvo e, ainda, pelo mero acesso a páginas específicas da *web.*

---

[328] FILIOL, Eric. *Computer Viruses: from theory to application*. Paris: Springer, 2005, p. 86. *Apud:* VACIAGO, Giuseppe; RAMALHO, David Silva. *Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings,* Digital Evidence and Electronic Signature, Law Review, 13 (2016), p. 88.

[329] CASTRO, Luiz Augusto Sartori de. *Busca e apreensão mediante uso de 'malware'.* In: Boletim do Instituto Brasileiro de Ciências Criminais, São Paulo, ano 21, n.º 251, outubro de 2013, p. 06-08.

[330] VACIAGO e RAMALHO apontam que "(...) when referring to the use of such software in criminal investigations, the doctrine usually refers only to Trojan horses or simply trojans. However, trojans represent just one of many types of malware which may be used in criminal investigations in the digital environment, alongside, among others, logic bombs, spyware, rootkits, viruses, worms or even the increasingly common blended threats, which include more than one type of malware (…)" (VACIAGO, Giuseppe; RAMALHO, David Silva. *Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings,* Op. cit. p. 88).

De toda forma, independentemente da forma de acesso, o *malware* permite a criação de uma forma de comunicação oculta e remota entre o dispositivo monitorado e o comando, permitindo-se o monitoramento em tempo real, de áudio, vídeo, funções de microfones e câmeras, acesso a dados armazenados, o fluxo de comunicações, dentre outras funcionalidades[331]. Trata-se, pois, de um meio de investigação ou obtenção de provas, podendo vir a ser considerada sua natureza cautelar probatória[332].

O uso do *malware* permite um grande dinamismo na atividade investigativa, trazendo-se a possibilidade se operacionalizar técnicas de interceptações telemáticas, *roving bug*, buscas *online*, vigilância *online* e investigações por gravação de vídeo ou observação em tempo real, além de acesso a geolocalização dos dispositivos informáticos.

Conforme doravante se analisará, o *malware* permitirá o acesso a dados em trânsito – especialmente quanto ao fluxo da comunicação, como no caso de interceptações telemáticas – e a apreensão de dados armazenados nos dispositivos.

Dentre os meios de obtenção de provas mediante utilização de recursos remotos de *malware,* destaca-se a busca e apreensão *online,* que consiste na técnica que permite a recolha de dados armazenados de forma remota, mediante a instalação de um *malware* no sistema informático cujo acesso se pretende avançar.

Por intermédio deste *software* malicioso e mediante autorização judicial nas hipóteses regulamentares, possibilita-se que os investigadores tenham acesso aos dados armazenados em suporte físico (*v.g.*, aparelho celular) ou em "nuvem", bem como às chaves de criptografia. Ainda, os investigadores poderão identificar onde estariam as possíveis fontes de provas (busca *online*) e, ainda, realizar a apreensão dos dados, através de cópia dos dados e sua transmissão para o sistema informático administrado pelo invasor (apreensão *online*)[333].

---

[331] MENDES, Carlos Hélder Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software.* Op. cit. p. 163-164.
[332] Idem, ibidem, p. 165-166.
[333] Para David Ramalho, é possível que o uso do *malware* seja relevante para "(...) monitorizar a actividade do respectivo utilizar em ambiente digital, possivelmente activando funcionalidade de hardware (GPS, câmera, microfone, etc.) e/ou recolher dados a partir daí enviados ou aí introduzidos, armazenados, recebidos, eliminados ou por qualquer forma tratados, para subsequente acesso ou envio remoto para o intrusor, neste

A técnica adotada é substancialmente vantajosa, porquanto econômica e efetiva. Em verdade, a busca e apreensão *online* evita o manejo desnecessário de recursos pessoais dos órgãos investigativos, notadamente o deslocamento de policiais e membros do Ministério Público para a apreensão física do suporte eletrônico onde condensadas as informações, bem como garante a estabilidade dos dados e sua permanência, assegurando-se seu acesso de maneira rápida e eficaz, evitando-se que o alvo venha a destruí-los juntamente com o próprio aparelho celular.

Outrossim, o acesso às chaves de criptografia imprime inevitável velocidade à investigação, já que tornaria prescindível a utilização de técnicas informáticas para revelação das senhas e barreiras pessoais aos dados, caso não sejam informados de maneira consentida pelo acusado.

A busca e apreensão mediante o uso de *malware*, embora não tenha sido previsto expressamente na Convenção de Budapeste, já é objeto de expressa previsão em ordenamentos jurídicos estrangeiros[334].

caso, o órgão de polícia criminal (...)" (RAMALHO, David Silva. *Métodos Ocultos de Investigação*. Coimbra: Almedina, 2017, p. 313-314).

[334] Em Portugal, o artigo 19 da Lei do Cybercrime n.º 109/2009 estabelece a possibilidade da utilização de técnicas de "acções encobertas", previstas na Lei n.º 101/2001, para determinados tipos penais, bem como estabelece que, em sendo necessário, sejam utilizados outros meios e dispositivos informáticos, observando-se, naquilo que for aplicável, as regras previstas para a interceptação das comunicações. Diante da previsão expressa de que as "acções encobertas" podem ser realizadas mediante meios e dispositivos informáticos, tem-se interpretado a possibilidade do uso de malware, já que estes recursos se amoldariam à elevada margem de discricionariedade conferido pelo artigo 19, 2, da Lei n.º 109/2009. Em verdade, a previsão legislativa genérica procurou colmatar eventual insuficiência dos demais meios de obtenção de provas eventualmente existentes e, segundo DAVID RAMALHO, permitiu a veiculação de "(...) meios e dispositivos que operam de modo materialmente semelhante à figura do agente encoberto (...) e que devem ser utilizados quando a própria ação encoberta e os demais métodos ocultos forem incapazes de dar respostas às exigências da investigação. Trata-se (...) da consagração do hacking e da utilização (...) de malware como método oculto de investigação criminal em ambiente digital (...)" (RAMALHO, David Silva. *Métodos Ocultos de Investigação*. Coimbra: Editora Almedina, 2017, p. 304. Na mesma linha: JESUS, Francisco Marcolino. *Os Meios de Obtenção da Prova em Processo Penal*, 2.ª edição, Coimbra: Editora Almedina, 2015, p. 246. Em sentido contrário: MESQUITA, Paulo Dá. *Processo Penal, Prova e Sistema Judiciário*, Coimbra: Editora Coimbra (Wolters Kluwer), 2010, p. 115). Na Espanha, o artigo 588 *septies a* da *Ley de Enjuiciamiento Criminal* prevê expressamente a possibilidade da utilização de software que permita, de forma remota e telemática, o exame à distância e sem o conhecimento do seu titular ou do usuário do conteúdo de um computador, dispositivo eletrônico, sistema informático, instrumento de armazenamento massivo de dados informáticos ou base de dados, sempre que se pretenda investigar determinados tipos de crimes. Por sua vez, na França, o article 706-102-1 do *Code de Procedure Penale* também admite a utilização de malware. Na Itália, a utilização do *captatore informático* foi introduzido de maneira taxativa nas recentes reformas legislativas, como instrumento de investigação para determinados delitos, conforme art. 266 do *Codice di Procedura Penale* e seguintes. Relevante anotar que, antes mesmo de sua previsão expressa, a jurisprudência já admitia o recurso tecnológico, em algumas hipóteses bem específicas (CAPRIOLI, Francesco. *Il 'captatore informatico' come strumento di ricerca della prova in Italia.* Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 3, n. 2, p. 483-510, mai.-ago. 2017).

Finalmente, destaca-se que a infiltração de sistemas informáticos por intermédio de *malware* é um recurso que permite a obtenção de dados de geolocalização[335] do aparelho inoculado, identificando-se sua exata posição geográfica ainda que este não esteja sendo utilizado como instrumento de comunicação no momento.

4.2.3.1. A (im)possibilidade do uso do *malware* como meio de obtenção de prova no Brasil

No Brasil, a obtenção de provas por intermédio de medidas de infiltração, com a utilização de *malwares*, é controvertida.

Ao menos na perspectiva doutrinária, refuta-se a utilização da técnica em apreço. Dentre os argumentos lançados, sustenta-se que a invasão de sistemas informáticos por *malware* corresponderia a um meio atípico de produção de provas, não regulamentado, o que malferiria o princípio da legalidade e proporcionaria uma indevida investida em direitos e garantias fundamentais.

Assim, a tipicidade processual e a preexistência de um procedimento regular, com a determinação de condutas ilícitas em um rol de crimes passíveis da utilização do referido meio invasivo de obtenção de provas, com relação de proporcionalidade entre o dano alcançado pelo ilícito e o grau de lesividade do instituto processual[336], constituiriam fundamentos de legalidade da intervenção, servindo ainda como limitação à atuação investigativa estatal e regulação para a eventual determinação da prova a ser produzida[337].

Sem embargos, para além da ausência de regulamentação legal, a impossibilidade da utilização de *malware* repousa também na forma de utilização da técnica

---

[335] Os dados de localização, previstos no artigo 2º, *c*, da Diretiva n.º 2002/58/CE, são conceituados por GUARDIA como "dados eventualmente de tráfego", à medida que podem ser direcionados a viabilizar o próprio processo comunicativo ou, ainda, ser considerando como dados distintos de tráfego, nas hipóteses em que a localização do aparelho permite a constituição de um rastro digital a permitir a individualização do usuário, ainda que uma comunicação não esteja sendo realizada (GUARDIA, Gregório Edoardo Raphael Selingardi. *Comunicações Eletrônicas e dados digitais no processo penal*. Op. cit., p. 106-111).

[336] MENDES, Carlos Hélder Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software.* Op. cit. p. 171. Esta necessidade foi constatada pelos ordenamentos jurídicos que admitem a utilização do malware, de modo que muitos deles, à exemplo do artigo *588 septies a* da *Ley de Enjuiciamiento Criminal*, reserva a técnica para a investigação de delitos cometidos por intermédio de organização criminosas, de terrorismo, praticados contra menores ou pessoas com capacidade modificada judicialmente, contra a Constituição, de traição ou relativos à defesa nacional, bem como delitos cometidos através de instrumentos informáticos ou de qualquer outra tecnologia de informação, telecomunicação ou serviço de comunicação.

[337] *Idem*, p. 167-168.

e a subsequente afronta a direitos e garantias fundamentais, tendo em vista que o referido meio oculto atípico de produção de provas, inoculado de maneira sub-reptícia e com potencial excessivamente invasivo, permitiria o acesso indiscriminado a uma profusão de dados pertencentes ao titular e representativos de sua intimidade e privacidade[338].

Em outras palavras, o avanço sobre direitos e garantias individuais é hiperbólico mediante a infiltração por intermédio de *malware,* diante da possibilidade de se colacionar uma maior variedade de dados do que a simples busca e apreensão pelas vias tradicionais de apreensão do aparelho, à medida que o auxílio destes recursos permite que obstáculos de privacidade naturalmente impostos sejam facilmente violados.

Assim, as chaves de criptografia que guarnecem alguns dados, em uma diligência comum, poderiam ser fornecidas pelo acusado ou demandariam a utilização de tecnologias aplicadas para sua decodificação. Em se tratando de um acesso remoto por *malware*, as mesmas senhas e chaves seriam obtidas de maneira facilitada, sem o conhecimento e a concordância do acusado, o que se revela ainda mais afrontoso às suas garantias constitucionais de privacidade e ampla defesa.

Não bastasse, a invasão a um sistema informático permitiria que o agente realizasse a inclusão, modificação ou supressão de arquivos, dificultando-se a realização do contraditório judicial sobre as informações angariadas e, por conseguinte, comprometeria a prova a ser produzida. Nesta senda, a utilização de meios de investigação por *malware* demandaria uma regulamentação quanto ao procedimento a ser seguido para se acautelar a admissibilidade da prova, sob pena de se comprometer a integridade e confiabilidade do material arrecadado[339].

---

[338] Em verdade, a utilização de um *malware* para a realização de uma busca e apreensão não pode se equiparar, em espectro de possível violação à intimidade e privacidade, a uma diligência da mesma natureza, mas de forma física. *Ad exemplum*, a busca e apreensão do suporte físico que armazena os dados (smartphone) é uma diligência visível, materialmente concreta e de conhecimento do acusado – ainda que operacionalizada mediante necessária surpresa –, tendo ele a possibilidade de, por si ou por um defensor, acompanhar os atos perpetrados e afiançar a correção do trabalho investigativo . Já a busca e apreensão remotas, diante da realização da diligência de maneira secreta, sem qualquer conhecimento por parte do acusado, representa um maior grau de violação e exposição à sua privacidade e ao sigilo de seus dados, o que constituiria natural afronta a seus direitos e garantias individuais.

[339] MENDES, Carlos Hélder Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software.* Op. cit. p. 165-166. Na Alemanha, como destaca Gustavo Torres Soares, a jurisprudência tem sinalizado a necessidade de haver regulamentação legislativa suficiente para as medidas investigativas inovadoras, tais como a imposição de limites à utilização de "programas espiões", que demandariam a prévia autorização judicial e sua admissão estaria condicionada aos casos de concreta ameaça à vida humana, a

Outrossim, reconhece-se que a técnica investigativa realizada de forma secreta e mediante utilização meios maliciosos – que avançariam sobre o sistema informático de um *gadget* por intermédio da aceitação inconsciente do próprio acusado, ao executar um arquivo ou conteúdo infectado –, em razão de seu elevado potencial de atentar contra a privacidade do acusado, deveria ser reservada para situações excepcionais.

Portanto, como anteriormente mencionado, não se trata de uma simples inadmissão absoluta de meios de produção de provas atípicos, mas sim a impossibilidade de sua utilização quando se verificar que direitos e garantias fundamentais são violados, notadamente o da privacidade e do sigilo de dados, aliado à insegurança da técnica relacionada à confiabilidade e integridade da prova.

GILMAR MENDES e JURANDI BORGES PINHEIRO, em análise sobre a infiltração clandestina em computadores pessoais, sob a perspectiva da confidencialidade e da integridade dos sistemas informacionais no direito alemão[340], pontificam que:

> inexiste, no direito brasileiro, lei específica sobre infiltração clandestina em sistemas de tecnologia da informação para fins de investigações

estabilidade estatal ou outro interesse igualmente relevante (BVerfGE 27/02/2008, 1BvR370/07, 1BvR 595/07 (SOARES, Gustavo Torres. *Investigação criminal e inovações técnicas e tecnológicas: perspectivas e limites*, Op. cit. p. 202).

[340] Em 27 de fevereiro de 2008, o Tribunal Federal Constitucional alemão reconheceu que a técnica do *hacking* vai além de preocupações concernentes ao sigilo das comunicações e da privacidade, fazendo parte de um direito fundamental à confiabilidade e integridade do *sistema de tecnologia da informação*, que conteria dados técnicos que tornariam possíveis avançados conhecimentos sobre a vida do indivíduo e de sua personalidade. Nesta linha, seria excepcional a admissão da *"busca online"* (*Online-Durchsuchung*), como forma de prevenir práticas criminosas, mediante prévia autorização judicial (Disponível em https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html. Acesso em: 20 de dezembro de 2020). Sobre o tema, recomenda-se: MENKE, Fabiano. *A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão.* Revista Jurídica Luso-Brasileira, Ano 5, (2019), n.º 1, p. 781-809.
De igual sorte, em 20 de abril de 2016, o Tribunal Federal Constitucional alemão reconheceu que as infiltrações clandestinas seriam medidas excepcionais e somente se legitimariam para investigação de crimes graves contra a vida ou a liberdade das pessoas, sacramentando que "(...) powers that constitute a serious interference with privacy must be limited to the protection or legal reinforcement of sufficiently weighty legal interests; require that a threat to these interests is sufficiently specifically foreseeable; may, only under limited conditions, also extend to third parties from whom the threat does not emanate and who belong to the target person's sphere; require, for the most part, particular rules for the protection of the core area of private life as well as the protection of persons subject to professional confidentiality; are subject to requirements of transparency, individual legal protection, and supervisory control; and must be supplemented by deletion requirements with regard to the recorded data (…)" (Disponível em https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2016/04/rs20160420_1bvr096609en.html. Acesso em: 20 de dezembro de 2020).

> criminais. Não há, em nosso ordenamento jurídico, nenhuma disposição legal que autorize, de forma inequívoca, a utilização de 'software' espiões para o monitoramento 'on-line' de atividades cibernéticas. Diante dessa lacuna, cabe indagar sobre a possibilidade de aplicação, por analogia, dos procedimentos estabelecidos na Lei n. 9.296/96 para interceptações telefônicas e telemáticas. Embora a Lei n. 9.296/96 indique os procedimentos a serem observados nas interceptações por ela disciplinadas, há que se ponderar que, em razão da diversidade de tecnologias que podem ser empregadas nesse tipo de espionagem, a suscitarem dúvidas, por exemplo, acerca do alcance e da duração das infiltrações, da forma de registro dos dados capturados, entre outras cautelas, não há como sustentar, com razoável segurança, que as disposições da referida lei possam servir de parâmetro, sem o risco de abusos. Em face, portanto, da inexistência de lei específica sobre a matéria e da manifesta insuficiência das disposições da Lei n.º 9.296/96, a infiltração clandestina em computadores pessoais mostra-se de difícil conformação com a garantia constitucional do direito à privacidade. Tendo em conta o elevado grau de ingerência de medida dessa natureza na intimidade e na vida privada, com o consequente incremento dos riscos de abuso, afigura-se indispensável a sua disciplina em lei, com clara indicação dos requisitos, procedimentos e cautelas a serem observados em seu deferimento (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. Volume 1. São Paulo: Editora Saraiva, 2015, p. 237-40).[341]

No âmbito das recentes reformas legislativas, cogitou-se que a Lei n.º 12.850/2013, a partir da reforma trazida pela Lei n.º 13.964/2019, teria conferido legitimidade ao precitado meio de acesso remoto a dados armazenados em aparelhos celulares, ao admitir a infiltração de agentes policiais virtuais (artigo 10-A) nas hipóteses do artigo 10º da precitada lei, para investigar os crimes praticados por organizações criminosas e a eles conexos, desde que demonstrada a necessidade da medida e indicados o alcance das tarefas dos policiais, os nomes das pessoas investigadas e os dados de conexão ou cadastrais.

[341] No mesmo sentido: KIST, Dario José. *Prova digital no processo penal.* Op. cit. p. 278-279.

A previsão contida na lei de organizações criminosas é bastante semelhante àquela trazida nos artigos 190-A a 190-E da Lei n.º 8.069/1990, alterada pela Lei n.º 13.441/2007, que também regulamenta a possibilidade de infiltração virtual para investigação de uma gama de crimes praticados contra a dignidade sexual de criança e de adolescente[342].

Entretanto, há dúvidas se a autorização conferida para a infiltração policial de forma virtual, nas hipóteses previstas nos diplomas legais indicados, justificaria a utilização de *softwares* espiões ou outros recursos clandestinos e maliciosos ou, em verdade, estaria limitado à participação infiltrada do agente em fóruns de *internet*, redes sociais, grupos privados de comunicação. Nestas hipóteses, o ingresso do policial se daria de forma legítima, ao ser voluntariamente incluído pelos integrantes destes grupos justamente por estar com sua real identidade disfarçada, ocultando-se sua deliberada intenção investigativa.

Eventuais controvérsias que pairavam sobre o tema parecem ter sido dirimidas a partir da análise do Projeto Anticrime[343], que redundou na aprovação da Lei n.º 13.964/2019.

Com efeito, constava do projeto original um dispositivo legal, a ser acrescido à Lei n.º 9.296/1996 (Lei de Interceptação Telefônica): "Art. 9º-A. A interceptação de comunicações em sistemas de informática e telemática poderá ocorrer por qualquer meio tecnológico disponível desde que assegurada a integridade da diligência e poderá incluir a apreensão do conteúdo de mensagens e arquivos eletrônicos já armazenado em caixas postais eletrônicas".

O texto contido no projeto, ao prever expressamente a interceptação de comunicações informáticas e telemáticas por "qualquer meio tecnológico disponível desde que assegurada a integridade da diligência", permitiria, em tese, o uso de *malware* e outros artifícios clandestinos para se perpetrar a interceptação de sistemas informáticos e

---

[342] ANTONIALLI, Dennys M.; ABREU, Jacqueline de Souza. *E quando o policial vira hacker?*. Disponível em: <https://www.internetlab.org.br/pt/privacidade-e-vigilancia/e-quando-o-policial-vira-hacker/:. Acesso em: 20 de dezembro de 2020.

[343] Disponível em: <https://www.justica.gov.br/news/collective-nitf-content-1549284631.06/projeto-de-lei-anticrime.pdf>. Acesso em: 20 de dezembro de 2020.

telemáticos[344]. Todavia, o dispositivo previsto não foi aprovado, afastando-se a normativa autorizativa destes novos meios de obtenção de provas digitais.

Ademais, especialmente no tocante à confiabilidade e integridade das provas a serem produzidas – um dos óbices à admissão das provas produzidas a partir do recurso técnico malicioso –, importa registrar que o Superior Tribunal de Justiça (STJ), ao apreciar a possibilidade da utilização da interceptação de conversas do aplicativo de comunicação *WhatsApp*, refutou a possibilidade da adoção da técnica do "espelhamento"[345] do aparelho investigado, acarretando a produção de um meio híbrido e anômalo de obtenção de prova[346].

---

[344] A previsão legal contida no projeto é bastante semelhante àquela prevista no artigo 19, 2, da Lei n.º 109/2009 da legislação portuguesa, que legitimaria a utilização de *malware* e outros recursos para as *acções encobertas.*

[345] O "espelhamento" das mensagens do *Whatsapp* e viabilizado através de um *site* oferecido pela própria empresa (https://web.whatsapp.com/) em que, por intermédio de uma espécie de código de barras gerado (denominado "*Quick Response" – "QR"*), que é compatível única e exclusivamente pelo celular do usuário que se deseja valer desta funcionalidade. A partir de então, há um instantâneo emparelhamento entre o aparelho celular e o computador, de modo que a funcionalidade é mantida ativa até que, no aparelho celular ou no computador, o usuário marque um campo específico para finalizar o emparelhamento realizado. Nesta funcionalidade, o usuário tem a possibilidade de se utilizar do *Whatsapp* vinculado à sua conta através do computador onde o emparelhamento foi realizado, gozando de todas as funcionalidades destacadas pelo referido aplicativo, enviando e recebendo arquivos, mídias e outros dados correlatos de forma instantânea e simultânea no aparelho celular e no computador. Portanto, toda e qualquer comunicação mantida através do computador ou do celular é "espelhada" no recurso digital correspondente, ainda que não utilizado no momento. Para mais informações sobre o procedimento a ser realizado para o emparelhamento, confira-se: https://faq.whatsapp.com/pt_br/web/28080003 (Acesso em: 20 de dezembro de 2020).

[346] No caso submetido à apreciação do Superior Tribunal de Justiça (STJ), durante uma investigação sobre os crimes de tráfico ilícito de entorpecentes e associação para o tráfico, policiais obtiveram autorização judicial franqueando a apreensão e o acesso aos dados armazenados no aplicativo Whatsapp, além do monitoramento e captura de arquivos (mensagens e consequente gravação de telas de conversas e áudios), pelo prazo de 60 (sessenta) dias. Em posse da ordem judicial autorizativa, policiais promoveram o "espelhamento" do *Whatsapp* do aparelho celular investigado e o devolveram ao seu proprietário, passando a monitorar, instantaneamente, todas as mensagens e contatos entabulados pelo investigado e, inclusive, as comunicações pretéritas já realizadas, sem qualquer limitação no tocante ao destinatário e ao período de tempo correspondente. A partir dos dados obtidos, foi decretada a prisão do investigado por envolvimento com os crimes de tráfico ilícito de entorpecentes e associação para o tráfico. A conduta de "espelhamento" do aplicativo *Whatsapp* foi questionada perante o Tribunal de Justiça de Santa Catarina (TJSC), que indeferiu a pretensão do recorrente, aventando a aplicação analógica da Lei n.º 9.296/1996, por entender que a conduta dos policiais consistiu, propriamente, em uma hipótese de interceptação telemática prevista no artigo 1º, parágrafo único, da Lei de Interceptação Telefônica. Posteriormente, o assunto foi submetido à apreciação do Superior Tribunal de Justiça (STJ), no bojo do Recurso em Habeas Corpus n.º 99.735/SC , em que se reconheceu a nulidade do procedimento realizado pela polícia, apontando a impossibilidade de, analogicamente, estender-se a disciplina da Lei n.º 9.296/1996 à hipótese versada. Para tanto, sustentou-se que a analogia exigiria a demonstração de similitude jurídica e operacional para os dois sistemas de obtenção de prova, o que não se demonstrou por três razões. Em primeiro lugar, apontou-se que a Lei de Interceptação Telefônica permite que uma terceira pessoa, alheia às pessoas dos interlocutores, acompanhe o diálogo mantido, mas na condição de "mero observador". Assim, o agente policial que monitora a interceptação realizada não tem o condão de interferir, positiva ou negativamente, na conversa sustentada. Na operacionalização do *Whatsapp Web*, o investigador poderia participar ativamente do diálogo mantido, interagindo com os contatos do investigado, enviando e até mesmo excluindo mensagens pretéritas, presentes e futuras, sem deixar qualquer vestígio de prova (diante da "criptografia de ponta a ponta", que impossibilita a armazenagem das mensagens em qualquer servidor da empresa responsável pelo aplicativo). A segunda razão invocada foi, justamente, o fato de que a interceptação

Ainda que o recurso do "espelhamento" não configure, de *per si*, uma invasão por técnica de *malware,* forçoso reconhecer a similitude entre os institutos, já que em ambos o acusado é alvo de um procedimento invasivo, operacionalizado de forma sub-reptícia, com grande projeção de acesso a diversos dados anteriores e futuros, sem um marco temporal mínimo e tampouco confiabilidade técnica que possa assegurar a integridade dos dados extraídos.

Diante de todos estes aspectos já lançados e, muito embora se reconheça a infiltração por *malware* como relevante iniciativa técnica investigativa - sendo inclusive albergada por expressa disposição legal ou interpretação jurisprudencial por ordenamentos jurídicos estrangeiros -, vê-se com dificuldade sua admissão no contexto constitucional e processual pátrios, sem uma legislação prévia que confira limites objetivos à utilização do meio de busca em questão, bem como a adoção de técnicas que não coloquem em risco o sistema invadido e evitem danos colaterais desnecessários, além de mecanismos para se atestar a confiabilidade e integridade da prova produzida[347].

4.2.3.2. Ações encobertas em meio digital

A terceira forma de acesso a dados armazenados em aparelhos celulares se dá por intermédio de ações encobertas, em meio digital, para a investigação de determinados crimes.

Em verdade, trata-se de uma forma bastante restrita de acesso aos dados armazenados em um aparelho celular, já que se circunscreve às hipóteses de afluência

telefônica autoriza o monitoramento de conversas mantidas pelo investigado a partir da ordem judicial autorizativa, sempre com efeitos prospectivos (ex nunc). Já o *Whatsapp Web* permite que o policial tenha acesso tanto às mensagens futuras quanto àquelas anteriores à ordem judicial concessiva, operando-se com efeito retroativo (*ex tunc*) e sem qualquer limitação temporal das mensagens trocadas. Finalmente, o terceiro motivo que afastou a aplicabilidade da Lei n.º 9.296/1996 foi a de que a interceptação telefônica é operacionalizada sem a necessidade da apreensão física do aparelho, o que não ocorre no *Whatsapp Web*, em que a posse efetiva do aparelho e a leitura do código "QR" na tela é imprescindível. Outrossim, a utilização da tecnologia do *Whatsapp Web* não permitiria se assegurar, com higidez, a rastreabilidade da prova produzida, o que comprometeria sua "cadeia de custódia", impossibilitando-se o exercício do contraditório defensivo, a quem deve se assegurar a possibilidade de fiscalizar e conferir a integridade, confiabilidade e originalidade dos elementos trazidos aos autos (STJ, RHC n.º 99.735/SC, 6ª Turma, Rel. Min. Laurita Vaz, julgado em 27 de novembro de 2018, DJe 12/12/2018).

[347] VAZ, Denise Provazi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório.* Op. cit. p. 100; MOURA, Maria Thereza Rocha de Assis; BARBOSA, Daniel Marchionatti. *Dados digitais: interceptação, busca e apreensão e requisição.* Op. cit., p. 484-485.

ao conteúdo de comunicações privadas estabelecidas em aplicativos que operam em rede *peer to peer*, o que gera a impossibilidade técnica do fornecimento do conteúdo das comunicações privadas por intermédio de seus respectivos servidores.

A infiltração de agentes policiais é um meio bastante conhecido de investigação de provas em determinados delitos[348]. Consiste, resumidamente, na atuação policial disfarçada, mediante prévia autorização judicial e para investigação de crimes específicos, permitindo que o agente se insira em um grupo criminoso e, fazendo-se passar por um dos integrantes, ganhe a confiança destes para ter acesso a relevantes elementos de prova que dificilmente seriam obtidos por intermédio de outras técnicas investigativas[349].

A figura do agente infiltrado também é bastante utilizada em ordenamentos jurídicos estrangeiros, à exemplo da legislação portuguesa (Lei n.º 101/2001), espanhola (*artículo* 282-bis da *Ley de Enjuiciamiento Criminal*), francesa (*article 706-32* e *706-81* a *706-87* do *Code de Procédure Pénale*) e suíça (*article 286 a 298* do *Code de procédure pénale suisse*).

Entretanto, ainda que a modalidade de infiltração de agentes seja uma técnica utilizada há muito no cenário nacional, é certo que a forma de infiltração virtual, em ambiente digital, é objeto de previsão normativa deveras recente, sendo prevista nos artigos 190-A a 190-E da Lei n.º 8.069/1990, a partir da edição da Lei n.º 13.441/2017, bem como no artigo 10-A da Lei n.º 12.850/2013, com a reforma implementada pela Lei n.º 13.964/2019.

---

[348] A referida técnica investigativa está prevista no artigo 53, inciso I, da Lei de Drogas (Lei n.º 11.343/2006), no artigo 1º, § 6º, da Lei de Lavagem de Capitais (Lei n.º 9.613/1998), no artigo 3º, inciso VII, da Lei de Organizações Criminosas (Lei n.º 12.850/2013);

[349] Em razão da proposta metodológica adotada no presente trabalho, não se realizará um estudo abrangente quanto à infiltração de agentes, seus requisitos legais e procedimentais. Para um conhecimento sobre o tema, recomenda-se: SARAIVA, Wellington Cabral. *Obtenção de prova decorrente de agente infiltrado.* In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro de (Org.). A prova no enfrentamento à macrocriminalidade. Op. cit. p. 385-407; LIMA, Renato Brasileiro. *Manual de Processo Penal.* Op. cit. p. 915-927; MOREIRA, Rômulo de Andrade. *A nova lei que permite a infiltração de agentes na investigação criminal.* In: SIDI, Ricardo, LOPES, Anderson Bezerra (orgs.) *Temas atuais da investigação preliminar no processo penal*. Belo Horizonte: Editora D' Plácido, 2017, p. 491-496.

5. FORMAS DE ACESSO AOS DADOS ARMAZENADOS EM APARELHOS CELULARES: A AUSÊNCIA DE VOLUNTARIEDADE E A ADOÇÃO DE MEDIDAS INVASIVAS MEDIANTE APREENSÃO FÍSICA DO APARELHO CELULAR

Estabelecidas as formas de acesso remoto aos dados armazenados em aparelhos celulares, caminha-se para o estudo de outra via de acesso, mais usual e rudimentar[350], que se dá mediante a apreensão física do suporte eletrônico que contenha os dados, com a subsequente análise do seu conteúdo.

Tal como já mencionado no capítulo precedente, vasculhar o conteúdo de um aparelho constitui uma medida deveras invasiva, já que a imensa quantidade e variedade de dados contidas pode ser mais representativo da personalidade e intimidade do seu titular do que, propriamente, alguns objetos físicos encontrados em uma eventual busca e apreensão domiciliar[351].

O acesso ao conteúdo dos dados armazenados no suporte eletrônico de particulares desperta relevantes discussões atinentes ao marco legal que o ampara e a forma processual a ser observada para o precitado acesso e apreensão dos dados.

A Convenção de Budapeste, verdadeiro marco legal regulatório das provas digitais, estabeleceu em seu artigo 19 a necessidade de os Estados adotarem medidas para se permitir a efetiva busca, apreensão e coleta de dados digitais, bem como dispôs sobre a preservação da integridade deste conteúdo, embora o dispositivo legal não tenha optado por distinguir a busca e a apreensão realizadas de forma remota daquela feita de forma clássica, com a apreensão do suporte físico que armazena os dados.

---

[350] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de Direito Constitucional*. 13ª Edição, São Paulo: Ed. Saraiva, 2018, p. 609.

[351] GUARDIA menciona que "(...) a retenção de um aparelho eletrônico, para fins de investigação ocorre excepcionalmente para o acesso de dados armazenados. Poucas providências investigativas afiguram-se tão gravosas quanto a apreensão, que repercutirá no interesse de preservação da intimidade e vida privada (e por vezes em outros direitos como a inviolabilidade do domicílio), além de comprometer processos comunicativos e dificultar o exercício de atividades profissionais (...)" (GUARDIA, Gregório Edoardo Raphael Selingardi. *A intervenção nas comunicações eletrônicas e o acesso a dados digitais armazenados em suporte eletrônico como meios de investigação no processo penal.* Revista Fórum de Ciências Criminais. Imprenta: Belo Horizonte, Fórum, 2014, v. 3, n. 5, jan.-jun., 2016, p. 76)

As provas digitais gozam de características próprias, que devem ser consideradas no momento de sua valoração. Entretanto, o desafio não está relacionado apenas à tecnologia materialmente utilizada para extração dos elementos digitais e sua integração ao processo, mas também à imprescindibilidade de se revisitar e aprimorar o aparato legislativo para se lidar com essas novas formatações de provas digitais.

Em verdade, ferramentas legislativas disponíveis para acesso aos dados podem não ser mais eficazes a depender da nova tecnologia trazida ao mercado. Daí decorre a necessidade de a legislação estar e permanecer amplamente atualizada para inovadores meios tecnológicos.

Como já mencionado, não há propriamente um marco legal regulamentar que estabeleça requisitos mínimos para que este acesso seja realizado. Esta insuficiência legislativa, na atual quadra investigativa de inovações tecnológicas e comunicação por vias digitais, suscitou discussões atinentes à aplicabilidade de regulações – muitas vezes igualmente insuficientes –, inerentes a outros institutos.

Urge, pois, a criação de um modelo de regulação que possa prever um mínimo de requisitos que legitimariam este acesso, tais como os crimes passíveis da grave medida perpetrada, a imprescindibilidade da autorização judicial, o período e a janela de investigação, a forma de registro dos dados, dentre outros elementos cruciais à utilização do referido meio de obtenção de prova.

5.1 A apreensão do aparelho celular mediante busca e apreensão

A busca e apreensão destes dados armazenados, mediante acesso ao suporte eletrônico que os contém (*v.g.*, aparelhos celulares e *smartphones*), tem sido regulada pelo regime jurídico aplicável à busca e apreensão "tradicional", prevista nos artigos 240 a 250 do Código de Processo Penal[352].

Entretanto, inegável que referido meio de busca de provas, cuja regulamentação se deu a partir da realidade social de 1940, não é capaz de atender a todas

[352] O objeto do presente trabalho científico dispensa um estudo aprofundado do instituto da busca e apreensão, de modo que apenas alguns apontamentos, essenciais para o tema, serão objeto de análise ao longo da pesquisa.

as especificidades atinentes ao avanço tecnológico e à nova formatação de fontes de provas de cunho digital[353]. Em verdade, a busca e apreensão foi moldada sob a ideia de que os bens, objetos e elementos de convicção seriam tangíveis e efetivamente materiais, não estando plenamente adaptado à realidade virtual de dados.

Conforme será visto adiante, embora a busca e a apreensão sejam operacionalizadas com a efetiva arrecadação de um suporte eletrônico – o *smartphone* –, é certo que o objeto de interesse para a investigação são os dados digitais que dele fazem parte[354].

5.1.1. A busca e apreensão de dados digitais

O estudo dos dispositivos processuais relativos à busca e apreensão retratam a projeção social encontrada no momento da edição da norma, especialmente em

---

[353] GUARDIA, Gregório Edoardo Raphael Selingardi. *A intervenção nas comunicações eletrônicas e o acesso a dados digitais armazenados em suporte eletrônico como meios de investigação no processo penal.* Op. cit. p. 77. Tércio Sampaio Ferraz Júnior, refletindo sobre a aplicabilidade de institutos jurídicos tradicionais ao novo cenário digital da busca e apreensão de dados, reconhece que "(...) nessa situação, desse mundo telemático, em que eu não tenho doutrina, e estou jogando tudo para o juiz, a posição dos juízes é terrivelmente complicada, eu diria que é de uma brutal angústia: você continua lidando com doutrinas antigas no mundo físico e lidando com situações como se elas pudessem ser resolvidas desse modo. Eu tenho a impressão que isso é de fato apenas uma fachada, muita coisa se perde nessa relação (...)" (FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados, o direito à privacidade e os limites do poder do Estado: 25 anos depois.* In: ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (eds.). *Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate*. Vol. I. São Paulo. Internet Lab, 2018, p. 41).

[354] Nesta linha as reflexões de Danilo Knijnik, para quem "(...) a associação direta da busca com elementos tangíveis condicionou pesadamente a teoria e a prática jurídicas e o modo de pensar a prova. Contudo, a penetração do mundo virtual como nova realidade, embora despida de seu conteúdo tangível, acabaria demonstrando que tais elementos vinculados à propriedade ou à posse de coisas longe estão de abarcar todo o âmbito de incidência de buscas e apreensões, que, de ordinário, exigiriam mandado judicial. Chega-se, então, ao ponto de perguntar o que são "coisas" ou "qualquer elemento de convicção" hoje. Nesse sentido, tome-se o exemplo de um smartphone: ali, estão e-mails, mensagens, informações sobre usos e costumes do usuário, locais em que se encontrara, viagens e países visitados, números discados e recebidos, compras, operações financeiras, enfim, um conjunto extenso e exaustivo de informações que extrapolam em muito o conceito de coisa, a que bem se amolda um telefone. Claro, o smartphone é uma coisa. Mas essa coisa contém inúmeras outras bases informacionais que não são coisas. Supondo-se, então, que a polícia encontre incidentalmente a uma busca um smartphone, poderá apreendê-lo e acessá-lo sem ordem judicial para tanto? Suponha-se, de outra parte, que se pretenda utilizar um sistema capaz de captar emanações de calor de uma residência, para, assim, levantar indícios suficientes à obtenção de um mandado de busca e apreensão a fim de conhecer o que ali dentro ocorre: estar-se-á a restringir algum direito fundamental do interessado, a demandar a obtenção de um mandado expedido por magistrado imparcial e equidistante, sob pena de inutilizabilidade? O e-mail incidentalmente alcançado por via da apreensão de um smartphone é uma "carta aberta"? Ou está fechada, exigindo providências adicionais? Enfim, o conceito de coisa, enquanto res tangível e sujeita a uma relação de pertencimento, ainda representa um referencial constitucionalmente exaustivo à tutela dos direitos fundamentais ou, caso contrário, há de ser substituído por outro paradigma? (...)" (KNIJNIK, Danilo. *A trilogia Olmstead-Katz-Kyllo: o art. 5º da Constituição Federal do século XXI.* Revista Escola da Magistratura do TRF da 4ª Região, ano 2, número 4. Porto Alegre/RS, 2016, p. 84).

um panorama social definido por modestos recursos tecnológicos e de comunicação eletrônica quase inexistente.

Ainda que as disposições contidas no Código de Processo Penal não tenham acompanhado a evolução tecnológica, é inegável que sua base regulamentar pode se amoldar, no que couber, à busca e apreensão de provas digitais[355], com a ressalva de que o procedimento é operado em duas etapas, conforme bem esmiuçado na lição de OLIN KERR:

> in physical searches, the investigators seek permission to look through a particular physical space for a particular piece of evidence, and then to take that evidence away. Executing a warrant for digital evidence generally adds a step. The investigator seeks permission to search a physical space for computer storage devices, and then takes away the computer storage devices that are found for analysis off-site at a later date. Weeks or even months later, the computer forensic analyst performs what is, in a sense, a second search: an electronic search for digital evidence, occurring long after the physical search for physical evidence. The dynamic is physical search, physical seizure, and then electronic search (KERR, Orin S., *Search Warrants in an Era of Digital Evidence*. 75 Mississippi Law Journal 85 (2005), p. 91)[356].

A busca e a apreensão é tratada de maneira conjunta pelo Código de Processo Penal, no Capítulo XI de seu Título VII do Livro I, nos artigos 240 a 250 do Código de Processo Penal e, também, nos artigos 200 a 204 da Lei n.º 9.279/1996, com relação aos delitos contra a propriedade imaterial[357].

---

[355] Orin Kerr, ao tratar da busca e apreensão de dados digitais, chega à mesma conclusão sob a ótica do ordenamento jurídico norte-americano, reconhecendo que "(...) the bridge from a physical conception of the Fourth Amendment to a virtual conception of the Fourth Amendment can, at least in some cases, be reasonably straightforward to cross. It is possible to translate the familiar principles of the Fourth Amendment from the physical world and to apply them to computers and computer data in a way that restores the function of the old doctrine in the new environment. The way forward may not be obvious. Indeed, in this instance I started out with the wrong approach. But at least in some cases, the basic principles of the Fourth Amendment can be readily translated from the old to the new (…)*"* (KERR, Orin S., *Fourth Amendment Seizures of Computer Data*. 119 Yale Law Journal 700 (2010), p. 724).; GOODISON, Sean E., DAVIS, Robert C., JACKSON, Brian A. *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*. Santa Monica, CA: RAND Corporation, 2015, Disponível em <https://www.rand.org/pubs/research_reports/RR890.html>. Acesso em 20 de dezembro de 2020 p. 9.

[356] KERR, Orin S., *Search Warrants in an Era of Digital Evidence*. 75 Mississippi Law Journal 85 (2005), p. 91.

[357] Para uma análise comparativa entre a busca e apreensão nos regimes jurídicos da Argentina, Inglaterra e Itália, confira-se: CESCA, Brenno Gimenes; GUARDIA, Gregório Edoardo Raphael Selingardi. *Busca e*

Embora sejam referidas como um conceito jurídico único, em razão de ostentarem uma relação próxima e consequencial, impende destacar que é possível individualizá-los, enquanto institutos autônomos e independentes[358].

A busca, na acepção jurídica prevista pela legislação processual penal, consiste na "procura" realizada em determinado lugar, com o objetivo de encontrar uma pessoa ou coisa que se procura[359]. Trata-se de procedimento investigativo penal[360] e restritivo de direito individual, consistente na procura de pessoas ou coisas, estando vinculada, via de regra, a uma ordem emanada de uma autoridade judiciária competente, que impõe limites ao espectro de alcance dessa busca, especialmente no tocante ao local a ser verificado e os objetos, elementos e vestígios que devem ser pesquisados.

Por sua vez, a apreensão[361] é o ato subjetivamente complexo[362] de apossamento, remoção ou guarda de uma pessoa ou coisa que se buscava e que foi encontrada, podendo ser coercitiva ou espontânea. Por se tratar de um ato que, geralmente, se segue à busca, a apreensão é o meio pelo qual, de forma coercitiva, se toma a pessoa ou a coisa de quem regularmente a possui ou detém[363].

As particularidades relacionadas à prova digital não trazem dificuldades na fase antecedente da busca, especialmente em seus pressupostos legitimadores. Um exercício de interpretação sob a ótica do atual contexto social e tecnológico permite a releitura do artigo 240, § 1º, do Código de Processo Penal, legitimando-se a busca para, *verbi gratia,* se apreender documentos digitais obtidos por

---

apreensão: o regime jurídico de Argentina, Inglaterra e Itália. Revista Liberdades, Edição n.º 24, julho/dezembro de 2017, p. 53-72.

[358] Para Sérgio Marcos de Moraes Pitombo, o tratamento unitário dos institutos ocorre porque "(...) a apreensão, no mais das vezes, segue a busca. Emerge, daí, o costume de vê-las unidas. Conceitos que se teriam fundido, como se fossem uma e mesma coisa, ou objetivamente, inseparáveis. As buscas, contudo, se distinguem da apreensão, como os meios diferem dos fins (...)" (PITOMBO, Sérgio Marcos de Moraes. *Do sequestro no processo penal brasileiro.* São Paulo: Ed. Bushatsky, 1993, p. 60). Como sintetiza Aury Lopes Júnior, "(...) são institutos diversos, mas que foram tratados de forma unificada. Nem sempre a busca gera a apreensão (pois pode ocorrer que nada seja encontrado) e nem sempre a apreensão decorre da busca (pode haver a entrega voluntária do bem) (...)" (LOPES JR., Aury. *Direito Processual Penal.* Op. cit, p. 555).

[359] BORGES DA ROSA, Inocêncio. *Processo penal brasileiro*, Porto Alegre: Editora Globo, 1942, p. 144.

[360] PITOMBO, Cleunice Valentim Bastos. *Da Busca e da Apreensão no Processo Penal*. Op. cit. p. 96.

[361] Como bem adverte Cleunice Pitombo, poucos autores pretenderam tratar a apreensão como um instituto autônomo, sendo que grande parte da doutrina sequer o conceitua individualmente, ao passo que outros a insere como finalidade da busca (PITOMBO, Cleunice Valentim Bastos. *Da Busca e da Apreensão no Processo Penal*. Op. cit. p. 189, nota de rodapé n.º 11).

[362] PITOMBO, Cleunice Valentim Bastos. *Da Busca e da Apreensão no Processo Penal*. Op. cit. p. 192.

[363] TORNAGHI, Hélio. *Curso de processo penal*. Op. cit., p. 468.

intermédio de meio criminoso (alínea *b*), descobrir dados digitais necessários à prova da infração ou à defesa do réu (alínea *e*), bem como colher qualquer dado digital que venha a ser considerado elemento de convicção (alínea *h*).

Igualmente, com relação aos parâmetros legais para a realização da medida, não há grandes dificuldades. Enquanto medida restritiva de direitos e garantias individuais, sua imposição não deve se lastrear em meras suspeitas, mas deve se amparar em motivos concretos, de fortes indícios da existência dos elementos de convicção que se pretenda encontrar[364].

Assim, a busca somente será autorizada caso esteja devidamente comprovado o *periculum in mora* – decorrente do risco de desaparecimento ou ocultação indevida da pessoa ou coisa que interessem à prova de uma infração penal – e o *fumus commissi delicit* ou *fumus boni iuris,* que consiste nos indícios de autoria e prova da materialidade delitiva do crime a ser investigado, aliado ao juízo de probabilidade sobre o possível encontro, no local ou na pessoa a serem revistados, dos objetos que possam configurar prova de infração penal, bem como na probabilidade de que estes objetos e pessoas procuradas tenham relação com a investigação do fato criminoso[365].

Caberá ao julgador realizar, à luz da proporcionalidade, um juízo de ponderação a partir do conflito de interesses subjacente, notadamente o da eficiência da persecução penal e a tutela aos direitos e garantias fundamentais assegurados constitucionalmente[366].

---

[364] PITOMBO, Cleunice Valentim Bastos. *Da Busca e da Apreensão no Processo Penal*. Op. cit. p. 115.

[365] GOMES FILHO, Antonio Magalhães. *Da busca e apreensão*. In: GOMES FILHO, Antonio Magalhães; TORON, Alberto Zacharias; e BADARÓ, Gustavo Henrique (coords.). *Código de Processo penal comentado*. São Paulo: Editora Thomson Reuters Brasil, 2018, p. 477. Para Aury Lopes Jr., a medida deve ser legitimada pela prova anteriormente colhida e não ser o primeiro instrumento a ser utilizado (LOPES JR., Aury. *Direito Processual Penal.* Op. cit, p. 557).

[366] ANTUNES, Leonardo Leal Peret. *(Re)pensando a busca e apreensão no processo penal.* Op. cit. p. 100. Como bem sintetiza CLEUNICE PITOMBO, "(...) a autoridade judicial, portanto, em nosso sistema processual penal, para autorizar a busca domiciliar deve, de forma inequívoca, demonstrar nos 'fundados motivos', que a restrição ao direito individual aflora inafastável, para a persecução penal; evidenciar o interesse social concreto, prevalecendo sobre o individual; ser proporcional ao fim almejado; estar ajustada, em sua concretude, com a finalidade perseguida. E, mais, patentear sua imprescindibilidade, oportunidade e conveniência (...)" (PITOMBO, Cleunice Valentim Bastos. *Da Busca e da Apreensão no Processo Penal*. Op. cit. p. 116-117)

Conclui-se, pois, que o mesmo juízo de proporcionalidade relacionado à busca e apreensão tradicional deve ser realizado para a quebra de dados digitais, com sua subsequente apreensão.

Uma vez concedida a ordem judicial para a apreensão do *smartphone*, não se afigura necessária a concessão de uma nova autorização específica para o acesso aos dados que ali estão armazenados. Em verdade, o aparelho celular isoladamente considerado é um mero objeto físico que desperta pouca relevância probatória, já que o interesse em sua apreensão decorre da necessidade de se acessar os dados que ali estejam armazenados, os quais efetivamente poderão auxiliar na confirmação ou refutação da hipótese investigatória traçada[367].

A apreensão física do *smartphone* é uma etapa prévia, de mera passagem, para que se possibilite o acesso ao conteúdo dos dados armazenados. Desta feita, a avaliação dos requisitos necessários para a concessão do mandado de busca e apreensão é feita a partir da perspectiva dos dados que poderão ser encontrados, e não do mero suporte que os armazena. São estes dados que representam aspectos significativos da personalidade do indivíduo e que, por óbvio, deverão ser contemporizados diante da necessidade da produção da prova para a investigação.

A menção constante no mandado judicial, por evidente, se limita à apreensão do *smartphone*. Trata-se de uma providência natural diante da impossibilidade de se antever todos os dados de interesse investigativo que poderão ser encontrados no aparelho apreendido. Portanto, na diligência para cumprimento da ordem de busca e apreensão, é

[367] Tércio Sampaio Ferraz Júnior aponta que "(...) no direito penal a gente estava acostumado a falar em busca e apreensão, e busca e apreensão é busca e apreensão de coisas, você busca e apreende coisas. O que é que eu busco e apreendo quando eu lido com essa não-coisa? Eu posso buscar e apreender computadores – isso é uma coisa. Mas não é da coisa que realmente estamos falando; mas sim da busca e apreensão relacionada com dados. Aliás, o que menos importa ali é a coisa; o que importa é o conteúdo que está lá dentro e que eu só chego a ele mediante esse neologismo que nós criamos – tivemos que criar – mediante o verbo acessar, que não é ter acesso no velho sentido. "Acessar" – qualquer criança hoje sabe, eu tenho dificuldade de entender – significa ter a capacidade de movimentar essas constantes na verdade, os tais algoritmos que estão ali, mas que não são nem as coisas que eu vejo e nem aquilo que eu possa imaginar como coisa; são puras constantes que, giradas ou mexidas, fazem com que um livro inteiro surja, um documento, uma petição apareça e que eu possa protestar e dizer que ela não foi conhecida etc. Então, quando eu busco e apreendo esse mundo eu não estou mais lidando com nada referente àquele mundo físico (...)" (FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados, o direito à privacidade e os limites do poder do Estado: 25 anos depois.* Op. cit., p. 29).

humanamente impossível filtrar os dados que, dentro daquela universalidade, sejam relevantes para a atividade investigativa.

Por esta ordem de ideias, a simples autorização judicial para apreensão do aparelho celular constitui, por evidente, uma legítima concessão para a perscrutação dos dados que ali estejam armazenados, uma vez que o aparelho celular desprovido de conteúdo não ostentaria virtualidade de ser utilizado como prova criminal[368].

Sob o aspecto formal, os mandados de busca e apreensão deverão indicar o local preciso da diligência a ser realizada, a pessoa investigada, os motivos e a finalidade da ordem expedida[369], os fatos e delitos investigados e o objeto da busca expedida, conforme artigo 243 do Código de Processo Penal.

Especialmente no tocante às provas digitais, reconhece-se a necessidade de que o mandado de busca e apreensão descreva os suportes eletrônicos que deverão ser apreendidos[370], tais como o *smartphone* do acusado, especificando-se ainda, tanto quanto seja possível, os dados que interessariam à investigação[371], a forma de sua apreensão e extração.

---

[368] STJ, RHC n.º 75.800/PR, 5ª Turma, Rel. Min. Felix Fischer, julgado em 15 de setembro de 2016, DJe 26/09/2016; STJ, HC n.º 428.369/PE, 6ª Turma, Rel. Ministra Laurita Vaz, julgado em 17 de setembro de 2019, DJe 03/10/2019; STJ, HC n.º 372.762/MG, 5ª Turma, Rel. Min. Felix Fischer, julgado em 3 de outubro de 2017, DJe 16/10/2017; STJ, HC n.º 530.282/SE, 6ª Turma, Rel. Min. Antônio Saldanha Pinheiro, julgado em 18 de fevereiro de 2020, DJe 27/02/2020; STJ, AgRg no HC n.º 567.637/RS, 5ª Turma, Rel. Min. Ribeiro Dantas, julgado em 3 de novembro de 2020, DJe 12/11/2020). No mesmo sentido o Parecer n.º 38.333/2019-novembro-JV/MS, da Procuradoria Geral da República, no bojo do Recurso Ordinário em *Habeas Corpus* n.º 177.585/PE, do Supremo Tribunal Federal (STF).

[369] FISCHER, Douglas. OLIVEIRA, Eugênio Pacelli de. C*omentários ao Código de Processo Penal e sua Jurisprudência*. Rio de Janeiro: Editora Lumen Juris. 2010, p. 461; BADARÓ, Gustavo Henrique Righi Ivahy. *Direito processual penal*. Rio de Janeiro: Editora Elsevier, 2008, Tomo I, p. 277.

[370] GUARDIA, Gregório Edoardo Raphael Selingardi. *Comunicações Eletrônicas e dados digitais no processo penal*. Op. cit., p. 201; MENDES, Carlos Hélder Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software.* São Paulo: Ed. Juspodivm, 2020, p. 144. O Supremo Tribunal Federal (STF) já reconheceu a nulidade da busca e apreensão de um aparelho celular que não constava expressamente de um mandado judicial. Na ocasião, o Ministro Gilmar Mendes sustentou que "(...)não há qualquer menção, na decisão judicial que decretou a medida de busca e apreensão, quanto à possibilidade de apreensão de aparelho telefônico (eDOC 3). A determinação consta apenas do mandado de busca e apreensão. Trata-se, portanto, de ordem não fundamentada, em contrariedade ao disposto no art. 93, IX, da Constituição (...)" (STF, Reclamação n.º 33.711/SP, 2ª Turma, Rel. Min. Gilmar Mendes, julgado em 11 de junho de 2019, DJe 22/08/2019).

[371] A especificação das provas a serem obtidas, na medida do possível, visa evitar a utilização do procedimento da *fishing expedition*, que consiste na utilização de meios probatórios legais para a obtenção de toda e qualquer evidência em face de uma pessoa, tenha ou não relação com o caso concreto, desenvolvendo-se, por conseguinte, uma investigação especulativa e demasiadamente ampla (SILVA, Viviane Ghizoni da; MELO E SILVA, Philipe Benoni; MORAIS DA ROSA, Alexandre. *Fishing Expedition e Encontro Fortuito na Busca e Apreensão*. Florianópolis: Editora Emais, 2019, p. 41). Em caso análogo, o Tribunal Europeu de Direitos

Entretanto, a ausência de descrição pormenorizada dos dados digitais contidos no aparelho não deve servir de óbice ao seu cumprimento, haja vista que os *smartphones* guardam uma imensa variedade de dados, sendo impossível ao julgador, em exercício de futurologia, identificar e individualizar todos os dados que tenham relação com os fatos apurados no procedimento investigatório e que autorizaram a medida investigativa em questão[372].

Com relação à apreensão dos dados, algumas particularidades merecem destaque. Tendo em vista que os dados serão acessíveis mediante apreensão física do suporte eletrônico que os contém, é necessário que apenas aqueles que guardem relação com os dados digitais pretendidos sejam objeto da apreensão, evitando-se a colheita indiscriminada de outros dispositivos ou de outros bens e objetos pertencentes a terceiros, quando claramente não guardem relação com o propósito investigativo que motivou a busca e apreensão[373].

Outrossim, na linha do que dispõe o artigo 19.3 da Convenção de Budapeste, a apreensão de dados digitais poderá ser otimizada a partir da realização de cópia[374] dos dados contidos no dispositivo móvel, mediante aparato técnico suficiente e com o auxílio de profissionais capacitados para a medida[375], sempre preservando-se a integridade dos dados e sua cadeia de custódia.

Humanos (TEDH), no julgamento do caso *Robathin vs. Austria*, considerou ser violador do artigo 8º da Convenção Europeia de Direitos Humanos a determinação judicial genérica para busca ilimitada e inespecífica de dados em um escritório de advocacia, sem delimitação daqueles que guardam pertinência com o objeto da investigação (Disponível em <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-5567%22]}>. Acesso em: 20 de dezembro de 2020).

[372] "(...) 3. É inexigível a discriminação, no mandado de busca, de todos os bens a serem apreendidos, uma vez que dele constava a determinação para "apreender coisas achadas ou obtidas por meios criminosos", "descobrir objetos necessários à prova da infração ou à defesa do réu" e "colher qualquer elemento de convicção" (art. 240, § 1º, b, e e h, do Código de Processo Penal). 4. Dada a impossibilidade de indicação, *ex ante*, de todos os bens passíveis de apreensão no local da busca, é mister conferir-se certa discricionariedade, no momento da diligência, à autoridade policial. (...) 6. Recurso não provido." (STF, Petição n.º 5173 AgR, Relator(a): Min. DIAS TOFFOLI, Primeira Turma, julgado em 30/09/2014).

[373] VAZ, Denise Provazi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório.* Op. cit. p. 88.

[374] A cópia de dados informáticos tem sido considerada, via de regra, uma efetiva *search and seizure* para fins da *Fourth Amendment,* o que demanda a demonstração da *probable cause* para implementação da medida (KERR, Orin S., *Fourth Amendment Seizures of Computer Data*. 119 Yale Law Journal 700 (2010). *Op. cit.* p. 714)

[375] MENDES, Carlos Hélder Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software.* São Paulo: Ed. Juspodivm, 2020, p. 145.

Como forma de se preservar a cadeia de custódia do material arrecadado, é imprescindível o registro e a descrição pormenorizada dos suportes eletrônicos apreendidos em auto próprio, com descrição quanto à marca, modelo, ano, numeração de série, lacre e outras informações que possam individualizá-los[376] adequadamente em auto próprio (artigo 245, § 7º, do Código de Processo Penal), haja vista não ser possível descrever, individualmente, cada um dos dados apreendidos com o próprio dispositivo móvel.

5.2. A apreensão do aparelho celular sem prévia busca determinada judicialmente

No tópico precedente, cuidou-se de estabelecer o procedimento para o acesso aos dados armazenados em *smartphone*, mediante busca e subsequente apreensão física do aparelho, a partir de autorização judicial prévia. Assim, vislumbrando-se a necessidade da obtenção dos dados contidos no suporte eletrônico pretendido, a autoridade policial e/ou o membro do Ministério Público pleiteiam ao julgador a concessão de um mandado de busca para que, legitimamente, se possa apreender o aparelho visando o acesso aos dados nele contidos.

Entretanto, reconhecendo-se a apreensão como instituto autônomo e independente da busca, é inegável a possibilidade de se apreender objetos e coisas relacionadas ao fato investigado, independentemente da ordem judicial autorizativa da busca.

Em verdade, durante uma prisão em flagrante delito ou durante o exercício de atividades investigativas policiais (artigo 6º, incisos II e III, do Código de Processo Penal), é possível que o aparelho celular venha a ser apreendido antes mesmo de uma ordem judicial concessiva da medida.

Desta feita, a apreensão decorrente da busca pode ocorrer[377] nas hipóteses de busca domiciliar, precedidas de mandado judicial quando presentes "fundadas razões" que a autorizem, salvo nas exceções contempladas no dispositivo constitucional (artigo 240, § 1º, do Código de Processo Penal e artigo 5º, inciso XII, da Constituição Federal); e também nas de busca pessoal, quando houver "fundada suspeita" de que alguém

[376] PITOMBO, Cleunice Valentim Bastos. *Da Busca e da Apreensão no Processo Penal*. Op. cit. p. 233.
[377] PITOMBO, Cleunice Valentim Bastos. *Da Busca e da Apreensão no Processo Penal*. Op. cit. p. 225.

oculte consigo uma arma proibida ou outros objetos (artigo 240, § 2º, do Código de Processo Penal), salvo nos casos de prisão, quando implementada durante o cumprimento de busca domiciliar ou sempre que houver "fundada suspeita" de que alguém oculte consigo uma arma proibida ou outros objetos que constituam corpo de delito (artigo 244, do Código de Processo Penal)[378].

De igual sorte, poderá ocorrer a apreensão do objeto sempre que venha a ser exibido voluntariamente à autoridade policial ou judiciária[379]. Por fim, a apreensão será legítima também nas hipóteses de encontro fortuito do bem durante o cumprimento de um mandado de busca e apreensão, desde que guarde relação com o fato investigado.

O artigo 6º, incisos II e III, do Código de Processo Penal prevê que a autoridade policial poderá apreender os objetos que tenham relação com o fato, além de colher todas as provas que sirvam ao seu esclarecimento e identificação de suas circunstâncias[380]. Ao mesmo tempo, o artigo 118 do Código de Processo Penal veda a restituição das coisas apreendidas enquanto interessarem ao processo.

A análise dos dispositivos legais indica que a apreensão somente será considerada legítima quando o objeto tenha relação com o fato investigado e seja útil e pertinente para a investigação ou o processo, sob pena do ato de apreensão ser considerado abusivo e extravagante.

Nesta ordem, revela-se legítima a apreensão, sem autorização judicial, de um aparelho celular abandonado em uma cena de crime, assim como também a autoridade

---

[378] BADARÓ, Gustavo Henrique Righi Ivahy. *Processo Penal*. Op. cit., p. 149.

[379] O assunto foi tratado nos tópicos precedentes, dentro das hipóteses de acesso consentido aos dados armazenados em aparelhos celulares, que poderá ocorrer mediante exibição voluntária do aparelho ou, ainda, com o consentimento do titular para a exploração dos dados ali contidos, após uma apreensão desprovida de ordem judicial anterior. Para Cleonice Pitombo, nem toda apresentação sujeita a apreensão do bem, o que somente ocorrerá quando se verificar a licitude na obtenção da coisa exibida, a necessidade de retirá-la do poder de quem a retém e a imprescindibilidade do objeto para a instrução criminal (PITOMBO, Cleunice Valentim Bastos. *Da Busca e da Apreensão no Processo Penal*. Op. cit. p. 227)

[380] Cleunice Pitombo reconhece que "(...) é induvidoso que a polícia judiciária, logo que tiver conhecimento da infração penal, deve preservar o lugar de crime: 'dirigir-se ao local, providenciado para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais'; e, fazendo o levantamento do local da infração, dentre outras atividades: 'apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais' (art. 6.º, I e II, do CPP). Nesta hipótese, ocorrendo flagrante, ou não, a apreensão dispensa autorização judicial. Tal permissão não significa, porém, que se possa apreender toda e qualquer coisa, 'sem qualquer relação com o fato investigado' (...)" (PITOMBO, Cleunice Valentim Bastos. *Da Busca e da Apreensão no Processo Penal*. Op. cit. p. 227).

policial poderá determinar a apreensão de um *smartphone* nos casos de prisão em flagrante delito[381], sempre que houver indicativos de que os dados ali contidos possam colaborar para a atividade investigativa[382].

A pedra de toque reside na discussão quanto à necessidade de autorização judicial para acesso aos dados armazenados nestes aparelhos, bem como sobre a licitude da prova produzida a partir deste acesso. É necessário averiguar se a apreensão do aparelho, nas situações já mencionadas, permite o acesso imediato aos dados ali armazenados, prescindindo-se de uma ordem judicial específica para o acesso a este conteúdo.

Estabelecida a problemática sobre o tema, buscar-se-á analisar, a partir de contextos fáticos distintos, a legalidade do acesso aos dados contidos em aparelhos celulares nas hipóteses de uma simples abordagem policial motivada por fundada suspeita, bem como após a concretização de uma prisão em flagrante delito, com a respectiva apreensão do aparelho.

---

[381] Como já pontuou o Superior Tribunal de Justiça (STJ), "(...) se a lei autoriza a prisão em flagrante, evidentemente que faculta – também – a apreensão de coisas, objeto do crime (...)" (STJ, RHC n.º 7.916/SP, Rel. Ministro Fernando Gonçalves, 6ª Turma, julgado em 15 de outubro de 1998, DJ de 9 de novembro de 1998). Na mesma linha, a mesma Corte já decidiu que "(...) embora seja despicienda ordem judicial para a apreensão dos celulares, pois os réus encontravam-se em situação de flagrância, as mensagens armazenadas no aparelho estão protegidas pelo sigilo telefônico, que deve abranger igualmente a transmissão, recepção ou emissão de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza, por meio de telefonia fixa ou móvel ou, ainda, através de sistemas de informática e telemática. Em verdade, deveria a autoridade policial, após a apreensão do telefone, ter requerido judicialmente a quebra do sigilo dos dados nele armazenados, de modo a proteger tanto o direito individual à intimidade quanto o direito difuso à segurança pública" (...)" (STJ, RHC n.º 67.379/RN, 5ª Turma, Rel. Min. Ribeiro Dantas, julgado em 20 de outubro de 2016, DJe de 9/11/2016)

[382] Marcos Alexandre Coelho Zilli pontua que "(...) a apreensão de smartphones por ocasião dos procedimentos que cercam a prisão em flagrante é possível. Para tanto, há que se configurar situação justificante daquela restrição, como por exemplo, a presença de suspeitas de que outras provas sobre a prática delituosa possam ali ser encontradas (...)" (ZILLI, Marcos Alexandre Coelho. *A prisão em flagrante e o acesso de dados em dispositivos móveis. Nem utopia, nem distopia. Apenas a racionalidade.* In: ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. I. São Paulo. InternetLab, 2018, p. 96).

5.3. Da necessidade de ordem judicial para acesso a dados armazenados em aparelhos celulares

A existência de uma cláusula de reserva de jurisdição para acesso aos dados armazenados em aparelhos celulares apreendidos vem protagonizando os mais recentes debates jurisprudenciais.

A importância da apreensão do aparelho celular e do exame de seu conteúdo ganha relevância diária, especialmente considerando que medidas investigativas de outrora relevante sucesso probatório, como a interceptação telefônica, se tornaram obsoletas diante do advento de novas formas de comunicação, muitas vezes integrada por vários interlocutores em tempo real, operacionalizada pela *internet* e protegida por uma forte criptografia.

5.3.1. Cláusula constitucional de reserva de jurisdição

A existência de uma cláusula legal ou constitucional de reserva de jurisdição demanda, inicialmente, uma análise quanto aos dispositivos que resguardam o sigilo dos dados pessoais armazenados em suportes eletrônicos. Para a proteção de direitos fundamentais caros ao cidadão, o constituinte e o legislador estabeleceram que caberia ao Poder Judiciário, em determinados casos, legitimar previamente as intervenções no espectro de direitos e garantias do cidadão.

Portanto, delegou-se ao Poder Judiciário a análise dos pressupostos necessários para, dentro de um juízo de proporcionalidade estabelecido de forma contextual com as garantias do cidadão na proteção a seus dados e a necessidade de uma efetiva atividade investigativa, decidir sobre a legitimação de se impor, momentânea e circunstancialmente, uma restrição aos direitos e garantias fundamentais do acusado.

Como melhor se verá adiante, a Constituição Federal de 1988 estabeleceu expressamente três hipóteses de reserva de jurisdição para a tutela dos direitos e garantias fundamentais, dispondo ainda sobre as exceções constitucionais à imprescindibilidade da tutela judicial: a inviolabilidade de domicílio (artigo 5º, inciso XI);

o direito ao sigilo das comunicações (artigo 5º, inciso XII); e o direito à liberdade ambulatória do cidadão (artigo 5º, inciso LXI).

5.3.1.1. A tutela da privacidade e intimidade dos dados armazenados: a inexistência de reserva constitucional de jurisdição no artigo 5º, inciso X, da Constituição Federal

O artigo 5º, inciso X, da Constituição Federal dispôs sobre a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, assegurando-se uma reparação em caso de violação. Todavia, ao contrário de outros dispositivos constitucionais, deixou-se de prever a necessidade de prévia autorização judicial para a intervenção nesta gama de direitos[383].

É inegável que os dados armazenados em aparelhos celulares são representativos da personalidade do indivíduo e compõem, à semelhança dos dados bancários, fiscais e telefônicos, a esfera de conteúdo privado e íntimo. Com efeito, basta ver que os dados ali armazenados conseguem exprimir a rotina particular do seu titular, exteriorizada a partir de fotografias, vídeos, dados de geolocalização, documentos escritos, aplicações de *internet* e conversas que gozam de conteúdo inegavelmente íntimo.

Portanto, caso a proteção aos dados armazenados se subsumam apenas e tão somente à proteção constitucional conferida no artigo 5º, inciso X, não há como se reconhecer a existência de uma cláusula de reserva de jurisdição constitucional.

Entretanto, tem-se defendido, doutrinária e jurisprudencialmente, a aplicação do regime jurídico constitucional previsto no artigo 5º, incisos XI e XII da Constituição Federal aos dados armazenados em aparelhos celulares.

[383] Conforme se depreende da redação do dispositivo legal, o constituinte não estabeleceu a expressa necessidade de autorização judicial para se legitimar a tutela de dados relacionados à privacidade e intimidade. Desta feita, em razão da disposição constitucional, tem-se admitido que o afastamento de sigilo bancário, fiscal e telefônico seja perpetrado por outros poderes no exercício de funções atípicas, tais como pelas Comissões Parlamentares de Inquéritos (CPI) do Poder Legislativo. Neste sentido: STF, MS n.º 23.639, Tribunal Pleno, Rel. Ministro Celso de Mello, julgamento em 16 de novembro de 2000, DJe 16/02/2001

Ao assegurar as inviolabilidades de domicílio e das comunicações, o constituinte buscou estabelecer um reforço protetivo[384] à previsão genérica do artigo 5º, inciso X, da Carta Política. Vale dizer, a intenção do constituinte foi a de proteger determinadas formas de projeção da personalidade do cidadão, resguardando-se seu domicílio – enquanto local reservado e íntimo – e o sigilo das comunicações, impedindo-se o indevido acesso às informações privadas que venham a ser compartilhadas.

Nesta ordem, as previsões constitucionais contidas no artigo 5º, incisos XI e XII podem ser consideradas verdadeiras complementações da previsão genérica do inciso X, formando-se uma teia de proteção à privacidade e intimidade do indivíduo[385].

Estabelecidas essas premissas, impende analisar se os dados armazenados estão efetivamente sujeitos, também, aos regramentos constantes no artigo 5º, incisos XI e XII, da Constituição Federal.

5.3.1.2 Os dados armazenados em aparelhos celulares e a proteção ao domicílio: abrangência da tutela contida no artigo 5º, inciso XI, da Constituição Federal

Conforme já visto anteriormente, a Constituição Federal tutela a inviolabilidade da casa do indivíduo (artigo 5º, inciso XI), vedando-se o ingresso sem

---

[384] O artigo 5º, inciso XI, da Constituição Federal não busca tutelar um local físico inanimado, mas sim a projeção da privacidade do indivíduo que o titularize. Para José Afonso da Silva, a proteção constitucional da inviolabilidade do domicílio assegura o "(...) recesso do lar (...)" como "(...) o ambiente que resguarda a privacidade, a intimidade e a vida privada (...)" (SILVA, José Afonso. *Curso de Direito Constitucional Positivo*. Op. cit. p. 441). Também milita na mesma posição Manoel Gonçalves Ferreira Filho, para quem "(...) a inviolabilidade de domicílio visa a proteger a 'intimidade' do homem. Busca-lhe um espaço reservado, proibindo as intromissões dos homens e do próprio Estado. Garante-lhe, pois, a base necessária para o desenvolvimento de sua personalidade (...)" (FERREIRA FILHO, Manoel Gonçalves. *Comentários à Constituição Brasileira de 1988*. São Paulo: Editora Saraiva, 1990, v. 36). Ainda sobre o tema, Márcio Schusterschitz da Silva Araújo, ao discutir sobre a utilização do "lixo" como fonte de prova no processo penal, reconhece que o lixo, enquanto bem abandonado, não serve mais como espaço de isolamento da pessoa ou de controle informacional nas projeções da privacidade, o que torna lícita sua apreensão (ARAÚJO, Márcio Schusterschitz da Silva. *O lixo como fonte de prova no processo penal.* In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro de (Org.). A prova no enfrentamento à macrocriminalidade. Op. cit. p. 409-422).

[385] PITOMBO, Cleunice Valentim Bastos. *Da Busca e da Apreensão no Processo Penal*. São Paulo, Revista dos Tribunais, 1999. p. 77-78 e 81-82; ARAÚJO, Luiz Alberto David; NUNES JÚNIOR, Vidal Serrano. *Curso de Direito Constitucional*. 10ª edição. São Paulo: Editora Saraiva, 2006, p. 156; QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Pedigone. *Tércio Sampaio Ferraz Júnior e sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do estado: o que permanece e o que deve ser reconsiderado*. *Internet* & sociedade. N.1., volume 1, fevereiro de 2020. Disponível em <https://revista.internetlab.org.br/tercio-sampaio-ferraz-junior-e-sigilo-de-dados-o-direito-a-privacidade-e-os-limites-a-funcao-fiscalizadora-do-estado-o-que-permanece-e-o-que-deve-ser-reconsiderado/>. Acesso em 20 de dezembro de 2020).

consentimento do morador, salvo nas hipóteses de flagrante delito, desastre ou socorro ou, ainda, durante o dia, por determinação judicial.

O conceito de "casa" assume uma projeção bastante ampla, expandindo-se seu viés interpretativo para diversos locais, privados ou coletivos, em que seja possível a realização de atividades pertinentes à intimidade e à vida privada do indivíduo[386].

A partir dessa interpretação extensiva do conceito de "domicílio", parte da doutrina tem reconhecido que os aparelhos celulares, embora móveis, podem ser a ele equiparados e, por conseguinte, receberiam a proteção constitucional prevista no artigo 5º, inciso XI, da Constituição Federal.

GUILHERME DEZEM reconhece a necessidade de uma evolução interpretativa no conceito de "domicílio", para se afastar as amarras interpretativas que o limitavam a uma perspectiva de proteção à propriedade e, por conseguinte, a um espaço físico determinado. Para tanto, desenvolve seu raciocínio a partir da adoção de um conceito ontológico de domicílio, enquanto espaço normal da intimidade, aliando-o à pós-modernidade e ao avanço tecnológico que trouxeram um conceito próprio de espiritualização e desmaterialização de determinados bens que, antigamente, somente eram acessíveis fisicamente.

Em reforço a seu argumento, o autor sustenta que o artigo 6º da Lei n.º 12.965/2014 (Lei do Marco Civil da *Internet*) estabeleceu que a interpretação dos dispositivos da lei deveriam ser feitos levando-se em consideração os usos e costumes particulares, bem como a natureza da *internet*, o que, na visão de DEZEM, permitiu que se estendesse a proteção domiciliar à *internet*, que é utilizada como local de exercício da vida íntima e privada, o que nada mais é do que o conceito clássico de "domicílio".

---

[386] AMARAL, Cláudio do Prado. *Inviolabilidade do domicilio e flagrante de crime permanente.* Revista Brasileira de Ciências Criminais, vol. 95, p. 165, São Paulo: Ed. RT, mar. 2012, *Apud* DEZEM, Guilherme Madeira. A espiritualização do domicílio. In: MASSO, Fabiano Del. ABRUSIO, Juliana, FILHO, Marco Aurélio Florêncio (orgs.). Marco Civil da *Internet* – Lei n.º 12.965/2014. São Paulo: Editora Revista dos Tribunais, 2014, 2ª tiragem, p. 70.

Finalmente, a evolução tecnológica permitiu que os aparelhos celulares não mais sejam comparados a uma mera agenda telefônica, especialmente aqueles dotados de computação em nuvem, por conterem mais dados e informações íntimas da vida privada do que a própria residência, não sendo pertinente um tratamento jurídico distinto simplesmente por não ser dotado de espaço físico[387].

Nesta ordem, DEZEM conclui ser fundamental que o conceito de domicílio seja ressignificado, para abarcar também os meios eletrônicos, uma vez que "(...)esses aparelhos contêm inúmeras informações de fórum íntimo, nos permitindo exercer atos da vida privada não mais somente em ambientes físicos fechados e privativos, mas sim em qualquer lugar (...)"[388]

Como consequência jurídica da equiparação dos modernos aparelhos celulares a verdadeiros "domicílios" merecedores da proteção conferida ao domicílio (artigo 5º, inciso XI), extraem-se algumas consequências práticas.

É certo que a inviolabilidade de domicílio contempla algumas exceções constitucionais: o ingresso poderá se dar mediante ordem judicial, durante o dia; ou independentemente de ordem judicial, de dia ou de noite, em situações de desastre, para prestar socorro ou em flagrante delito.

Adotando-se a premissa de que o aparelho celular, por ser equiparado ontologicamente a um "domicílio", deva se subsumir às disposições do artigo 5º, inciso XI, da Constituição Federal, conclui-se pela indispensabilidade de ordem judicial para acesso ao conteúdo dos aparelhos celulares, salvo em situações de flagrante delito[389].

---

[387] DEZEM, Guilherme Madeira. *A espiritualização do domicílio.* In: MASSO, Fabiano Del. ABRUSIO, Juliana, FILHO, Marco Aurélio Florêncio (orgs.). *Marco Civil da Internet – Lei n.º 12.965/2014.* São Paulo: Editora Revista dos Tribunais, 2014, 2ª tiragem, p. 70. No mesmo sentido é a posição de Benjamim Silva Rodrigues, que traz a ideia de "casa digital" aos computadores (SILVA RODRIGUES, Benjamim. *Da prova penal: Tomo II – Bruscamente...a(s) face(s) oculta(s) dos métodos ocultos de investigação criminal.* Lisboa: Editora Rei dos Livros, 2010, p. 473).

[388] Idem. p. 78.

[389] GUILHERME DEZEM sustenta que "(...) o problema está no caso envolvendo busca e apreensão pessoal fora das hipóteses de prisão em flagrante. Nessa situação não é possível que sejam violados os dados contidos no aparelho celular ou em qualquer outro 'gadget' similar. Busca e apreensão pessoal ocorre nas hipóteses previstas no art. 240, § 2.º, do CPP. A busca e apreensão pessoal independe de mandado, bastando que haja fundada suspeita de que o indivíduo carregue consigo os objetos mencionados no art. 240, §1.º, do CPP. Uma vez que atualizamos o conceito de domicílio e reconhecemos sua espiritualização, não é possível que a busca e apreensão recaia nestes objetos sem autorização judicial. O policial pode fazer a busca e apreensão pessoal

Portanto, a equiparação do celular ao domicílio permitiria a incidência da disciplina legal relativa à busca domiciliar (artigo 240, § 1º, do Código de Processo Penal), mas não necessariamente a da busca pessoal, que independerá de mandado judicial nas hipóteses previstas no artigo 244 da Lei Adjetiva Penal.

Desta feita, o acesso a dados em aparelhos celulares dependerá, necessariamente, de ordem judicial fundamentada, salvo nas situações de desastre, para prestar socorro ou em flagrante delito. Assim, *ad exemplum,* em uma abordagem policial realizada sem a constatação de um flagrante delito, não seria legítima a busca e apreensão realizada no aparelho celular. Entretanto, caso na abordagem seja localizada uma arma de fogo ilegalmente portada ou, ainda, uma quantidade de entorpecentes aparentemente destinada ao tráfico, conclui-se pela situação flagrancial e, por conseguinte, legitima-se o acesso aos dados armazenados no aparelho celular, independentemente de prévia autorização judicial.

Entretanto, a interpretação evolucionista da abrangência do conceito de "domicílio", não foi infensa a críticas. MARCOS ZILLI, em esclarecedor artigo sobre o tema, reconhece que o raciocínio é sedutor, mas se move pela tentativa de se buscar soluções racionais ao tema, pecando-se em suas premissas. Aponta o Professor das Arcadas a dificuldade em se desconectar a noção de "casa" da ideia de abrigo e espaço físico de proteção pessoal e dos familiares, de modo que imaginar-se a portabilidade do próprio domicílio constituiria uma "metáfora que soa exagerada". Reconhece, também, que a única proximidade possível entre os conceitos de "domicílio" e o conteúdo de "*smartphones"* residiria nas expectativas de privacidade depositadas pelo morador e o usuário naqueles espaços[390].

---

no indivíduo, no entanto esta busca e apreensão não pode abranger os objetos acima mencionados, ou seja, objetos que atuem com computação em nuvem. Uma vez que o indivíduo carrega hoje consigo seu domicílio, devemos fazer esta distinção: a fundada suspeita autoriza a busca e apreensão pessoal no indivíduo, no entanto não está abarcada nesta busca e apreensão o celular ou qualquer aparelho equivalente que possa arquivos de dados em nuvem (...)" (Ibidem, p. 72)

[390] Zilli destaca que "(...) é difícil desconectar da noção de casa a ideia de abrigo e de espaço físico de proteção pessoal, dos familiares e de entes queridos. É um espaço de projeção de várias relações que se desdobram em diferentes graus de abertura (contatos sociais) e de restrição (privacidade e intimidade). Trata-se de uma construção conceitual secular que se manifesta em diferentes sociedades e civilizações. Não parece razoável o redimensionamento de um conceito com fortes raízes históricas, culturais e sociais, por mais que se apresentem revolucionários os avanços tecnológicos. A moradia é um espaço de abrigo que não pode ser transportado por qualquer pessoa. O morador quando ali ingressa, protegido que é pela liberdade reservada, pode dar vazão à sua intimidade e à sua privacidade. E mesmo nesse espaço, poderá estabelecer subníveis de privacidade com restrições ainda maiores de acesso, como no caso de armários ou gavetas trancadas, diários com cadeados, ou

Ainda em uma perspectiva prática, ZILLI também reconhece a dificuldade em se admitir o acesso direto, sem autorização judicial, aos dados armazenados em aparelhos celulares em situações de flagrante delito, haja vista que embora a ordem judicial para a busca domiciliar seja excepcionada nestas hipóteses, a busca não deverá ser realizada de forma ampla e irrestrita, porquanto deve estar necessariamente orientada e dirigida para uma finalidade relacionada à situação flagrancial, a qual legitimou o ingresso em domicílio.

Em verdade, em que pese a tentativa de se buscar uma harmonização jurídica entre a proteção constitucional ao domicílio e aos dados armazenados em aparelhos celulares, não nos pareça ser legítima a extensão do conceito de "domicílio", para a ele se equipararem os dispositivos móveis.

Com efeito, o domicílio é um conceito jurídico de natureza civil[391], que está relacionado, necessariamente, a um lugar em que alguém estabeleça residência de forma definitiva (artigo 70 do Código Civil), o que pressupõe a existência de um espaço físico em que a pessoa tenha a intenção de se estabelecer definitivamente.

Nota-se que a noção clássica e secular de domicílio possui repercussão em outras searas jurídicas[392], de modo que uma ressignificação, para finalidades eminentemente processuais penais, poderia romper a estrutura sistemática e integrativa do ordenamento jurídico brasileiro, trazendo graves consequências para outros ramos.

---

mesmo computadores com senhas de acesso. Tem a tranquilidade para assim proceder diante dos limites físicos que estabelecem aquela reserva de liberdade privada. Os domicílios atuais ainda estão distantes daquele desenhado por Zamiátin em seu romance distópico. Logo, imaginar-se na portabilidade de um aparelho multifuncional, a 'portabilidade' do próprio domicílio é metáfora que soa exagerada. Até mesmo porque os aparelhos podem carregar dados que vão além das relações domésticas, como aqueles relativos ao trabalho e, inclusive, de outras pessoas estranhas à relação doméstica. Em realidade, a portabilidade ínsita a esses aparelhos traz a conveniência de se levar consigo uma radiografia de sua própria personalidade em suas múltiplas facetas, relações e interpelações. Assim, a única proximidade possível entre o espaço domiciliar e o conteúdo dos smartphones reside nas expectativas que o morador e o usuário possuem, respectivamente, quanto ao resguardo da privacidade e da intimidade manifestadas naqueles espaços (...)" (ZILLI, Marcos Alexandre Coelho. *A prisão em flagrante e o acesso de dados em dispositivos móveis. Nem utopia, nem distopia. Apenas a racionalidade.* Op. cit., p. 88-89).

[391] DINIZ, Maria Helena. *Código Civil Anotado.* 15ª edição, São Paulo: Editora Saraiva, 2010, p. 119. De acordo com Carlos Roberto Gonçalves, o conceito de domicílio é composto por dois elementos: a residência, enquanto mero estado factual material, de cunho objetivo; a intenção de permanecer-se no local de forma permanente, requisito de caráter subjetivo de natureza psicológica e íntima (GONÇALVES, Carlos Roberto. *Direito civil brasileiro*, volume 1: parte geral, 10ª edição, São Paulo: Editora Saraiva, 2012).

[392] *Verbi gratia*, verifica-se que o domicílio do réu é referência para fixação de competência no direito civil (artigo 46 do Código de Processo Civil). De igual sorte, o domicílio tributário do Código Tributário Nacional pressupõe um local de residência habitual (artigo 127, inciso I, da Lei n.º 5.172/1966).

Não bastasse, o artigo 5º, inciso XI, da Constituição Federal, ao mencionar a expressão "casa", também guarda a noção de um local previamente delimitado, de natureza física e, via de regra, dotado de inamovibilidade, conforme se extrai a descrição estabelecida pelo artigo 150, § 4º, do Código Penal.

Assim, ainda que os *smartphones* armazenem dados e informações que, no mais das vezes, seriam usualmente encontrados em uma busca domiciliar, não nos pareça ser possível equipará-los à noção de um espaço físico e permanente, onde a pessoa viva e resida.

Para TELLES, a interpretação extensiva da garantia de proteção à inviolabilidade domiciliar teria sido encampada pela jurisprudência do Superior Tribunal de Justiça (STJ), especialmente na apreciação quanto à legitimidade do acesso a dados armazenados em aparelhos celulares[393].

Porém, ao que parece, a jurisprudência não incorporou as consequências do reconhecimento da extensão do artigo 5º, inciso XI, da Carta Política aos aparelhos celulares, especialmente com relação à admissibilidade do acesso direto aos dados armazenados nas hipóteses de prisão em flagrante delito.

Em verdade, na contramão da extensão domiciliar proposta, a jurisprudência do Superior Tribunal de Justiça (STJ) firmou posicionamento no sentido de

[393] Na visão de Rodrigo Telles de Souza, "(...) a compreensão do Superior Tribunal de Justiça tanto se baseia em uma extensão da garantia à inviolabilidade domiciliar que, ao mesmo tempo que tal posicionamento foi-se estabelecendo, firmou-se também o juízo de que, caso o telefone celular tenha sido apreendido no cumprimento de um mandado judicial de busca e apreensão expedido contra o investigado, não seria necessária uma segunda autorização do Poder Judiciário, desta feita especificamente para acesso aos dados do dispositivo móvel, pois isso constituiria uma duplicidade inútil (...)" (SOUZA, Rodrigo Telles de. *A exigência de autorização judicial para acesso ao conteúdo de telefone móvel apreendido: uma ampliação da garantia à inviolabilidade domiciliar incompatível com o sistema jurídico brasileiro.* In: SALGADO, Daniel Resende. KIRCHER, Luis Felipe Schneider. QUEIROZ, Ronaldo Pinheiro. *Altos Estudos sobre a prova no processo penal*. Ed. Juspodium, 2020, p. 417). Na mesma linha a posição de Juliano Maranhão, ao comentar o voto-vista do Ministro Rogério Schietti no julgamento pelo Superior Tribunal de Justiça do RHC n.º 51.531/RO: "(...) faz menção a um caso da Suprema Corte norte-americana, que é o Riley vs. California de 2010, para discutir justamente aquele precedente do STF do Gilmar Mendes de 2004, julgado em 2012. No fundo ele considera que aquela mensagem do WhatsApp não é propriamente comunicação, é dado, mas diferentemente daquela decisão de 2004, ou seja, 10 anos depois, considera que o celular evoluiu, não é simplesmente um aparelho para realização de comunicações e, portanto, ele reúne todos os dados íntimos da vida – quase que considera o celular uma espécie de domicílio. Conclui que seria necessário ter mandado específico para acessar aqueles dados (...)" (MARANHÃO, Juliano. *O que é dado não é comunicado?* In: ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. I. São Paulo. Internet Lab, 2018, p. 47).

ser ilícito "(...) o acesso aos dados do celular extraídos do aparelho celular apreendido em flagrante, quando ausente de ordem judicial para tanto, ao entendimento de que, no acesso aos dados do aparelho, se tem a devassa de dados particulares, com violação à intimidade do agente (...)"[394].

5.3.1.3. Os dados armazenados em aparelhos celulares e a inviolabilidade das comunicações: incidência do artigo 5º, inciso XII, da Constituição Federal e Lei n.º 9.296/1996

Uma segunda hipótese de cláusula constitucional expressa de reserva jurisdicional é a relativa ao sigilo das comunicações, já tratada anteriormente[395]. Assim, afigura-se necessário analisar a possibilidade de se estender a disciplina constitucional aplicável ao artigo 5º, inciso XII, da Constituição Federal e, ainda, as disposições aos dados armazenados em aparelhos celulares.

Outrossim, o reconhecimento da incidência do artigo 5º, inciso XII, da Constituição Federal aos dados comunicados armazenados em aparelhos celulares ensejará um debate acerca da aplicabilidade da Lei n.º 9.296/1996 como marco legal regulamentar para o tema, já que a lei expressamente *"*regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal".

A questão parte de uma premissa a ser confirmada ou rechaçada: se a tutela constitucional aos "*dados",* prevista no artigo 5º, inciso XII, da Constituição Federal, diz respeito exclusivamente à sua comunicação ("dados em tráfego" ou "em fluxo") ou abarcaria também as hipóteses de dados estáticos e armazenados em aparelhos celulares.

---

[394] STJ, AgRg no RHC n.º 120.172/SP, 6ª Turma, Rel. Min. Néfi Cordeiro, julgado em 2 de junho de 2020, DJe 08/06/2020. No mesmo sentido: STJ, RHC n.º 67.379/RN, 5ª Turma, Rel. Ministro Ribeiro Dantas, julgado em 20 de outubro de 2016, DJe 09/11/2016; STJ, HC n.º 378.374/MG, 6ª Turma, Rel. Min. Maria Thereza de Assis Moura, julgado em 14 de março de 2017, DJe 30/03/2017.
Sobre o tema, conclui DEZEM que "(...) o problema da posição inicial do STJ é que ela protegeu o celular em forma não desejada pela Constituição Federal, ou seja, em forma não dada de proteção nem mesmo ao domicílio. Chega-se ao seguinte paradoxo com a decisão do STJ: alguém que é preso em flagrante dentro de sua residência pode ter a residência vasculhada, salvo o celular, que precisa de autorização judicial. Não nos parece razoável este posicionamento (...)" (DEZEM, Guilherme Madeira. *Curso de processo penal.* Op. cit. p. 795).

[395] O assunto já foi trazido à baila no primeiro capítulo, especialmente no tocante à abrangência do artigo 5º, inciso XII, da Constituição Federal. Aqui, de maneira especial, a discussão ganha realce para se determinar se o acesso ao conteúdo dos dados armazenados em aparelho celular, especialmente as conversas mantidas em aplicativos de comunicação instantânea, demandam a observância dos requisitos previstos no artigo 2º da Lei n.º 9.296/1996.

O assunto se desenvolveu, doutrinaria e jurisprudencialmente, a partir da clássica lição de Tércio Sampaio Ferraz Júnior, para quem o artigo 5º, inciso XII regularia a comunicação dos dados, e não seu conteúdo propriamente dito[396].

Inicialmente, cogitou-se a incidência da Lei n.º 9.296/1996 às hipóteses de sigilo dos registros telefônicos[397], consistente na relação de chamadas realizadas e efetuadas, o horário, tempo de duração, dentre outras providências que não se relacionavam, propriamente, com o conteúdo da conversa mantida entre os interlocutores. Entretanto, a jurisprudência caminhou para reconhecer que o artigo 5º, inciso XII, da Constituição Federal resguardaria a proteção apenas à comunicação de dados, de modo que a Lei n.º 9.296/1996 também versaria apenas sobre este fluxo, e não propriamente a outros dados relacionados à comunicação[398], que estariam resguardados pela tutela constitucional à privacidade[399] (artigo 5º, inciso X, da CF).

Em verdade, estabeleceu-se que os registros telefônicos, protegidos pelo artigo 3º, incisos V, VII e IX da Lei n.º 9.472/1997, assim como outros dados correlatos, possuem uma efetiva base fática que os torna passíveis de serem apreendidos ou

[396] Para o autor "(...) a distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho à comunicação (...)" (FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado*. Revista da Faculdade de Direito, Universidade de São Paulo, São Paulo, v. 88, p. 447, jan. 1993. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67231/69841>. Acesso em: 20 de dezembro de 2020).

[397] Vicente Greco Filho sustenta que seria aplicável a Lei n.º 9.296/1996 também à quebra do sigilo das comunicações telefônicas, ainda que não se tratem, propriamente, de "interceptação" (GRECO FILHO, Vicente. *Interceptação Telefônica.* Op. cit. p. 6-7). Em sentido contrário, Luiz Flávio Gomes aduz que a Lei de Interceptação Telefônica versa apenas sobre as "comunicações", não alcançando os registros telefônicos pretéritos (GOMES, Luiz Flávio CERVINI, Raúl. *Interceptação Telefônica: Lei 9.296, de 24.07.96*, São Paulo, op. cit. p. 103).

[398] O Superior Tribunal de Justiça (STJ) firmou posicionamento de que não se confundiriam as medidas de quebra de sigilo telefônico com a interceptação de comunicação telefônica, tendo a última uma expressa cláusula de reserva de jurisdição. Portanto, o acesso aos registros telefônicos não demandaria a observância das cautelas estabelecidas pela Lei 9.296/1996 (STJ, HC n. 237.006/DF, Sexta Turma, Relª. Minª. Maria Thereza de Assis Moura, julgado em 27/6/2014, DJe 4/8/2014; STJ, RHC 82.868/MS, Rel. Ministro Felix Fischer, 5ª Turma, julgado em 27/06/2017, DJe 01/08/2017; STJ, RMS 17.732/MT, Rel. Ministro Gilson Dipp, 5ª Turma, julgado em 28/06/2005, DJ 01/08/2005, p. 477). .

[399] MOURA, Maria Thereza Rocha de Assis. *Interceptação Telefônica e Telemática na Jurisprudência Brasileira.* In: AMBOS, Kai; ROMERO, Eneas (orgs.) Crime Organizado: Análise da Lei n.º 12.850/2013. São Paulo: Editora Marcial Pons, 2017, p. 168; DEZEM, Guilherme Madeira. *Curso de processo penal.* Op. cit. p. 1453-1454.

devidamente requisitados, razão pela qual não se submeteriam à disciplina da Lei n.º 9.296/1996[400].

Já os dados em comunicação, diante de sua instantaneidade, não seriam passíveis de apreensão posterior[401], porquanto não se solidificariam em meio ou suporte material apreensíveis, o que justificaria a medida de interceptação.

No tocante aos dados telemáticos e informáticos, aos que admitem a constitucionalidade do artigo 1º, parágrafo único, da Lei n.º 9.296/1996[402], há de se estabelecer o mesmo raciocínio, vedando-se a interceptação de dados passíveis de serem perenizados num suporte fático apreensível *a posteriori*[403].

Portanto, inevitável reconhecer que foram estabelecidos dois regimes jurídicos para: *a)* o fluxo das comunicações telefônicas e telemáticas, que poderá ser interceptado a partir da observância dos requisitos constitucionais (artigo 5º, inciso XII, da Carta Política) e legais (Lei n.º 9.296/1996); *b)* o acesso ao conteúdo dos dados comunicados já armazenados em um suporte fático, material ou digital, que deverá se nortear pela

---

[400] STJ, Agravo Regimental no Recurso Especial n.º 1.760.815/PR, 6ª Turma, Rel. Min. Laurita Vaz, julgado em 23 de outubro de 2018, DJe 13/11/2018, STJ, Recurso Especial n.º 1.851.312/RJ, 5ª Turma, Rel. Min. Ribeiro Dantas, julgado em 17 de dezembro de 2019, DJe 19/12/2019.

[401] BADARÓ, Gustavo Henrique Righi Ivahy. *Interceptação de Comunicações Telefônicas e Telemáticas: limites ante o Avanço da Tecnologia.*, In CASARA, Rubens Roberto R.; Lima, Joel Correa de (Org.). Temas para uma Perspectiva Crítica do Direito - Homenagem ao Professor Geraldo Prado. Rio de Janeiro: Editora Lumen Juris, 2010, p. 483-499.

[402] O tema suscita controvérsias. Parte da doutrina sustenta a inconstitucionalidade do referido artigo (GRECO FILHO, Vicente. *Interceptação Telefônica.* São Paulo: Ed. Saraiva, 1996, p. 9-13; DELMANTO, Roberto e DELMANTO JÚNIOR, Roberto. *A permissão constitucional e a nova lei de interceptação telefônica,* em Boletim *IBCCrim* n. 47, p. 2.), enquanto outros militam pela constitucionalidade "restrita" do dispositivo legal, de modo que ele seria válido apenas no que se relaciona com a comunicação telemática feita por telefone (combinação da informática e telefonia), bem como que a expressão "comunicação telefônica" não se restringiria à "conversação telefônica" (FERNANDES, Antônio Scarance. *A lei de interceptação telefônica.* In: Justiça Penal, n. 4, coord. de Jaques de C. Penteado, São Paulo: Editora RT, 1997). Finalmente, uma terceira vertente reconhece a plena constitucionalidade do dispositivo legal, afirmando que a Constituição Federal apenas exigiu, explicitamente, a regulamentação relativa às comunicações telefônicas, mas não impediu que o legislador disciplinasse outras formas de comunicação (GOMES, Luiz Flávio CERVINI, Raúl. Interceptação Telefônica: Lei 9.296, de 24.07.96, São Paulo, op. cit. p. 171-176). Partilhando deste entendimento, Maria Thereza Rocha de Assis Moura afirma que, levando-se em conta o desenvolvimento tecnológico, parece coerente se admitir uma interpretação progressiva da norma constitucional, para que se compreenda que as mesmas razões que justificam a interceptação telefônica autorizem, também, a interceptação telemática, entendendo que a Lei n.º 9.296/1996 se aplicar não apenas aos meios antigos de comunicação telefônica mas, também, a todos os mecanismos modernos, ainda que não conjugados com a via telefônica, tais como *Messenger, Skype, Facetime, Whatsapp,* etc (MOURA, Maria Thereza Rocha de Assis. *Interceptação Telefônica e Telemática na Jurisprudência Brasileira.* In: AMBOS, Kai; ROMERO, Eneas (orgs.) Crime Organizado: Análise da Lei n.º 12.850/2013. São Paulo: Ed. Marcial Pons, 2017, p. 171-172).

[403] PRADO, Geraldo. *Limite às interceptações telefônicas e a jurisprudência do Superior Tribunal de Justiça*. 2ª edição, Rio de Janeiro: Editora Lumen Juris, 2006. p. 73.

observância à proteção constitucional conferida à privacidade (artigo 5º, inciso X, da Constituição Federal).

Dessume-se, pois, que há um maior rigor no padrão probatório exigido para se operacionalizar a interceptação das comunicações telefônicas e telemáticas, que possui uma expressa cláusula de reserva de jurisdição de índole constitucional, além de demandar uma conjugação de requisitos específicos e de difícil superação para sua admissibilidade, inclusive não sendo admissível para todo e qualquer delito investigado.

Com relação ao acesso de dados comunicados já armazenados, especialmente quando integram um arcabouço reflexivo da integridade moral da pessoa, remanesceria[404] a tutela constitucional conferida à privacidade e intimidade (artigo 5º, inciso X, da Constituição Federal), sem qualquer cláusula de reserva constitucional de jurisdição e tampouco requisitos legais mínimos exigíveis para que se permita o acesso aos dados pretendidos, seja em relação à natureza do crime ou ao *standard probatório* exigido para adoção da medida invasiva.

Na pretensão de se buscar uma harmonia interpretativa que prestigiasse a tutela ao sigilo e à privacidade e intimidade, sustentou-se a aplicação dos requisitos da Lei n.º 9.296/1996 para balizar o acesso ao conteúdo de dados contidos em aparelhos celulares[405]. Entrementes, não parece ser essa é a melhor interpretação, ainda que

---

[404] Nesta categoria, inserem-se os "(...) dados que a pessoa guarda para si e que dão consistência à sua pessoalidade – dados de foro íntimo, expressões de autoestima, avaliações personalíssimas com respeito a outros, pudores, enfim dados que, quando constantes de processos comunicativos, exigem do receptor extrema lealdade e alta confiança, e que, se devassados, desnudariam a personalidade, quebrariam a consistência psíquica, destruindo a integridade moral do sujeito (...)", bem como os "dados que envolvam relações de convivência privada"; "dados que envolvam avaliações (negativas) do comportamento que, publicadas, podem ferir o bom nome do sujeito, isto é, o modo como ele supõe e deseja ser visto pelos outros"; dados que alguém fornece a alguém e não deseja ver explorados (comercialmente, por exemplo) por terceiros (...)" (FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado*. Revista da Faculdade de Direito, Universidade de São Paulo, São Paulo, v. 88, p. 448-449, jan. 1993. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67231/69841>. Acesso em: 20 de dezembro de 2020).

[405] SIDI, Ricardo. *A interceptação de e-mails e a apreensão física de e-mails armazenados*. Revista Fórum de Ciências Criminais – RFCC, Belo Horizonte, ano 2, n. 4, p. 101-121, jul./dez. 2015. É a posição de Rafael Mafei Rabelo Queiroz e Paula Pedigoni Ponce, para quem "(...) já não faz sentido distinguir entre dados em trânsito e dados estáticos como critério para maior ou menor proteção à privacidade: o barateamento do armazenamento de dados e a migração das comunicações humanas para serviços providos pela *Internet*, com opções de armazenamento de segurança em servidores ("backups na nuvem"), torna o conjunto de dados armazenados sobre um indivíduo, por seu considerável volume e abrangência temporal, mais sensível à sua intimidade do que conversas telefônicas interceptadas. A hierarquia protetiva que coloca dados em trânsito acima de dados armazenados simplesmente é anacrônica diante das mudanças na tecnologia e nas práticas

a Lei n.º 9.296/1996 possa contribuir para a formação de um marco regulamentar na apreensão destes dados armazenados, especialmente quando seus requisitos são trazidos como balizas para aferição da proporcionalidade.

Em verdade, a tentação de se estender integralmente a disciplina da Lei n.º 9.296/1996 à apreensão de dados comunicados armazenados se deve ao fato de que o mesmo objeto – aparelho de telefone celular – poderá veicular a transmissão em fluxo de dados comunicativos (*v.g.,* uma ligação telefônica) e também receber e armazenar outros dados passíveis de serem extraídos em procedimentos técnico-científicos, após a apreensão e exame do aparelho[406].

Entretanto, aos dados digitais, guardadas suas peculiaridades, deve se garantir o mesmo tratamento jurídico dispensado aos dados físicos, já que ambos são passíveis de armazenamento em um suporte fático que permita sua apreensão, de forma direta (através da carta ou da comunicação propriamente dita) ou indireta (do disco rígido ou do aparelho celular, por meio do qual se poderá ter acesso ao conteúdo das mensagens enviadas e recebidas).

Com efeito, os dados comunicados e já armazenados em aparelhos celulares se perenizam em um suporte eletrônico que os contém, sendo facilmente

---

comunicativas desde 1993 até os dias atuais (...)" (QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Pedigone. *Tércio Sampaio Ferraz Júnior e sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do estado: o que permanece e o que deve ser reconsiderado*. Op. cit.). Partilham do mesmo entendimento: QUITO, Carina. *As quebras de sigilo telemático no processo penal.* In: LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro. LAUX, Francisco de Mesquita; RAVAGNANI, Giovani dos Santos. Direito, processo e tecnologia. São Paulo: Editora RT, p. 185; MACHADO, André Augusto Mendes; KEHDI, André Pires de Andrade. *Sigilo das comunicações e de dados.* In: FERNANDES, Antônio Scarance; ALMEIDA, José Raul Gavião de; MORAES, Maurício Zanóide de. *Sigilo no processo penal: eficiência e garantismo.* São Paulo: Editora RT, 2008, p. 242; VIEIRA, Renato Stanziola. *Dados cadastrais na Lei n.º 12.850/2013.* In: AMBOS, Kai; ROMERO, Eneas (Orgs.). *Crime organizado: análise da Lei 12.850/2013*. 1ª Ed, São Paulo: Marcial Pons, 2017, p. 125-126; VAZ, Denise Provazi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório.* Op. cit. p. 122;

[406] Dario Kist afirma, com precisão, que "(...) poder-se-ia afirmar que a semelhança necessária entre as duas situações se situa no fato de os mensageiros eletrônicos, e de forma especial o 'Whatsapp', utilizarem-se, pelo menos na maioria das vezes, de aparelhos de telefone (na sua formatação de 'smartphones') para promoverem a comunicação. Contudo, usar de um aparelho destinado, também, à telefonia, concebido para a transmissão atual da palavra falada; e essa distinção entre transmissão da palavra falada e palavra escrita não é aqui essencial, pois ela tem relevância apenas no campo da transmissão atual, enquanto a comunicação estiver em curso, e já se disse que ambas as situações estão regulamentadas na Lei n.º 9.296/96 – na forma de interceptação da comunicação telefônica (palavra falada) e telemática (palavra escrita) -, de modo a não ser necessário demandar o uso da analogia. Em verdade, essencial mesmo, no âmbito desta discussão, é reconhecer a diferença entre comunicação em curso e comunicação concluída – cujo produto encontra-se estanque em arquivos digitais (...)", (KIST, Dario José. *Prova digital no processo penal.* Op. cit. p. 380-382).

apreensíveis mediante cumprimento de uma ordem judicial de busca e apreensão[407], já que não haveria uma efetiva instantaneidade dos dados que impeça a posterior apreensão de seu conteúdo.

Assim, o regime jurídico para acesso aos dados comunicados contidos em aparelhos celulares estaria mais próximo, propriamente, da tutela geral de proteção constitucional à privacidade (artigo 5º, inciso X, da Constituição Federal), porquanto os dados contidos nos aparelhos celulares, à sua maneira, poderiam ser apreendidos durante o cumprimento de uma ordem de busca e apreensão realizada.

Também em campo jurisprudencial tem-se encontrado resistência na extensão da Lei n.º 9.296/1996 para os dados comunicados já armazenados nos aparelhos celulares, conforme precedentes recentes do Supremo Tribunal Federal (STF) e do Superior Tribunal de Justiça (STJ)[408].

Nesta ordem de ideias, o acesso aos dados comunicados contidos em aparelhos celulares, por já terem sido materializados sobre uma base digital passível de posterior apreensão, não estaria adstrita aos rigores da Lei n.º 9.296/1996, que incidiria apenas no tocante às comunicações em "fluxo"[409].

---

[407] De acordo com Gustavo Badaró, "(...) do mesmo modo em que se faz com uma carta em papel, será possível a busca e apreensão dos discos rígidos dos computadores ou de qualquer outro suporte em que fique registrada tal correspondência eletrônica, segundo a disciplina legal dos arts. 240 e segs. do CPP (...)" (BADARÓ, Gustavo Henrique Righi Ivahy. *Interceptação de Comunicações Telefônicas e Telemáticas: limites ante o Avanço da Tecnologia.* Op. cit. p. 483-499).

[408] STF, HC n.º 91.867/PA, 2ª Turma, Rel. Min. Gilmar Mendes, j. 24/04/2012, DJe 19/09/2012; STF, AgRg no HC n.º 124.322/RS, 1ª Turma, Rel. Min. Luís Roberto Barroso, julgamento em 9 de dezembro de 2016, DJe 19/12/2016; STF, RE n.º 418.416/SC, relatoria Min. Sepúlveda Pertence, julgado em 10 de maio de 2006, DJ 19 de dezembro de 2006; STF, RHC n.º 132.062/RS, 1ª Turma, Relatoria Ministro Marco Aurélio, redator do acórdão Min. Edson Fachin, julgado em 22 de novembro de 2016, DJe 24 de outubro de 2017; STJ, REsp n.º 1.851.312/RJ, 5ª Turma, Rel. Min. Ribeiro Dantas, julgado em 17 de dezembro de 2019, DJe 19/12/2019; STJ, AgRg no REsp n.º 1.760.815/PR, 6ª Turma, Rel. Ministra Laurita Vaz, julgado em 23 de outubro de 2018, DJe 13/11/2018; STJ, AgRg no HC n.º 521.228/RJ, 5ª Turma, Rel. Min. Jorge Mussi, j. 03/12/2019.

[409] A inaplicabilidade da Lei de Interceptação Telefônica se restringiria, por óbvio, aos dados comunicados já armazenados nos respectivos aparelhos, à exemplo de e-mails enviados e recebidos, fotografias, vídeos e mensagens de texto e de voz enviadas e recebidas por aplicativos de comunicação instantânea. Ressalve-se que estes mesmos aplicativos permitem a realização de chamadas de voz instantâneas, operacionalizadas através de dados criptografados via *internet*, que, à exemplo das ligações telefônicas propriamente ditas, não permitem a apreensão a posteriori, por inexistência de solidificação em meio ou suporte material. Nestas situações, caso haja a necessidade de se realizar uma interceptação telemática instantânea desta chamada, faz-se necessário atender aos pressupostos e requisitos delimitados no artigo 1º, parágrafo único, e artigo 2º, ambos da Lei n.º 9.296/1996.

Não bastasse, a regulamentação da interceptação telefônica possui caráter prospectivo, visando a colheita de elementos probatórios futuros a partir das comunicações a serem estabelecidas, o que não se aplicaria integralmente ao acesso a dados armazenados, que versam sobre elementos probatórios já produzidos e consolidados.

Denota-se, portanto, a impossibilidade de se aplicar a Lei n.º 9.296/1996, como marco legal regulatório direto, às hipóteses de acesso a dados armazenados em aparelhos celulares, ainda que seus requisitos possam temperar a formação de um marco legal regulamentar para acesso a estes dados.

Registre-se, todavia, que o conceito de proteção à "comunicação" de dados e aos dados propriamente ditos, elucubrado por FERRAZ JÚNIOR, se formou a partir dos recursos tecnológicos existentes à época[410], os quais estavam intimamente relacionados à telegrafia, à correspondência e à comunicação telefônica, o que se permitia tratar de maneira distinta o *fluxo* dos dados e o seu resultado propriamente dito. Ademais, a divisão interpretativa da abrangência do artigo 5º, inciso XII, da Constituição Federal estaria sedimentado sob alguns fundamentos individualista relacionados à privacidade, especialmente ao direito de estar e permanecer só ("*right to be alone"*), bem como é tratada em uma ótica meramente defensiva, enquanto limite às intromissões ou devassas indevidas.

Atualmente, diante da massiva produção, coleta, armazenamento, tratamento e compartilhamento de dados, bem como de regulamentações nacionais e internacionais sobre o tema – *verbi gratia,* a Lei n.º 12.965/2014 (Marco Civil da *Internet*) e a Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados) –, a privacidade deve ser analisada sob uma concepção relacional e positiva, sendo uma prerrogativa do cidadão conhecer os dados relativos à sua individualidade que, em mãos de terceiros, sejam capazes de afetar sua autonomia e liberdade.

---

[410] Tércio Sampaio Ferraz Júnior, em uma reflexão recente sobre seu posicionamento, explicitou o contexto fático que o levou a debruçar sobre o tema e chegar às conclusões expostas à época (FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados, o direito à privacidade e os limites do poder do Estado: 25 anos depois.* Op. cit., p. 22). De igual sorte, confira-se: FERRAZ JÚNIOR, Tércio Sampaio. *Comunicação de dados e proteção ao sigilo.* In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas. Lei Geral de Proteção de Dados (Lei n.º 13.709/2018): a caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Editora RT, 2020, p. 165/176.

Outrossim, com o desenvolvimento tecnológico no processo comunicacional, sobreveio a necessidade de se reinterpretar a distinção anteriormente cunhada, especialmente diante do advento dos dados digitais e da comunicação telemática.

JULIANO MARANHÃO, em abordagem recente sobre o tema juntamente com FERRAZ JÚNIOR, rechaça a analogia estabelecida entre as cartas e os dados armazenados em aparelhos celulares, bem reconhece que, nas comunicações estabelecidas por aplicativos de mensagens instantâneas (*v.g.*, *WhatsApp*), haveria uma distinção entre a noção de tempo e de espaço do fluxo da comunicação e o curso da conversão, haja vista que o fluxo da comunicação pode ser momentâneo, representado em cada mensagem enviada e recebida, mas o curso da comunicação não tem uma delimitação precisa[411]. Nesta ordem, seria inevitável uma aproximação entre a tutela conferida ao conteúdo dos dados armazenados e do seu fluxo propriamente dito[412], restando superada a rígida distinção de tratamento constitucional sobre o tema.

Esta concepção, aparentemente, já encontra um sinal de aceitação pelo Supremo Tribunal Federal (STF), conforme julgamento do *Habeas Corpus* n.º 168.052/SP[413] e da *Reclamação n.º 33.711/SP*[414], ambos de relatoria do Ministro Gilmar Mendes.

Portanto, uma possível reinterpretação dos conceitos relacionados à distinção entre a tutela da comunicação dos dados e seu conteúdo poderá atrair a proteção

---

[411] MARANHÃO, Juliano. *O que é dado não é comunicado?* Op. cit., p. 51-54). Na mesma linha: MARANHÃO, Juliano. *O acesso ao WhatsApp pela operação Lava Jato*. Disponível em <http://jota.info/artigos/o-acesso-ao-whatsapp-pela-operacao-lava-jato-05122016>. Acesso em 20 de dezembro de 2020.

[412] Esta foi a conclusão adotada por Tércio Sampaio Ferraz Júnior, no "Painel 4: O alcance da proteção do sigilo das comunicações no Brasil", durante exposição no dia 2 de setembro de 2020 no IV Congresso Internacional Direitos Fundamentais e Processo Penal na era digital, promovido pelo centro independente de pesquisa e tecnologia do *InternetLab*.

[413] Em seu voto, o relator Ministro Gilmar Mendes cogita a possibilidade de se estender a previsão do artigo 5º, inciso XII, da Constituição Federal aos dados armazenados em aparelhos celulares, acenando com uma mudança na posição fixada no *Habeas Corpus* n.º 91.867/PA:"(...) naquela oportunidade, defendi a impossibilidade de interpretar-se a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral, porquanto a proteção constitucional seria da comunicação, e não dos dados. Creio, contudo, que a modificação das circunstâncias fáticas e jurídicas, a promulgação de leis posteriores e o significativo desenvolvimento das tecnologias da comunicação, do tráfego de dados dos aparelhos smart phones leva, nos dias atuais, à solução distinta. Ou seja, penso que se está diante de típico caso de mutação constitucional. Questiona-se se o acesso a informações e dados contidos nos. celulares se encontra ou não expressamente abrangido pela cláusula do inciso XII do art. 5º (...)" (STF, HC n.º 168.052/SP, 2ª Turma, Rel. Min. Gilmar Mendes, julgado em 9 de outubro de 2020).

[414] STF, Reclamação n.º 33.711/SP, 2ª Turma, Rel. Min. Gilmar Mendes, julgado em 11 de junho de 2019, DJe 22/08/2019.

constitucional conferida no artigo 5º, inciso XII, da Constituição Federal também aos dados armazenados em aparelhos celulares, admitindo-se a interceptação de toda e qualquer espécie de comunicação, ainda que posteriormente venham a ser armazenadas.

5.3.2. Cláusula legal de reserva de jurisdição

Embora a Constituição Federal tenha estabelecido cláusulas de reserva de jurisdição para a intromissão em determinada esfera de direitos e garantias individuais, é certo que a matéria não se exaure em campo constitucional.

É possível que diplomas normativos infraconstitucionais estabeleçam cláusulas legais de reserva de jurisdição para a restrição a determinados direitos e garantias fundamentais, especialmente quando relacionados à prestação de serviços que lidam com dados pessoais de grande parcela social[415]

Assim o acesso a dados financeiros, fiscais e telefônicos depende, via de regra, de prévia e fundamentada autorização judicial, conforme dispõem respectivamente o artigo 1º, § 4º, da Lei Complementar n.º 105/2001, o artigo 198, § 1º, inciso I, do Código Tributário Nacional e a interpretação conferida ao artigo 3º, incisos V, VI e IX da Lei n.º 9.472/1997.

Como visto, a guarda e a disponibilização de registros de conexão e de acesso a aplicações de *internet* também exigirá prévia ordem judicial, que buscará compatibilizar os interesses investigativos com a preservação da intimidade, vida privada, honra e imagem das pessoas direta ou indiretamente envolvidas (artigo 10 da Lei n.º 12.965/2014).

Conclui-se que determinados dados pessoais inseridos na proteção constitucionalmente conferida à privacidade e intimidade, embora não tenham encontrado cláusula constitucional de reserva de jurisdição no artigo 5º, inciso X, da Constituição Federal, foram contemplados com a necessidade de intervenção judicial por força de marcos

[415] SOUZA, Rodrigo Telles de. *A exigência de autorização judicial para acesso ao conteúdo de telefone móvel apreendido: uma ampliação da garantia à inviolabilidade domiciliar incompatível com o sistema jurídico brasileiro.* Op. cit. 409.

regulatórios infraconstitucionais. Entretanto, especialmente em relação ao tema, JACQUELINE ABREU e DENNYS ANTONIALLI apontam que:

> diferente é a situação da proteção (a conteúdo) de comunicações armazenadas, isto é, as que não estão mais em trânsito. A legislação infraconstitucional toca a questão em duas leis diferentes. Quando o acesso a essas comunicações se dá por meio de um intermediário, que detém os dados (como é o caso de provedores de aplicações de Internet), os dispositivos aplicáveis são aqueles previstos no Marco Civil da Internet, o qual determina que o acesso ocorra mediante 'ordem judicial' (art. 7º, III) nas hipóteses e na forma que a lei o estabelecer (art. 10, § 2º), sem, entretanto, explicitar requisitos substantivos de padrão probatório. Quando o acesso se dá diretamente no aparelho apreendido, o regime não é claro. Não há regras específicas desenhadas e aplicadas para a busca de dispositivos eletrônicos, dando lugar a discricionariedade judicial, insegurança jurídica e abusos. Diante disso, pode-se dizer que, atualmente, comunicações armazenadas, registradas em celulares e computadores, provavelmente por anos a fim, gozam de um grau de proteção menor do que comunicações em fluxo, cujo acesso se encontra regulamentado de forma mais rigorosa pela Lei de Interceptações (ANTONIALLI, Dennys M.; ABREU, Jacqueline de Souza. *O conto do baú do tesouro: a expansão da vigilância pela evolução e popularização dos celulares no Brasil*. Surveillance in Latin America, v. 5, p. 353, 2017).

Assim, sob a égide de legislações infraconstitucionais, é relevante se analisar a aplicabilidade do artigo 3º, inciso V, da Lei n.º 9.472/1997 e do artigo 7º, inciso III, da Lei n.º 12.965/2014 como marcos legais para o acesso aos dados estáticos armazenados em aparelhos celulares, no curso de investigações criminais.

5.3.2.1. (In)aplicabilidade da Lei n.º 9.472/1997 e da Lei n.º 12.965/2014 como marcos legais para o acesso aos dados estáticos armazenados em aparelhos celulares, no curso de investigações criminais

É indiscutível que o artigo 7º, inciso III, da Lei n.º 12.965/2014 disciplina as condições para o acesso remoto do conteúdo das comunicações privadas

armazenadas em aparelho celular, que devem ser fornecidas mediante requisição judicial aos provedores de aplicação de *internet.* De igual sorte, o artigo 3º, inciso V, da Lei n.º 9.472/1997 é aplicável aos usuários dos serviços de telecomunicação, estabelecendo-se ser direito deles a inviolabilidade e ao segredo de sua comunicação, salvo nas hipóteses e condições constitucional e legalmente previstas.

Entretanto, é certo que os referidos dispositivos legais vêm sendo invocados como marco legal para se fundamentar a exigência quanto à indispensabilidade de autorização judicial no acesso aos dados armazenados em aparelhos celulares[416].

Convém trazer à análise a efetiva aplicabilidade do artigo 7º, inciso III e artigo 10, § 2º, ambos da Lei n.º 12.965/2014 e do artigo 3º, inciso V, da Lei n.º 9.472/1997 ao acesso direto ao conteúdo das comunicações pelas autoridades investigativas, mediante apreensão e análise física do conteúdo do aparelho celular, após apreensão em situações de flagrante ou em cumprimento a mandado de busca e apreensão expedido.

De forma autônoma e remetendo a disciplina procedimental para uma lei a ser editada, o legislador assegurou, no artigo 10, § 2º, da Lei n.º 12.965/2014 que os provedores deverão fornecer o próprio conteúdo das comunicações registradas em seus respectivos servidores[417]. Entretanto, a referida lei nunca foi editada, deixando-se de estabelecer os requisitos formais e materiais e o procedimento a ser observado para acesso ao conteúdo[418]. Para tanto, delegou textualmente estas questões a uma nova lei, que nunca fora editada.

Inobstante a ausência de regulamentação[419], reconhece-se a possibilidade da requisição judicial do conteúdo das comunicações privadas aos provedores de aplicação de *internet,* mediante analogia aos requisitos e procedimentos aplicáveis à busca e apreensão[420].

---

[416] STJ, RHC n.º 51.531/RO, 6ª Turma, Rel. Nefi Cordeiro, julgado em 19 de abril de 2016, DJe 09/05/2016.
[417] KIST, Dario José. *Prova digital no processo penal.* Op. cit. p. 259-260.
[418] MENDES, Gilmar Ferreira.; PINHEIRO, Jurandi Borges. *Interceptações e privacidade: novas tecnologias e a Constituição*. In: Direito, Inovação e Tecnologia; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (Coord.). *Direito, inovação e tecnologia*. São Paulo: Saraiva, 2015. p. 231-250.
[419] JEZLER JÚNIOR, Ivan. *Prova penal digital: tempo, risco e busca telemática.* Florianópolis: Ed. Tirant lo Blanch, 2019, p. 155.
[420] Abreu e Antonialli apontam que "(...) para limitar esse tipo de acesso a casos em que é legítimo e apropriado, cabe interpretar o silêncio da lei à luz da Constituição Federal, do instituto análogo da busca e apreensão do

Ressalte-se que, embora a requisição judicial dos dados aos provedores de conexão e de aplicações de *internet*, a eventual resistência imotivada para acesso aos dados demandados poderá redundar na adoção de medidas de busca e apreensão em face destes terceiros, para obtenção do conteúdo pretendido.

Entretanto, é possível que os provedores de serviço deixem de armazenar o conteúdo das informações de seus usuários ou, ainda, o façam sob criptografia, com o propósito de impedir o acesso por seus agentes, em estratégia deliberada para tornar o serviço interessante aos usuários[421]. Neste caso, a falta de disposição legal obrigando a entrega dos dados desobriga os provedores a fornecê-los, sob pena de violação ao princípio da legalidade (artigo 5º, inciso II, da Constituição Federal) [422].

Código de Processo Penal e de precedentes de tribunais superiores que lidaram com o tema, como o HC 315.220/RS do STJ. Em se tratando de conteúdo de comunicações, o pedido de quebra de sigilo deve apresentar fundados indícios de ocorrência de ilícito penal e indícios de autoria e/ou participação contra o alvo investigado. Em atenção ao princípio da proporcionalidade, deve ser provado que a medida é adequada à instrução, sendo pertinente para o crime investigado com base em fatos já configurados. Quanto à necessidade, essa fonte de prova deve ser imprescindível ao prosseguimento da investigação e consecução do arcabouço probatório, bem como delinear o período ou abrangência dos dados a serem coletados em íntima correlação ao aos elementos concretos do caso investigado. A ordem judicial concedida deve ser minuciosamente fundamentada também nestes termos, em atenção ao art. 93, IX da Constituição Federal (...)" (ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. *Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais.* São Paulo: InternetLab, 2017, p. 31-33). Em outro sentido, ao comentarem o artigo 13-B, § 2º, inciso I, do Código de Processo Penal, que guarda redação bastante semelhante ao do dispositivo legal em estudo, CUNHA e PINTO defendem a aplicabilidade extensiva dos requisitos legais e procedimentais da Lei n.º 9.296/1996 (CUNHA, Rogério Sanches; PINTO, Ronaldo Batista. *Código de Processo Penal e Lei de Execução Penal Comentados.* 2ª ed. São Paulo: Editora Juspodivm, 2018, p. 75).

[421]MOURA, Maria Thereza Rocha de Assis; BARBOSA, Daniel Marchionatti. *Dados digitais: interceptação, busca e apreensão e requisição.* Op. cit., p. 491.

[422] Alguns provedores de aplicação de *internet*, tais como o *Whatsapp*, *Telegram*, têm deixado de fornecer o conteúdo das comunicações privadas mantidas através dos referidos aplicativos, sob alegação de que utilizam a rede "*peer-to-peer"* (P2P ou "ponto a ponto"). Trata-se de "(…) a self-organizing system of equal, autonomous entities (peers) [which] aims for the shared usage of distributed resources in a networked environment avoiding central services (…)" (STEINMETZ, R. WEHRLE, K. *Peer-to-Peer Systems and Applications. Lecture Notes in Computer Science*, vol. 3485. Springer, Berlin: Heidelberg, cap. 2, p. 10). Como se depreende, por intermédio do referido sistema, não há uma relação de cliente e servidor, já que todos os pontos funcionam, equivalentemente, tanto como cliente quanto como servidor. Nesta linha, permite-se o compartilhamento de conteúdo sem a necessidade de que atravessem um servidor central, o que impediria, por conseguinte, o fornecimento das comunicações requisitadas. Especialmente com relação ao aplicativo *Whatsapp,* destaca-se que este fora alvo de sanções e até mesmo bloqueios temporários (conforme http:// bloqueios.info. Acesso em 20 de dezembro de 2020), com esteio no artigo 12 da Lei n.º 12.965/2014, em razão do descumprimento de ordens judiciais que determinavam o fornecimento do conteúdo das comunicações privadas, no bojo de inquéritos policiais e procedimentos penais. Sustentam, para tanto, que a empresa não poderia operar em território nacional (artigo 11 da Lei n.º 12.965/2014), com a utilização de tecnologia que não esteja de acordo com as disposições da Lei do Marco Civil da *Internet* e também a possibilidade de interceptação do fluxo das conversas mantidas, conforme artigo 5º, inciso VII, da Constituição Federal. O bloqueio nacional do referido provedor de aplicativos está sendo objeto de discussão no âmbito da Arguição de Descumprimento de Preceito Fundamental (ADPF) n.º 403-SE, de relatoria do Ministro Edson Fachin e da Ação Direta de Inconstitucionalidade n.º 5527-DF, de relatoria da Ministra Rosa Weber. Em julgamento iniciado em 28 de maio de 2020, o Ministro Edson Fachin julgou procedente o pedido formulado na arguição

Portanto, vislumbra-se que o conteúdo das comunicações privadas pode ser acessado de duas formas: *a)* por intermediários, notadamente os provedores de aplicação de *internet*, cuja disponibilização do conteúdo demanda prévia autorização judicial[423] (artigo 10, § 2º, combinado com artigo 7º, inciso III, ambos do Marco Civil da *Internet*), bem como pelos serviços de telecomunicação (artigo 3º, inciso V, da Lei n.º 9.472/1997); *b)* diretamente pela autoridade investigativa competente (policiais e Ministério Público), mediante acesso físico ao aparelho de telefonia celular apreendido.

Especialmente em relação a esta forma física e direta de acesso, sem intermediários, é que se questiona a extensão da previsão normativa contida nos precitados dispositivos legais e, por conseguinte, a imprescindibilidade de autorização judicial para acesso ao conteúdo das comunicações privadas.

Ao menos duas linhas interpretativas se formaram na jurisprudência, com relação à extensão das previsões normativas e sua aplicabilidade ao acesso direto, pela autoridade policial e pelo Ministério Público, do conteúdo dos dados armazenados em aparelhos celulares, durante investigações criminais.

A primeira delas reconhece a aplicação do conteúdo normativo do artigo 7º, inciso III, da Lei n.º 12.965/2014 e do artigo 3º, inciso V, da Lei n.º 9.472/1997 ao

---

de descumprimento de preceito fundamental para declarar a inconstitucionalidade parcial sem redução de texto tanto do inciso II do art. 7º, quanto do inciso III do art. 12 da Lei 12.965/2014, de modo a afastar qualquer interpretação do dispositivo que autorize ordem judicial que exija acesso excepcional a conteúdo de mensagem criptografada ponta-a-ponta ou que, por qualquer outro meio, enfraqueça a proteção criptográfica de aplicações da *internet*. A Ministra Rosa Weber acompanhou a decisão do Min. Edson Fachin, mas dava interpretação conforme à Constituição a esses dispositivos, sendo que ambos reconheceram que o sigilo das comunicações, inclusive pela *internet*, é uma garantia constitucional, tendo ambos afastado qualquer interpretação das normas do Marco Civil da *Internet* (Lei 12.965/2014) que permita que, por meio de ordem judicial, as empresas deem acesso ao conteúdo de mensagens criptografadas ponta-a-ponta. Em seguida, o julgamento foi interrompido por um pedido de vista (http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=444384. Acesso em 20 de dezembro de 2020). No mesmo sentido, confira-se: STJ, RMS n.º 60.531/RO, 3ª Seção, Rel. Min. Nefi Cordeiro, Rel. p/ acórdão Min. Ribeiro Dantas, julgado em 9 de dezembro de 2020, DJe 17/12/2020.
Para uma análise no tocante à criptografia e as dificuldades investigativas relacionadas à implementação da tecnologia, recomenda-se: ABREU, Jacqueline de Souza. *Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação*. Rev. Bras. Polít. Públicas, Brasília, v. 7, nº 3, 2017 p.24-42; STARR, Adriana Galvão. *A dificuldade de acesso ao conteúdo das mensagens ilícitas trocadas via WhatsApp para uso em procedimento de investigação e ação penal.* In. Caderno de Estudos de Investigação e prova nos crimes cibernéticos, da Escola de Magistrados da Justiça Federal da 3ª Região, São Paulo: 1ª edição, 2017, p. 85-109.
É certo que, se de fato comprovada tecnicamente a impossibilidade de fornecimento, não há como se punir o provedor de aplicações, na esteira do quanto disposto no artigo 17 da Lei n.º 12.965/2014.

[423] DOMINGOS, Fernanda Teixeira Souza. RÖDER, Priscila Costa Schreiner. *Obtenção de provas digitais e jurisdição na Internet.* In. *Caderno de Estudos de Investigação e prova nos crimes cibernéticos*, da Escola de Magistrados da Justiça Federal da 3ª Região, São Paulo: 1ª edição, 2017, p. 74.

acesso direto aos dados armazenados em aparelhos celulares. Sustenta-se, para tanto, que se os dispositivos legais objetivaram assegurar a privacidade e intimidade do usuário com relação ao conteúdo das comunicações privadas por ele mantidas, é evidente que esta proteção se justifica pela densidade do conteúdo tutelado, que expõe sobremaneira o seu titular. Assim, em sendo a chancela judicial para acesso aos dados uma garantia conferida ao cidadão, não haveria razão lógica para se permitir sua dispensa nos casos de acesso direto pelas autoridades investigativas[424].

Por sua vez, uma segunda corrente conclui pela inaplicabilidade das disposições das Leis n.º 9.472/1997 e 12.965/2014 às hipóteses de acesso aos dados comunicados por autoridades, em uma investigação criminal. Argumenta-se que os regramentos relacionados ao artigo 7º, inciso III, destinam-se à proteção do sigilo de dados em ambiente virtual, quando os usuários estariam conectados à rede mundial de computadores. Nesta senda, por força de uma interpretação literal do artigo 7º, *caput*, concluem que as disposições legais estariam restritas às hipóteses de acesso à *internet*, o que não ocorreria na apreensão física do aparelho celular. Nesta hipótese, o acesso ao conteúdo das comunicações privadas poderia ser realizado sem a correspondente autorização judicial, já que o usuário não estaria, naquele momento, conectado à *internet.*

Ademais, aponta-se também que o artigo 22 do Marco Civil da *Internet*, ao mencionar a expressão "parte interessada", teria consignado a necessidade de chancela judicial em um pedido formulado por uma parte, o que não se aplicaria a uma autoridade investigativa[425].

Finalmente, em reforço a esta posição, tem-se afirmado que a inaplicabilidade do artigo 7º, inciso III, da Lei n.º 12.965/2014 e do artigo 3º, inciso V, da Lei n.º 9.472/1997 decorrem do fato de que a proteção legal conferida ao sigilo dos dados é direcionada aos prestadores dos serviços públicos ou privados de especial interesse público

[424] STJ, REsp n.º 1.675.501/MG, 6ª Turma, Rel. Min. Sebastião Reis Júnior, j. 17/10/2017, DJe 27/10/2017. Ainda no tocante a esta primeira linha interpretativa, há precedentes jurisprudenciais que, conquanto admitam a aplicação do artigo 7º, inciso III, da Lei n.º 12.965/2014, acabam por excepcionar sua incidência a partir da necessidade de preservação do interesse público de repressão à prática de crimes. Nesta linha: TJSP, Apelação n.º 0005715-61.2016.8.26.0196, 7ª Câmara de Direito Criminal, Rel. Otávio Rocha, julgado em 28 de fevereiro de 2018).

[425] TJSP, Apelação n.º 0019072-94.2015.8.26.0309, 12ª Câmara Criminal, Rel. Jaime Ferreira Menino, j. 05/04/2017; TJSP, Apelação n.º 1500011-25.2018.8.26.0583, 3ª Câmara Criminal, Rel. Jaime Ferreira Menino, j. 24/07/2019.

que possuem a guarda dos referidos dados. Assim, o direito do usuário de *internet* e das telecomunicações ao sigilo das comunicações privadas incide em relação aos dados detidos pelas pessoas jurídicas de direito privado que prestam o serviço de acesso aos serviços de telecomunicação e à rede mundial de computadores[426].

O Superior Tribunal de Justiça (STJ), em julgamento posteriormente referendado pelo o Supremo Tribunal Federal (STF)[427], afastou a aplicabilidade do artigo 22, parágrafo único, da Lei n.º 12.965/2014, às hipóteses de quebra de sigilo telemático, uma vez o dispositivo legal "(...) indica o que deve conter no requerimento para o fornecimento de 'registros de conexão' ou de 'registros de acesso a aplicações de *internet* ', que são, em suma, informações de início e de término de uma conexão à *internet* ou de uso de determinada aplicação, incluindo o número do endereço IP utilizado. Não se aplica, assim, ao pedido de quebra de sigilo telemático, que busca, basicamente, a obtenção do conteúdo de comunicações privadas (...)"[428].

Entretanto, ainda que os marcos legais acima indicados não sejam aplicáveis diretamente para regulamentar o acesso aos dados armazenados, é certo que poderão servir de parâmetro[429] - haja vista que as previsões normativas são destinadas diretamente aos provedores de aplicação de *internet* (artigo 7º, incisos II e III e artigo 2º do Decreto n.º 8.771/1996, que regulamentou a Lei n.º 12.965/2014) e aos serviços de

[426] RODRIGO TELLES DE SOUZA, compartilhando da mesma opinião, aponta que "(...) os dados legalmente protegidos por sigilo com base no art. 5º, inciso X, da Constituição de 1988, tais como as informações fiscais, bancárias, telefônicas e telemáticas, são revestidos dessa especial modalidade de tutela jurídica apenas enquanto são detidos pelos prestadores de serviços públicos ou privados de especial interesse públicos a que eles se referem. A partir do momento em que essas informações são obtidas pelos seus titulares e por eles arquivadas de qualquer modo, perdem automaticamente o caráter sigiloso (...)" (SOUZA, Rodrigo Telles de. *A exigência de autorização judicial para acesso ao conteúdo de telefone móvel apreendido: uma ampliação da garantia à inviolabilidade domiciliar incompatível com o sistema jurídico brasileiro.* Op. cit., p. 423-424).

[427] STF, Agravo Regimental no *Habeas Corpus* n.º 170.376/SP, 1ª Turma, Rel. Min. Rosa Weber, julgado em 9 de junho de 2020, DJe 23/06/2020.

[428] STJ, Recurso em *Habeas Corpus* n.º 100.709/SP, 6ª Turma, Rel. Min. Laurita Vaz, julgado em 2 de abril de 2019, DJe 16/04/2019.

[429] Foi neste sentido a posição do Ministro Gilmar Mendes no julgamento do Agravo n.º 1.042.075/RJ, apontando-se que "(...) a legislação infraconstitucional avançou para possibilitar a proteção dos dados armazenados em comunicações privadas, os quais só podem ser acessados mediante prévia decisão judicial – matéria submetida à reserva de jurisdição. Entendo que o avanço nesse importante tema da proteção do direito à intimidade e à vida privada deve ser considerado na interpretação do alcance das normas do art. 5º, X e XII, CF (...)", especialmente considerando o incrível desenvolvimento dos mecanismos de comunicação e armazenagem de dados pessoais em smartphones, o avanço tecnológico e a necessidade de ressignificações do direito à privacidade e à intimidade, invocando-se precedentes norte-americanos, alemães e também a lei de proteção de dados europeia (General Data Protection Regulation – GDPR) (STF, Repercussão Geral no Recurso Extraordinário com Agravo n.º 1.042.075/RJ, Rel. Min. Dias Toffoli, julgado em 23 de novembro de 2017, DJe 12/12/2017).

telecomunicação -, para se estabelecer um marco regulamentar e procedimental para acesso a dados previamente armazenados em aparelhos celulares.

5.3.3. A imprescindibilidade da autorização judicial para o acesso aos dados armazenados

Como visto nos tópicos precedentes, há um déficit legislativo com relação ao procedimento a ser adotado para o acesso a dados armazenados em aparelhos celulares.

Nesta perspectiva, por se tratar de tema que envolve a limitação a direitos e garantias fundamentais, e considerando que a realidade social e investigativa tem revelado a necessidade da utilização do referido meio de obtenção de prova, é imprescindível se avançar na definição de parâmetros para o acesso aos dados armazenados, dentro de uma ponderação de valores constitucionais relacionados à intimidade e à eficiência da atividade investigativa.

Ainda que se admita ser o referido meio de obtenção de prova esteja subsumido apenas à regulação do artigo 5º, inciso X, da Constituição Federal que, como destacado, não apresenta cláusula expressa de reserva de jurisdição, não há como se afastar a imprescindibilidade da análise judicial para o acesso aos referidos dados.

Com efeito, tomando-se por base as lições de GUSTAVO TORRES SOARES, a Constituição Federal exige autorização judicial prévia na implementação de meios de obtenção de prova significativamente compressores de direitos e garantias fundamentais, classificando-os em três categorias: *a)* a dos meios não sujeitos a autorização judicial prévia, por não serem considerados significativamente compressores de direitos fundamentais (*v.g.*, tomada de depoimentos); *b)* os sujeitos a autorização judicial prévia, por serem considerados significativamente compressores de direitos fundamentais (*v.g.*, interceptação telefônica); *c)* os que, embora significativamente compressores de direitos fundamentais, são excepcionalmente dispensados de autorização prévia, por força de situação justificante (*v.g.*, a gravação da própria conversa).

Adotando-se a classificação proposta e transportando-a para os novos e recentes meios investigativos criminais – dentre os quais o acesso aos dados – , é inegável

que os meios de busca de provas representativos de inovação, ainda que toleráveis, sujeitam-se a autorização judicial prévia por serem análogos ou extensivamente interpretados com base em meios já positivados e considerados significativamente compressores de direitos fundamentais[430].

Depreende-se que o acesso aos dados armazenados em aparelhos celulares, enquanto meio atípico de obtenção de provas[431] – diante da ausência de regulamentação precisa sobre o tema –, insere-se fatalmente nesta categoria, especialmente considerando que a volumosa quantidade de dados armazenados permite uma ampla e irrefreável exposição da privacidade do cidadão, tornando-o suscetível também da ação de vigilância e monitoramento por aplicações remotas[432].

Em verdade, sendo necessária a utilização da analogia para se dar substrato regulatório ao referido meio de obtenção de prova, é possível se valer da regulação aplicável à busca e apreensão[433] (artigo 240 e seguintes do Código de Processo Penal), bem como das disposições relacionadas ao artigo 22, parágrafo único, da Lei n.º 12.965/2014 e dos requisitos estabelecidos no artigo 2º da Lei n.º 9.296/1996, que regulamenta as hipóteses de interceptação telefônica e telemática.

De início, nota-se que todos tem em comum a necessidade de uma prévia e fundamentada decisão judicial autorizativa para a obtenção dos dados e elementos de informação a ser amealhados a partir dos referidos meios de investigação de prova[434].

---

[430] Segundo GUSTAVO SOARES, "(...) é tolerável a adoção de inovação investigativa sem satisfatória regulamentação jurídica, ainda que cause significativo impacto em direitos fundamentais, desde que, obedecido o mandamento da proporcionalidade, seja compensado seu déficit de regulamentação por método judicial que a trate como 'praeter legem', excepcional, temporária, decorrente de interpretação extensiva ou aplicação analógica inserida em contexto de evolução legislativa progressiva (...)" (SOARES, Gustavo Torres. *Investigação criminal e inovações técnicas e tecnológicas: perspectivas e limites.* Tese (Doutorado em Direito Processual Penal) - da Faculdade de Direito da Universidade de São Paulo. São Paulo, SP, 2014, p. 270).

[431] ZILLI, Marcos Alexandre Coelho. *A prisão em flagrante e o acesso de dados em dispositivos móveis. Nem utopia, nem distopia. Apenas a racionalidade.* Op. cit., p. 90.

[432] MENDES, Laura Schertel. *Uso de softwares espiões pela polícia: prática legal?*, disponível em: www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espioes-pela-policia-pratica-legal-04062015. Acesso em: 20 de dezembro de 2020).

[433] QUITO, Carina. *As quebras de sigilo telemático no processo penal.* Op. cit. 170.

[434] A busca e apreensão pessoal e domiciliar exigem, como regra, decisão judicial autorizativa, na forma do artigo 5º, inciso X, da Constituição Federal e artigos 244 e 245, ambos do Código de Processo Penal. A interceptação telefônica, por sua vez, demanda autorização judicial e o preenchimento dos requisitos previstos no artigo 2º da Lei n.º 9.296/1996. Por fim, a Lei do *Marco Civil da Internet* (Lei n.º 12.965/2014) estabelece a necessidade de autorização judicial para que se obtenha o conteúdo das comunicações armazenadas e também para o fornecimento de outros dados disponíveis em poder de prestadores de serviços, conforme artigo 10, § 2º e artigo 22, parágrafo único, do referido Diploma Legal.

Ademais, com o surgimento dos *smartphones*, dotados de expansionista capacidade de processamento e armazenamento de dados, ousa-se dizer que, no atual dinamismo das relações cotidianas[435], haveria uma maior exposição da privacidade e intimidade do cidadão caso os dados armazenados venham a ser revelados do que se o conteúdo de uma ligação telefônica instantaneamente capturada, ou os elementos possivelmente encontrados em uma busca e apreensão domiciliar, venham a ser expostos.

Não bastasse, dados eminentemente sigilosos e cujo acesso não prescinde de autorização judicial, tais como os de natureza financeira e fiscal[436], podem ser encontrados facilmente no acesso ao aparelho celular do cidadão. Em outras palavras, com o advento da era digital e a utilização de meios tecnológicos e imateriais para a guarda e armazenamento de dados, é senso comum que o acesso ao conteúdo de um aparelho poderá exteriorizar uma plêiade de informações que, de certa forma, somente seriam obtidas mediante prévia e fundamentada aquiescência judicial[437].

Neste cenário, vislumbra-se uma paradoxal discrepância legislativa, à medida que situações potencialmente danosas de violação à privacidade estariam sendo, na

---

[435] Não há como fechar os olhos para uma nova realidade no tocante à forma de comunicação do indivíduo. Por questões econômicas, de segurança e praticidade, as ligações telefônicas têm se tornado, paulatinamente, um meio de comunicação obsoleto, à medida que o dinamismo das relações humanas vem exigindo formas rápidas e instantâneas de contatos, por vezes entre várias pessoas ao mesmo tempo. Assim, uma mensagem de texto ou uma chamada de voz operacionalizada através de aplicativos populares como o *Whatsapp* substituíram o contato telefônico anteriormente mantido através da plataforma das operadoras de telefonia. Mas talvez o principal aspecto que indique a superlativa utilização de aplicativos seja a segurança trazida por intermédio da "*criptografia de ponta a ponta*", que assegura a privacidade dos interlocutores, de modo que a própria empresa não guarda registros das informações trocadas. Ademais, em uma perspectiva dos atores da criminalidade, é reconhecidamente um meio mais seguro para o planejamento e organização de empreitadas criminosas, diante da dificuldade operacional e técnica para a realização de interceptações telefônicas ou acesso à distância dos dados trocados.

[436] Os sigilos financeiro e fiscal encontram fundamento no artigo 5º, inciso X, da Constituição Federal (BELLOQUE, Juliana Garcia. *Sigilo Bancário: Análise Crítica da LC 105/2001.* São Paulo, Ed. Revista dos Tribunais: 2003, p. 77) e poderão ser afastados, respectivamente, nas hipóteses estabelecidas no artigo 1º, § 4º, da Lei Complementar n.º 105/2001 e artigo 198 do Código Tributário Nacional.

[437] Ricardo Gloeckner e Daniela Eilberg convidam à reflexão de que "(...) se o sigilo telefônico deve ser objeto de autorização judicial, mais afrontoso seria o acesso aos dados contidos no telefone móvel, pois nesses dispositivos estão congregadas as mais amplas e irrestritas ebulições e manifestações do direito à personalidade (cuja segmentação pode ser conferida nos aplicativos para celulares e em seus utilitários). No campo político criminal, em um país com mais telefones celulares do que pessoas, a permissão para que a polícia devasse e acesse sem restrições e autorização judicial o conteúdo dos aparelhos móveis equivaleria, no ponto, a esvaziar o direito à privacidade. Mandados de busca e apreensão de computadores, por exemplo, seriam medidas írritas, posto que a polícia poderia ter acesso livre ao computador perfectibilizado no telefone celular. Requerer uma autorização judicial para análise das contas de e-mail seria medida nula, posto que bastaria à polícia invadir o aparelho móvel
e verificar as correspondências do suspeito (...)" (GLOECKNER, Ricardo Jacobsen. EILBERG, Daniela Dora. *Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos.* Op.cit. p. 6).

prática, tuteladas de maneira mais branda e insuficiente que outras concretamente menos danosas à esfera de direitos e garantias individuais[438].

Como exemplo, se a interceptação telefônica é considerado meio verdadeiramente compressor de direitos fundamentais a ponto de exigir, por força legal e constitucional, a prévia autorização judicial e o preenchimento de qualificados requisitos legais para sua utilização, seria de incoerência sistêmica deixar de se exigir ao menos a análise dos elementos constitutivos da proporcionalidade para o acesso ao conteúdo dos aparelhos celulares, especialmente considerando que, nestas condições, os dados ali contidos espelham profunda e sensivelmente a personalidade do seu titular.

Ainda que a Lei n.º 12.965/2014 seja aplicável diretamente aos prestadores de serviços, seria incoerente deixar de estender a proteção conferida à privacidade e intimidade para outras situações de acesso a estes dados, independentemente de quem seja o responsável, onde estejam armazenados[439] e tampouco da forma implementada para o seu acesso. Vale dizer, os dados são pessoais e sigilosos, estejam ou não em poder de um terceiro prestador de serviços ou do próprio titular, a quem caberá decidir se tem intenção de expô-los.

Neste diapasão, se os provedores de serviço devem respeitar a privacidade, intimidade, honra e imagem do usuário da *internet* e dos serviços de telecomunicação, exigindo-se ordem judicial para que entreguem o conteúdo das comunicações privadas armazenadas em seus servidores, com maior razão esta interpretação

---

[438] ANTONIALLI, Dennys Marcelo; BRITO CRUZ, Francisco; VALENTE, Mariana Giorgetti. *Smartphones: treasure chests of the Lava-Jato investigation*. Disponível em: <https://www.internetlab.org.br/en/policy-watch/smartphones-treasure-chests-of-the-lava-jato-investigation/>. Acesso em: 20 de dezembro de 2020. Ao comentar o tratamento legal dispensado pela Lei n.º 12.965/2014 ao acesso às comunicações armazenadas, QUITO registra que a redação vaga do dispositivo acaba por permitir que extensos registros de comunicação passada sejam vasculhados para instruir investigações e processos de crimes punidos com detenção, além de procedimentos cíveis. Ainda, a autoria aponta mais uma situação paradoxal, uma vez que "(...) enquanto em tráfego, as mensagens trocadas são protegidas com rigor; no instante seguinte ao seu armazenamento – momento esse que sequer pode ser precisado – o rigor desaparece, viabilizando acesso praticamente irrestrito aos registros de conteúdos comunicados, desde que haja, para tanto, autorização judicial (...)" (QUITO, Carina. *As quebras de sigilo telemático no processo penal.* Op. cit. 179-180).

[439] Como bem destacam Maria Thereza Moura e Daniel Marchionatti, "(...) a proteção é aplicável independentemente do local em que os dados estão armazenados. Dados armazenados no dispositivo do usuário ou em nuvem – em servidores dos provedores de aplicação de internet – estão igualmente protegidos. Dispositivos ligados em redes internas ou mesmo sem conexão, como discos rígidos de computadores pessoais, 'pen drives' ou outras mídias portáteis, são igualmente invioláveis. Em parte, o Marco Civil da Internet e a legislação penal apenas desenvolvem sua defesa (...)" (MOURA, Maria Thereza Rocha de Assis; BARBOSA, Daniel Marchionatti. *Dados digitais: interceptação, busca e apreensão e requisição.* Op. cit., p. 487).

deve ser conferida para se balizar o acesso por autoridades em uma investigação processual penal, em que os direitos e garantias individuais se mostram ainda mais relevantes frente o poder persecutório estatal.

Desta feita, embora não haja segurança no tocante à aplicabilidade direta do artigo 7º, inciso III, da Lei n.º 12.965/2014, como marco legal, às hipóteses de acesso direto ao conteúdo das comunicações privadas por parte das autoridades investigativas, impende reconhecer uma nítida intenção legislativa, iniciada a partir do Marco Civil da *Internet* e posteriormente encampada na Lei Geral de Proteção de Dados (Lei n.º 13.709/2018), de estabelecer uma proteção adicional e relevante ao conteúdo destes dados, prevendo-se a autorização judicial prévia e fundamentada, como regra, para acesso ao conteúdo[440].

Sob quaisquer das vertentes que a questão venha a ser analisada, é inegável a necessidade de autorização judicial para o acesso ao conteúdo dos dados armazenados nos aparelhos celulares, ainda que se reconheça a inexistência de cláusula constitucional e legal expressas de reserva de jurisdição.

5.3.3.1. A autorização judicial para o acesso: o juízo de proporcionalidade

Uma vez exigida a autorização judicial, é necessário se analisar os requisitos a serem observados pelo julgador na apreciação do requerimento de acesso aos dados, sob pena da decisão não passar de uma mera formalidade facilmente transponível e desprovida de relevância e significação assecuratória de direitos fundamentais.

A apreensão de dados armazenados em suportes eletrônicos ou físicos que os contenham é evidente meio de obtenção que impõe, a certa medida, uma restrição ao

[440] GILMAR MENDES bem pontifica que "(...) a Lei n. 12.965/2014 consagra expressamente a inviolabilidade, salvo ordem judicial, dos dados armazenados – art. 7º, III. Por se tratar de uma lei voltada à regulamentação da internet, pode se argumentar que não há proteção contra a busca local no conteúdo do aparelho apreendido. Ainda que essa interpretação venha a prevalecer, o fato é que o legislador reconheceu de forma clara a importância dos dados informáticos armazenados para a privacidade. A leitura do art. 5º, X, da CF, tendo em vista, ainda, o disposto no art. 7º, III, da Lei n. 12.965/2014 recomenda que, em qualquer caso, a intromissão exija mandado judicial (...)" (MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de Direito Constitucional*. 13ª Edição, São Paulo: Ed. Saraiva, 2018, p. 609-610).

direito fundamental à privacidade e intimidade, assegurados no artigo 5º, inciso X e em diversas normativas internacionais.

Nesta perspectiva, WINTER destaca que:

> se exige que en la adopción de cualquier medida restrictiva de un derecho fundamental se cumpla el principio de proporcionalidad em sentido estricto (...) El principio de proporcionalidad, por consiguiente, actúa como un importante factor de corrección y limitación de la adopción de medidas restrictivas de derechos fundamentales (BACHMAIER WINTER, Lorena. *Investigación criminal y protección de la privacidad en la doctrina del Tribunal Europeo de Derechos Humanos*. In: 2º Congresso de Investigação Criminal. Coordenação: Maria Fernanda Palma, Augusto Silva Dias e Paulo de Sousa Mendes. Lisboa: Almedina, 2010, p. 173).

Ademais, todas as normativas previamente mencionadas, utilizadas analogicamente como referência para se estabelecer um procedimento legal para o acesso aos dados, exigem a observância da proporcionalidade[441].

GUSTAVO TORRES SOARES destaca que os pressupostos para análise da proporcionalidade passam, necessariamente, pela constatação da previsão legal da medida; a finalidade pública constitucionalmente legítima; a fundamentação; e o satisfatório controle jurídico, o qual deverá ser judicial em situações especialmente invasivas[442].

Sob a perspectiva da legalidade, infere-se que a medida não constitui, propriamente, uma inovação legislativa. Com efeito, sempre se teve por permitida a realização de buscas e apreensões de computadores, *notebooks*, servidores e outros instrumentos de armazenamento massivo de dados. O aparelho celular não deixa de ser uma forma assemelhada de microcomputador, cujos dados podem ser acessados em um procedimento regular de busca.

---

[441] ALEXY, Robert. *Teoria dos direitos fundamentais.* 2ª edição, São Paulo: Editora Malheiros, 2015, p. 588.
[442] SOARES, Gustavo Torres. *Investigação criminal e inovações técnicas e tecnológicas: perspectivas e limites.* Tese (Doutorado em Direito Processual Penal) - Faculdade de Direito da Universidade de São Paulo. São Paulo, SP, 2014, p. 272.

A finalidade pública do acesso é constitucionalmente legítima, à medida que as facilidades tecnológicas dos modernos *smartphones* são utilizadas para a perpetração de diversos crimes. Nesta ordem, a tutela do interesse público, representada no dever de resguardo à segurança pública e projetada na imprescindibilidade de uma investigação criminal eficiente, constitui interesse passível de cotejo na perspectiva da proporcionalidade.

De igual sorte, a fundamentação é dever constitucional previsto no artigo 93, inciso IX, da Constituição Federal e deverá ser exercido pelo julgador, permitindo-se o controle intrínseco e extrínseco de sua decisão[443] e tornando-a como meio garantidor de proteção ao interesse público e, ao mesmo tempo, assegurador de direitos e garantias fundamentais.

O afastamento do sigilo dos dados armazenados no aparelho celular também demanda a presença de *fumus boni iuris* e o *periculum in mora,* além da observância do princípio da proporcionalidade e de seus requisitos.

Para se estabelecer o *fumus boni iuris,* a doutrina tem se valido de uma interpretação analógica com os requisitos trazidos pela legislação infraconstitucional, no tocante à concessão da interceptação telefônica. Dispõe o artigo 2º, inciso I, da Lei n.º 9.296/1996, que a interceptação somente será deferida quando houver indícios razoáveis de autoria ou participação, requisito que se estende, por consectário lógico, à hipótese do afastamento do sigilo dos dados armazenados nos aparelhos celulares.

Assim, o *fumus boni iuris* estaria preenchido com a necessidade de se observar a existência de indícios mínimos de autoria ou participação. Alguns autores, por sua vez, tratam essa exigência sob o manto da *"justa causa"*[444].

No tocante ao *periculum in mora*, trata-se de requisito que, geralmente, não é exigível considerando a própria natureza do meio de produção de prova em questão. A bem da verdade, salvo em situações excepcionais a serem melhor exploradas

[443] GOMES FILHO, Antônio Magalhães. *A motivação das decisões penais.* São Paulo: Revista dos Tribunais, 2001.
[444] BELLOQUE, Juliana Garcia. *Sigilo Bancário:* p. 899-100.

adiante, não há que se cogitar na urgência para a medida, porquanto os dados a serem obtidos estarão armazenados e preservados no aparelho celular, sendo acessíveis a qualquer tempo desde que estejam acautelados de quaisquer intromissões externas.

Com a obediência destes pressupostos, parte-se para a análise dos requisitos integrativos que permitem aferir a proporcionalidade, consistente no reconhecimento concomitante da: (a) motivação do ato impugnado; (b) pertinência temática com o que se investiga; (c) necessidade absoluta da medida, no sentido de que o resultado por apurar não possa advir de nenhum outro meio ou fonte lícita de prova, e (d) limitação temporal do objeto da medida"[445].

A proporcionalidade, como critério balizador do julgamento, deve ser analisada à luz dos requisitos da idoneidade, necessidade e proporcionalidade em sentido estrito, tanto em uma perspectiva de proteção positiva quanto naquela relacionada à proibição da proteção deficiente[446].

A "idoneidade" ou "adequação" da medida está relacionada a um juízo abstrato, de constatação se a busca dos dados estanques tem a aptidão de atingir a finalidade investigativa pretendida e for condizente com esta[447]. Assim, é imprescindível verificar se a medida será adequada para se chegar à finalidade investigativa proposta.

---

[445] Supremo Tribunal Federal (STF), Medida Cautelar no Mandado de Segurança n.º 25.966/DF, Relatoria Ministro Cezar Peluso, julgado em 17 de maio de 2006, DJ 22/05/2006, pp-00023, RDDP n.º 40, p. 189-191.

[446] Como leciona MOUGENOT BONFIM: "(...) a outra modalidade do princípio da proporcionalidade - esta praticamente desconhecida na doutrina e jurisprudência nacionais - é a da 'proibição da proteção deficiente' ou princípio da Infraproteção (*Untermassverbot*, dos alemães), pela qual se compreende que, uma vez que o Estado se compromete pela via constitucional a tutelar bens e valores fundamentais (vida liberdade, honra etc.), deve fazê-lo obrigatoriamente na melhor medida possível. Desse modo, assegura-se não somente uma garantia do cidadão perante os excessos do Estado na restrição dos direitos fundamentais (princípio da proibição de excesso) - a chamada 'proteção vertical', na medida em que os cidadãos têm no princípio da proporcionalidade (modalidade proibição de excesso) um anteparo constitucional contra o poder do Estado (verticalizando, portanto, 'de cima para baixo') - mas também uma garantia dos cidadãos contra agressões de terceiros - 'proteção horizontal' -, no qual o Estado atua como garante eficaz dos cidadãos, impedindo tais agressões (tutelando eficazmente o valor "segurança", garantido constitucionalmente) ou punindo os agressores (valor 'justiça' assegurado pela Constituição Federal). Dessa forma, pelo 'princípio da proibição da infraproteção', toda atividade estatal que infringi-lo seria nula, ou seja, inquina-se o ato jurídico violador do princípio com a sanção de nulidade (...)" (BONFIM, Edilson Mougenot. *Curso de Processo Penal*. São Paulo: Editora Saraiva, 2012, p. 103/104).

[447] FERNANDES, Antônio Scarance. *O sigilo financeiro e a prova criminal*. In "*Direito Penal, Processo Penal e Direitos Fundamentais. Uma visão Luso-brasileira*", p.457/477, 2006, p. 473.

O segundo requisito, relacionado à "necessidade", está consubstanciado na obrigação de que o afastamento do sigilo e, por conseguinte, a busca aos dados armazenados, enquanto atenuação da proteção constitucional à intimidade, seja utilizada como *ultima ratio* no amplo rol de ferramentas investigativas disponíveis, a fim de que outras menos invasivas ou restritivas sejam veiculadas antes da própria medida invasiva[448]. Há uma relação direta com o artigo 2º, inciso II, da Lei n.º 9.296/1996, que estabelece que a interceptação telefônica não será admitida quando houver outros meios para a produção da prova pretendida.

Finalmente, o terceiro requisito é o da "proporcionalidade em sentido estrito", que se relaciona à ponderação casuística entre a profundidade e extensão dos valores envolvidos, notadamente a proteção à intimidade e os benefícios oriundos da utilização da medida investigativa[449]. Mais uma vez, possível traçar uma relação com o artigo 2º, inciso III, da Lei n.º 9.296/1996, que estabelece a inadmissibilidade da interceptação telefônica quando o fato investigado constituir infração penal punida, no máximo, com pena de detenção[450].

---

[448] O Supremo Tribunal Federal, no julgamento da Medida Cautelar no Mandado de Segurança n.º 25.812/DF (DJ 23/02/2006), assentou os requisitos para a quebra do sigilo financeiro, os quais podem ser perfeitamente aplicáveis à quebra do sigilo dos dados armazenados em aparelhos celulares: "(...) ao lado dos requisitos da motivação (a) e da pertinência temática com o que se investiga (b), outros de não menor peso. Um deles é a necessidade absoluta da medida (c), no sentido de que o resultado por apurar não possa advir de nenhum outro meio ou fonte lícita de prova. Esta exigência é de justificação meridiana, suscetível de ser entendida por toda a gente, pela razão óbvia de que não se pode sacrificar direito fundamental tutelado pela Constituição - o direito à intimidade -, mediante uso da medida drástica e extrema da quebra de sigilos, quando a existência do fato ou fatos sob investigação pode ser lograda com recurso aos meios ordinários de prova. Restrições absolutas a direito constitucional só se justificam em situações de absoluta excepcionalidade. O outro requisito é a existência de limitação temporal do objeto da medida (d), enquanto predeterminação formal do período que, constituindo a referência do tempo provável em que teria ocorrido o fato investigado, seja suficiente para lhe esclarecer a ocorrência por via tão excepcional e extrema (...)". De igual sorte, confira-se: STF, AC 3872 AgR/DF, Pleno, rel. Min. Teori Zavascki, julgamento em 22/10/2015, DJe-13/11/2015.

[449] FERNANDES, Antônio Scarance. *Processo penal constitucional.* Op. cit. 57-64.

[450] Gilmar Mendes e Paulo Gonet Branco sustentam que "(...) a quebra de sigilo de dados informáticos somente é tolerável para produzir prova em um caso concreto. Ainda assim, há de reconhecer que os marcos legislativos deveriam ser mais precisos. Não obstante o significativo avanço representado pela proteção expressa pela Lei n.º 12.965/2014, a nova lei deixou de especificar os requisitos a serem observados na autorização judicial de acesso a dados armazenados. Parece claro que pode ser inferido do sistema que o juízo de admissibilidade da medida deve ser baseado na ponderação entre a relevância da prova e a gravidade da intromissão na privacidade que ela representa. Uma medida tão invasiva dificilmente seria cabível num caso cível. Mesmo em casos criminais, não se imagina sua aplicação a infrações penais de menor potencial ofensivo. Um bom parâmetro, quanto à gravidade do fato, é a exigência de cominação de reclusão, por analogia ao estabelecido para as interceptações telemáticas (...)" (MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de Direito Constitucional*. 13ª Edição, São Paulo: Ed. Saraiva, 2018, p. 609).

Nesta ordem de ideias, encampa-se a sugestão proposta por MARIA THEREZA ROCHA DE ASSIS MOURA e DANIEL MARCHIONATTI BARBOSA, elencando os requisitos para a quebra do sigilo de dados armazenados:

> a) prova da existência de crime punido com reclusão;
> b) indícios de responsabilidade pelo ilícito, pelo titular dos dados. Muito excepcionalmente, pode-se cogitar da adoção da medida contra terceiros, como a vítima falecida;
> c) identificação, o mais precisa possível, dos dados a serem buscados ou requisitados;
> d) impossibilidade de obter a prova por outro meio menos gravoso;
> e) adequação da medida para provar o fato a ser apurado;
> f) proporcionalidade em sentido estrito da medida, lavando em conta, especialmente, o custo aos direitos individuais que a ela representa
> (MOURA, Maria Thereza Rocha de Assis; BARBOSA, Daniel Marchionatti. *Dados digitais: interceptação, busca e apreensão e requisição.* In: LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro. LAUX, Francisco de Mesquita; RAVAGNANI, Giovani dos Santos. Direito, processo e tecnologia. São Paulo: Editora RT, 2020, p. 489-491)[451]

Nota-se que a exigência de que os crimes sejam apenados com reclusão é emprestado, por analogia, do artigo 2º, inciso III, da Lei n.º 9.296/1996. Trata-se de exigência ponderada e racional, uma vez que o acesso aos dados estanques, medida invasiva dos direitos à personalidade e intimidade, não pode ser razoavelmente admitida para a investigação de crimes dotados de baixa ofensividade e periculosidade, o que feriria um juízo abstrato de proporcionalidade.

[451] Os autores arrematam que "(...) os dados armazenados são muito protegidos pelo direito – ainda que um pouco menos do que o fluxo telemático. Dados armazenados correspondem ao conteúdo das comunicações e da produção humana, pelo que sua aquisição pode ser muito custosa à privacidade e à intimidade. A quebra do sigilo somente pode ocorrer com autorização judicial, amparada em juízo de proporcionalidade – o custo da medida aos direitos fundamentais pode ser suportado apenas no interesse da apuração de ilícitos graves. Na falta de uma legislação específica, deve-se observar, por analogia, as normas quanto a busca e apreensão, interceptação telemática e quebra de sigilo de dados de registro. A quebra de sigilo de dados armazenados não pode ocorrer no interesse da apuração de ilícitos civis ou de delitos leves. A execução da ordem judicial pode ser feita pelos próprios policiais, mediante busca e apreensão de dados, ou mediante requisição a terceiros que sobre eles tenham controle – normalmente, provedeores de aplicações de internet (...)".

Ainda que não mencionado expressamente pelos autores, o exame da proporcionalidade recomenda que a decisão judicial estabeleça, se possível, um lapso temporal limite para a busca dos dados produzidos e armazenados, que deverão ser vasculhados apenas dentro período específico.

Com efeito, não seria proporcional e tolerável uma devassa completa e atemporal dos dados arquivados no aparelho celular, sob pena de indevida e desnecessária exposição da privacidade e intimidade do cidadão quando a necessidade legítima da investigação dos atos ilícitos demande o acesso a dados em determinado período específico[452].

Portanto, conclui-se que, a partir das referências[453] estabelecidas em normativas utilizadas por analogia (*v.g.*, busca e apreensão; interceptação telemática; e a Lei n.º 12.965/2014), o acesso aos dados estanques contidos em aparelhos celulares exige a presença concomitante[454] dos seguintes requisitos: *a)* indícios de autoria ou participação; *b)* a adequação da medida para a prova pretendida, especialmente diante da natureza do crime investigado, que deve ser punido com reclusão; *c)* a necessidade da prova para a apuração dos fatos e a formação do arcabouço probatório; *d)* a proporcionalidade com relação ao período de abrangência dos dados a serem coletados e fornecidos, todos reconhecíveis em decisão judicial devidamente fundamentada e motivada.

---

[452] O Supremo Tribunal Federal, no julgamento da Medida Cautelar no Mandado de Segurança n.º 25.812/DF (DJ 23/02/2006), exigiu a fixação de um período delimitado para a quebra do sigilo financeiro, raciocínio que pode ser estendido para o afastamento da proteção conferida aos dados armazenados em aparelhos celulares. De igual sorte, confira-se: STF, AC 3872 AgR/DF, Pleno, rel. Min. Teori Zavascki, julgado em 22 de outubro de 2015, DJe 13/11/2015; STF, Agravo Regimental no *Habeas Corpus* n.º 170.376/SP, 1ª Turma, Rel. Min. Rosa Weber, julgado em 9 de junho de 2020, DJe 23/06/2020).

[453] Igualmente, a análise da proporcionalidade é invocada de maneira implícita no artigo 22, parágrafo único, da Lei n.º 12.965/2014, o qual estabelece que o requerimento para que sejam fornecidos registros de conexão ou de acesso a aplicações de internet deverão conter: I - fundados indícios da ocorrência do ilícito; II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e III - período ao qual se referem os registros.

[454] O Superior Tribunal de Justiça (STJ), em apreciação a uma hipótese de quebra do sigilo do correio eletrônico, deliberou que a medida demandaria a análise da proporcionalidade, mediante reconhecimento de indícios de autoria; da ocorrência do fato ilícito investigado; a comprovação de sua imprescindibilidade, como meio de obtenção de prova em detrimento de outros menos invasivos; sua relação com os fatos apurados; a delimitação de um período proporcional, "moderado, justo e racionalmente compreensivo" dos dados a serem coletados e fornecidos; e uma ordem judicial suficientemente fundamentada e motivada (artigo 93, inciso IX, da Constituição Federal) (STJ, *Habeas Corpus* n.º 315.220-RS, 6ª Turma, Rel. Ministra Maria Thereza Rocha de Assis Moura, julgado em 15 de setembro de 2015, DJe 09/10/2015)

5.4. O acesso a dados armazenados em aparelhos celulares, durante as abordagens policiais

A discussão relacionada à imprescindibilidade de autorização judicial para acesso aos dados armazenados ocupou a pauta dos tribunais, especialmente diante de uma situação corriqueira: a praxe adotada por policiais de, durante as abordagens realizadas em patrulhamento ostensivo, analisarem o conteúdo dos aparelhos celulares encontrados em poder dos acusados, especialmente após a constatação de um crime praticado.

Tal como se verá adiante, a insuficiência legislativa no tratamento do tema, aliado a uma jurisprudência vacilante, trouxeram insegurança e motivaram o enfrentamento do tema perante a Suprema Corte, em decisão dotada de repercussão geral[455].

A análise do tema exige o estabelecimento de uma linha distintiva com relação ao momento da abordagem policial e as repercussões jurídicas que se sucedem.

5.4.1 Acesso aos dados armazenados durante a busca pessoal, sem a prévia constatação da situação flagrancial

A busca pessoal[456] está prevista nos artigos 240, § 2º, 244 e 249, todos do Código de Processo Penal, bem como deve observar as disposições constitucionais relativas à proteção da privacidade, intimidade e vida privada (artigo 5º, inciso X, da Constituição Federal), à proibição e tratamento desumano ou degradante na execução do ato (artigo 5º, inciso III, da Carta Constitucional) e o respeito, aos presos, à integridade física e moral (artigo 5º, inciso XLIX, da Constituição Federal).

Para a busca pessoal, o artigo 240, § 2º, do Código de Processo Penal exige que a medida seja realizada sempre que houver "fundada suspeita"[457] de que alguma

---

[455] STF, Repercussão Geral no RE com Agravo n.º 1.042.075/RJ, Rel. Min. Dias Toffoli, julgado em 23 de novembro de 2017, DJe 12/12/2017.

[456] Trata-se da hipótese de revista corporal realizada no corpo da pessoa abordada e também em seus bolsos, vestimentas, bolsas, malas, etc, que denotem uma relação de porte e conexão por contato direto com o suspeito (GRASSI, Roberto Joacir. *Busca e apreensão (Processo Penal).* Enciclopédia Saraiva do Direito. São Paulo: Saraiva, 305, 1978., v. 12, p. 306, *apud* PITOMBO, Cleunice Valentim Bastos. *Da Busca e da Apreensão no Processo Penal*. Op. cit. p. 128; MIRABETE, Júlio Fabbrini, *Processo Penal*, 18ª edição, São Paulo: Editora Atlas, 2008, p. 323)

[457] A "fundada suspeita" é uma expressão dotada de ampla vagueza e indeterminação (BADARÓ, Gustavo Henrique Righi Ivahy. *Processo Penal*. Op. cit., p. 587-588; LOPES JR., Aury. *Direito Processual Penal.* Op. cit, p. 574), trazendo elevado grau de subjetivismo. Registre-se que a fundada suspeita não se contenta com o

pessoa oculte consigo uma arma proibida e, ainda, para as finalidades e objetivos indicados no artigo 240, § 1º, alíneas *b, c, d, e,* e *f*), além da colheita de qualquer elemento de convicção (artigo 240, § 1º, alínea *h*). Nestas hipóteses, poderá ser expedida uma ordem judicial autorizativa da busca pessoal realizada.

Entretanto, o artigo 244 prevê exceções à necessidade de mandado judicial, autorizando-se a busca pessoal quando houver prisão ou "fundada suspeita" de que a pessoa esteja na posse de arma proibida ou objetos ou papéis que constituam corpo de delito, ou quando a medida for determinada no curso de busca domiciliar.

A busca pessoal por "fundada suspeita", juízo de cognição formulado pelos policiais no momento da abordagem, pode evoluir para uma autuação em flagrante delito (*v.g.*, com a localização de arma de fogo sem autorização ou de entorpecentes em posse do abordado). Todavia, é também possível que, após a abordagem e busca pessoal por

---

simples estado anímico e subjetivo do agente, lastreado em arbitrárias impressões pessoais que poderiam, inevitavelmente, estar consciente ou inconscientemente apegadas aa estigmas relacionados à raça, condição social, religião, sexo e pobreza (ACILA, Carlos Roberto. *Criminologia e estigmas – um estudo sobre os preconceitos*. 4. ed. São Paulo: Atlas, 2015. p. 23, *Apud*, NETO, Francisco Alves Cangerana. *Meios de Obtenção de Prova no Processo Penal*, Juruá Editora, 2018, p. 30). Ao revés, a suspeita deve estar suficientemente fundamentada em elementos e fatos de que a autoridade disponha antes da realização da busca, ainda que, posteriormente, se verifique que a suposição não corresponda à realidade (PITOMBO, Cleunice Valentim Bastos. *Da Busca e da Apreensão no Processo Penal*. Op. cit. p. 138).
Para parte da doutrina, o requisito seria similar à *probable cause* do direito norte-americano (GOMES FILHO, Antonio Magalhães. *Notas sobre a terminologia da prova.* Op. cit. p. 312; DEZEM, Guilherme Madeira. *Curso de processo penal*. Op. cit. p. 791), embora alguns sustentem que estaria situada entre a "preponderância de provas" e a "prova clara e convincente" (MARQUES, Pedro Campanholo. *Busca e apreensão: juízo de admissibilidade.* Florianópolis: Ed. Tirant Lo Blanch, 2019, p. 240). Todavia, analisando os regimes jurídicos brasileiro e norte-americano, conclui-se que a busca pessoal, no cenário nacional, não exigiria os qualificados requisitos jurídicos da *probable cause.* Rolando V. Del Carmen aponta que a "(...) probable cause compared to other levels of proof: probable cause is lower in certainty than clear and convincing evidence but higher than reasonable suspicion (…)", sendo que a "reasonable suspicion", por sua vez, "(…) is lower in certainty than probable cause but higher than mere suspicion (…)". Portanto, no cenário norte-americano, Carmen estabelece uma relação comparativa entre a *probable cause* e a *reasonable suspicion*, apontando que para a busca pessoal realizada em uma abordagem policial (*stop and frisk*), com a eventual revista pessoal para segurança do policial, bastaria a *reasonable suspicion,* sendo desnecessária a *probable cause*, salvo para eventuais medidas de constrição à liberdade física (CARMEN, Rolando V. Del. *Criminal procedure Law and Practice*, Wadsworth Publishing; 8 edition, p. 86-88. Importante destacar que a busca pessoal prevista no artigo 244 do Código de Processo Penal, embora guarde relação com a *stop and frisk* norte-americana, com ela não se confunde (SOUSA, Marllon. *Busca Pessoal v. Stop and Frisk: um breve exame sobre a abordagem policial de rua no Brasil e nos EUA*. Revista Brasileira de Ciências Criminais, vol. 151/2019, jan./2019, p. 317-343). Portanto, diante da limitação atinente à amplitude da busca e revista pessoais, a jurisprudência norte-americana tem se contentado com a *reasonable suspicion* para a medida de *stop and frisk*, conforme decisão adotada no caso *Terry v. Ohio, 392 U.S. 1 (1968)* (Disponível em <https://supreme.justia.com/cases/federal/us/392/1/>. Acesso em: 20 de dezembro de 2020)

"fundada suspeita", não se vislumbrem elementos flagranciais, especialmente quando nenhum material ilícito é localizado.

Nestas situações, em que havia a "fundada suspeita" mas, por qualquer razão, não se identificou a prática de um fato criminoso que demandasse um ato flagrancial, perquire-se a possibilidade de os policiais realizarem, sem o consentimento do abordado, a busca do conteúdo do seu aparelho celular.

Se não há qualquer crime sendo praticado pela pessoa abordada, o acesso direto aos dados encontrados no aparelho celular constitui injustificável afronta à privacidade e intimidade do abordado, nos termos do artigo 5º, inciso X, da Constituição Federal. Nesta linha, a consulta compulsória dos dados armazenados em aparelhos celulares ou sua apreensão, antes mesmo da constatação de um crime em estado flagrancial, é evidente caracterização da reprovável prática do *fishing expedition*[458], verdadeiras investigações genéricas, randômicas e especulativas, sem qualquer motivação concreta e destinada à captura prospectiva de elementos incriminatórios aleatórios, desprovidos de embasamento prévio.

A 2ª Turma do Supremo Tribunal Federal (STF) reconheceu a ilicitude das provas obtidas mediante acesso a conversas registradas no aplicativo *WhatsApp*, a partir da apreensão do celular antes mesmo da comprovação da situação flagrancial, com posterior ingresso em domicílio sem autorização judicial[459].

---

[458] A utilização da *fishing expedition*, também chamada de "efeito hidra" (SCHÜNEMANN, Bernd. *La Reforma del Proceso Penal*. Madrid: Dykinson, 2005, p. 33), é medida ilegal, conforme jurisprudência da Corte Suprema: STF, HC n.º 163.461/PR, 2ª Turma, Rel. Min. Gilmar Mendes, julgado em 5 de fevereiro de 2019, DJe 03/08/2020; STF, RE n.º 1.055.941, Rel. Min. Dias Toffoli, julgado em 4 de dezembro de 2019, DJe 06/10/2020; STF, Inq n.º 4.831/DF, decisão do Min. Celso de Mello, 5 de maio de 2020.

[459] Conforme se infere do histórico do caso submetido à apreciação da Corte Suprema, policiais acessaram o aparelho celular de uma pessoa abordada antes mesmo da comprovação da situação flagrancial, ocasião em que, a partir da análise dos dados armazenados no aparelho, logrou-se descobrir que havia drogas guardadas em uma residência, motivando-se a apreensão e a subsequente prisão em flagrante do indivíduo abordado. O Ministro relator Gilmar Mendes apontou a necessidade de se revisitar a clássica distinção relacionada à inviolabilidade dos dados e da comunicação propriamente dita, bem como apontou que o avanço normativo - especialmente decorrente do artigo 7º, inciso III, da Lei n.º 12.965/2014 - bem como o desenvolvimento de mecanismos de comunicação e armazenamento de dados pessoais em smartphones e telefones celulares, motivaram a alteração de seu posicionamento no Habeas Corpus n.º 91.867/PA, sinalizando que o acesso aos dados contidos em aparelhos celulares é possível, desde que condicionado a prévia decisão judicial (STF, Habeas Corpus n.º 168.052/SP, 2ª Turma, Rel. Min. Gilmar Mendes, julgado em 9 de outubro de 2020).

Entretanto, há precedentes de Tribunais Estaduais admitindo a possibilidade do acesso aos dados armazenados em aparelhos celulares nestes casos, independentemente de autorização judicial.

Em um avançado trabalho estatístico[460] a partir da análise de jurisprudência dos tribunais estaduais[461], os pesquisadores identificaram, em acórdãos analisados a partir de 2017, ao menos quatro tipos-padrões de acesso de policiais a celulares, que suscitariam discussões acerca da prova[462]. Porém, apenas dois deles mereceram especial atenção do trabalho metodológico: o acesso policial a dados armazenados em celular durante abordagens policiais, antes da configuração do flagrante; e o acesso policial a dados armazenados em celular, após a constatação da efetiva situação flagrancial.

O resultado das pesquisas revela que a jurisprudência das Cortes Estaduais ainda vacila com relação à admissibilidade do acesso, sem autorização judicial, a dados armazenados em aparelhos celulares.

Especificamente no tocante ao acesso aos dados antes da configuração efetiva da situação flagrancial, constatou-se que a jurisprudência estadual é francamente dividida no tocante à admissibilidade da prova. Assim, em 50% dos casos a prova foi

---

[460] ABREU, Jacqueline de Souza ; ANTONIALLI, Dennys Marcelo; MASSARO, Heloisa Maria Machado. LUCIANO, Maria. *Acesso de autoridades policiais a celulares em abordagens e flagrantes: retrato e análise da jurisprudência de tribunais estaduais.* In: Revista Brasileira de Ciências Criminais, vol. 154/2019, p. 177-214, abril/2019.

[461] Extrai-se da metodologia do trabalho divulgada pelos autores que foram realizadas pesquisas nos Tribunais de Justiça do Amazonas, Roraima, Rio Grande do Norte, Rio Grande do Sul, Paraná, Ceará, Mato Grosso do Sul, Goiás, Rio de Janeiro e São Paulo.

[462] Como destacam os pesquisadores, "(...) na categoria (i) de 'acesso policial durante abordagens', acarretando prisão em flagrante, foram catalogados os casos nos quais o acesso ao celular se deu em meio a abordagem policial sem que, anteriormente, houvesse sido apurado ou apreendido quaisquer elementos sugestivos da prática de crime, de modo que os dados consultados no aparelho foram decisivos para a consequente configuração do crime e/ou prisão em flagrante. Na categoria (ii) de 'acesso policial após flagrante delito' foram catalogadas todos os acórdãos em que o acesso ao celular ocorreu associado à configuração da situação de flagrante delito (e à consequente prisão em flagrante), tal como definida no Código de Processo Penal (LGL\1941\8): agente está cometendo infração ou acaba de cometê-la; é perseguido em situação que faça presumir ser autor de infração; ou é encontrado, logo depois, com instrumentos, armas, objetos ou papéis que levem à presunção de autoria. Assim, incluímos nessa categoria os casos em que o acesso aos celulares se deu após a verificação ou apreensão pelos policiais de qualquer elemento considerado como indicativo de prática de crime – sejam documentos falsos usados para estelionato ou, ainda, pequena quantidade de drogas –, ainda que isso tenha derivado, inicialmente, de abordagem (...)" (ANTONIALLI, Dennys Marcelo. ABREU, Jacqueline de Souza. MASSARO, Heloisa Maria Machado. LUCIANO, Maria. *Acesso de autoridades policiais a celulares em abordagens e flagrantes: retrato e análise da jurisprudência de tribunais estaduais.* Op. cit. p. 6).

considerada lícita e, na mesma proporção percentual, o acesso e as provas decorrentes foram reputados ilícitos.

5.4.2. Acesso aos dados armazenados durante a busca pessoal incidental à prisão em flagrante

O acesso ao conteúdo dos aparelhos celulares ganha outra perspectiva quando a apreensão e busca dos dados é realizada de maneira incidental a uma prisão em flagrante.

O componente adicional é, indiscutivelmente, o flagrante delito, medida de urgência formada por atos complexos e de natureza precautelar[463], com posterior jurisdicionalização, cujo objetivo é impedir a prática criminosa, deter o seu autor e tutelar a prova da ocorrência do crime e sua autoria[464].

A situação de flagrante delito, diante da violação à ordem proibitiva legal por parte do acusado, permite a restrição de direitos e garantias individuais a ele inerentes[465], autorizando-se a prisão ou o ingresso em domicílio, independentemente de prévia autorização judicial[466].

Nesta linha, perquire-se se, dentre estes direitos e garantias fundamentais relativizados pela situação flagrancial, estaria a possibilidade de se mitigar a privacidade e intimidade da pessoa detida, assegurando-se acesso direto e imediato ao conteúdo dos dados armazenados no aparelho celular.

---

[463] LOPES JR., Aury. *Direito Processual Penal.* São Paulo: Saraiva, 2020, p. 651.
[464] BADARÓ, Gustavo Henrique Righi Ivahy. *Processo Penal*, Op. cit., p. 1154.
[465] Como bem destaca Zilli, "(...)a situação em flagrante confere ao Estado legitimidade de reação imediata a qual se concretiza com a possibilidade de restrição de direitos fundamentais, independentemente de prévia ordem judicial. A prisão e o ingresso domiciliar são os exemplos mais eloquentes. É que o ataque frontal e atual ao mandamento proibitivo justifica a restrição de importantes direitos, o que, diga-se, é próprio de um regime que preconiza o convívio entre as liberdades. Assim, a pronta restrição da liberdade reforça as mensagens de imperatividade da lei e da eficácia do sistema que outorga ao Estado o monopólio do uso legítimo da violência. A relativização da inviolabilidade domiciliar marcada pelo contexto do flagrante delito viabiliza não só a interrupção da prática delituosa, com a preservação de direitos de eventual vítima, como possibilita a obtenção, desde já, de elementos de prova que confiram justa causa às medidas persecutórias. Soa racional, portanto, que da prisão em flagrante decorram a busca e a apreensão de objetos, de instrumentos ou de quaisquer outros bens relacionados com a prática delituosa (...)" (ZILLI, Marcos Alexandre Coelho. *A prisão em flagrante e o acesso de dados em dispositivos móveis. Nem utopia, nem distopia. Apenas a racionalidade.* Op. cit., p. 68).
[466] Conforme exceção constitucional prevista no artigo 5º, inciso X, da Constituição Federal.

Em uma primeira vertente interpretativa, tem-se admitido a possibilidade do acesso aos referidos dados[467]. Para tanto, sustenta-se que a tutela da privacidade e intimidade não encontra qualquer cláusula legal ou constitucional de reserva de jurisdição[468], uma vez que os dados armazenados estariam sujeitos à tutela do artigo 5º, inciso X, da Constituição Federal, porquanto são dados estanques e já comunicados.

Deste modo, se a situação flagrancial autorizaria até mesmo o ingresso policial em domicílio, expoente físico e perspectivo da intimidade do cidadão, não seria razoável se estabelecer restrições ao acesso dos dados armazenados em aparelhos celulares, sob pena de se estabelecer proteção mais efetiva ao aparelho do que à própria moradia[469].

Não bastasse, para os que assumem a necessidade de uma ressignificação do conceito de domicílio[470], para nele se incluir os aparelhos celulares, o flagrante delito configura uma das hipóteses excepcionais que autorizariam a dispensa de ordem judicial.

O Superior Tribunal de Justiça (STJ), no Habeas Corpus n.º 66.368-PA[471], reconheceu que não configuraria quebra indevida do sigilo telefônico a análise das últimas ligações feitas e recebidas pelos celulares apreendidos, ainda que sem autorização judicial, fundamentando-se no dever da autoridade policial de apreender os objetos que tiverem relação com o fato.

---

[467] Neste sentido é o parecer da Procuradoria Geral da República, nos autos do Recurso em *Habeas Corpus* n.º 90.200/RN, do Superior Tribunal de Justiça, disponível em http://www.mpf.mp.br/pgr/documentos/TREnoRHC90200TraficoLicitudedaprovaAcessodadoscelularaplicativosmensagemearmazenamentoquandodoflagrante.pdf. Acesso em: 20 de dezembro de 2020; BARRETO, Alesandro Gonçalves; ALMEIDA, Everton Ferreira de. *Perícia em celular: necessidade de autorização judicial?* Revista Direito & TI, Porto Alegre, 04.06.2016. Disponível em: <http://direitoeti.com.br/artigos/pericia-em-celular-necessidade-de-autorizacao-judicial>. Acesso em: 20 de dezembro de 2020; SANNINI NETO, Francisco. *Dados de telefone celular apreendido podem ser vasculhados em investigação criminal*. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 21, n. 4762, 15 de julho de 2016. Disponível em: <https://jus.com.br/artigos/40053/investigacao-criminal-e-os-dados-obtidos-de-aparelhos-de-celular-apreendidos>. Acesso em: 20 de dezembro de 2020; SOUZA, Rodrigo Telles de. *A exigência de autorização judicial para acesso ao conteúdo de telefone móvel apreendido: uma ampliação da garantia à inviolabilidade domiciliar incompatível com o sistema jurídico brasileiro.* Op. cit., p. 423-424.

[468] Vide subtópicos 5.1.2 e 5.1.3.

[469] Conforme bem expôs o Ministro Gilmar Mendes, relator do *Habeas Corpus* n.º 91.867/PA, se a "(...) própria liberdade sofre restrição no flagrante delito. Um aparelho de celular receberia proteção diversa? (...)". No mesmo sentido: MAGALHÃES, Vlamir Costa. Ilicitude probatória em processo penal e regra de exclusão (*exclusionary rule*): comentários sobre a legitimidade do acesso a aparelhos eletrônicos apreendidos em situação flagrancial. Direito Federal: Revista da AJUFE. São Paulo, v. 31, n. 97, jan./jun. 2019, p. 547.

[470] Vide subtópico 5.3.1.2.

[471] STJ, HC n.º 66.368/PA, 5ª Turma, Rel. Gilson Dipp, julgado em 5 de junho de 2007, DJ 29/06/2007.

De igual sorte, em 2013, a mesma Corte reconheceu que a análise do conteúdo gravado na memória de computadores e aparelhos celulares não se confunde com a interceptação das comunicações telefônicas ou a interceptação de comunicações em sistemas de informática e telemática, o que tornaria prescindível a autorização judicial para análise da caixa de mensagens de texto contidas na memória interna do aparelho[472].

Partilhando deste entendimento, o Supremo Tribunal Federal (STF), por intermédio de sua 2ª Turma, admitiu a legalidade do acesso realizado por policiais aos registros telefônicos de chamadas efetuadas e recebidas[473].

Em âmbito estadual, a pesquisa mencionada no subtópico precedente[474] constatou que, nas hipóteses em que o acesso aos dados se deu após a situação

---

[472] STJ, *Habeas Corpus* n.º 210.003-MG, 5ª Turma, decisão monocrática Min. Regina Helena Costa, DJe 03/12/2013.

[473] HABEAS CORPUS. NULIDADES: (1) INÉPCIA DA DENÚNCIA; (2) ILICITUDE DA PROVA PRODUZIDA DURANTE O INQUÉRITO POLICIAL; VIOLAÇÃO DE REGISTROS TELEFÔNICOS DO CORRÉU, EXECUTOR DO CRIME, SEM AUTORIZAÇÃO JUDICIAL; (3) ILICITUDE DA PROVA DAS INTERCEPTAÇÕES TELEFÔNICAS DE CONVERSAS DOS ACUSADOS COM ADVOGADOS, PORQUANTO ESSAS GRAVAÇÕES OFENDERIAM O DISPOSTO NO ART. 7º, II, DA LEI 8.906/96, QUE GARANTE O SIGILO DESSAS CONVERSAS. VÍCIOS NÃO CARACTERIZADOS. ORDEM DENEGADA. (...) 2. Ilicitude da prova produzida durante o inquérito policial - violação de registros telefônicos de corréu, executor do crime, sem autorização judicial. 2.1 Suposta ilegalidade decorrente do fato de os policiais, após a prisão em flagrante do corréu, terem realizado a análise dos últimos registros telefônicos dos dois aparelhos celulares apreendidos. Não ocorrência. 2.2 Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta. Não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados. 2.3 Art. 6º do CPP: dever da autoridade policial de proceder à coleta do material comprobatório da prática da infração penal. Ao proceder à pesquisa na agenda eletrônica dos aparelhos devidamente apreendidos, meio material indireto de prova, a autoridade policial, cumprindo o seu mister, buscou, unicamente, colher elementos de informação hábeis a esclarecer a autoria e a materialidade do delito (dessa análise logrou encontrar ligações entre o executor do homicídio e o ora paciente). Verificação que permitiu a orientação inicial da linha investigatória a ser adotada, bem como possibilitou concluir que os aparelhos seriam relevantes para a investigação. 2.4 À guisa de mera argumentação, mesmo que se pudesse reputar a prova produzida como ilícita e as demais, ilícitas por derivação, nos termos da teoria dos frutos da árvore venenosa (fruit of the poisonous tree), é certo que, ainda assim, melhor sorte não assistiria à defesa. É que, na hipótese, não há que se falar em prova ilícita por derivação. Nos termos da teoria da descoberta inevitável, construída pela Suprema Corte norte-americana no caso Nix x Williams (1984), o curso normal das investigações conduziria a elementos informativos que vinculariam os pacientes ao fato investigado. Bases desse entendimento que parecem ter encontrado guarida no ordenamento jurídico pátrio com o advento da Lei 11.690/2008, que deu nova redação ao art. 157 do CPP, em especial o seu § 2º. (...). 4. Ordem denegada (STF, *Habeas Corpus* n.º 91.867/PA, 2ª Turma, Rel. Min. Gilmar Mendes, j. 24/04/2012, DJe 19/09/2012).

[474] As conclusões estabelecidas pela percuciente pesquisa realizada apontam, segundo os pesquisadores, que "(...) entre as observações gerais dos resultados obtidos, estão (i) a persistente relevância de uma distinção antiga (e por muitos já considerada ultrapassada) entre comunicações em fluxo e comunicações armazenadas no que diz respeito à interpretação do art. 5º, XII, da Constituição Federal (LGL\1988\3); (ii) o papel "autorizador" encontrado nas diligências previstas no art. 6º do CPP (LGL\1941\8), não revisadas pela maioria dos tribunais estaduais diante da revolução digital experimentada nas últimas duas décadas que aumentaram a popularidade e potencializaram as funcionalidades de celulares; (iii) a influência limitada do HC 51.531/RO do STJ, decidido em abril de 2016, que paradigmaticamente sustentou a proteção a informações digitais

de flagrante delito – ocasião em que foi possível se obter informações complementares para identificação de outros suspeitos ou elementos de corroboração que auxiliaram na formação do acervo probatório –,as Cortes Estaduais, ao serem confrontadas com a alegação de ilicitude do acesso realizado, decidiram majoritariamente pela licitude da prova produzida.

Com efeito, em 86,5% dos casos a prova obtida não teve sua nulidade declarada, sendo que, em 73% deles, a prova foi considerada lícita e, em 13,5%, a alegação de nulidade sequer foi analisada. Finalmente, em 13,5% dos casos as Cortes Estaduais reconheceram a ilicitude da prova[475].

Entretanto, sob prismas tecnológicos e jurídicos, a posição trazida não parece estar absolutamente alinhada a um sistema processual e constitucional pautado pela proteção aos direitos e garantias individuais.

5.4.2.1. A busca realizada a partir da prisão em flagrante: a evolução tecnológica e a exposição à privacidade e intimidade do abordado

A prisão em flagrante delito é uma das hipóteses autorizativas da realização da busca pessoal desprovida de ordem judicial (artigo 244 do Código de Processo Penal), com o propósito de se assegurar a integridade do executor da medida e do próprio acusado, bem como para se localizar eventuais objetos que, eventualmente, estejam sob a

contidas em celulares, nos tribunais analisados; e, por fim, (iv) a surpreendente "presunção de consentimento" para acesso a celular, que parece se esboçar em muitas decisões (...)" (ANTONIALLI, Dennys Marcelo. ABREU, Jacqueline de Souza. MASSARO, Heloisa Maria Machado. LUCIANO, Maria. *Acesso de autoridades policiais a celulares em abordagens e flagrantes: retrato e análise da jurisprudência de tribunais estaduais.* In: Revista Brasileira de Ciências Criminais, vol. 154/2019, p. 177-214, abril/2019).

[475] Adicionalmente, em complementação de pesquisa realizada para fins do presente trabalho científico, constatou-se que o Tribunal de Justiça do Estado de São Paulo já: 1) equiparou as conversas de Whatsapp armazenadas em um aparelho às cartas, abertas ou não, destinadas ao acusado ou que estejam em seu poder, na forma do artigo 240, §§ 1º e 2º do Código de Processo Penal, o que autorizaria seu imediato acesso sem autorização judicial (TJSP, Apelação n.º 0000136-45.2015.8.26.0592, 5ª Câmara Criminal, Rel. Pinheiro Franco, julgado em 27/04/2017) ; 2) reconheceu que o recebimento de mensagens em um aparelho celular, durante uma abordagem policial realizada e antes mesmo da constatação visual do flagrante, configuraria uma situação de urgência que permitiria o acesso imediato ao conteúdo armazenado em um aparelho celular (TJSP, Apelação n.º 0000679-77.2016.8.26.0571, 14ª Câmara Criminal, Rel. Laerte Marrone, julgado em 15/03/2018); 3) admitiu o acesso aos registros de chamadas efetuadas e recebidas e à agenda telefônica armazenada no aparelho mas, ao mesmo tempo, tomou por ilícito o acesso às conversas mantidas via aplicativo *Whatsapp* (TJSP, *Habeas Corpus* n.º 2098819-74.2019.8.26.0000, 1ª Câmara Criminal, Rel. Márcio Bartoli, julgado em 03/06/2019).

posse do acusado (*v.g.*, um *smartphone* ou uma carteira), prevenindo-se a destruição dos elementos de prova[476].

No âmbito desta busca realizada, é possível que se vasculhem mochilas, cadernos, agendas, e outros itens que estejam sob a imediata posse ou detenção do abordado, com o intuito de localizar armas ou instrumentos que possam trazer perigo à ação policial, identificar produtos que possam ser objeto de crimes ou, ainda, encontrar elementos de prova que possam corroborar ou infirmar as circunstâncias que justificaram a abordagem policial.

Evidentemente, em sendo o aparelho celular um desses possíveis objetos a serem vasculhados, exsurgem os questionamentos relativos à admissibilidade do acesso ao seu conteúdo, haja vista serem dispositivos capazes de reunir as mesmas informações que, antes mesmo da vertical ascensão tecnológica, poderiam ser facilmente obtidas em cadernos, agendas, papéis e outros itens normalmente analisados em uma busca pessoal[477].

Embora sedutora, a comparação realizada não pode ser estabelecida, especialmente considerando as perspectivas tecnológicas modernas relativas à elevada quantidade de dados passíveis de serem encontrados nos modernos aparelhos celulares.

Não bastasse, os aplicativos de comunicação disponíveis possibilitam que informações privadas de terceiros venham a ser indevidamente expostas, violando-se a intimidade destas pessoas que mantiveram uma interlocução com a pessoa abordada[478] e cujo teor da conversa ainda esteja armazenada no aparelho.

---

[476] MARQUES, Pedro Campanholo. *Busca e apreensão: juízo de admissibilidade.* Op. cit. p. 202.

[477] Foi este um dos fundamentos lançados pelo Ministro relator Gilmar Mendes para, no bojo do *Habeas Corpus* n.º 91.867/PA, rechaçar a necessidade de acesso, conforme se verifica do seguinte excerto do voto: "(...) abstraindo-se do meio material em que o dado estava registrado (aparelho celular), indago: e se o número estivesse em um pedaço de papel no bolso da camisa usada pelo réu no dia do crime, seria ilícito o acesso pela autoridade policial? E se o número estivesse anotado nas antigas agendas de papel ou em um caderno que estava junto com o réu no momento da prisão?(...)".

[478] Ainda que, em uma interceptação telefônica realizada, a conversa mantida pelo alvo da investigação com terceiros exponha aspectos relativos à privacidade e intimidade deste interlocutor, é certo que o referido meio de obtenção de provas está sujeito a rígidos critérios de proporcionalidade para ser concedido (artigo 2º da Lei n.º 9.296/1996), em um período de tempo previamente delimitado, sendo devidamente autorizado mediante ordem judicial fundamentada.

Assim, inegável reconhecer que, antes do advento tecnológica dos *smartphones,* uma busca pessoal jamais teria condição de vasculhar a mesma quantidade de informações disponíveis no aparelho celular, já que é fisicamente impossível que a pessoa abordada consiga carregar, em formato material, papéis, documentos, agendas e outros objetos que representassem todos os elementos disponíveis no aparelho celular.

Desta feita, sob a perspectiva tecnológica, é impossível se estabelecer uma comparação racional entre o grau de exposição à intimidade e privacidade que ocorre com o acesso aos dados armazenados em um aparelho celular e com a localização de alguns documentos e informações geralmente isoladas, durante uma corriqueira prisão em flagrante[479].

De igual sorte, no espectro jurídico, a prisão em flagrante não parece configurar hipótese legitimadora, de *per si*, para a realização de buscas desmedidas no conteúdo do aparelho celular.

Com efeito, ainda que a situação flagrancial permita a relativização do exercício de direitos e garantias fundamentais, um sistema pautado pelo resguardo à intimidade exige que as limitações sejam mínimas e estritamente vinculadas aos propósitos e motivos determinantes da prisão em flagrante realizada. A partir desta premissa, a constrição da liberdade ambulatória do cidadão e o ingresso ao domicílio, com a subsequente busca, estão cingidas aos limites da situação flagrancial, não podendo se permitir uma relativização da privacidade do cidadão para além do necessário à realização do ato[480].

---

[479] Como bem destaca Zilli, "(...) se por um lado os avanços tecnológicos propiciam novos meios de realização de práticas ilícitas, por outro é inegável a carga lesiva à intimidade que o acesso ilimitado ao conteúdo armazenado nesses aparelhos pode trazer. De fato, é possível traçar não só o perfil do usuário, mas eventualmente de outras pessoas de seu estreito relacionamento. Tais circunstâncias, sem dúvida, devem orientar a melhor solução. Uma restrição absoluta leva à utopia da supremacia da individualidade. Por sua vez, o acesso irrestrito, ainda que incidental à prisão, reduz consideravelmente os espectros de proteção da privacidade. Nesse ponto, não parece mais válida a analogia feita pelo STF à apreensão de um pedaço de papel com o conhecimento do conteúdo das anotações ali apostas. É que a capacidade de armazenamento de dados dos aparelhos multifuncionais, somada à grande variedade do conteúdo, torna as situações incomparáveis, como de fato o são. (...)" (ZILLI, Marcos Alexandre Coelho. *A prisão em flagrante e o acesso de dados em dispositivos móveis. Nem utopia, nem distopia. Apenas a racionalidade.* Op. cit., p. 86).

[480] *Ad exemplum,* a Lei n.º 12.403/2010 extinguiu a possibilidade da manutenção indeterminada da prisão em flagrante e exigiu sua apreciação em até 24h (vinte e quatro horas), exigindo que o juiz, fundamentadamente, determinasse o relaxamento da prisão ilegal; convertesse a prisão em flagrante em preventiva, na forma do artigo 312 do Código de Processo Penal; ou concedesse a liberdade provisória, com ou sem fiança. Denota-se, portanto, a clara intenção legislativa de afastar a autonomia da prisão em flagrante, reconhecendo-a como medida *subcautelar* adotada para impedir que um crime continue sendo praticado ou que se identifique e detenha o suspeito de ter violado as normas penais.

É indiscutível que, a partir da busca pessoal ou domiciliar realizada durante uma prisão em flagrante delito, o aparelho celular poderá ser apreendido, sempre que se entender por pertinente a medida visando a apuração dos fatos ou que neles poderão ser encontradas provas que sirvam para o esclarecimento destes fatos e suas respectivas circunstâncias (artigo 6º, incisos I e III do Código de Processo Penal).

Todavia, a apreensão do aparelho não autoriza, necessariamente, seu acesso imediato e desprovido de autorização judicial concessiva. Rememorando-se o fato de que os atuais aparelhos celulares armazenam uma elevada gama de informações que retratam aspectos inerentes à personalidade do cidadão, o acesso imediato do seu conteúdo, sem qualquer situação de urgência que o justifique, poderá configurar indevida exposição à privacidade e intimidade da pessoa detida, para além dos limites necessários ao flagrante delito.

Como exemplo, se a pessoa é flagrada em um ponto de venda de entorpecentes trazendo consigo uma sacola contendo diversificada quantidade de drogas, prontas ao comércio e distribuição a terceiros e, durante a abordagem, um aparelho celular é encontrado em poder da pessoa detida, o acesso imediato aos dados, desprovido de justificativa válida ou excepcional, poderá acarretar vilipêndio à sua privacidade e intimidade de maneira desproporcional às necessidades circunstanciais da hipótese flagrancial.

Nestas hipóteses, em uma pretensa relação de equilíbrio e proporcionalidade entre a eficiente atuação policial e a preservação dos direitos e garantias individuais, o acesso aos dados sem qualquer justificativa lógica e urgencial preexistente, que permita concluir pela necessidade da busca imediata, constitui desmedida e irremediável violação à privacidade e intimidade do indivíduo.

Ademais, em sendo o aparelho apreendido e preservado de quaisquer formas de acesso ou interferências externas indevidas, o conteúdo poderá ser analisado futuramente em exame pericial, após prévia determinação judicial que apreciará, a partir da situação exposta, se há proporcionalidade[481] no afastamento do sigilo conferido.

[481] Vide subtópico 5.3.3.1.

Com a adoção deste procedimento, estarão preservados os direitos e garantias individuais, sem prejuízo da vindoura identificação de elementos de prova que possam ser oportunamente utilizados[482]. Ainda, estará garantida a higidez da cadeia de custódia da prova, com o subsequente afastamento de alegações relacionadas à sua quebra em razão do acesso indevido por parte dos policiais.

O Superior Tribunal de Justiça (STJ), embora tenha flertado inicialmente com a desnecessidade da autorização judicial para acesso aos dados, alterou seu posicionamento a partir do paradigmático julgamento do *Recurso em Habeas Corpus n.º 51.531/RO*[483] pela 6ª Turma, ocasião em que policiais degravaram as conversas armazenadas em aparelho celular de uma acusada denunciada por tráfico de entorpecentes, associação para o tráfico e resistência. Posteriormente, a 5ª Turma do mesmo sodalício[484] encampou o posicionamento fixado.

Em levantamento realizado no *site*[485] oficial do Superior Tribunal de Justiça (STJ), a partir de buscas com os termos "acesso", "aparelho celular" e "flagrante", identificaram-se diversos precedentes recentes, de ambas as Turmas, ratificando-se o

---

[482] FAYET, Fábio Agne; CARVALHO, Andersson Vieira. *Whatsapp, sigilo de dados e prova ilícita: para dizer o óbvio*. Revista Brasileira de Ciências Criminais, vol. 140/2018, p. 297-322, fevereiro/2018; SILVA, Gabriela Buarque Pereira; MOURA, Tâmara. *Prisão em flagrante e acesso a dados de celular: deságios entre a privacidade e a investigação criminal*. In: ARAS, Vladimir Barros; MENDONÇA, Andrey Borges de; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira da; COSTA, Marcos Antônio da Silva. Proteção de dados pessoais e investigação criminal. Associação Nacional do Procuradores da República, 3ª Câmara de Coordenação e Revisão. Brasília: ANPR, 2020, p. 399-430.

[483] Reconhecendo a evolução tecnológica que tornou o aparelho celular mais do que um simples instrumento de comunicação e admitindo-se expressamente a superação do precedente estampado no Habeas Corpus n.º 91.867/PA do Supremo Tribunal Federal (STF) –, o Superior Tribunal de Justiça (STJ) invocou o artigo 5º, incisos X e XII da Constituição Federal e os artigos 1º e 5º da Lei n.º 9.296/1996 (Lei de Interceptação Telefônica), o artigo 3º, inciso V, da Lei n.º 9.472/1997 e artigo 7º, inciso III, da Lei n.º 12.965/2014, para sustentar que a devassa dos dados armazenados, ainda que em situação flagrancial, somente seria possível mediante prévia autorização judicial devidamente motivada. Enfrentando a inexistência de uma cláusula constitucional de reserva de jurisdição, a Corte Superior apontou que, muito embora o artigo 5º, inciso X, da Constituição Federal não tenha estabelecido a possibilidade da restrição dos direitos fundamentais nele abarcados, é certo que o sistema constitucional brasileiro não contemplaria direitos e garantias que se revistam de caráter absoluto, de modo que todas as normas possuiriam a mesma hierarquia. Assim, conquanto a apreensão tenha sido realizada de maneira correta, à luz do artigo 6º, incisos II e III do Código de Processo Penal, a quebra do sigilo dos dados nele armazenados exigiria a observância da proporcionalidade entre os interesses constitucionais envolvidos, a saber, o direito difuso à segurança pública (artigo 144 da Constituição Federal) e o direito fundamental à intimidade (artigo 5º, inciso X, da Constituição Federal) (STJ, RHC n.º 51.531/RO, 6ª Turma, Rel. Nefi Cordeiro, julgado em 19 de abril de 2016, DJe 09/05/2016).

[484] STJ, RHC n.º 77.232/SC, 5ª Turma, Rel. Min. Felix Fischer, DJe 16/10/2017; STJ, HC n.º 372.762/MG, 5ª Turma, Rel. Ministro Felix Fischer, julgado em 3 de outubro de 2017, DJe 16/10/2017).

[485] Levantamento realizado em 20 de dezembro de 2020, no site: www.stj.jus.br, na seção "jurisprudência".

posicionamento da Corte[486] e inadmitindo-se o acesso a dados armazenados em aparelhos celulares por policiais, mesmo em situação de flagrante delito[487], salvo mediante prévio consentimento do titular[488].

Já na perspectiva da jurisprudência do Supremo Tribunal Federal (STF), ainda não há decisão definitiva sobre o tema, à exceção do já mencionado *Habeas Corpus n.º 91.867/PA*, que apreciou o acesso a registros telefônicos por policiais, após prisão em flagrante.

Todavia, já se antevê uma sinalização de mudança da orientação concebida no julgamento mencionado, especialmente no *Habeas Corpus* n.º 168.052/SP[489] e na *Reclamação* n.º 33.711/SP[490], ambos da 2ª Turma da Suprema Corte, ocasião em que o Ministro Gilmar Mendes, relator, sinalizou pretender a revisitação da clássica distinção relacionada à inviolabilidade dos dados e da comunicação propriamente dita, bem como destacou que o avanço normativo - especialmente decorrente do artigo 7º, inciso III, da Lei n.º 12.965/2014 - e o desenvolvimento de mecanismos de comunicação e armazenamento de dados pessoais em *smartphones* e telefones celulares, motivaram a alteração de seu posicionamento anterior, passando a defender que o acesso aos dados contidos em aparelhos celulares é possível, desde que condicionado a prévia decisão judicial.

---

[486] Uma vez reafirmada a posição da Corte Superior quanto à ilicitude do acesso sem autorização judicial, a orientação extraída dos precedentes foi sendo repassada e assimilada pelas forças policiais, especialmente considerando que o policiamento ostensivo é responsável por grande parte das prisões em flagrante seguidas do indevido acesso imediato aos dados armazenados.
No Estado de São Paulo, foi expedida orientação aos policiais militares para que, havendo suspeita de que o aparelho celular contenha informações hábeis para esclarecimento da autoria e materialidade, o procedimento correto é a apreensão do aparelho e seu encaminhamento ao Distrito Policial, para que seja periciado durante a fase investigatória. Ainda, orientou-se quanto à inadmissibilidade da colocação do aparelho em "viva-voz", para que policiais captassem conversas entre o infrator e terceiros. Finalmente, a orientação esclareceu que o IMEI não configura dado pessoal, mas sim do aparelho, sendo possível a extração do número sem a necessidade de prévia autorização judicial, mas ressaltando que o detentor do aparelho não é obrigado a fornecer sua senha de acesso para que o policial manuseie o teclado e obtenha a informação (Despacho n.º PM3-005/02/19 – Circular, de 22 de julho de 2019, do Subcomandante Geral da Polícia Militar do Estado de São Paulo).
[487] STJ, AgRg no HC n.º 611.762, 5ª Turma, Rel. Ministro Felix Fischer, julgado em 20 de outubro de 2020, DJe 26/10/2020; STJ, AgRg no AREsp n.º 1.573.424/SP, 5ª Turma, Rel. Reynaldo Soares da Fonseca, julgado em 8 de setembro de 2020, DJe 15/09/2020.
[488] STJ, Agravo Regimental no Recurso em *Habeas Corpus* n.º 116.792/SP, 5ª Turma, Rel. Ministro Leopoldo de Arruda Raposo, julgado em 20 de fevereiro de 2020, DJe 03/03/2020.
[489] STF, Habeas Corpus n.º 168.052/SP, 2ª Turma, Rel. Min. Gilmar Mendes, julgado em 9 de outubro de 2020.
[490] STF, Reclamação n.º 33.711/SP, 2ª Turma, Rel. Min. Gilmar Mendes, julgado em 11 de junho de 2019, DJe 22/08/2019.

A importância da matéria motivou o reconhecimento de repercussão geral no Agravo n.º 1.042.075/RJ[491], em que a Suprema Corte fixou o Tema 997 da Repercussão Geral: "Aferição da licitude da prova produzida durante o inquérito policial relativa ao acesso, sem autorização judicial, a registros e informações contidos em aparelho de telefone celular, relacionados à conduta delitiva e hábeis a identificar o agente do crime".

O julgamento teve início no plenário judicial[492], sendo colhidos três votos: o do Min. Dias Toffoli, que votou pela procedência do agravo e a fixação de tese favorável à possibilidade do acesso aos dados armazenados sem autorização judicial; e o dos Ministros Gilmar Mendes e Edson Fachin, que votaram pela rejeição do agravo e pela

---

[491] STF, Repercussão Geral no Recurso Extraordinário com Agravo n.º 1.042.075/RJ, Rel. Min. Dias Toffoli, julgado em 23 de novembro de 2017, DJe 12/12/2017).

[492] Iniciado o julgamento, o relator Ministro Dias Toffoli reconheceu que os múltiplos dados armazenados em aparelhos celulares estariam resguardados pelo direito à intimidade (artigo 5º, inciso X, da Constituição Federal), e não pela tutela ao sigilo das comunicações (artigo 5º, inciso XI, da Carta Política).
Ainda, apontou que o aparelho celular havia sido deixado no local do crime pelo acusado, o qual estava em situação de flagrância, o que reforçaria a urgência no acesso aos dados, potencializando-se o poder de investigação policial (artigo 6º, inciso II, do CPP), com a finalidade de se coletar o máximo de informações possíveis relacionadas às circunstâncias do crime e sua autoria.
Finalmente, concluiu que a autorização seria necessária para a interceptação da transmissão e recepção das informações, o que não ocorreu no caso em análise, bem como que, ainda se constatasse a ilegalidade no acesso às fotografias, agendas e registro de chamadas do aparelho, a ilicitude das provas não contaminaria o restante das evidências, invocando-se a teoria da fonte independente.
Destacando que a análise estaria limitada às circunstâncias do caso concreto - notadamente à regularidade do acesso à agenda e aos registros telefônicos do aparelho celular apreendido no local do crime, não se estendendo necessariamente ao acesso de conversas mantidas por aplicativos de comunicação instantânea -, foi proposta a seguinte tese: "É lícita a prova obtida pela autoridade policial, sem autorização judicial, mediante acesso a registro telefônico ou agenda de contatos de celular apreendido ato contínuo no local do crime atribuído ao acusado, não configurando esse acesso ofensa ao sigilo das comunicações, à intimidade ou à privacidade do indivíduo (CF, art. 5º, incisos X e XII)" (O voto do Ministro Dias Toffoli pode ser encontrado em <https://www.conjur.com.br/dl/toffoli-stf-suspende-julgamento.pdf>. Acesso em: 20 de dezembro de 2020)
Entretanto, abrindo a divergência, o Ministro Gilmar Mendes tornou a invocar a possível incidência do artigo 5º, inciso XII, da Constituição Federal para regular o acesso aos dados armazenados e, em raciocínio sucessivo, registrou que, ainda que não se entenda pela incidência da previsão constitucional referida, seria inegável que os dados estaria protegidos pela tutela à intimidade prevista no artigo 5º, inciso X, da Constituição Federal.
Nesta linha, lastreando-se no art. 3º, II, III; 7º, I, II, III, VII e artigos 10 e 11, todos da Lei n.º 12.965/2014, concluiu que os avanços da legislação infraconstitucional indicaram a pretensão legislativa de que os dados estivessem sob reserva de jurisdição, especialmente considerando o incrível desenvolvimento dos mecanismos de comunicação e armazenagem de dados pessoais em smartphones, o avanço tecnológico e a necessidade de ressignificações do direito à privacidade e à intimidade.
Concluiu, assim, ser possível o acesso aos dados contidos em aparelhos celulares, mas condicionado a prévia decisão judicial que demonstre, de maneira concreta, a necessidade, adequação e proporcionalidade do acesso aos dados e informações requeridas, como forma de se impedir buscas genéricas e desarrazoadas ou, ainda, constrangimentos ilegais para o fornecimento de senhas de acesso aos aparelhos.
Ao final, o Ministro Gilmar Mendes propôs a seguinte tese: "O acesso a registro telefônico, agenda de contatos e demais dados contidos em aparelhos celulares apreendidos no local do crime atribuído ao acusado depende de prévia decisão judicial que justifique , com base em elementos concretos, a necessidade e a adequação da medida e delimite a sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade e ao sigilo das comunicações e dados dos indivíduos (CF, art. 5º, X e XX)." (O voto do Ministro Dias Toffoli pode ser encontrado em <https://www.conjur.com.br/dl/gilmar-stf-suspende-julgamento-violacao.pdf>. Acesso em: 20 de dezembro de 2020)

necessidade de prévia autorização judicial para acesso aos dados. O julgamento não foi concluído, em razão de pedido de vista formulado pelo Ministro Alexandre de Moraes[493].

5.4.2.2. A excepcionalidade do acesso direto aos dados armazenados em aparelhos celulares

Entretanto, uma vez firmada a premissa de que o acesso ao conteúdo do aparelho celular não é automático, é certo que não há como se impossibilitar, de maneira peremptória, que policiais tenham acesso imediato aos dados armazenados em algumas hipóteses excepcionais e plenamente justificadas.

Com efeito, em hipóteses de urgência[494] ou emergência identificáveis no contexto da abordagem[495], a apreensão do aparelho celular e o requerimento de autorização judicial para acesso aos dados poderá trazer prejuízos irremediáveis. Assim, em um juízo de urgência realizado pelos próprios policiais, poderá se concluir por legítima a consulta imediata aos dados em caso de vítimas mantidas em cativeiro e cuja localização puder ser realizada pela consulta ao conteúdo dos dados; quando a medida for necessária para, concretamente, se evitar o cometimento de novos delitos que estejam na iminência de serem praticados; para descortinar outros indivíduos envolvidos naquela situação flagrancial, cuja identificação deve ser realizada imediatamente, sob pena de prejuízo às investigações[496].

Caberá ao juiz, posterior e oportunamente, exercer o controle de legalidade e proporcionalidade da medida, tomando-se por base as circunstâncias aventadas pelo policial no momento da abordagem, especialmente considerando a vagueza de expressões como "urgência" ou "emergência". Deverá o julgador analisar se, na situação

---

[493] Acesso em: 20 de dezembro de 2020, consulta disponível no sítio eletrônico do Supremo Tribunal Federal: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5173898.

[494] MAGALHÃES, Vlamir Costa. Ilicitude probatória em processo penal e regra de exclusão (*exclusionary rule*): comentários sobre a legitimidade do acesso a aparelhos eletrônicos apreendidos em situação flagrancial. Op. cit. p. 558. Ainda, durante o VII Fórum Nacional de Juízes Federais Criminais (FONACRIM), aprovou-se o enunciado com seguinte teor: "É possível o acesso, sem prévia ordem judicial, aos dados do dispositivo eletrônico, desde que realizado imediatamente após a prisão em flagrante do investigado ou apreensão, presente o requisito da urgência na produção dos elementos de prova, devidamente justificada pela autoridade."

[495] A definição das situações de urgência e emergência geram inegável insegurança jurídica (SOUZA, Rodrigo Telles de. *A exigência de autorização judicial para acesso ao conteúdo de telefone móvel apreendido: uma ampliação da garantia à inviolabilidade domiciliar incompatível com o sistema jurídico brasileiro.* Op. cit. p. 428-429).

[496] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de Direito Constitucional*. 13ª Edição, São Paulo: Ed. Saraiva, 2018, p. 610.

casuística com a qual se deparou o policial, inferia-se a existência de elementos que sugeriam a urgência ou emergência no acesso aos dados, especialmente para se colher indicativos da boa-fé do agente na realização da medida ou, ainda, eventual atuação flagrantemente irregular e passível de configurar abuso de autoridade (artigo 25 da Lei n.º 13.869/2019).

Entretanto, nestas hipóteses excepcionais, é precisa a advertência de ZILLI, para quem:

> o acesso ao conteúdo, independentemente de ordem judicial, deve ser executado com cautela e nos estritos limites da finalidade que o informa: busca de informações importantes que componham a situação de urgência. É a mesma cautela que deveria orientar a busca domiciliar que se realiza em contexto de flagrante delito. Com efeito, o ingresso autorizado em lei na casa alheia não traz em si uma autorização para uma busca ampla, geral e irrestrita. Ao contrário, a busca tem foco certo e determinado qual seja, aquele indicado pela situação flagrancial. Cuidando-se de medida excepcional, seria conveniente que o acesso imediato fosse alvo de registro por parte dos policiais, discriminando, assim, o conteúdo acessado e as informações obtidas. Trata-se de providência que conferiria maior base e fundamento para um exame judicial posterior sobre a legalidade e proporcionalidade da ação (ZILLI, Marcos Alexandre Coelho. *A prisão em flagrante e o acesso de dados em dispositivos móveis. Nem utopia, nem distopia. Apenas a racionalidade.* In: ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. I. São Paulo. InternetLab, 2018, p. 97).

Também na perspectiva jurisprudencial, o Superior Tribunal de Justiça reconheceu a possibilidade de que os dados pudessem ser acessados imediatamente, em situações excepcionais, afirmando que "(...) a depender do caso concreto, caso a demora na obtenção de um mandado judicial pudesse trazer prejuízos concretos à investigação ou especialmente à vítima do delito, mostre-se possível admitir a validade da prova colhida através do acesso imediato aos dados do aparelho celular (...)"[497]

[497] STJ, Recurso em *Habeas Corpus* n.º 51.531/RO, 6ª Turma, Rel. Min. Nefi Cordeiro, j. 19/04/2016, DJe 09/05/2016. No mesmo sentido: STJ, Recurso Especial n.º 1.661.378/MG, 6ª Turma, Rel. Min. Maria Thereza Rocha de Assis Moura, julgado em 23 de maio de 2017, DJe 30/05/2017

Para além das situações de urgência ou emergência, tem-se por legítimo o acesso ao conteúdo dos dados quando a materialidade de um crime estiver incorporada no aparelho celular. Com efeito, em determinados crimes praticados essencialmente pela via informática ou telemática, tais como o compartilhamento de conteúdos relacionados a sexo explícito ou pornografia envolvendo criança ou adolescente (artigo 241-A da Lei n.º 8.069/1990) ou o armazenamento destes registros (artigo 241-B do mesmo Diploma Legal), a materialidade do crime estará encrustada nos dados contidos no aparelho celular, de modo que a efetiva certeza da configuração do crime exigirá, necessariamente, o acesso a seu conteúdo. Em outras palavras, o próprio objeto servirá de base para o "corpo de delito"[498].

Assim, em uma situação flagrancial relacionada a um delito desta natureza, o acesso ao conteúdo do aparelho não configuraria ato ilícito, porquanto a materialidade estará umbilicalmente vinculada aos dados armazenados no aparelho[499].

De igual sorte, não configura indevida violação aos direitos e garantias individuais da pessoa abordada a realização de consulta, por policiais, do IMEI (*International Mobile Equipment Identity*) do aparelho, sempre que houver fundadas razões para se acreditar que o objeto possa ser produto de um crime anterior. O Estado de São Paulo adotou, no âmbito policial, uma resolução[500] determinando que, durante o registro de boletins de ocorrência de celulares furtados, roubados ou extraviados, fosse apontado o IMEI dos aparelhos, o que facilitaria o bloqueio por parte da operadora, além de permitir a consulta facilitada por terminais integrados quanto à origem ilícita do bem.

Nestes casos, se durante uma abordagem policial houver dúvidas quanto à licitude do aparelho celular encontrado, não seria invasiva a consulta policial ao IMEI do objeto, especialmente considerando que a numeração não se insere na categoria de "dado pessoal", porquanto o conteúdo está relacionado ao objeto, e não a seu detentor.

---

[498] STJ, *Habeas Corpus* n.º 139.312/SP, 5ª Turma, Rel. Min. Laurita Vaz, julgado em 2 de setembro de 2010, DJe 04/10/2010.
[499] STJ, Recurso em *Habeas Corpus* n.º 108.262/MS, 6ª Turma, Rel. Min. Antonio Saldanha Pinheiro, julgado em 5 de setembro de 2019.
[500] Resolução SSP-3, de 06 de dezembro de 2015.

Outrossim, em alguns casos a numeração pode ser localizada em exame externo do objeto[501], o que descaracterizaria o acesso ao conteúdo dos dados.

Por derradeiro, o acesso direto e imediato do aparelho celular poderá ocorrer sempre que o aparelho estiver abandonado e a medida for necessária para se identificar o proprietário do objeto[502] ou, ainda, quando se tratar de bem pertencente a uma vítima falecida, tendo o aparelho sido entregue aos policiais por familiares[503], uma vez que, neste caso, não haveria mais direito à privacidade a ser tutelado.

5.5. As consequências jurídicas do acesso indevido aos dados armazenados em aparelhos celulares

Firmadas as premissas necessárias para o acesso aos dados armazenados em aparelhos celulares, cumpre destacar as consequências jurídicas decorrente do acesso indevido ao conteúdo dos aparelhos.

Inevitável que, para tanto, se faça uma breve digressão com relação à teoria da prova ilícita e seus consectários no Código de Processo Penal.

5.5.1. Premissas conceituais e a distinção entre *prova ilícita* e *prova ilegítima*

Com efeito, a doutrina nacional sempre se referenciou na clássica e importante distinção entre prova ilícita e ilegítima, cunhada por GRINOVER[504] a partir dos ensinamentos de NUVOLONE, para quem a as provas contrárias à lei são consideradas dentro de um gênero chamado "provas ilegais", no qual faria parte a "prova ilícitas" e a "prova ilegítima"[505].

---

[501] Nos casos em que a localização do IMEI exigir o acesso e manuseio do teclado do dispositivo, é certo que o desbloqueio do aparelho deverá ser realizado de forma voluntária pelo seu possuidor, não sendo admitida qualquer forma de constrangimento para que a medida seja operada.

[502] STJ, AgRg em REsp n.º 1.573.424/SP, 5ª Turma, Rel. Min, Reynaldo Soares da Fonseca, julgado em 8 de setembro de 2020, DJe 15/09/2020.

[503] STJ, RHC n.º 86.076/MT, 6ª Turma, Rel. Min. Rogério Schietti Cruz, julgado em 19 de outubro de 2017, DJe 12/12/2017.

[504] GRINOVER, Ada P. Liberdades públicas e processo penal. 2. edição., São Paulo: Revista dos Tribunais, 1982, p. 93-103.

[505] Como bem sustentam GRINOVER, FERNANDES e GOMES FILHO, "(...) no campo das proibições da prova, a tônica é dada pela natureza processual quando for colocada em função de interesses atinentes à lógica e à finalidade do processo; tem, pelo contrário, natureza substancial quando, embora servindo imediatamente

Nesta ordem, sempre que a prova for produzida com patente violação às normas de direito processual, estar-se-ia diante da "prova ilegítima", ao passo que, quando a violação se der às normas de direito material ou às garantias processuais, a prova seria considerada "ilícita"[506].

Ocorre que, diante da relevância dos bens jurídicos protegidos – especialmente relacionados à proteção das liberdades públicas e dos direitos da personalidade[507]–, o legislador reconheceu a necessidade de criminalizar suas violações, tal como o fez com o segredo profissional (artigo 154 do Código Penal), o delito de tortura (Lei n.º 9.455/1997) e, mais recentemente, com a previsão de se obter prova, em procedimento de investigação ou fiscalização, por meio manifestamente ilícito ou, ainda, fazer uso da prova em desfavor do investigado ou fiscalizado, com prévio conhecimento de sua ilicitude (artigo 25 da Lei n.º 13.964/2019).

Todavia, diferentemente do que ocorre com a prova ilegítima, a criminalização das violações às normas de direito material não gera, necessariamente, uma sanção processual. Assim, enquanto a violação ao impedimento de cunho processual acarreta, via de regra, a nulidade[508] do ato praticado, com a subsequente anulação para que,

---

também a interesses processuais, é colocada essencial em função dos direitos que o ordenamento reconhece aos indivíduos, independentemente do processo (...)" (GRINOVER, Ada Pellegrini; FERNANDES, Antônio Scarance; GOMES FILHO, Antônio Magalhães. *As nulidades no processo penal*. 7ª edição, São Paulo: Editora RT, 2001, p. 133). GOMES FILHO prossegue nas distinções, indicando que "(...) outra diferença entre elas decorre do momento em que se configura a ilegalidade: nas ilícitas, ela ocorre quando da sua 'obtenção'; nas ilegítimas, na fase de 'produção'. Também é diversa a consequência dos respectivos vícios: as ilícita são 'inadmissíveis' no processo (não podem ingressar e, se isso ocorrer, devem ser desentranhadas); as 'ilegítimas' são nulas e, por isso, a sua produção pode ser renovada, atendendo-se então às regras processuais pertinentes (...)" (GOMES FILHO, Antonio Magalhães. Provas. Lei 11.690, de 09.06.2008. In. ASSIS MOURA, Maria Thereza Rocha de (Coord.). *As reformas no processo penal. As novas leis de 2008 e os projetos de reforma*. São Paulo: Revista dos Tribunais, 2008, p. 266). Ainda sobre o tema, as Mesas de Processo Penal, ligadas ao Departamento de Direito Processual da Faculdade de Direito da Universidade de São Paulo e coordenada pela Professora Ada Pellegrini Grinover, edificaram três súmulas versando sobre o tema: Súmula nº 48– Denominam-se ilícitas as provas colhidas com infringência a normas e princípios de direito material; Súmula nº 49 – São processualmente inadmissíveis as provas ilícitas que infringem normas e princípios constitucionais, ainda quando forem relevantes e pertinentes, e mesmo sem cominação processual expressa; Súmula nº 50 – Podem ser utilizadas no processo penal as provas ilicitamente colhidas, que beneficiem a defesa.

[506] Sobre a evolução do conceito de prova ilícita e sua análise à luz do direito comparado, recomenda-se: Idem, AVOLIO, Luiz Francisco Torquato. *Provas Ilícitas Interceptações telefônicas e gravações clandestinas*, Op. cit, p. 48-72.

[507] BADARÓ, Gustavo Henrique Righi Ivahy. *Processo Penal*, Op. cit., p. 452.

[508] Como bem esclarece AVOLIO, "(...) a sanção para o descumprimento dessas normas encontra-se na própria lei processual. Então, tudo se resolve dentro do processo, segundo esquemas processuais que determinam as formas e as modalidades de produção da prova, com a sanção correspondente a cada transgressão, que pode ser uma sanção de nulidade (...)" (AVOLIO, Luiz Francisco Torquato. *Provas Ilícitas Interceptações telefônicas e gravações clandestinas*, Op. cit, p. 48). O reconhecimento da nulidade exigirá a comprovação do prejuízo (artigo 563 do CPP), a proibição de que a parte aproveito à nulidade a que haja dado causa

sendo possível, seja refeito[509], o responsável pela produção ou utilização da prova ilícita era punido apenas no campo do direito material, sem que a prova ilícita realizada deixasse de produzir efeitos no processo.

Neste panorama, a Constituição Federal de 1988 buscou diminuir o abismo existente entre as provas ilícita e ilegítimas e, de maneira abrangente, estabeleceu no artigo 5º, inciso LVI, que "são inadmissíveis, no processo, as provas obtidas por meios ilícitos".

Diante desta previsão, o constituinte estendeu a "inadmissibilidade" como "pena processual" às provas ilícitas, reconhecendo sua absoluta inexistência jurídica[510] e o dever de ser banida, ainda que relevantes os fatos apurados[511].

A reforma operada pela Lei n.º 11.690/2008 novamente atenuou a distinção entre provas ilícitas e ilegítimas[512], ao estabelecer que "são inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais" (artigo 157, *caput*, do Código de Processo Penal), determinando as consequências decorrentes de sua inadmissibilidade: o desentranhamento dos autos do processo[513].

Embora a adoção de um conceito legal tenha despertado críticas doutrinárias[514], em razão de uma possível confusão na definição da sanção processual

(artigo 564 do CPP), a proibição de arguição de nulidade que só interesse à parte contrária (artigo 565 do CPP) e a proibição de reconhecimento da nulidade de ato que não houver influído na apuração da verdade ou na decisão da causa (artigo 566 do CPP).

[509] DEZEM, Guilherme Madeira. *Curso de processo penal*. Op. cit. p. 629.

[510] GOMES FILHO, Antonio Magalhães. *Direito à prova no processo penal*. Op. cit. p. 94.

[511] GRINOVER, Ada Pellegrini; FERNANDES, Antônio Scarance; GOMES FILHO, Antônio Magalhães. *As nulidades no processo penal.* Op. cit. p. 135-136.

[512] LOPES JR., Aury. *Direito Processual Penal.* Op. cit, p. 437.

[513] Se, inadvertidamente, houver a admissibilidade da prova ilícita, AVOLIO reconhece que as consequências desta vulneração perpassam pela análise dos conceitos de atipicidades e nulidade, chegando-se ao conceito de "atipicidade constitucional". Assim, as provas ilícitas, porquanto inadmissíveis pela Constituição Federal, são consideradas juridicamente inexistentes, o que implica sua ineficácia desde sua origem, deixando de surtir efeitos em qualquer momento processual (AVOLIO, Luiz Francisco Torquato. *Provas Ilícitas Interceptações telefônicas e gravações clandestinas*, Op. cit, p. 90-102). Entretanto, o desentranhamento das provas não alcança a exclusão de peças processuais que a elas façam referência (STF, RHC n.º 137.368/PR, 2ª Turma, Rel. Min. Gilmar Mendes, julgado em 29 de novembro de 2016, DJe 02/08/2017).

[514] GOMES FILHO, Antonio Magalhães. *Provas. Lei 11.690, de 09.06.2008*. In. ASSIS MOURA, Maria Thereza Rocha de (Coord.). *As reformas no processo penal. As novas leis de 2008 e os projetos de reforma*. Op. cit. p. 266.

aplicável à violação da norma, há vertentes doutrinárias que reconhecem a perda de relevância prática da tradicional distinção entre prova ilícita e prova ilegítima[515].

Entretanto, é certo que parte da doutrina ainda reconhece a validade da distinção proposta entre as provas ilícitas e ilegítimas, especialmente considerando que os institutos são distintos quanto aos efeitos e à forma de convalidação, já que a prova ilícita deve ser desentranhada e inutilizada (artigo 157, § 3º, do Código de Processo Penal), ao passo que a prova ilegítima é causa de possível nulidade e refazimento do ato, quando possível[516].

5.5.2. A ilicitude do acesso indevido aos dados armazenados em aparelhos celulares

A partir das premissas conceituais estabelecidas, é inevitável reconhecer que os dados armazenados, em razão de serem representativos da personalidade do seu titular, gozam de proteção constitucional. Com efeito, o acesso indevido aos dados armazenados em aparelhos celulares acarreta violação direta às normas constitucionais que protegem as liberdades públicas do cidadão[517], especialmente o direito à privacidade,

[515] Para tanto, BADARÓ sustenta que há violações de dispositivos constitucionais e legais que, de maneira bifronte, vulneram garantias de proteção às liberdades públicas e, ao mesmo tempo, regras processuais, à exemplo de uma interceptação telefônica autorizada por juiz incompetente. Não bastasse, do ponto de vista material, ambas seriam inutilizáveis, porquanto não poderão ser valoradas pelo julgador na formação de seu convencimento. Outrossim, sob a ótica da dinâmica processual, não haveria diferença prática entre o desentranhamento da prova ilícita e a nulidade ocasionada pela produção da prova ilegítima e tampouco nas repercussões do reconhecimento da prova ilícita, especialmente na prova ilícita por derivação, já que a prova lícita derivada da ilícita, via de regra, será atingida pela inadmissibilidade (artigo 157, § 1º, do Código de Processo Penal), nos mesmos moldes decorrentes da aplicação do princípio da causalidade às provas ilegítimas (artigo 573, § 1º, do Código de Processo Penal). Embora reconheça a importância da doutrina clássica que estabeleceu a distinção entre provas ilícitas e ilegítimas, o Professor das Arcadas arremata que "(...) podem ser definidas como provas ilícitas as provas obtidas, admitidas ou produzidas, com violação das garantias constitucionais, sejam as que asseguram liberdades públicas, sejam as que estabelecem garantias processuais. Os meios de provas obtidos ilicitamente são inadmissíveis no processo, e, se nele indevidamente ingressarem, devem ser desentranhados. Em um ou em outro caso, jamais poderão ser valorados pelo juiz. O desentranhamento da prova dos autos é apenas o mecanismo técnico para assegurar uma proibição de valoração da prova ilícita (...)" (BADARÓ, Gustavo Henrique Righi Ivahy. *Processo Penal*, Op. cit., p. 454-458). No mesmo sentido: LOPES JR., Aury. *Direito Processual Penal.* Op. cit, p. 437-438. Na jurisprudência: STF, HC n.º 82.788/Rj, 2ª Turma, Rel. Min. Celso de Mello, julgado em 12 de abril de 2005, DJ 02/06/2006, p. 43; STJ, AgRg no REsp n.º 1.611.856/PR, 5ª Turma, Rel. Reynaldo Soares da Fonseca, julgado em 7 de fevereiro de 2017, DJe 10/02/2017.

[516] DEZEM, Guilherme Madeira. Curso de processo penal. Op. cit. p. 631-633); LIMA, Renato Brasileiro. Manual de Processo Penal. Op. cit. p. 687; FERNANDES, Antônio Scarance. *Processo penal constitucional.* Op. cit. 86. Na jurisprudência, destaca-se o recente precedente do STJ no HC n.º 598.886-SC, ocasião em que o Min. Rogério Schietti Cruz apontou, em seu voto, a distinção entre as provas ilícitas e ilegítimas, indicando a relevância da distinção (STJ, HC n.º 598.886-SC, 6ª Turma, Rel. Min. Rogério Schietti Cruz, julgado em 27 de outubro de 2020).

[517] BADARÓ, Gustavo Henrique Righi Ivahy. *Processo Penal*, Op. cit., p. 452.

assegurado no artigo 5º, inciso X, da CF[518]. Por consequência, os dados acessados irregularmente estariam inseridos na categoria classificatória de provas ilícitas.

O Superior Tribunal de Justiça (STJ), no já citado precedente que lastreou a jurisprudência formada por aquela Corte, reconheceu ser "ilícita" a devassa dos dados e das conversas de *WhatsApp*, declarando que "(...) a nulidade das provas obtidas no celular do paciente sem autorização judicial, cujo produto deve ser desentranhado dos autos (...)"[519].

Para os adeptos da clássica distinção entre provas ilícitas e ilegítimas, há uma aparente confusão conceitual: ao reconhecer a nulidade da prova, o Superior Tribunal de Justiça teria reconhecido que a prova é ilegítima, já que a "nulidade" é uma das consequências à violação de regras processuais. Entretanto, ao determinar o "desentranhamento" da prova, a Corte teria sinalizado que a prova seria "ilícita", já que esta, em razão de sua inadmissibilidade, deve ser desentranhada e inutilizada, diferentemente do que ocorre com a prova nula[520].

Ainda que se reconheça que, com a redação conferida ao artigo 157, *caput*, do Código de Processo Penal, a jurisprudência tem evitado a utilização do termo "prova ilegítima"[521], é certo que a menção à "nulidade[522]" da prova parecem ter sido realizadas sem a observância do rigorismo processual próprios, especialmente em relação às consequências jurídicas das provas ilegítimas e ilícitas.

---

[518] Sem prejuízo, conforme já estabelecido nos tópicos precedentes, há posições doutrinárias de que os dados armazenados e já comunicados estariam sob a proteção constitucional do artigo 5º, incisos XI e XII, da Constituição Federal.

[519] STJ, RHC n.º 51.531/RO, 6ª Turma, Rel. Nefi Cordeiro, julgado em 19 de abril de 2016, DJe 09/05/2016.

[520] DEZEM, Guilherme Madeira. *Curso de processo penal*. Op. cit. p. 633.

[521] Idem.

[522] Como bem reconhece Zilli, "(...) a rigor a questão é de inadmissibilidade, proclamação que levaria a prova para o terreno da inexistência jurídica. Para além de mera querela terminológica, a distinção entre nulidade e inadmissibilidade no campo das provas ilícitas é mais profunda. Afinal, as nulidades comportam convalidações o que é impossível quando o tema envolve inadmissibilidade da prova. No caso das provas ilícitas, estas ficam permanentemente contaminadas não podendo jamais ser aproveitadas (...)" (ZILLI, Marcos Alexandre Coelho. *A prisão em flagrante e o acesso de dados em dispositivos móveis. Nem utopia, nem distopia. Apenas a racionalidade.* Op. cit., p. 74). Para Jennifer Badaró, a prova seria ilícita por violação ao artigo 157 do Código de Processo Penal, tratando-se de nulidade absoluta arguida a qualquer tempo e em qualquer grau de jurisdição (BADARÓ, Jennifer Falk. *Produção de provas: WhatsApp, Facebook, e-mail.* AASP Boletim, Edição n.º 3096, Dezembro/2019).

Em verdade, apesar da menção à "nulidade" da prova, quer-nos parecer que a prova deve ser tida como "ilícita", porquanto obtidas com violação às normas constitucionais que resguardam a intimidade e privacidade, bem como que o vício ocorre, via de regra, no momento da obtenção da prova, em atividade notadamente extraprocessual.

Ademais, outra problemática exsurge em decorrência do reconhecimento da ilicitude do acesso ao conteúdo. Isto porque a consequência processual da inadmissibilidade é a irrepetibilidade das provas ilícitas, uma vez que o vício se liga à obtenção e descoberta da prova, e não à sua introdução no processo[523].

BADARÓ aponta que a impossibilidade de renovação da prova ilícita não é uma regra absoluta, por não decorrer de uma natureza ontológica das provas. Em verdade, a irrepetibilidade se dá porque o vício da ilicitude costuma ocorrer na obtenção da fonte de prova, de forma que o fator surpresa desaparece após a sua produção, sendo inútil a repetição da prova. Entretanto, em medidas que prescindem de um fator surpresa, não haveria óbice à repetição da prova. Assim, caso reconhecida a ilicitude da quebra de sigilo bancário em decorrência da falta de autorização judicial, nada impediria que uma ordem judicial válida determinasse o fornecimento dos mesmos elementos de prova[524].

Nesta razão, poder-se-ia reconhecer, em tese, a possibilidade da repetição da prova decorrente do acesso ilícito ao conteúdo do aparelho celular, haja vista que o fator surpresa, inerente ao meio de prova, está mais relacionado ao momento da apreensão do aparelho do que ao acesso a seu conteúdo. Sem embargos, em um caso de ilicitude reconhecida diante do acesso sem a correspondente autorização judicial, a prova poderia ser, em tese, repetida a partir de uma nova ordem judicial devidamente fundamentada, especialmente se o aparelho estiver acautelado, livre de influências externas

---

[523] ZILLI, Marcos. *O Pomar e as Pragas*. Boletim do IBCCrim, n. 188, julho/2008; DEZEM, Guilherme Madeira. *Curso de processo penal*. Op. cit. p. 632; LOPES JR., Aury. *Direito Processual Penal.* Op. cit, p. 437. A Lei n.º 13.964/2019 introduziu, no artigo 157, § 5º, do Código de Processo Penal, a obrigação de o juiz, ao tomar conhecimento do conteúdo da prova declarada inadmissível, deixar de proferir a sentença ou o acórdão, com o intuito de impedir que, do ponto de vista psicológico, seja influenciado pelos elementos probatórios ilícitos introduzidos nos autos. Ao que parece, o legislador quis afastar a possibilidade de repetição da prova ilícita, determinando a completa desvinculação do julgador com o conteúdo da prova inadmissível. Registre-se que, por força de liminar concedida pelo Ministro Luiz Fux, nas Ações Diretas de Inconstitucionalidade n.º 6.298, 6.299, 6.300 e 6.305, o dispositivo está com sua vigência suspensa.
[524] BADARÓ, Gustavo Henrique Righi Ivahy. *Processo Penal*, Op. cit., p. 455.

e com seu conteúdo devidamente preservado, impedindo-se a modificação ou remoção física e remota dos dados.

Ao menos em campo jurisprudencial, parece prevalecer o entendimento de que o acesso indevido aos dados armazenados acarreta a irrepetibilidade da prova, com seu subsequente desentranhamento[525] e sem se permitir, ao menos expressamente, a possibilidade de futura renovação[526].

5.5.3. A prova ilícita por derivação e as exceções à inadmissibilidade da prova ilícita: a teoria da fonte independente e da descoberta inevitável

Conforme já mencionado, a prova ilícita deverá ser considerada inadmissível e, por conseguinte, desentranhada dos autos. Entretanto, é certo que a inadmissibilidade não alcança apenas a prova ilícita, mas todas aquelas que dela derivam, em relação de nexo causal[527].

Inspirando-se em precedentes oriundos da jurisprudência norte-americana[528], o legislador acabou por incorporar um conceito extensivo da regra da inadmissibilidade da prova ilícita, admitindo-se a aplicabilidade da "teoria dos frutos da árvore envenenada", pela qual se reconhece o princípio da contaminação[529], por meio do qual se inquina a prova que, embora lícita, seja obtida por intermédio de informações ou elementos decorrentes de uma prova ilicitamente obtida[530].

---

[525] STJ, RHC n.º 75.055/DF, 5ª Turma, Rel. Min. Ribeiro Dantas, julgado em 21 de março de 2017, DJe 27/03/2017.
[526] STJ, HC n.º 542.293/SP, 6ª Turma, Rel. Min. Rogério Schietti Cruz, julgado em 17 de dezembro de 2019, DJe 19/12/2019.
[527] O artigo 157, § 1º, do Código de Processo Penal, dispõe que "são também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras". A doutrina tem reconhecido que a redação do dispositivo é infeliz, já que prevê, como uma das exceções, a ausência de verificação do nexo de causalidade. Como bem aponta GOMES FILHO, "(...) era perfeitamente desnecessária a previsão normativa, na medida em que o conceito de prova derivada supõe, por si só, a existência de uma relação de causalidade entre a ilicitude da primeira prova e a obtenção da segunda. Se o vínculo não estiver evidenciado, é intuitivo que não se trata de prova derivada (...)" (GOMES FILHO, Antonio Magalhães. *Provas. Lei 11.690, de 09.06.2008*. Op. cit. p. 268).
[528] Caso Silverthorne Lumber Co. v. United States, 251 U.S. 385 (1920). Disponível: <https://supreme.justia.com/cases/federal/us/251/385/>. Acesso em: 20 de dezembro de 2020; e caso Nardone v. United States, 302 U.S. 379 (1939). Disponível: <https://supreme.justia.com/cases/federal/us/308/338/>. Acesso em: 20 de dezembro de 2020.
[529] LOPES JR., Aury. *Direito Processual Penal.* Op. cit, p. 444.
[530] BADARÓ, Gustavo Henrique Righi Ivahy. *Processo Penal*, Op. cit., p. 459.

Novamente a partir de conceitos extraídos de julgamentos da Suprema Corte norte-americana[531], o ordenamento jurídico incorporou algumas regras de exceção à inadmissibilidade da prova ilícita por derivação, pelas quais se admite a validade dos elementos probatórios amealhados.

Dentre estas exceções, destacam-se as teorias da "fonte independente" e da "descoberta inevitável", porquanto incorporadas textualmente no Código de Processo Penal e invocadas jurisprudencialmente em julgados relacionados ao acesso a dados armazenados em aparelhos celulares.

A parte final do artigo 157, § 1º, do Código de Processo Penal, estabelece uma regra de exceção à inadmissibilidade da prova ilícita, deixando-se de aplicar a extensão derivativa da prova ilícita aos casos em que as provas "derivadas puderem ser obtidas por uma fonte independente das primeiras". De igual sorte, o artigo 157, § 2º, do mesmo Diploma Legal aponta que "considera-se fonte independente aquela que por si só, seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto da prova".

Embora em uma primeira leitura se verifique que o legislador usou a expressão "fonte independente", em clara tentativa de se positivar a exceção decorrente da "*independent source"* norte-americana (*Murray v. United States, 487 U.S. 533, 1988*)[532], a redação do artigo 157, § 2º indica que, sob o nome de "fonte independente", o legislador definiu o conteúdo da teoria da "descoberta inevitável"[533].

---

[531] Dentre as exceções reconhecidas pela jurisprudência norte-americana (*exclusionary rules*), destacam-se: a exceção de boa-fé (United States v. Leon, 468 U.S. 897, 1984); a exceção de impugnação (Walder v. United States, 347 U.S. 62, 1954); as limitações quanto à legitimidade para requerer a exclusão da prova (United States v. Padilla, 508 U.S. 77. 1993), a teoria dos campos abertos e das buscas particulares (*Open Fields doctrine e Private Searches Doctrine* – Hester v. United States, 265 U.S. 57, 1924; Katz v. United States. 389 U.S. 347, 1967); a teoria da visão ampla (*plain view doctrine* - Coolidge v. New Hampshire, 403 U.S. 443, 1971; Horton v. California, 496 U.S. 128, 1990); a exceção de erro inócuo (Chapman v. California 386 U.S. 18, 1967); a teoria da fonte independente (Murray v. United States, 487 U.S. 533, 1988); a exceção da descoberta inevitável (*Inevitable Discovery* - Nix v. Williams, 467 U.S. 431, 1984); a teoria do nexo causal atenuando (*Purged Tainted Limitation* - Wong Sun v. United States, 371 U.S. 471, 1963), dentre outras.

[532] Disponível em: <https://supreme.justia.com/cases/federal/us/487/533/>. Acesso em: 20 de dezembro de 2020.

[533] GOMES FILHO aponta que o dispositivo "(...) subverte o espírito da garantia constitucional do art. 5.º, LVI. Parece ter havido aqui uma confusão do legislador entre as exceções da 'fonte independente' e da 'descoberta inevitável' (...)", apontando, ao final, a inconstitucionalidade do artigo 157, § 2º, do Código de Processo Penal (GOMES FILHO, Antonio Magalhães. *Provas. Lei 11.690, de 09.06.2008*. Op. cit. p. 269-270). No mesmo sentido: LOPES JR., Aury. *Direito Processual Penal.* Op. cit, p. 446. Para GUILHERME DEZEM, o artigo 157, § 1º, do Código de Processo Penal positiva a teoria da "fonte independente", ao passo que o § 2º

Com efeito, a teoria da "fonte independente" prevê que, em havendo duas fontes das quais a prova pode ser obtida, sendo uma delas considerada lícita e a outra ilícita, não há contaminação da prova derivada, pois outra fonte independente sustentaria a produção da prova. Trata-se, pois, de uma exclusão da própria relação de causalidade.

Já a teoria da "descoberta inevitável", também de inspiração norte-americana (*Inevitable Discovery - Nix v. Williams, 467 U.S. 431,* 1984[534]), é também nominada de "exceção da fonte hipotética independente"[535] e preceitua que a prova derivada da ilícita poderá ser admitida quando as circunstâncias especiais do caso concreto revelarem que a prova seria inevitavelmente descoberta, ainda que suprimida a fonte ilícita.

Entretanto, a doutrina adverte que a redação do dispositivo sob forma condicional ("*puderem ser obtidas"*) abre as portas para a convalidação de toda e qualquer prova derivada da ilícita, uma vez que passa a operar no campo da "possibilidade", prescindindo-se da efetiva comprovação da existência de uma fonte independente[536]. Nesta linha, tem-se recomendado que, somente a partir de circunstâncias do caso concreto, seja analisada a inevitabilidade da descoberta da prova, a partir da linha investigativa desenvolvida naquela investigação, afastando-se, por conseguinte, um juízo meramente abstrato e teórico[537].

No que toca ao acesso a dados armazenados em aparelho celular, o Superior Tribunal de Justiça (STJ) já reconheceu a aplicabilidade da teoria da "fonte independente"[538], admitindo a condenação de réus por tráfico de entorpecentes, mesmo reconhecendo a ilicitude do acesso ao aparelho celular sem a correspondente autorização judicial. Sustenta-se, para tanto, que a existência de outros elementos probatórios licitamente

---

do mesmo dispositivo dispõe sobre o conteúdo da "descoberta inevitável" (DEZEM, Guilherme Madeira. *Curso de processo penal*. Op. cit. p. 650).

[534] Disponível em: <https://supreme.justia.com/cases/federal/us/467/431/>. Acesso em: 20 de dezembro de 2020).

[535] LIMA, Renato Brasileiro. *Manual de Processo Penal.* Op. cit. p. 693.

[536] GOMES FILHO, Antonio Magalhães. *Provas. Lei 11.690, de 09.06.2008*. Op. cit. p. 269-270).

[537] BADARÓ, Gustavo Henrique Righi Ivahy. *Processo Penal*, Op. cit., p. 460; DEZEM, Guilherme Madeira. *Curso de processo penal*. Op. cit. p. 651; LOPES JR., Aury. *Direito Processual Penal.* Op. cit, p. 449-450. No mesmo sentido: STJ, HC n.º 351.407/PR, 5ª Turma, Rel. Min. Reynaldo Soares da Fonseca, julgado em 1º de dezembro de 2016, DJe 14/12/2016.

[538] STJ, RHC n.º 120.726/SP, 5ª Turma, Rel. Min. Reynaldo Soares da Fonseca, julgado em 18 de fevereiro de 2020, DJe 28/02/2020; STJ, HC n.º 588.135/SP, 5ª Turma, Rel. Min. Reynaldo Soares da Fonseca, julgado em 8 de setembro de 2020, DJe 14/09/2020.

obtidos, tais como a apreensão de drogas, valores em dinheiro e outros objetos[539] ou, ainda, provas testemunhais indicando a localização dos entorpecentes[540] e a própria confissão dos acusados[541], podem ser consideradas fontes independentes aptas para se autorizar a condenação.

Por sua vez, o Supremo Tribunal Federal (STF) já reconheceu a aplicabilidade da teoria da "descoberta inevitável", afirmando que mesmo que se pudesse reputar a prova produzida como ilícita, seria aplicável o artigo 157, § 2º, do Código de Processo Penal, pelo que "(...) só fato de serem apreendidos os aparelhos celulares, indubitavelmente, levaria — como de fato aconteceu — à quebra do sigilo dos dados telefônico do corréu com a consequente identificação dos usuários das linhas móveis e fixas que com ele mantiveram contato, mormente na data do cometimento do crime — trâmite esse, friso, típico e de praxe em casos análogas aos dos autos (...)"[542].

[539] STJ, HC n.º 537.274-MG, 5ª Turma, Rel. Min. Leopoldo de Arruda Raposo, julgado em 19 de novembro de 2019, DJe 26/11/2019.
[540] STJ, HC n.º 378.374/MG, 6ª Turma, Rel. Min. Maria Thereza Rocha de Assis Moura, DJe 30/03/2017.
[541] STJ, AgRg no HC n.º 521.228/RJ, 5ª Turma, Rel. Min. Jorge Mussi, julgado em 3 de dezembro de 2019, DJe 16/12/2019.
[542] STF, HC n.º 91.867/PA, 2ª Turma, Rel. Min. Gilmar Mendes, j. 24/04/2012, DJe 19/09/2012. A decisão é alvo de ponderadas críticas de Marcos Zilli, para quem "(...) fica evidente o equívoco do raciocínio manifestado quando do julgamento do HC 91.867/PA, pelo STF. Naquela oportunidade, o Min. Gilmar Mendes entendeu que os dados armazenados no aparelho seriam inevitavelmente descobertos, caso os agentes tivessem simplesmente apreendido o aparelho, provocando, na sequência, uma decisão judicial autorizadora do acesso. A descoberta inevitável, contudo, rompe o efeito contaminatório entre a ilicitude original e as provas derivadas. Não se trata de regra de convalidação da ilicitude original. Logo, o acesso indevido é que constitui o ponto nevrálgico. Representa o "pecado original" que induz à imprestabilidade absoluta do material diretamente obtido. A partir deste ponto surge o efeito irradiador da ilicitude. E é sobre este efeito irradiador que se projetam as regras limitadoras da contaminação como é o caso da descoberta inevitável. A aplicabilidade da regra supõe ao menos dois percursos. Um ilícito que se concretiza até o fim. E outro lícito que é interrompido diante da antecipação da ação ilegal. Tome-se, mais uma vez, o precedente do caso Nix v Williams. A confissão é a prova ilícita. O encontro do corpo não. Ainda que o local tivesse sido revelado pela confissão, paralelamente existia um movimento lícito – ação dos voluntários – que, se ultimado, levaria à localização do corpo. No acesso indevido aos dados, não há esta opção. É ele a fonte ilícita original (...)" (ZILLI, Marcos Alexandre Coelho. *A prisão em flagrante e o acesso de dados em dispositivos móveis. Nem utopia, nem distopia. Apenas a racionalidade.* Op. cit., p. 92-93).

6. O ACESSO A DADOS ARMAZENADOS EM APARELHOS CELULARES: UM ESTUDO SOB O PRISMA DO DIREITO COMPARADO

Nunca é tarefa fácil avançar sobre a experiência de diversos países sobre determinado tema jurídico, especialmente considerando as dificuldades e peculiaridades inerentes à circulação de ideias jurídicas entre sistemas processuais bastante distintos[543].

Entretanto, é certo que as perspectivas trazidas a partir do direito comparado contribuem para o estudo e conhecimento do tema, ao menos sob um prisma argumentativo. Nesta ordem, sem a pretensão de se imiscuir densamente sobre a matéria, é relevante destacar como alguns países[544] têm lidado com o acesso a dados armazenados em aparelhos celulares.

6.1. Argentina

O *Código Procesal Penal* argentino, em uma previsão bastante similar àquela contida no artigo 6º, inciso I, do Código de Processo Penal brasileiro, estabelece em seu artigo 184, 2[545] a necessidade das forças policiais e de segurança zelarem e conservarem os rastros materiais do delito que forem deixados em uma cena de crime.

De igual sorte, em previsão bastante semelhante ao artigo 240, § 2º, do Código de Processo Penal brasileiro, o ordenamento processual penal argentino prevê,

---

[543] Sobre o tema, especialmente com relação às hipóteses de transplantes jurídicos e traduções jurídicas, recomenda-se a obra de Máximo Langer (LANGER, Maximo. *From Legal Transplants to Legal Translations: The Globalization of Plea Bargaining and the Americanization Thesis in Criminal Procedure*. In Harvard International Law Journal. v. 45. n. 01, 2004. p. 01-65).

[544] A escolha dos países estudados não se deu de forma aleatória. No julgamento do *Habeas Corpus* n.º 51.531/RO, perante o Superior Tribunal de Justiça (STJ), a Ministra Maria Thereza Rocha de Assis Moura destacou o desenvolvimento do tema sob a perspectiva jurisprudencial norte-americana, canadense e espanhola. Assim, estendeu-se a pesquisa para mais dois países pautados pelo sistema da *civil law* (México e Argentina), bem como para mais um país regido pelo sistema jurídica da *common law* (Inglaterra).

[545] Art. 184. - Los funcionarios de la policía o de las fuerzas de seguridad tendrán las siguientes atribuciones:
(...)
2°) Cuidar que los rastros materiales que hubiere dejado el delito sean conservados y que el estado de las cosas no se modifique hasta que lo disponga la autoridad competente.

em seu artigo 230-bis[546], as hipóteses de requisição e inspeção direta, pelas forças policiais e de segurança, de pessoas e seus pertencentes pessoais, incluindo-se o interior de veículos, aeronaves e barcos, dispondo sobre os requisitos legais para a realização da busca sem autorização judicial.

Em um caso submetido à apreciação judicial, discutiu-se a legalidade do acesso aos dados de um aparelho celular supostamente furtado, encontrado em poder de um suspeito.

Na ocasião, o agente policial retirou o *chip* do aparelho encontrado e o inseriu em outro telefone, com o intuito de identificar a vítima. Em seguida, telefonou para o primo da vítima, a quem informou sobre o delito.

A *Camara Nacional de Apelaciones en lo Criminal y Correccional*[547], em apreciação ao recurso de apelação interposto pelo investigado, determinou a nulidade da prova produzida e a liberação do suspeito, haja vista que o acesso aos dados contidos no aparelho não estariam circunscritos às hipóteses dos artigos 184, 2 e 230-bis, do *Código Procesal Penal*.

Sustentou-se, para tanto, a irregularidade da atuação policial, já que não se verificou uma situação de urgência ou gravidade que o legitimou a atuar desta forma, o que poderia comprometer a cadeia de custódia da prova.

---

[546] Art 230 bis. - Los funcionarios de la policía y fuerza de seguridad, sin orden judicial, podrán requisar a las personas e inspeccionar los efectos personales que lleven consigo, así como el interior de los vehículos, aeronaves y buques, de cualquier clase, con la finalidad de hallar la existencia de cosas probablemente provenientes o constitutivas de un delito o de elementos que pudieran ser utilizados para la comisión de un hecho delictivo de acuerdo a las circunstancias particulares de su hallazgo siempre que sean realizadas: a) con la concurrencia de circunstancias previas o concomitantes que razonable y objetivamente permitan justificar dichas medidas respecto de persona o vehículo determinado; y, b) en la vía pública o en lugares de acceso público. La requisa o inspección se llevará a cabo, de acuerdo a lo establecido por el 2° y 3er. párrafo del artículo 230, se practicarán los secuestros del artículo 231, y se labrará acta conforme lo dispuesto por los artículos 138 y 139, debiendo comunicar la medida inmediatamente al juez para que disponga lo que corresponda en consecuencia. Tratándose de un operativo público de prevención podrán proceder a la inspección de vehículos

[547] CCC 37443/2018/2/CA2, julgado em 31 de julho de 2018.

Ainda, apontou-se que o procedimento adotado vulnerou o direito de defesa do imputado, que não teve a oportunidade de controlar a produção da prova, a qual fora produzida sem a presença de testemunhas, resultando em uma medida irreproduzível.

Finalmente, a Corte Argentina reconheceu a violação à privacidade, especialmente diante da proteção aos dados pessoais contidos no aparelho celular, em cotejo com a análise quanto ao avanço da tecnologia e dos meios de comunicação.

6.2. Estados Unidos

A *Fourth Amendment* da Constituição dos Estados Unidos tutela a inviolabilidade do cidadão, de suas casas e papéis contra buscas e apreensões irrazoáveis, de modo que um mandado judicial somente poderá ser expedido com base em causa provável ("*probable cause*"), confirmada por juramento ou declaração, com a descrição particular do lugar a ser buscado, as pessoas e coisas a serem apreendidas.

A tutela da inviolabilidade de domicílio, em sua pretensão originária, busca estabelecer uma linha para se proteger os direitos e garantias individuais em face da tirania investigativa estatal, salvaguardando-se a privacidade e a liberdade dos cidadãos[548].

A precitada disposição constitucional integra o corpo constitucional desde 1792 e, desde então, vem sendo alvo de sucessivas reinterpretações de modo a adaptá-la à evolução das circunstâncias sociais, das escolhas políticas[549], econômicas e tecnológicas, sem alteração da redação constitucional que se manteve inalterada por séculos[550].

---

[548] Nos dizeres de Renée Hutchins, a *Fourth Amendment* deve ser reconhecida como "(...) a wall between a free society and overzealous police action - a line of defense implemented by the framers to protect individuals from the tyranny of the police state (...)" (HUTCHINS, Renée McDonald, *Tied Up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L. Rev. 409, 444, 2007).

[549] TOKSON, Matthew. *Knowledge and Fourth Amendment Privacy.* Vol. 111, n.1, Northwestern University Law Review, p. 194.

[550] Dentre as diversas teorias interpretativas, uma delas ganha especial relevância, notadamente a do "equilibrium-adjustment", que foi bem desenvolvida por Orin S. Kerr como sendo "(...) a judicial response to changing technology and social practice. When new tools and new practices threaten to expand or contract police power in a significant way, courts adjust the level of Fourth Amendment protection to try to restor the prior equilibrium. The result is a correction mechanis. When changing technology or social practice makes evidence substantially harder for the government to obtain, the Supreme Court generally adopts lower Fourth Amendment protections for these new circumstances to help restore the status quo ante level of government power. On the other hand, when changing technology or social practice makes evidence substantially easier for the government to obtain, the Supreme Court often embraces higher protections to help restore the prior level of privacy protection. Fourth Amendment protection resembles the work of drivers trying to maintain

Uma evolução clássica da interpretação da *Fourth Amendment* ao longo do tempo se deu na extensão do alcance protetivo conferido pela previsão constitucional em questão, especialmente com relação aos objetos passíveis de apreensão e de proteção pelas *Fourth Amendment*.

Em uma primeira fase interpretativa, simbolizada pelo julgamento do "*Olmstead v. United States*" (277 U.S. 438-1928)[551], reconheceu um direito probatório de primeira geração, cuja interpretação se atém a uma perspectiva física e estrita de objetos, lugares ou coisas. Trata-se da teoria da *trespass-doctrine*, segundo a qual a infringência à *Fourth Amendment* ocorreria apenas nos casos de violação ou penetração a uma área tangível e demarcável de um espaço físico e privado, o que não teria ocorrido, já que a interceptação da conversa se deu diretamente na fiação da empresa telefônica e em via pública[552].

Mais de quarenta anos depois, a Suprema Corte tornou a revisitar o assunto no caso "*Katz v. United States*" (389 U.S. 347-1967)[553] e deu início a uma segunda

---

constant speed over mountainous terrain: judges add extra gas when facing an uphill climb and ease off the pedal on the downslopes (…) " (KERR, Orin S., *An Equilibrium-Adjustment Theory of the Fourth Amendment.* 125 Harvard Law Review 476. 2011, p. 478). Revela-se que a relação do "*Equilibrium-Adjustment*" assume um papel relevante de mecanismo de correção, servindo como guia de referência para a interpretação jurisprudencial sobre conceitos genéricos e indeterminados da Constituição Federal, especialmente quando confrontados com estes novos cenários, servindo ainda como referência histórica visando restaurar um status quo de equilíbrio e ponderação entre ferramentas investigativas na atuação policial e os direitos e garantias inerentes aos cidadãos.
Com isso, a teoria em questão consegue restaurar a fidelidade da intenção do constituinte, quando da edição do comando normativo sobre o tema, permitindo-se uma maior coerência nas decisões judiciais, além de aumentar a estabilidade e segurança jurídica, assegurando-se que mudanças interpretativas somente serão implementadas quando e tão somente se as circunstâncias sociais e tecnológicas também se alterarem.

[551] "Olmstead" teve conversas telefônicas interceptadas, sem autorização judicial, mediante a inserção de um equipamento na fiação da empresa telefônica, em via pública. Apreciando-se a regularidade, a Suprema Corte reverteu decisão judiciária local e sustentou que a escuta telefônica realizada por agentes policiais, sem autorização judicial, não constituiria violação *Fourth Amendment*, haja vista que não teria ocorrido efetiva penetração ou violação ao seu domicílio enquanto propriedade privada. Assim, a medida não se enquadraria na situação de "search and seizure" especificados no precitado comando constitucional, já que as comunicações telefônicas "(...) are not part of his house or office, any more than are the highways along which they are streched (...)" (Chief Justice Taft) (Disponível em: <https://supreme.justia.com/cases/federal/us/277/438/>. Acesso em: 20 de dezembro de 2020).

[552] DOENES, William S. *Search and Seizure: The Physical Trespass Doctrine and the Adaption of the Fourth Amendment to Modern Technology*, 2 Tulsa L. J. 180 (2013), Disponível em: https://digitalcommons.law.utulsa.edu/cgi/viewcontent.cgi?article=1038&context=tlr. Acesso em: 20 de dezembro de 2020. No mesmo sentido: KNIJNIK, Danilo. *A trilogia Olmstead-Katz-Kyllo: o art. 5º da Constituição Federal do século XXI.* Op. cit., p. 85. GRAY, David. *The Fourth Amendment in an Age of Surveillance.* Cambridge University Press, 2017, p. 72-100.

[553] No caso, agentes de polícia instalaram, sem autorização judicial uma escuta em uma cabine de telefone pública, passando a gravar as conversas mantidas por Charles Katz, suspeito de apostas ilegais. Posteriormente, estes registros foram utilizados como elementos probatórios, já que a intervenção se deu em uma cabine de telefone público, sem qualquer ingresso a espaço físico, privado e delimitado, de Katz. Entretanto, a Suprema Corte Americana sustentou que, a despeito da gravação ter se dado em uma cabine telefônica, a medida adotada

fase interpretativa, que culminou na formação dos direitos probatórios de segunda geração, evoluindo-se para a tutela de uma proteção constitucional integral, segundo a qual a proteção à *Fourth Amendment* protege pessoas e suas respectivas comunicações, não estando limitados aos espaços e coisas físicas e tangíveis.

Entretanto, o advento de novas técnicas investigativas deu impulso à necessidade de uma releitura da proteção conferida pela *Fourth Amendment*, estampado no caso "*Kyllo v. United States*" (533 U.S. 27. 2001)[554], consagrando-se os direitos probatórios

---

pelas autoridades investigativas caracterizou uma violação à razoável expectativa de privacidade de Katz ("reasonable expectation of privacy"), anulando-se a condenação por entender que a medida constituiu uma efetiva busca e apreensão em violação à Fourth Amendment. Portanto, em uma medida de readequação da interpretação da *Fourth Amendment*, a maioria da Corte formou o convencimento de que, ainda que em uma cabine pública, "(...) one who occupies it, shuts the door behind him, and pays the toll that permits him top lace a call surely entitled to assume that the words he utters into the moughtpiece will not be broadcast to the world (...)" (Justice Stewart).
Assim, havendo uma expectativa de privacidade nas conversas telefônicas e diante do desenvolvimento da tecnologia em questão, houve um fortalecimento da tutela à privacidade, com a determinação de que as escutas telefônicas somente poderiam ser implementadas mediante autorização judicial. A partir do caso Katz v. United States, firmou-se duas premissas concebidas por Justice Harlan, nominadas de "the reasonable expectation of privacy test", que balizariam a interpretação se uma busca realizada estaria sujeita aos limites da Fourth Amendment: será considerada uma busca invasiva quando violar (a) a existência de uma real e efetiva expectativa subjetiva de privacidade; (b) que esta expectativa de privacidade seja reconhecida, socialmente, como razoável e legítima (Disponível em: <.https://supreme.justia.com/cases/federal/us/389/347/>. Acesso em 20 de dezembro de 2020). Sobre o tema, recomenda-se: WINN, Peter. *Katz and the Origins of the "Reasonable Expectation of Privacy"* Test. 40 McGeorge L. Rev. (2016). Disponível em https://scholarlycommons.pacific.edu/mlr/vol40/iss1/1. Acesso em: 20 de dezembro de 2020.

[554] No caso, agentes policiais conseguiram identificar, através da utilização de dispositivos capazes de obter imagens térmicas ("termal imaging device"), que Kyllo estava plantando e cultivando entorpecentes ("marijuana") em sua residência, utilizando-se de lâmpadas térmicas para propiciar um melhor desenvolvimento da planta. Assim, por intermédio dos dispositivos térmicos, conseguiu-se colher indicativos de que elevadas atividades de calor se desenvolviam no interior do imóvel e, com isso, foi requerido a um juiz uma ordem de busca e apreensão. A ordem foi concedida e, durante as buscas, conseguiu-se localizar os entorpecentes plantados por Kyllo, motivando-se sua prisão. Durante o julgamento do caso, Kyllo pretendeu suprimir a prova produzida a partir das imagens térmicas, aduzindo que, a despeito do mandado judicial de busca e apreensão posterior, é certo que a própria captação térmica demandaria autorização judicial específica. Entretanto, adotando-se os critérios estabelecidos no "Reasonable of Expectation Test", o Estado reconhecia que não teria havido busca, já que as radiações de calor não constituem coisas ou pertences, bem como que Kyllo, ao deixar de tentar conter a emanação de calor oriunda de sua propriedade em razão do cultivo de entorpecentes, revelou não ter real expectativa de privacidade. Ademais, o equipamento técnico utilizado não descortinou detalhes íntimos da vida de Kyllo. A Suprema Corte, em apertada decisão, sustentou que uso de imagens térmicas da residência de Kyllo constituiu, indevidamente, uma espécie de busca e apreensão. Sustentou-se, para tanto, que a tecnologia utilizada não era de domínio público, o que colocaria qualquer pessoa em sua residência a mercê do avanço tecnológico que exploraria detalhes de uma residência que não seriam acessíveis sem uma intrusão física. Desta feita, tendo em vista que a Polícia não dispunha de mandado judicial quando da utilização do dispositivo, a busca foi considerada presumivelmente desarrazoada e inconstitucional. A decisão pecou ao não estabelecer referenciais claros para nortear as interpretações vindouras. Ao decidir pela ilegalidade da ação policial em razão do equipamento de coleta de imagens térmicas não estar disponível ao uso comum, a Suprema Corte deixou margem para se legitimar as ações com uso destes equipamentos, tão logo sejam difundidos para uso generalizado. Entretanto, parece claro que a decisão da Suprema Corte sinalizou sua preocupação com o excessivo avanço tecnológico, que passou a quebrar a relação de equilíbrio no contraste entre a eficiência da atividade investigativa e as garantias da proteção domiciliar (Disponível em <https://supreme.justia.com/cases/federal/us/533/27/>. Acesso em 20 de dezembro de 2020).

de terceira geração, que são exigidos no tratamento de "provas de terceira geração", assim consideradas aquelas decorrentes de buscas superintrusivas ("hyper-intrusive searches"), observações virtuais ("virtual surveillance") e decorrentes de organização de grandes volumes de informações ("high volume collection")[555].

É certo, pois, que a utilização de tecnologias bastante avançadas, que permitem um elevado grau de intrusão na privacidade alheia, encontram resistência legítima na tutela constitucional conferida à privacidade e à inviolabilidade domiciliar. Não se desconhece, portanto, que a definição de qual tecnologia se sujeitará ao prévio escrutínio judicial é uma zona bastante cinzenta, especialmente diante da impossibilidade de se acompanhar, jurisprudencialmente, a farta evolução tecnológica[556].

Registre-se que estes direitos probatórios de terceira geração foram reconhecidamente apontados pelo Superior Tribunal de Justiça (STJ), em acórdão precursor sobre o tema, como um dos fundamentos que para se decidir pela imprescindibilidade da autorização judicial no acesso a dados armazenados em aparelhos celulares[557].

---

[555] DI PAOLO, Gabriella. *Tecnologie del controllo e prova penale: l'esperienza statunitense e spunti per la comparazione*. Padova: Editora Cedam, 2008, p. 18, *apud* KNIJNIK, Danilo. *A trilogia Olmstead-Katz-Kyllo: o art. 5º da Constituição Federal do século XXI.* Op. cit. p. 82.

[556] Entretanto, KNIJNIK busca estabelecer um critério interpretativo, ao estabelecer que: "(...) A questão de verificar, portanto, quando uma ação policial representa restrição a direito fundamental, estando na área da reserva de jurisdição por meio de mandado, dependerá, para além de seus requisitos gerais, do estabelecimento de três requisitos: (a) que a observação ou ação policial tenha alcançado determinadas informações ou elementos de prova que, de outro modo, não seriam disponíveis; (b) que os recursos tecnológicos utilizados na diligência superem ou agucem as capacidades sensórias normais, inerentes ao ser humano; (c) que os aparelhos e mecanismos empregados sejam estranhos ao uso geral da sociedade. Embora difícil, o ponto inicial da linha divisória está entre o que pode ser alcançado mediante observação a olho nu ou não, sendo essa uma primeira indagação a fazer. Uma busca ou observação a olho nu não é "busca" ou restrição ao direito fundamental à privacidade. Uma busca ou observação com recursos tecnológicos pode ou não ser conduzida à revelia de um mandado, dependendo da natureza da tecnologia empregada e, obviamente, dos locais em que realizada. Nesse caso, ela é mais que uma observação. Dito de outra forma, é preciso levar em consideração 'as capacidades tecnológicas do instrumento utilizado e que tipo de informação ele é apto a revelar'(...) Em conclusão, toda vez que, não obstante em lugares públicos, as autoridades investigatórias lançarem mão de recursos tecnológicos não disponíveis ao público, capazes de observar o que os órgãos dos sentidos não alcançariam, por meio de equipamentos que não são de domínio da sociedade, estaremos em presença de uma restrição a direito fundamental, sujeita, portanto, à reserva de jurisdição. Somente assim evitar-se-á que a tecnologia leve a uma compressão definitiva dos espaços mínimos protegidos pelas garantias constitucionais fundamentais, o que entre nós também supõe, ao fim e ao cabo, a construção de um art. 5º da Constituição Federal compatível com as necessidades do século XXI, ou seja, com as provas e o direito probatório de terceira geração (...)" (KNIJNIK, Danilo. *A trilogia Olmstead-Katz-Kyllo: o art. 5º da Constituição Federal do século XXI.* Op. cit. p. 95-96).

[557] Conforme voto do Min. Rogério Schietti Cruz em: STJ, Recurso em *Habeas Corpus* n.º 51.531/RO, 6ª Turma, Rel. Min. Nefi Cordeiro, julgado em 19 de abril de 2016, DJe 09/05/2016.

A partir das premissas fixadas e diante do sensível avanço tecnológico, a Suprema Corte foi desafiada a apreciar a constitucionalidade do acesso ao conteúdo de aparelhos celulares, por policiais, sem prévia ordem judicial autorizativa.

Nos casos *Riley v. California* (573 U.S. 373 2014)[558] e no precedente *"United States, Petitioner v. Brima Wurie"*[559], a Suprema Corte enfrentou a mesma questão: a constitucionalidade do acesso a dados armazenados em aparelhos celulares, sem prévia ordem judicial autorizativa. No julgamento, a Corte analisou[560] se precedentes jurisprudenciais anteriores, que excepcionavam a prévia necessidade de ordem judicial para a realização de busca e apreensões, poderiam ser aplicados aos casos.

Em oposição a diversos julgamentos anteriores, a Suprema Corte afastou as exceções previstas nos precedentes existentes[561] e reconheceu que as informações armazenadas em celulares não podem ser utilizadas, via de regra, como instrumento para

---

[558] Riley foi abordado por um policial, haja vista que conduzia o automóvel com a habilitação vencida. Porém, em averiguação realizada no automóvel, os policiais localizaram uma arma de fogo escondida, municiada, o que motivou sua prisão. Em seguida, durante as vistorias realizadas no interior do automóvel, os policiais suspeitaram que Riley poderia integrar uma quadrilha de roubadores que praticariam diversos crimes na região. Por esta razão, os policiais retiraram o smartphone do bolso de Riley e passaram a examinar seu conteúdo, encontrando iniciais e gírias que remetiam à gangue da qual suspeitavam, motivando-se ainda uma análise dos registros de fotos e vídeos do aparelho. Com as provas obtidas, Riley foi condenado por ocultação da arma, porte de munição e também pelos fatos praticados enquanto integrante da quadrilha de roubadores, notadamente tentativa de homicídio e agressão com arma de fogo, recebendo uma pena de 15 (quinze) anos de prisão. Após ter apelado às instâncias superiores, os recursos de Riley não foram providos, tendo a discussão quanto à constitucionalidade do acesso aos dados chegado à Suprema Corte (Disponível em: <https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf>. Acesso em: 20 de dezembro de 2020).

[559] Brima Wurie teria sido preso por, supostamente, estar comercializando entorpecentes. Levado à Delegacia de Polícia, seus dois aparelhos celulares foram apreendidos, tendo os agentes identificado diversas chamadas em curso, todas provenientes de uma identificação de "minha casa", o que permitiu que os policiais identificassem o número de origem da chamada e rastreassem a ligação. Identificada a residência de Wurie, os policiais solicitaram um mandado de busca e apreensão para a entrada no local, que fora concedido. Em diligências, os policiais constataram que localizaram grande quantidade de entorpecentes, armas, munição e dinheiro, motivando-se uma condenação à pena de mais de 20 (vinte) anos de reclusão.

[560] Com efeito, a regra estabelecida na *Fourth Amendment* é de que as buscas e apreensões exigem prévia ordem judicial, mediante comprovada "probable cause". Entretanto, uma dentre diversas exceções é a da busca durante uma prisão, nominada "search incident to a lawful arrest" ou "search incident to arrest (SITA)", formada a partir de diversos precedentes, dentre os quais se destacam os casos Chimel v. California (395 U.S. 752, 1969) , United States v. Robinson (414 U.S. 218, 1973) , Maryland v. Buie (494 U.S. 325, 1990) e Arizona v. Gant (556 U.S. 332, 2009). Sob essas premissas, a Suprema Corte analisou se o acesso a dados armazenados em aparelhos celulares poderia estar inserido nas hipóteses excepcionais da "search incident to a lawful arrest" ou "search incident to arrest (SITA)". Assim, a Suprema Corte reconheceu que as buscas realizadas durante uma prisão devem se limitar à área de imediato controle e alcance do suspeito (*reachable, grabbable area*), sempre justificada para se evitar a fuga, a destruição de provas ou para proteção e segurança dos próprios policiais, não se autorizando uma extensão da busca ao imóvel do investigado sem prévia autorização judicial (https://supreme.justia.com/cases/federal/us/395/752/. Acesso em 20 de dezembro de 2020).

[561] Para uma análise detida sobre o tema, confira-se: SHOEBOTHAM, Leslie A. *The Strife of Riley: The Search-Incident Consequences of Making an Easy Case Simple.* Loyola University New Orleans College of Law, 75 La. L. Rev. 29 (2014), p. 48-57.

ferir ou ofender a integridade corporal do policial que realizou a prisão e tampouco como meio de fuga para o acusado. Assim, ainda que seja facultada ao policial a análise das características do celular[562], a fim de garantir que não poderia ser usado como arma, o acesso aos dados do telefone não estaria incluído nesta análise[563].

Ainda, a Suprema Corte afirmou que não há como se equiparar a violação à privacidade do indivíduo durante uma simples busca corporal com a perscrutação digital dos dados armazenados no aparelho celular, os quais são vastos e extensivos, permitindo-se uma desproporcional violação à privacidade e intimidade da pessoa detida[564].

Finalmente, admitiu-se que, na busca realizada em dados armazenados, as fontes de informações potencialmente pertinentes são virtualmente ilimitadas, de modo que a combinação de variadas fontes de dados, de longa abrangência temporal e guardados em dispositivos modernos dotados de elevado poder de armazenamento, são elementos representativos da absoluta exposição à privacidade e intimidade que o acesso aos dados pode oferecer, justificando-se a necessidade de prévia autorização judicial[565].

Por derradeiro, a Suprema Corte admite que a decisão pode trazer sensíveis impactos na capacidade de combate à criminalidade, já que os celulares se tornaram importantes ferramentas para facilitar a coordenação e comunicação entre membros de organizações criminais, bem como pode fornecer valiosas informações sobre perigosos agentes criminosos.

Entretanto, a Corte arremata que a privacidade tem um preço e que os modernos aparelhos celulares, ao permitirem que os indivíduos carreguem inúmeros dados representativos de sua vida íntima, gozam da proteção antevista pelos constituintes norte-americanos.

---

[562] PASCHOAL, Jorge Coutinho. *Caso Riley v. California (Suprema Corte dos Estados Unidos da América) – o acesso aos dados registrados em aparelhos de telefonia móvel e o resguardo da intimidade*. Revista Fórum de Ciências Criminais (RFCC), v. 4, p. 257, 2015.

[563] Disponível em: <https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf>, p. 7. Acesso em: 20 de dezembro de 2020.

[564] Disponível em: <https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf>, p. 9-10. Acesso em: 20 de dezembro de 2020)

[565] Disponível em: <https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf>, p. 3. Acesso em: 20 de dezembro de 2020)

Assim, os julgadores concluem que "(…) our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple - get a warrant (…)[566]"

Ressalte-se, todavia, que a Suprema Corte admitiu como exceção à necessidade de ordem judicial a busca realizada por policiais quando houver suspeita de que o indivíduo estaria digitando no aparelho celular para acionar um dispositivo explosivo e, ainda, nas hipóteses em que o acesso for imprescindível por conter a localização de uma criança sequestrada[567].

A despeito da manifestação da Suprema Corte sobre o tema, é certo que precedentes de outras Cortes Federais têm admitido a possibilidade do acesso direto, independentemente de ordem judicial, do conteúdo dos aparelhos celulares pertencentes a imigrantes que aportam às fronteiras dos Estados Unidos[568]. Não bastasse, ainda há discussões doutrinárias se a decisão adotada alcança também os dados armazenados em sistema de nuvem (*cloud computing*) e em outros dispositivos móveis eletrônicos[569].

---

[566] https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf, p. 25-28. Acesso em: 20 de dezembro de 2020. Em tradução livre: *"*(...) Nossa resposta à questão do que a polícia deve fazer antes de pesquisar um telefone celular apreendido incidente para uma prisão é, portanto, simples: obter um mandado"

[567] https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf, p. 27. Acesso em: 20 de dezembro de 2020.

[568] No caso *United States v. Molina-Isidoro, 884, F. 3d 287 (March 1, 2018)* a United States Court of Appeals for the Fifth Circuit reconheceu ser legítima a busca realizada, sem ordem judicial, no telefone celular de um imigrante que teria sido flagrado carregando metanfetamina em sua mala. Para tanto, a Corte apontou que as abordagens de rotina, em fronteiras norte-americanas, podem ser realizadas independentemente de qualquer suspeita, bem como que "(...) Riley v. California left open the possibility that other case-specific exceptions may still justify a warrantless search of a particular phone. That caveat means it is reasonable for border agents to continue to rely on the robust body of pre-Riley caselaw that allows warrantless border searches of computers and cell phones. Not a single court addressing border searches of computers since Riley has read it to require a warrant (…)". De igual sorte, a United States District Court for the Eastern District of New York, no caso *United States v. Oladokun 2016 U.S. Dist. LEXIS 98164 (July 27, 2016*), reconheceu como legítima a busca a um aparelho celular de um nigeriano que pretendia ingressar nos Estados Unidos, diante das suspeitas de fraude na obtenção do visto.

[569] Como bem definem Moore, Langton e Pochron, "(...) Riley, however, is not the last word on searching digital information on cell phones and other devices. The justices left many areas open for interpretation and future Supreme Court decisions. Specifically, Riley's application to other electronic devices remains uncertain. Similarly, Riley deliberately fails to address cell phone searches in the context of other warrantless searches such as plain view or the automobile exception. For now, law enforcement must work within the confines of Riley and obtain warrants in most search incident to arrest situations. The small blueprint of acceptable techniques provided by the Supreme Court should be carefully followed as the legal wrangling continues. While seemingly straightforward, the Riley decision has provided the platform from which contentious debate will undoubtedly rise, as the intersection of technology and criminal procedure continues to impact the law (…)" (MOORE, Jennifer L.; LANGTON, Jonathan; POCHRON, Joseph. *The cost of privacy: Riley v. California's impact on cell phone searches*, JDFSL, vol. 9, number 3)

6.3. Canadá

A *Section 8* da *"The Canadian Charter of Rights and Freedoms"* prevê que "everyone has the right to be secure against unreasonable search or seizure". Diante da previsão genérica contida no dispositivo, coube à jurisprudência definir o alcance interpretativo da previsão, especialmente com relação às hipóteses de "unreasonable search and seizure".

A jurisprudência da Corte Suprema canadense definiu que as buscas e apreensões ("searchs and seizures"[570]) somente serão consideradas "reasonables" quando, geralmente, precedidas de ordem judicial autorizativa[571]. Assim, serão consideradas presumivelmente "unreasonables" as buscas e apreensões realizadas sem prévio mandado judicial, salvo nas hipóteses em que: 1) as buscas forem autorizadas por lei; 2) que a lei autorizativa seja, ela mesma, "reasonable"[572]; 3) que a maneira pela qual a busca é realizada seja considerada razoável[573].

Da mesma forma estabelecida pela jurisprudência norte-americana, a busca realizada durante uma detenção somente poderá ser feita diante de objetivos bem definidos, notadamente para se garantir a segurança da pessoa detida e dos oficiais, para

---

[570] Saliente-se que nem todas as formas de inspeção, exame ou apreensão serão consideradas dentro do contexto normativo de *"search or seizure"*. Como definiu a jurisprudência canadense, "(…) not every form of examination conducted by the government will constitute a 'search' for constitutional purposes. On the contrary, only where those state examinations constitute an intrusion upon some reasonable privacy interest of individuals does the government action in question constitute a 'search' within the meaning of s. 8' (…). 11. It is only '[i]f the police activity invades a reasonable expectation of privacy, [that] the activity is a search'; R. v. Wise, [1992] 1 S.C.R. 527, at p. 533. Second, as the language of s. 8 implies, even those investigations that are 'searches' are permissible if they are 'reasonable'. A search will not offend s. 8 if it is authorized by a reasonable law and carried out in a reasonable manner (…)" (R. v. Tessling, [2004] 3 S.C.R. 432, 2004, SCC 67, at p. 18, disponível em <https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/2183/index.do>. Acesso em: 20 de dezembro de 2020).

[571] R. v. Nolet, 2010 SCC 24, [2010] 1 S.C.R. 851, at p. 21, disponível em <https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/7865/index.do>. Acesso em: 20 de dezembro de 2020.

[572] Disponível em: <https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art8.html>. Acesso em: 20 de dezembro de 2020*).*

[573] Conforme já decidiu a Suprema Corte canadense, "(...) any search incidental to the limited police power of investigative detention described above is necessarily a warrantless search. Such searches are presumed to be unreasonable unless they can be justified, and hence found reasonable, pursuant to the test established in R. v. Collins, [1987] 1 S.C.R. 265. Under Collins, warrantless searches are deemed reasonable if (a) they are authorized by law, (b) the law itself is reasonable, and (c) the manner in which the search was carried out was also reasonable (p. 278). The Crown bears the burden of demonstrating, on the balance of probabilities, that the warrantless search was authorized by a reasonable law and carried out in a reasonable manner: R. v. Buhay, [2003] 1 S.C.R. 631, 2003 SCC 30, at para. 32 (...)" (R. v. Mann, [2004] 3 S.C.R. 59, 2004 SCC 52, disponível em <https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/2167/index.do>. Acesso em: 20 de dezembro de 2020). No mesmo sentido: R. v. Nolet, 2010 SCC 24, [2010] 1 S.C.R. 851, at p. 46.

evitar a destruição de provas, bem como para identificação de elementos que possam ser utilizados no processo, em face da pessoa detida[574]. Ainda, a busca poderá ser feita diante de "exigent circumstances"[575], que impediriam a obtenção de um mandado a tempo, especialmente em razão de urgência na ação policial, para preservar as provas, a segurança pública e do próprio policial.

A mesma discussão levada a efeito nos Estados Unidos (*Riley v. California*), relacionada ao acesso a dados armazenados em aparelhos celulares, se repetiu no Canadá, especialmente quanto à possibilidade de, na busca durante uma prisão ("search incident to a lawful arrest"[576]), os agentes policiais terem acesso aos dados digitais armazenados em aparelhos celulares.

No caso "*Kevin Fearon x Her Majesty The Queen 2014 SCC 77, [2014] S.C.R. 621"*[577], a Suprema Corte concordou que os aparelhos celulares, independentemente de estarem ou não protegidos por senhas ou outras barreiras criptográficas, merecem a mesma proteção, já que a ausência de proteção não significa que o titular do aparelho tenha deixado de lado seu interesse na manutenção da privacidade do conteúdo do seu aparelho[578].

---

[574] R. v. Mann, [2004] 3 S.C.R. 59, 2004 SCC 52, at p. 37 e 30, disponível em <https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/2167/index.do>; R. v. Clayton, [2007] 2 S.C.R. 725, 2007 SCC 32 at p. 26 e 29, disponível em <https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/2372/index.do>. Ambos acessados em: 20 de dezembro de 2020

[575] R. v. Paterson, 2017 SCC 15, [2017] 1 S.C.R. 202, at p. 32-33, disponível em https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16484/index.do. Acesso em: 20 de dezembro de 2020.

[576] A busca durante uma prisão foi expressamente admitida no caso Cloutier v. Langlois, [1990] 1 S.C.R. 158, at pp. 180-82, disponível em https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/567/index.do. Acesso em: 20 de dezembro de 2020).

[577] https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14502/index.do. Acesso em: 20 de dezembro de 2020.

[578] No caso apreciado pela Corte Canadense, dois homens, sendo um deles armado com uma pistola, roubaram uma comerciante enquanto ela carregava joias em seu carro. De posse de mochilas, os roubadores se apossaram das joias e empreenderam fuga do local, em um carro preto. Iniciadas as investigações policiais, descobriu-se que o suposto roubo teria sido praticado por Fearon e Chapman, tendo a polícia canadense os detidos naquela noite, sem, contudo, localizar a arma ou as joias roubadas. Ainda, no curso da atividade investigativa, os policiais localizaram o veículo utilizado para fuga e o apreendeu, obtendo-se um mandado para uma busca, o que se sucedeu no dia seguinte. No momento da prisão de Fearon, os policiais realizaram uma revista pessoal ("search incident to a lawful arrest") e localizaram um aparelho celular no bolso da calça do abordado. Em acesso aos dados do aparelho, que estava desbloqueado e desprovido de senha, os policiais encontraram um rascunho de mensagem de texto, referindo-se às joias, com os dizeres "We did it". Em seguida, durante as buscas nos dados digitais, os policiais localizaram uma foto de uma arma, que fora a mesma encontrada durante as buscas no veículo de fuga. Posteriormente, a polícia obteve um mandado de busca para o aparelho celular, mas nenhuma nova evidência foi encontrada. Em seu julgamento, Fearon apontou que a busca realizada em seu aparelho celular violou a Section 8 da "The Canadian Charter of Rights and Freedoms". Entretanto, em primeiro e segundo grau de julgamento, as alegações de Fearon não foram acolhidas e a condenação fora mantida, sob alegação de que a busca realizada não violou os direitos e garantias de Fearon. O caso foi levado à Suprema Corte Canadense, que teve que decidir se a busca realizada em aparelhos celulares, durante uma

De igual sorte, a Suprema Corte considerou ser inviável se comparar um aparelho celular com uma pasta ou outro objeto similar, especialmente considerando a vastidão e diversidade de dados que são armazenados, o que excederia a capacidade de documentos que uma pessoa poderia, naturalmente, carregar. Ademais, os dados armazenados, quando conectados e analisados conjuntamente, permitem revelar intrínsecos aspectos da personalidade e vida privada do seu titular.

Ainda, a Corte reconheceu que aparelhos celulares e outros objetos digitais podem reter arquivos e dados que os usuários acreditavam que foram apagados, além de poderem gerar provas mesmo após sua apreensão, tais como ligações, mensagens ou e-mails recebidos no momento em que o objeto já está em poder de autoridades policiais[579].

Entretanto, os juízes que formaram a maioria reconheceram que a busca fora realizada dentro das hipóteses excepcionais relacionadas à "search incident to a lawful arrest", uma vez que a prisão fora legal – já que motivada para a localização da arma e das joias roubadas –, bem como realizada para se evitar a perda de provas e para se obter outros elementos que pudessem auxiliar no esclarecimento dos fatos ou identificar a participação de outros envolvidos[580].

Os julgadores rejeitaram uma proibição categórica à busca de aparelhos celulares[581] que exigisse, necessariamente, "reasonable and probable grounds" para a pesquisa dos dados armazenados[582], sob pena de se inviabilizar a aplicação da lei e eliminar os poderes da polícia. Porém, por maioria, foram propostas modificações à estrutura das buscas realizadas sem ordem judicial, durante abordagens seguidas de prisão, concluindo-se que o acesso será legítimo quando:

a) a prisão for legal;

---

prisão, é admitida dentre as regras consuetudinárias que excepcionam a exigência de mandado judicial e, em caso afirmativo, se na relação entre a necessária aplicação eficaz da lei e os interesses privados do indivíduo, é necessária a imposição de restrições adicionais para as buscas, especificando-as.

[579] R. *v.* Fearon, 2014 SCC 77, [2014] S.C.R. 621, at par. 126-134.

[580] R. *v.* Fearon, 2014 SCC 77, [2014] S.C.R. 621, at par. 33.

[581] R. *v.* Fearon, 2014 SCC 77, [2014] S.C.R. 621, at par. 45.

[582] R. *v.* Fearon, 2014 SCC 77, [2014] S.C.R. 621, at par. 61.

b) A busca é verdadeiramente incidental à prisão, o que se dá quando a polícia tiver um motivo objetivamente razoável para a realização da diligência, amparado por lei, para os seguintes propósitos: *b.1.)* proteger a integridade dos policiais e do próprio acusado; *b.2.)* preservar evidências e provas; *b.3.)* descobrir novas provas, tais como a identificação e localização de outros suspeitos, desde que comprovadamente, a investigação puder ser frustrada ou severamente prejudicada diante da não realização da imediata pesquisa[583];

c) a natureza e extensão da busca incidental à prisão devem ser limitadas às informações e dados que possuam inegável vínculo com os propósitos da diligência e os crimes apurados, os quais deverão ser considerados graves, tais como aqueles cometidos com violência ou ameaça, que coloquem a população em risco, ofensas patrimoniais graves ou o tráfico de drogas, impedindo-se a realização da busca para crimes considerados menores[584];

d) os policiais que realizaram as buscas deverão documentar, de forma completa e detalhada, como se deu o exame do aparelho, o propósito, a extensão e duração da busca, bem como os aplicativos e informações acessadas[585].

Inobstante tenha reconhecido que, efetivamente, a busca realizada no aparelho celular de Fearon não tenha sido amparada na *Section 8* da *"*The Canadian Charter of Rights and Freedoms", a Suprema Corte deixou de determinar a supressão das provas obtidas mediante o acesso indevido[586], pautando-se na boa-fé da ação policial, na ausência de vulneração grave à privacidade de Fearon, bem como que a prova produzida era robusta, convincente e confiável, de modo que sua exclusão prejudicaria a busca da verdade no sistema de justiça.

---

[583] R. *v.* Fearon, 2014 SCC 77, [2014] S.C.R. 621, at par. 80.
[584] R. *v.* Fearon, 2014 SCC 77, [2014] S.C.R. 621, at par. 75-77.
[585] R. *v.* Fearon, 2014 SCC 77, [2014] S.C.R. 621, at par. 82.
[586] Conforme dispõe a *Section 24(2),* da *The Canadian Charter of Rights and Freedoms,* "24. (2) Where, in proceedings under section (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute."

6.4. México

A Constituição Mexicana de 1917 consagra, em seu artigo 16, a proteção ao direito à privacidade e intimidade. Em seu primeiro parágrafo, o constituinte mexicano assegurou a impossibilidade de que alguém seja incomodado em sua pessoa, família, papéis ou bens senão em virtude de ordem escrita de autoridade competente[587]

De igual sorte, o artigo 16, parágrafos décimo segundo e décimo terceiro[588] da Carta Mexicana, em redação bastante similar à do artigo 5º, inciso XII, da Constituição Federal Brasileira, estabeleceu que as comunicações privadas são invioláveis e que a lei punirá qualquer ato que atente contra sua liberdade e privacidade, exceto quando sejam aportadas de forma voluntária por algum dos particulares, bem como que compete exclusivamente ao juiz federal, em petição da autoridade federal ou do titular do Ministério Público da entidade federativa correspondente, autorizar a intervenção de qualquer comunicação privada, devendo o pedido ser fundamentado e motivado, expressando ainda o tipo de intervenção, seus sujeitos e duração.

Ainda, o dispositivo legal prevê que a autorização não poderá ser concedida quando se tratar de matérias de caráter eleitoral, fiscal, mercantil, civil, trabalhista ou administrativo, nem das comunicações mantidas entre o acusado e seu defensor.

Diante da expressa disposição constitucional relacionada às intervenções nas comunicações privadas, sucederam-se interpretações jurisprudenciais

---

[587] Artículo 16, primer párrafo: "Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridade competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimentos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto em este párrafo.

[588] Artículo 16, párrafo décimosegundo: "Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley"
Artículo 16, párrafo décimotercero: "Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor"

distintas quanto ao alcance da previsão normativa mencionada[589], especialmente se abrangeria também outros dados relacionados à própria comunicação, além de conversas mantidas por aplicativos de texto e fotografias armazenadas em aparelhos celulares.

Em face desta controvérsia, a *Suprema Corte de Justicia de la Nación* foi chamada a responder a seguinte indagação: "¿constituye o no una violación a la intervención de comunicaciones privadas, preservada en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, el que la autoridad ministerial o los agentes a su mando revisen, extraigan o utilicen como medio de prueba los archivos electrónicos almacenados en forma de texto, audio, imagen o video, del teléfono celular que traía consigo el detenido relacionado con la comisión de un delito?".

Em julgamento realizado, a Corte Suprema Mexicana sufragou o entendimento[590] de que "los alcances de protección de la inviolabilidade de las comunicaciones privadas, desde luego, se extienden también al llamado teléfono celular*",* bem como que a inviolabilidade protege não apenas as comunicações mantidas de maneira instantânea, mas também aquelas armazenadas e materializadas em um objeto, uma vez

---

[589] *Verbi gratia*, enquanto o *Segundo Tribunal Colegiado em Materias Penal y Administrativa del Décimo Séptimo Circuito* sustentou que o acesso às informações contidas nos aparelhos celulares e relacionados ao cometimento de um crime não constituem intervenções de comunicações privadas e, por conseguinte, exigem ordem judicial (artigo 16, parágrafo décimo terceiro), o *Cuarto Tribunal Colegiado del Décimo Octavo Circuito* apontou que o direito à intimidade e privacidade, assegurados no artigo 16, parágrafo primeiro, da Constituição Federal Mexicana, protege também os arquivos eletrônicos armazenados em aparelhos celulares, estendendo-se a proteção às comunicações privadas também para os dados íntimos e privados das pessoas, estejam eles em formato de texto, áudio, imagine, ou vídeo.

[590] DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SU ÁMBITO DE PROTECCIÓN SE EXTIENDE A LOS DATOS ALMACENADOS EN EL TELÉFONO MÓVIL ASEGURADO A UNA PERSONA DETENIDA Y SUJETA A INVESTIGACIÓN POR LA POSIBLE COMISIÓN DE UN DELITO.-En términos del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, para intervenir una comunicación privada se requiere autorización exclusiva de la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, por lo que todas las formas existentes de comunicación y las que son fruto de la evolución tecnológica deben protegerse por el derecho fundamental a su inviolabilidad, como sucede con el teléfono móvil en el que se guarda información clasificada como privada por la Primera Sala de la Suprema Corte de Justicia de la Nación; de ahí que el ámbito de protección del derecho a la inviolabilidad de las comunicaciones privadas se extiende a los datos almacenados en tal dispositivo, ya sea en forma de texto, audio, imagen o video. Por lo anterior, no existe razón para restringir ese derecho a cualquier persona por la sola circunstancia de haber sido detenida y estar sujeta a investigación por la posible comisión de un delito, de manera que si la autoridad encargada de la investigación, al detenerla, advierte que trae consigo un teléfono móvil, está facultada para decretar su aseguramiento y solicitar a la autoridad judicial la intervención de las comunicaciones privadas conforme al citado artículo 16 constitucional; sin embargo, si se realiza esa actividad sin autorización judicial, cualquier prueba que se extraiga, o bien, la que derive de ésta, será considerada como ilícita y no tendrá valor jurídico alguno (Décima Época. Primera Sala. Semanario Judicial de la Federación y su Gaceta, Libro XVII, febrero de 2013, Tomo 1, pág. 431, disponível em https://sjf2.scjn.gob.mx/detalle/tesis/2002741. Acesso em 20 de dezembro de 2020).

finalizado o processo comunicativo, alcançando-se inclusive os objetos e suportes materiais que armazenam as comunicações.

A inviolabilidade da comunicação abrange todos os meios novos e modernos de comunicação, mesmo aqueles frutos da evolução tecnológica, sendo certo que as provas obtidas mediante intervenção nas comunicações privadas à margem das disposições constitucionais são ineficazes, por afrontarem os direitos e garantias fundamentais, estendendo-se também às provas dela derivadas, ainda que, em sua consecução, se haja cumprido todos os requisitos constitucionais.

Portanto, como se vê, a legislação mexicana permite, em seu artigo 181, primeira parte[591], do "Código Federal de Procedimientos Penales", a apreensão do aparelho celular que estava em poder do acusado, mas exige autorização judicial para acesso a seu conteúdo, por entender que todos os dados ali contidos, incluindo-se as fotografias, vídeos, imagens e demais elementos configuram uma espécie de comunicação privada, aplicando-se o regramento contido no artigo 16 da Constituição Federal Mexicana.

6.5. Inglaterra

Na Inglaterra, não há unicidade legislativa para regulamentar o acesso a dados armazenados em aparelhos celulares, havendo tão somente previsões normativas individuais e esparsas sobre o tema.

O *Terrorism Act 2000* confere uma ampla gama de poderes aos agentes estatais, visando identificar, prevenir e reprimir ações de pessoas consideradas "terroristas"[592]. Especialmente no que tange às medidas de *counter-terrorism,* a *Section 43,*

[591] Artículo 181.- Los instrumentos, objetos o productos del delito, así como los bienes en que existan huellas o pudieran tener relación con éste, serán asegurados a fin de que no se alteren, destruyan o desaparezcan. El Ministerio Público, las policías y los peritos, durante la investigación y en cualquier etapa del proceso penal, deberán seguir las reglas referidas en los artículos 123 Bis a 123 Quintus. La administración de los bienes asegurados se realizará de conformidad con la ley de la materia. Las autoridades que actúen en auxilio del Ministerio Público pondrán inmediatamente a disposición de éste los bienes a que se refiere el párrafo anterior. El Ministerio Público, al momento de recibir los bienes, resolverá sobre su aseguramiento y sobre la continuidad o no del procedimiento al que se refieren los artículos 123 Bis a 123 Quintus de este Código, bajo su más estricta responsabilidad y conforme a las disposiciones aplicables. (...)

[592] A *Section 40* do *Terrorist Act 2000* prevê que serão considerados terroristas aqueles que"(a)has committed an offence under any of sections 11, 12, 15 to 18, 54 and 56 to 63, or: (b) is or has been concerned in the commission, preparation or instigation of acts of terrorism.

item 4 [593] e 4B, b, i e ii[594], prevê a possibilidade de policiais britânicos ("constable") realizarem, independentemente de prévia ordem judicial, a busca e retenção de qualquer objeto que seja localizado em meio à busca pessoal a um suspeito de terrorismo, condicionado à suspeita do agente policial de que possa constituir uma prova de que o indivíduo abordado seja um terrorista[595].

Embora a legislação deixe de prever, expressamente, quais seriam os objetos que poderiam ser vasculhados durante a busca realizada em suspeito de terrorismo, é certo que o aparelho celular pode ser considerado um item passível de verificação, conforme orientação expressa oficial da "Metropolitan Police"[596].

Para além desta possibilidade, a *Misuse of Drugs Act 1971*, previsão normativa relacionada ao tráfico de entorpecentes no Reino Unido, estabelece de maneira genérica – o que suscita discussões quanto à extensão da medida – que o policial, diante de fundadas razões que o levem a acreditar que a pessoa a ser abordada esteja sob a posse de drogas em contrariedade à legislação, poderá vasculhar e apreender, para os propósitos relacionados ao combate ao tráfico de drogas, qualquer coisa encontrada no curso de uma busca pessoal que o policial acredite ser uma prova de um crime previsto na lei (Section 23, 2, alínea c[597]).

Na mesma linha, o *Police and Criminal Evidence Act 1984* prevê, também de maneira genérica em sua *Section 1, 6*[598], que os policiais britânicos podem, no

(2)The reference in subsection (1)(b) to a person who has been concerned in the commission, preparation or instigation of acts of terrorism includes a reference to a person who has been, whether before or after the passing of this Act, concerned in the commission, preparation or instigation of acts of terrorism within the meaning given by section 1"

[593] A constable may seize and retain anything which he discovers in the course of a search of a person under subsection (1) or (2) and which he reasonably suspects may constitute evidence that the person is a terrorist.

[594] The constable: (…) (b)may seize and retain anything which the constable: (i)discovers in the course of such a search, and (ii)reasonably suspects may constitute evidence that the person is a terrorist.

[595] A constable may seize and retain anything which he discovers in the course of a search of a person under subsection (1) or (2) and which he reasonably suspects may constitute evidence that the person is a terrorist.

[596] Disponível em: <https://www.met.police.uk/advice/advice-and-information/ph/photography-advice/>. Acesso em: 20 de dezembro de 2020.

[597] (2)If a constable has reasonable grounds to suspect that any person is in possession of a controlled drug in contravention of this Act or of any regulations [F1or orders] made thereunder, the constable may (…) (c)seize and detain, for the purposes of proceedings under this Act, anything found in the course of the search which appears to the constable to be evidence of an offence under this Act.

[598] If in the course of such a search a constable discovers an article which he has reasonable grounds for suspecting to be a stolen or prohibited article, he may seize it

curso de uma abordagem pessoal, estender a busca para quais artigos sobre os quais recaiam razoáveis motivos para se acreditar serem roubados ou proibidos.

Como se vê, as previsões normativas são bastante lacônicas, inclusive em guias procedimentais de orientação policial[599], o que traz insegurança no tocante à possibilidade de acesso indiscriminado de aparelhos celulares por parte de policiais, em abordagens e buscas rotineiras.

Por esta razão, tem-se reconhecido a necessidade de uma alteração legislativa e procedimental[600] que permita regulamentar, de maneira específica, a necessidade de ordem judicial prévia para acesso aos dados armazenados em aparelhos celulares[601].

6.6. Espanha

A experiência espanhola merece um destaque especial, especialmente considerando possuir um sistema jurídico de "civil law", além de possuir dispositivos constitucionais que guarda íntima relação com normas previstas na Constituição Federal.

Não bastasse, a jurisprudência espanhola também enfrentou problemas de ordem prática na interpretação da proteção constitucional dispensada aos dados armazenados em aparelhos celulares, motivando-se uma reforma legislativa que regulamentou exaustivamente sobre o tema e serve de inspiração para a realidade brasileira.

---

[599] *Verbi gratia,* o Code A, que visa regular procedimentalmente a atuação policial durante buscas e apreensões, não dispõem expressamente sobre a apreensão de aparelhos celulares (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/384122/PaceCodeAWeb.pdf. Acesso em: 20 de dezembro de 2020).

[600] Call it off: are police searching mobile phones illegally?. https://www.stop-watch.org/uploads/documents/Call_it_Off_-_Are_police_searching_mobile_phones_illegally.pdf. Acesso em: 20 de dezembro de 2020.

[601] "(...) Across the country the police have expanded their use of mobile phone extraction without public attention and without effective oversight. It is not enough to rely on PACE to search mobile phones - a piece of legislation written long before a phone became a device that could be used as a pocket surveillance tool. Traditional search practices, where no warrant is required, are wholly inappropriate for such a deeply intrusive search (…)" (Privacy International. *Digital stop and search: how the UK police can secretly download everything from your mobile phone*. March 2018. <https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf>. Acesso em: 20 de dezembro de 2020)

Até o advento da *"Ley Orgánica n.º 13/2015"*, de 5 de outubro de 2015, que alterou a *Ley de Enjuiciamiento Criminal*, a legislação espanhola não trazia qualquer previsão expressa e sobre o tema. Neste sentido, coube à jurisprudência definir critérios para se verificar a incidência de restrições legais e constitucionais no acesso a dados armazenados, a partir do conteúdo, natureza e estágio de armazenamento do conteúdo afetado[602].

Desta forma, entendia-se que o direito à intimidade do usuário abrangia a proteção relacionadas às fotografias, vídeos, documentos e outros dados que estivessem armazenados em um dispositivo, porquanto todos eram suscetíveis de afetar o núcleo mais profundo da intimidade ao exporem ideologias, crenças religiosas, afeições pessoais, informações sobre a saúde e orientações sexuais[603]. Assim, a esfera de proteção constitucional que guardava este conteúdo é a do artigo 18, 1, da Constituição Espanhola[604], que não exige, expressamente, a necessidade de intervenção judicial para acesso aos dados.

Ao mesmo tempo, quando alcançados os dados armazenados que formavam parte de um processo comunicativo, invocava-se a proteção conferida ao artigo 18.3 da Constituição Espanhola[605], que demanda autorização judicial expressa para afastar o sigilo das comunicações e, em especial, das postais, telegráficas e telefônicas.

Neste prisma, a Suprema Corte Espanhola afastou, por diversas vezes, a interpretação de que toda e qualquer afetação a direito fundamental exige a necessária intervenção judicial[606], o que seria limitado às hipóteses trazidas nos artigos 18.2 e 18.3 da Constituição Espanhola.

---

602 "(...) Lo determinante para la delimitación del contenido de los derechos fundamentales recogidos en los arts. 18.1 y 18.3 CE no es el tipo de soporte, físico o electrónico, en el que la agenda de contactos esté alojada ni el hecho, de que la agenda sea una aplicación de un terminal telefónico móvil, que es un instrumento de y para la comunicación, sino el carácter de la información a la que se acede (...)" (STS nº 142/2012, de 2 de julho).

603 STC n.º 173/2011, de 7 de noviembre.

604 O dispositivo possui redação bastante similar a do artigo 5º, inciso X, da Constituição Federal brasileira.

605 O dispositivo possui redação bastante similar a do artigo 5º, inciso XII, da Constituição Federal brasileira, contemplando cláusula expressa de reserva constitucional de jurisdição.

606 Neste sentido, decidiu-se que "(...) ¿Es necesario que toda medida que afecte o pueda afectar a un derecho fundamental sea siempre acordada por un Juez? La respuesta no puede ser rotundamente afirmativa, por más que en ocasiones se puedan leer poco meditadas aseveraciones en ese sentido. Hay casos en que puede hacerlo la Policía Judicial de propia autoridad. En muchos supuestos -no todos- si concurre un consentimiento libre (por ejemplo, una exploración radiológica). En otros, incluso coactivamente (cacheos externos). No puede proclamarse precipitadamente el monopolio jurisdiccional como requisito indispensable de toda afectación de un derecho fundamental: la legitimidad constitucional de la detención policial es prueba clara de lo que se

A distinção de tratamento gerava problemas de ordem prática, especialmente considerando a diversidade de dados armazenados em um mesmo dispositivo, o que poderia conduzir a situações bastante inseguras[607], tais como a do regular acesso a dados meramente íntimos ser realizado sem a correspondente autorização judicial e, durante as buscas, deparar-se com um dado que tenha relação com o processo comunicativo, atraindo-se a incidência do artigo 18.3 da Carta Constitucional, para se demandar a necessária autorização judicial[608].

Em razão da insegurança jurídica nas interpretações desenvolvidas, desenvolveu-se uma nova concepção jurisprudencial que buscava alcançar o problema de maneira uniforme, passando a ser introduzido um conceito de "derecho al entorno virtual", que exigiria uma proteção jurisdicional própria frente à necessidade do Estado atuar perante

---

afirma. Ni siquiera sería totalmente exacto afirmar que ese es el principio general, solo excepcionado cuando la ley autorice a la policía expresamente. Actuaciones como la obligación a expulsar unas bolsas de la boca (STS de 25 de enero de 1993) o la toma de huellas dactilares (STS de 12 de abril de 1992) pueden resultar admisibles sin necesidad de una previa validación judicial ni de una ley específica habilitante. Será necesaria la previa intervención judicial cuando la Constitución o las Leyes así lo exijan (registros domiciliarios, interceptación de comunicaciones). La afectación de un derecho fundamental por sí sola no es argumento siempre suficiente para postular como presupuesto imprescindible la previa autorización judicial salvo explícita habilitación legal (vid SSTC 206/2007, de 29 de septiembre, ó 142/2012, de 2 de junio ...). Que una actuación pueda menoscabar la intimidad -registro de una maleta o unospapeles- no significa a priori y como afirmación axiomática que no pueda ser acordada por autoridades diferentes de la jurisdiccional. La jurisdiccionalidad es exigible en algunos casos; en otros, no. Por eso la constatación de la incidencia de la medida -análisis químico- en la intimidad no comporta automáticamente previa habilitación judicial inexcusable. Como no necesita autorización judicial el interrogatorio de un testigo por la policía a fin de averiguar datos precisos para una investigación, aunque haya afectación de la privacidad propia o de otras personas (preguntar sobre alguna de sus actividades, si el interrogado estuvo con determinada persona, tipo de relaciones mantenidas con ella...). No es que se quiera equiparar uno y otro tipo de diligencias. Es obvio que no son equiparables. Esta consideración se hace a los únicos efectos de destacar que no es legal ni constitucionalmente correcta la ecuación afectación de la intimidad-necesidad inexcusable de previa habilitación judicial. La incidencia en la privacidad no lleva a cuestionar que pueda recibirse declaración a un testigo por la policía como medio de averiguación del delito, sin necesidad de previa autorización judicial motivada, ni de ningún otro requisito especial. Ni siquiera cuando ese interrogatorio, por exigencias de la investigación, conduce a adentrarse en reductos más sensibles de la privacidade (...)" (STS n.º 777/2013, de 7 de outubro, Tribunal Supremo – Sala Segunda, de lo Penal).

[607] Por exemplo, as mensagens de e-mails enviados e ainda não lidos demandavam uma autorização judicial, porquanto não encerrado o processo comunicativo (artigo 18.3 da Carta Espanhola), ao passo que, com a leitura, o processo comunicativo estaria encerrado e, por conseguinte, seria afastado o espectro de incidência do artigo 18.3, migrando-se para a lacônica proteção conferida à intimidade, prevista no artigo 18.1 (STS n.º 864/2015, de 10 de dezembro de 2014, Tribunal Supremo – Sala Segunda, de lo Penal). De igual sorte, a Corte Suprema entendeu que a busca realizada na agenda de contatos de um telefone móvel prescindia de autorização judicial , ao passo que a análise dos registros telefônicos de chamadas efetuadas e recebidas, por afetar o direito fundamental ao sigilo das comunicações, demandaria autorização judicial (Sentencia n.º 115/2013, de 9 de maio de 2013, Tribunal Supremo – Sala Segunda, de lo Penal e Sentencia n.º 115/2013, de 9 de maio de 2013, Tribunal Supremo – Sala Segunda, de lo Penal).

[608] STS n.º 204/2016, de 10 de março de 2016, Tribunal Supremo – Sala Segunda, de lo Penal.

este entorno digital[609], concluindo-se pela necessidade de uma resolução jurisdicional que regulamentasse o tema[610].

A partir do desenvolvimento deste conceito e reconhecendo a necessidade de se estabelecer um tratamento unitário que permitisse salvaguardar as intromissões mais intensas à vida privada e à liberdade de comunicação do cidadão, sobreveio a edição da *Ley Orgánica n.º 13/2015*, de 5 de outubro de 2015, que alterou a *Ley de Enjuiciamiento Criminal.*

Por intermédio da reforma legislativa, conferiu-se um tratamento unitário[611] aos dados contidos em aparelhos celulares e fortaleceu-se as garantias processuais[612] e regulatórias na utilização das medidas de investigação tecnológica, além de se ter promovido a adaptação da legislação interna às diretrizes da Convenção de Budapeste sobre *cybercrime.*

Nesta ordem, o Capítulo IV do Título VIII da *Ley de Enjuiciamiento Criminal* dispôs sobre a utilização dos meios de investigação relacionados à "interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos".

---

[609] STS n.º 342/2013, de 17 de abril de 2013, Tribunal Supremo – Sala Segunda, de lo Penal.
[610] STS n.º 786/2015, de 4 de dezembro de 2015, Tribunal Supremo – Sala Segunda, de lo Penal.
[611] Como já antevia o Tribunal Supremo "(...) La necesidad de esta autorización judicial (subsidiaria del consentimiento: si el afectado accede de forma libre, no hay cuestión) obedece a la consideración de estos instrumentos como esferas de almacenamiento de una serie compleja y densa de datos que afectan de modo muy variado a la intimidad del investigado (comunicaciones tuteladas por el art 18 3º CE; contactos, fotografías, archivos personales, tuteladas por el art 18 1º CE; datos personales y de geolocalización, que pueden cobijarse en el derecho a la protección de datos, art 18 4º CE). La contemplación disgregada de cada una de esas realidades con regímenes de protección diferenciados resultaría ineficaz. Permitido, por ejemplo, el acceso directo de los agentes policiales a estos instrumentos para investigar datos únicamente protegidos por el derecho a la intimidad (v.gr., los contatos incluidos en la agenda), no se podría acceder o consultar también otros datos tutelados por el derecho a la inviolabilidad de las comunicaciones albergados en el mismo dispositivo. El Legislador con buen criterio há optado por otorgar un tratamiento unitario a los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, configurando ese derecho constitucional de nueva generación, el derecho a la protección del propio entorno virtual (...)" (STS 3754/2018, de 23 de outubro de 2018, Tribunal Supremo – Sala Segunda, de lo Penal)
[612] O Tribunal Supremo Espanhol, por sua vez, considerou serem inaplicáveis as novas disposições legais aos casos originados antes da entrada em vigor da lei: STS 4207/2017, de 21 de novembro de 2017, Tribunal Supremo – Sala Segunda, de lo Penal.

O *artículo 588 bis a*[613], implementado pela reforma legislativa da *Ley Orgánica n.º 13/2015*, em seu item 1, condicionou a utilização destes meios de investigação de prova à prévia autorização judicial, que deverá ser fundamentada tomando-se por base os alguns princípios reitores[614].

Analisando-se os dispositivos legais introduzidos pela reforma legislativa, constata-se que o legislador espanhol deixou de estabelecer um catálogo prévio de crimes que autorizam a busca de dispositivos de armazenamento massivo de informação, diferentemente do que se adotou na busca remota de equipamentos informáticos[615] *(artículo 588 septies a)*.

---

[613] Artículo 588 bis a. Principios rectores.
1. Durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.
2. El principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva.
3. El principio de idoneidad servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad.
4. En aplicación de los principios de excepcionalidad y necesidad solo podrá acordarse la medida:
a) cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o
b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida.
5. Las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho.

[614] 1) princípio da especialidade, de modo que a medida investigativa esteja relacionada a um crime específico, vedando-se a investigação tecnológica preventiva para descobrimento de crimes ou desprovidos de suspeitas claras; 2) princípio da adequação, a fim de que a medida sirva para definir o escopo objetivo e subjetivo e a duração da medida em virtude de sua utilidade; 3) princípios da excepcionalidade e necessidade, preconizando-se que os recursos tecnológicos sejam imprescindíveis para a descoberta ou verificação do fato e seus autores, evitando-se o uso da investigação tecnológica quando outras medidas menos onerosas aos direitos e garantias fundamentais forem suficientes para os propósitos investigativos; 4) princípio da proporcionalidade, determinando-se que as medidas somente sejam adotadas mediante ponderação entre os direitos e garantias dos investigados e o interesse público relacionado à seriedade do fato, seu significado social ou o escopo tecnológico da produção da prova.

[615] Na hipótese específica de busca remota, o legislador espanhol delimitou um rol de crimes abstratamente graves que legitimariam o acesso aos dispositivos informáticos, exigindo-se que estas medidas, por serem mais afrontosas ao direito à intimidade e privacidade do cidadão pelo fato de serem realizadas remotamente e sem seu conhecimento prévio – ao contrário do que ocorre com a apreensão física do aparelho, em que seu titular ou proprietário sabe da pretensa ação estatal para acesso e análise dos dados no suporte eletrônico apreendido –, venham a ser utilizadas para a persecução estatal de determinados delitos de especial relevância e gravidade.

Para além da expressa necessidade de autorização judicial, o art. 588 bis a, item 5 estabeleceu expressamente a necessidade da realização de um juízo de proporcionalidade, que será feito a partir da análise do caso concreto, de modo que a decisão judicial avaliará a admissibilidade da medida a partir da gravidade do crime apurado, sua transcendência social, bem como o âmbito tecnológico de produção e a intensidade dos indícios existentes juntamente com a relevância do resultado perseguido com a restrição do direito, estabelecendo-se uma maior exigência de suficiência probatória para a adoção de medidas mais invasivas aos direitos e garantias fundamentais.

Ainda, o *artículo 588 bis*, em seus itens *b* a *k*, disciplinam os requisitos mínimos para a realização do pedido e para o conteúdo da decisão judicial que disponha sobre a implementação de medidas de investigação tecnológica, bem como os procedimentos para destruição dos registros originais que possam constar em sistemas eletrônicos ou informáticos utilizados para execução da medida, preservando-se uma cópia.

O legislador espanhol, de maneira fragmentada, estabeleceu um capítulo para cuidar de cada um dos meios de investigação tecnológica. De todos, ganha destaque para o presente trabalho científico o Capítulo VIII, pertinente ao "Registro de dispositivos de almacenamiento masivo de información".

Especificamente com relação ao acesso a estes dados armazenados em dispositivos desta natureza, o legislador cuidou de estabelecer, em seu *artículo 588 sexies a*[616], que se durante o cumprimento de uma busca domiciliar for previsível a apreensão de computadores e instrumentos de comunicação telefônica ou telemática ou, ainda, dispositivos de armazenamento massivo de informações digitais ou que contenham repositórios telemático de dados, a decisão judicial deverá analisar se há justificativa para o acesso ao conteúdo destes dispositivos, de modo que a simples apreensão destes suportes eletrônicos não legitima o acesso ao seu conteúdo, salvo mediante autorização judicial.

[616] Artículo 588 sexies a. Necesidad de motivación individualizada.
1. Cuando con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos, la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos.
2. La simple incautación de cualquiera de los dispositivos a los que se refiere el apartado anterior, practicada durante el transcurso de la diligencia de registro domiciliario, no legitima el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el juez competente.

A normativa espanhola estabeleceu, expressamente, que a previsão alcança também as hipóteses de apreensão dos dispositivos em situações distintas da busca domiciliar (*artículo 588 sexies b*[617]), bem como que a autorização judicial deverá estabelecer os termos e o alcance da busca, dispondo sobre a possibilidade de se realizar a cópia dos dados informáticos, visando assegurar sua integridade (o *artículo 588 sexies c*[618]).

Como se vê, a legislação espanhola estabeleceu uma dupla necessidade de autorização judicial: para além da ordem autorizativa da realização da busca domiciliar ou de outra medida restritiva (*v.g.*, uma ordem de prisão), é imprescindível uma autorização judicial fundamentada e específica, concedida de forma prévia ou subsequente

[617] Artículo 588 sexies b. Acceso a la información de dispositivos electrónicos incautados fuera del domicilio del investigado. La exigencia prevista en el apartado 1 del artículo anterior será también aplicable a aquellos casos en los que los ordenadores, instrumentos de comunicación o dispositivos de almacenamiento masivo de datos, o el acceso a repositorios telemáticos de datos, sean aprehendidos con independencia de un registro domiciliario. En tales casos, los agentes pondrán en conocimiento del juez la incautación de tales efectos. Si éste considera indispensable el acceso a la información albergada en su contenido, otorgará la correspondiente autorización

[618] Artículo 588 sexies c. Autorización judicial.

1. La resolución del juez de instrucción mediante la que se autorice el acceso a la información contenida en los dispositivos a que se refiere la presente sección, fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos. Fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial.

2. Salvo que constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen, se evitará la incautación de los soportes físicos que contengan los datos o archivos informáticos, cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible la obtención de una copia de ellos en condiciones que garanticen la autenticidad e integridad de los datos.

3. Cuando quienes lleven a cabo el registro o tengan acceso al sistema de información o a una parte del mismo conforme a lo dispuesto en este capítulo, tengan razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático o en una parte de él, podrán ampliar el registro, siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este. Esta ampliación del registro deberá ser autorizada por el juez, salvo que ya lo hubiera sido en la autorización inicial. En caso de urgencia, la Policía Judicial o el fiscal podrán llevarlo a cabo, informando al juez inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, de la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la interceptación.

4. En los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida prevista en los apartados anteriores de este artículo, la Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fue ordenada la medida.

5. Las autoridades y agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria, siempre que de ello no derive una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en delito de desobediencia.

Esta disposición no será aplicable al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional

à apreensão do suporte eletrônico, que disponha sobre o alcance da busca e delimite quais os suportes eletrônicos a serem vasculhados e, ainda, o conteúdo dos dados informáticos neles contidos que podem ser acessados.

Entretanto, o próprio legislador excepcionou a possibilidade do acesso sem autorização judicial prévia.

Com efeito, em casos de urgência pautada pela existência de um interesse constitucional legítimo, a Polícia Judiciária poderá acessar diretamente os dados contidos no dispositivo apreendido, comunicando-se ao juiz competente, por escrito e no prazo máximo de 24 (vinte e quatro) horas, os motivos que justificaram a medida, a forma em que a ação foi empreendida e como se deu a sua execução e respectivo resultado, cabendo ao julgador, também de forma motivada e no prazo máximo de 72 (setenta e duas) horas após a realização da medida, confirmar ou revogar a ação adotada pela Polícia Judiciária (*artículo 588 sexies c, 4*).

Portanto, a legislação espanhola condiciona a busca policial, sem ordem judicial prévia, à presença de quatro requisitos: *a)* situação de urgência verificável pelo policial; *b)* legítimo interesse constitucional que torne imprescindível a medida; *c)* comunicação ao Juiz na forma e prazos estabelecidos; *d)* validação judicial da medida[619].

A urgência mencionada pelo dispositivo legal tem sido interpretada como aquela necessária para prevenção e investigação do crime, a descoberta de criminosos e a obtenção de provas incriminatórias[620], sempre que, em caso de atraso no acesso aos dados, sobrevenha a possibilidade de danos concretos. Nestes casos de urgência, a Polícia Judiciária poderá acessar não apenas os dados que afetem o direito à intimidade, mas também aqueles relacionados ao direito ao sigilo das comunicações, já que o artigo 18.3 da Constituição Espanhola não exige ordem judicial prévia, mas tão somente uma autorização judicial, a qual poderá ser obtida *a posteriori.*

---

[619] Nesta linha, confira-se a Circular n.º 5/2019, de 6 de março de 2019, da *Fiscal General del Estado*, dispondo sobre registro de dispositivos e equipamentos informáticos, publicado no BOE núm. 70, de 22 de março de 2019, páginas 30.159 a 30.197 (https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-4244. Acesso em: 20 de dezembro de 2020).

[620] STS n.º 70/2002, de 3 de abril de 2002, Tribunal Supremo – Sala Segunda, de lo Penal.

O legítimo interesse constitucional que torne imprescindível a medida, por sua vez, tem sido relacionado às possibilidades de ingerência do poder público na vida privada, na linha do estabelecido no artigo 8.2 da Convenção Europeia de Direitos Humanos (CEDH). Assim, seria considerado interesse constitucionalmente legítimo, a justificar a intervenção, as ingerências que visam tutelar a segurança nacional, a segurança pública, o bem-estar econômico do país, a defesa da ordem e a prevenção do crime, a proteção da saúde ou da moral ou a proteção dos direitos e liberdade de outrem,

Registre-se que a comunicação deverá ser realizada no prazo fixado em lei, de 72 (setenta e duas) horas contadas da realização da medida, cabendo ao julgador se lastrear nos princípios reitores dispostos no *artículo 588 bis a.*

Frise-se que a avaliação judicial não está condicionada à efetiva produção de resultados relevantes para a investigação no acesso policial direto, mas apenas visa analisar se presentes os pressupostos de urgência, necessidade ou proporcionalidade da medida, quando do momento da intervenção sem autorização judicial.

6.7. A contribuição para a formação de um modelo normativo processual

Ainda que o trabalho de pesquisa comparada tenha se limitado à experiência de alguns ordenamentos jurídicos, é inegável a contribuição para o aperfeiçoamento do tema, especialmente pela regulamentação trazida a partir da reforma legislativa operada pela Espanha.

Por se tratar de um país adepto do sistema jurídico da “civil law” e que buscou a positivação legislativa para o tema, a regulamentação espanhola pode servir de inspiração para uma vindoura reforma legislativa, que vise disciplinar não apenas a obtenção e tratamento das provas digitais[621] e, ainda, disciplinar o acesso a dados armazenados em aparelhos celulares.

[621] As propostas legislativas para a positivação de aspectos relacionados à prova digital foram sugeridas por Denise Vaz, em sua tese de doutorado na Faculdade de Direito da Universidade de São Paulo: VAZ, Denise Provazi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório*. Tese (Doutorado em Processo Penal) - Faculdade de Direito da Universidade de São Paulo, 2012, p. 138-145.

Com efeito, após também se deparar com uma jurisprudência vacilante sobre o tema[622], o legislador espanhol buscou adaptar as normativas internas aos preceitos da Convenção de Budapeste e, ao mesmo tempo, reconheceu a existência de um "derecho al entorno virtual", vindo a regulamentar os diversos meios de investigação digitais.

No âmbito nacional, o caminho a ser percorrido é a alteração legislativa, ocasião em que se poderá estabelecer balizas para se regulamentar o acesso aos dados armazenados em aparelhos celulares, à luz da eficiência e garantismo.

Para tanto, a proposta legislativa poderá estabelecer as formas pelas quais se colherá o consentimento do acusado, nos casos em que o acesso se dá de maneira voluntária[623], disciplinando se a medida exigirá a forma escrita, a presença de testemunhas, bem como a indispensabilidade de advogado para conferir validade ao ato.

Ainda, para as hipóteses em que o acesso se dá sem o consentimento do acusado, é imprescindível que a legislação a ser editada preveja a necessidade de autorização judicial para o acesso aos dados e os requisitos legais a serem observados, em respeito ao direito à privacidade e intimidade (artigo 5º, inciso X, da CF).

Caberá ao legislador, também, estabelecer as hipóteses de excepcional acesso direto por agentes policiais, em situações de urgência ou emergência, submetendo a decisão policial ao oportuno escrutínio judicial, dentro de um prazo legal conferido por lei (nos moldes parametrizados pelo *artículo 588 bis a*, da legislação espanhola).

Nestas hipóteses de acesso direto por agentes policiais, é prudente que se estabeleça a obrigatoriedade do agente policial documentar, de maneira ampla, completa e detalhada, como se deu o exame do aparelho, o propósito, a extensão e duração da busca,

---

[622] Como destacado no capítulo anterior, a jurisprudência ainda é francamente dividida sobre o tema, muito embora o Superior Tribunal de Justiça tenha pacificado o entendimento quanto à imprescindibilidade de autorização judicial para o acesso aos dados. Todavia, o assunto ainda está sendo apreciado pelo Supremo Tribunal Federal, em julgamento virtual já iniciado, mas ainda não concluído (STF, Repercussão Geral no Recurso Extraordinário com Agravo n.º 1.042.075/RJ, Rel. Min. Dias Toffoli, julgado em 23 de novembro de 2017, DJe 12/12/2017).

[623] Conforme capítulo 3 do presente trabalho científico.

bem como os aplicativos e informações acessadas[624], de forma a se verificar se o acesso realizado atendeu aos pressupostos de urgência ou emergência, bem como para se preservar a cadeia de custódia da prova, conforme se verá no próximo capítulo.

Finalmente, enquanto não promovida a alteração legislativa, a utilização do referido meio de obtenção de prova é possível, sempre mediante controle judicial em que se observará o mandamento da proporcionalidade[625], compensando-se o déficit de regulamentação mediante a utilização de interpretação extensiva ou analógica (*v.g.*, busca e apreensão – artigo 240 e seguintes do CPP; Lei de Interceptação Telefônica – artigo 2º da Lei n.º 9.296/1996; e Lei do Marco Civil da *Internet* – artigos 10, § 2º e 22, ambos da Lei n.º 12.965/2014), até a suplementação normativa que regulamente o referido meio de obtenção de prova[626].

[624] Conforme a decisão da Suprema Corte Canadense no caso "Kevin Fearon x Her Majesty The Queen 2014 SCC 77, [2014] S.C.R. 621" (R. *v.* Fearon, 2014 SCC 77, [2014] S.C.R. 621, at par. 82).
[625] Conforme subtópico 5.3.1.
[626] SOARES, Gustavo Torres. *Investigação criminal e inovações técnicas e tecnológicas: perspectivas e limites.* Tese (Doutorado em Direito Processual Penal) - da Faculdade de Direito da Universidade de São Paulo. São Paulo, SP, 2014, p. 288-292.

7. A CADEIA DE CUSTÓDIA DA PROVA ORIUNDA DO ACESSO AOS DADOS ARMAZENADOS EM APARELHOS CELULARES

Nos capítulos anteriores, discorreu-se sobre a forma de acesso aos dados armazenados em aparelhos celulares, distinguindo-se as hipóteses do acesso mediante consentimento do titular dos dados daquela oriunda da ausência de voluntariedade, que exige, em regra, uma decisão judicial autorizativa de intromissão a seu conteúdo.

A partir do momento em que se obtém o legítimo acesso aos dados armazenados no aparelho celular, é necessário avançar sobre a técnica para obtenção da prova digital, como forma de se preservar sua integridade e, por conseguinte, extrair sua capacidade de demonstração e convencimento.

7.1. Premissas conceituais

O processo penal, enquanto instrumento para se legitimar o exercício do poder punitivo estatal, tem por objetivo a reconstrução do fato histórico, mediante a avaliação racional de provas e sua subsunção à norma jurídica corretamente aplicável, com o objetivo de constatar a veracidade do enunciado fático estabelecido.

Esta análise retrospectiva dos fatos, que tem heuristicamente a verdade como parâmetro de justiça, abandonou a premissa de que essa descoberta seja a finalidade única do processo, a ser obtida a todo custo. Ao revés, a moderna doutrina sobre epistemologia da prova chega à conclusão de que a verdade assume contornos relativos e deve se aproximar, o tanto quanto possível e admissível, da realidade histórica dos fatos[627].

Sob essa perspectiva, demoliram-se sofismas relacionados à necessidade de uma verdade absoluta e incontestável dos fatos[628] para, então, se caminhar

---

[627] BADARÓ, Gustavo Henrique Righi Ivahy. *A cadeia de custódia e sua relevância para a prova penal* In. SIDI, Ricardo, LOPES, Anderson Bezerra (orgs.) Temas atuais da investigação preliminar no processo penal. Belo Horizonte: Editora D' Plácido, 2017, p. 517-538).

[628] Como destaca Luigi Ferrajoli, "(...) a oposição até agora conhecida entre garantismo e autoritarismo no direito penal corresponde, pois, a uma alternativa entre duas epistemologias judiciais distintas: entre cognoscitivismo e decisionismo, entre comprovação e avaliação, entre prova e inquisição, entre razão e vontade, entre verdade e potestade. Se uma justiça penal completamente 'com verdade' constitui uma utopia,

com a ideia de que a verdade seja um objetivo institucional do processo[629], a ser obtida mediante análise racional das provas em que, respeitados os limites epistêmicos e legais, se conclua pela escolha da hipótese fática mais provável, mediante motivação que atenue os riscos de escolhas individuais desconectadas da razão.

Dentre estes controles epistêmicos que limitam a produção de elementos probatórios que possam contribuir para a reconstrução histórica dos fatos, reconhece-se a necessidade de se documentar e preservar a cadeia de custódia ("chain of custody"), como forma de se atestar a integridade da prova[630].

Assim, a cadeia de custódia é uma metodologia[631] estabelecida pelo legislador para se comprovar, documental e ininterruptamente, os atos que sucederam a fonte de prova, desde sua recolha, o traslado e a conservação dos indícios e vestígios obtidos no curso de uma investigação criminal, que deverá percorrer determinadas etapas concatenadas em que cada uma proporciona a viabilidade ao desenvolvimento da seguinte[632], previamente estabelecidas para se assegurar a autenticidade, integridade e inalterabilidade da fonte de prova[633].

Como bem define o artigo 158-A, *caput*, do Código de Processo Penal, é "(...) 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 (...)".

A cadeia de custódia pretende, nos dizeres de GERALDO PRADO, "(...) garantir que não haja deturpação do conhecimento produzido ao longo do processo penal a que uma pessoa está sendo submetida transcende o caso concreto e cuida de legitimar

---

uma justiça penal completamente sem verdade equivale a um sistema de arbitrariedade (...)" (FERRAJOLI, Luigi. *Derecho y razón: Teoría del garantismo penal.* Madrid: Editora Trotta, 2014, p. 45, trad. Livre).

[629] FERRER BELTRÁN, Jordi. *La valoración racional de la prueba*. Madrid: Marcial Pons, 2007, p. 29.

[630] BADARÓ, Gustavo Henrique Righi Ivahy. Op. cit. p. 517-538.

[631] SOUZA, Gilson Sidney Amancio de. *Princípio da indenidade ou da Higidez da Prova.* In: HAMMERSCHMIDT, Denise (Org.). Código de Processo Penal Comentado. Curitiba: Editora Juruá, 2020, p. 279-280.

[632] DIAS FILHO, Claudemir Rodrigues. *Cadeia de custódia: do local de crime ao trânsito em julgado; do vestígio à evidência*. In: MOURA, Maria Thereza Rocha de Assis; NUCCI, Guilherme de Souza (orgs). Doutrinas Essenciais - Processo Penal. v. 3. São Paulo: Editora RT, 2012, p. 404.

[633] Definição extraída da decisão do Tribunal Supremo da Espanha no STS 208/2014, de 10 de março de 2014, Sala de lo Penal.

o exercício do poder de punir no marco do Estado de Direito, coibindo o abuso de poder (...)"[634].

Entretanto, como bem destacam DALLAGNOL e CÂMARA, é relevante se diferenciar a "cadeia de custódia" e a "prova da cadeia de custódia", já que a primeira seria a corrente histórica relativa a todos aqueles que, de maneira sucessiva e encadeada, tiveram contato com a fonte de prova real[635], ao passo que a última estaria relacionada com a produção de elementos probatórios que visem documentar esta reconstrução cronológica, desde sua geração até o seu aporte aos autos[636]. Assim, interessaria ao processo penal a "prova da cadeia de custódia".

A noção de "cadeia de custódia" tem inspiração norte-americana, por servir como uma das medidas utilizadas para "autenticação da prova", prevista especialmente nas *Rules* 901 e 902 do *Federal Rules of Evidence* dos Estados Unidos[637], em que se estabelece os requisitos para autenticação ou identificação de um item de evidência. Nesta ordem, a autenticação é um dos elementos que garantem a relevância da prova[638] – na forma da *Rule 401 (a)* do *Federal Rules of Evidence* – e, por conseguinte, a torna admissível de apreciação pelo Júri, após a chancela do juiz togado.

---

[634] PRADO, Geraldo. *A cadeia de custódia da prova no processo penal.* São Paulo: Editora Marcial Pons, 2019, p. 134.

[635] Gustavo Badaró também destaca que, quando se fala em "cadeia de custódia", a expressão deve ser entendida como a elipse de "documentação da cadeia de custódia". Nesta linha, não seria possível se falar em violação da "cadeia de custódia", haja vista que eventual adulteração ou falsificação somente incidiria sobre a própria fonte real de prova ou, ainda, com relação à documentação da cadeia de custódia. Portanto, uma adulteração da fonte de prova (substituição da droga por açúcar, *v.g.*), atinge a fonte real diretamente, e não sua "cadeia de custódia". De igual sorte, a completa ausência de registro quanto às pessoas que tiveram contato com a prova não traz eiva à "cadeia de custódia" propriamente dita, já que esta efetivamente existiu, à medida que um maior ou menor número de pessoas teve, documentadamente ou não, contato com a prova. O que ocorre, nesta hipótese, é um vício em relação à documentação da cadeia de custódia, que serve para se assegurar a autenticidade e integridade da prova (BADARÓ, Gustavo Henrique Righi Ivahy. *A cadeia de custódia e sua relevância para a prova penal* Op. cit. p. 524).

[636] DALLAGNOL, Deltan Martinazzo; CÂMARA, Juliana de Azevedo Santa Rosa. *A cadeia de custódia da prova.* In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro de (Org.). A prova no enfrentamento à macrocriminalidade. Salvador: Editora JusPodivm, 2019, cap. 18, p. 530. Os autores indicam, de maneira bem didática, que em relação à cadeia de custódia podem ser questionadas a falsidade da prova propriamente dita, a insuficiência da prova da cadeia de custódia da prova ou a falsidade da prova da cadeia de custódia da prova. Para fins do presente trabalho científico, passaremos a nos referir apenas a "cadeia de custódia", mas com o viés relacionado à prova desta cadeia de custódia.

[637] Para inteiro teor das normativas, confira-se: https://www.law.cornell.edu/rules/fre/rule_901; https://www.law.cornell.edu/rules/fre/rule_902; https://www.law.cornell.edu/rules/fre/rule_903. Acesso em: 20 de dezembro de 2020.

[638] Dallagon e Câmara apontam, com propriedade, que não se confundem os conceitos de "autenticação" e "autenticidade" da prova, sendo certo que a "autenticação" é um dos critérios pelos quais se atesta a relevância da prova (DALLAGNOL, Deltan Martinazzo; CÂMARA, Juliana de Azevedo Santa Rosa. *A cadeia de custódia da prova.* Op. cit. p. 533).

A "cadeia de custódia", embora umbilicalmente ligada à prova pericial, tem pertinência com todas as fontes de provas reais, servindo para assegurar a autenticidade e integridade destas quando a investigação envolver sua coleta, armazenamento ou análise[639].

Pretende-se, com a documentação da "cadeia de custódia", atender aos princípios da "mesmidade" e da "desconfiança", conforme explica PRADO[640].

A "mesmidade" seria um neologismo extraído a partir do direito espanhol[641], que estabelece que a prova da cadeia de custódia visa assegurar que a prova valorada é exatamente a mesma que fora colhida. Desta forma, evita-se que alguém seja julgado não com base no "mesmo", mas no "selecionado" pela acusação, desequilibrando-se a relação processual entre as partes[642].

Por sua vez, a "desconfiança" consistiria na exigência de que os elementos de prova sejam "acreditados", mediante submissão de procedimentos que demonstrem que os objetos correspondem ao que a parte alega ser, evitando-se a adoção de sistemas de confiança preestabelecidos em benefício de quaisquer das partes e nos elementos que por eles são introduzidos. Assim, todos os elementos devem ser "acreditados", para que detenham valor probatório[643], de modo que o julgador não pode colocar especial confiança em uma das partes, principalmente quando ela representa o Estado[644].

Em perspectiva distinta e primando pelas relações de boa-fé que pautam as relações humanas e jurídicas, DALLAGNOL e CÂMARA admitem a

---

[639] BADARÓ, Gustavo Henrique Righi Ivahy. *A cadeia de custódia e sua relevância para a prova penal* Op. cit. p. 522.
[640] PRADO, Geraldo. *Ainda sobre a quebra da cadeia de custódia das provas*, Boletim IBCCRIM, São Paulo, ano 22, n.º 262, setembro de 2014, p. 16-17.
[641] Conforme se extrai da *Sentencia Penal n.º 160/2015*, de 10 de março de 2015, Sección 1, Recurso n.º 10716/2014, na Sala de lo Penal do Tribunal Supremo "(...) garantizar la 'mismidad' de la prueba, es decir identidad de los efectos recogidos con los efectos trasladados hasta el lugar del examen y los efectos analizados, y en su caso destruídos (...)".
[642] LOPES JR., Aury. *Direito Processual Penal.* Op. cit, p. 459. Na jurisprudência, destaca-se que o Supremo Tribunal Federal (STF) já reconheceu o direito da defesa ter acesso aos arquivos originais enviados pela empresa *Blackberry*, em razão de fundadas dúvidas quanto à preservação da cadeia de custódia da prova (STF, Recl. n.º 32.722/MT, 2ª Turma, Rel. Min. Gilmar Mendes, julgado em 7 de maio de 2019, DJe 29/11/2019).
[643] PRADO, Geraldo. *A cadeia de custódia da prova no processo penal.* Op. cit. p. 94 e seguintes.
[644] MENEZES, Isabela Aparecida; BORRI, Luiz Antônio; SOARES, Rafael Júnior. *A quebra da cadeia de custódia da prova e seus desdobramentos no processo penal brasileiro.* Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 4, n. 1, jan.-abr. 2018, p. 283.

possibilidade de se realizar generalizações indutivas alcançadas com base na experiência, na boa-fé das pessoas, na correção do agir estatal e na veracidade da prova, o que permitiria admitir uma presunção relativa de regularidade da prova.

Assim, os autores apontam que, conquanto deva existir indicativos de que a prova trazida seja, efetivamente, aquilo que o proponente diz que ela é, bem como que seu conteúdo fora preservado, a avaliação dessas indicações deve se pautar pela presunção[645] de regularidade da prova e a boa-fé dos agentes. Portanto, "(...) conquanto a boa-fé ou regularidade da prova não se revista de caráter absoluto, se não demonstrada a má-fé, supõe-se a integridade da evidência, sob pena de subverter-se toda a lógica do sistema jurídico (...)".

Assentando-se nestas premissas, DALLAGNOL e CÂMARA reportam que a prova da cadeia de custódia possui valor relativo, não apenas em razão das possibilidades de adulteração e falsificação, na teoria e na prática, mas também pelo fato de que a adoção de uma preconcebida desconfiança conduziria ao regresso, *ad infinitum,* da justificação na epistemologia, já que em matéria da simples prova haveria a necessidade de uma metaprova que, por sua vez, novamente em razão do princípio da desconfiança, exigiria uma metaprova sobre a metaprova para sua aceitabilidade e suficiência, e assim sucessivamente.

De toda sorte, é evidente que a presunção de boa-fé e correção do agir no dever estatal não afastam a responsabilidade dos agentes estatais em documentar a cadeia de custódia, especialmente em um sistema de investigação criminal atribuída a órgãos estatais oficiais[646].

A adoção do princípio da boa-fé e da relativa regularidade da prova exige, por conseguinte, que o ônus probatório para comprovação de eventual violação à prova da cadeia de custódia parta da efetiva ocorrência de corrupção de evidência - e não

---

[645] STJ, AgRg no REsp n.º 1.668.560/PR, 5ª Turma, Rel. Min. Felix Fischer, julgado em 15 de maio de 2018, DJe 21/05/2018; STJ, AgRg no REsp n.º 911.137/PR, 5ª Turma, Rel. Min. Felix Fischer, julgado em 15 de maio de 2018, DJe 21/05/2018.

[646] BADARÓ, Gustavo Henrique Righi Ivahy. *A cadeia de custódia e sua relevância para a prova penal* Op. cit. p. 534.

apenas da mera possibilidade ou conjectura[647] -, sob pena de se impor à acusação o dever de comprovar uma infinitude de fatos negativos, para além de indicações relacionadas à boa-fé, regularidade, identidade e conservação da prova[648].

Extrai-se, portanto, que a cadeia de custódia tem relação direta com os princípios do contraditório, devido processo legal, paridade de armas e ampla defesa, especialmente com relação aos elementos de prova submetidos a contraditório diferido, permitindo-se ao acusado ter acesso[649] aos elementos de prova produzidos pela Polícia Judiciária e pelo Ministério Público, sindicando-os quanto à sua integridade, coerência e consistência[650].

7.2. A disciplina da cadeia de custódia no Código de Processo Penal

Até o advento da Lei n.º 13.964/2019, não havia uma previsão normativa expressa acerca da cadeia de custódia da prova. Entretanto, a inexistência de regulamentação não impedia que se reconhecesse a necessidade de preservação da cadeia de custódia, fruto de interpretação sistemática do artigo 6º, incisos I e III, artigo 159, § 6º e artigo 170, todos do Código de Processo Penal, especialmente em um processo penal lastreado em *standart* probatório elevado, em que a fundada possibilidade de adulteração da

---

[647] Como bem assentou o Superior Tribunal de Justiça (STJ), "(...) compete a defesa infirmar a presunção de validade e legitimidade dos atos praticados por agentes públicos, demonstrando de forma concreta o descumprimento das formalidades legais e essenciais, e especificamente no caso concreto, que o material apreendido e eventualmente não lacrado foi corrompido ou adulterado, de forma a causar prejuízo a defesa e modificar o conteúdo da prova colhida (...)" (STJ, RHC n.º 59.414/SP, 5ª Turma, Rel. Min. Reynaldo Soares da Fonseca, julgado em 27 de junho de 2017, DJe 03/08/2018).

[648] DALLAGNOL, Deltan Martinazzo; CÂMARA, Juliana de Azevedo Santa Rosa. *A cadeia de custódia da prova.* Op. cit. p. 543-549. Diferente é a visão de LOPES JR., para quem "(...) não se trata nem de presumir a boa-fé, nem a má-fé, mas sim de objetivamente definir um procedimento que garanta e acredite a prova independente da problemática em torno do elemento subjetivo do agente. A discussão acerca da subjetividade deve dar lugar a critérios objetivos, empiricamente comprováveis, que independam da prova de má-fé ou 'bondade e lisura' do agente estatal (...)", arrematando que a exigência do cumprimento das etapas da cadeia de custódia é "(...) uma forma de diminuir o espaço impróprio da discricionariedade judicial, fazendo com que a decisão não dependa da valoração do juiz acerca da interioridade/subjetividade dos agentes estatais, sob pena de incorrer numa dupla subjetividade com incontrolabilidade ao quadrado (...)" (LOPES JR., Aury. *Direito Processual Penal.* Op. cit, p. 456. No mesmo sentido, citando *Pilas Ladrón Tabuesca:* BADARÓ, Gustavo Henrique Righi Ivahy. *A cadeia de custódia e sua relevância para a prova penal* Op. cit. p. 534).

[649] Especialmente com relação ao acesso aos elementos de prova, destaca-se a Súmula Vinculante n.º 14 do Supremo Tribunal Federal (STF). Sobre o tema, recomenda-se: MACHADO, Vitor Paczek; JEZLER JUNIOR, Ivan. *A prova eletrônica-digital e a cadeia de custódia das provas: uma (re)leitura da Súmula Vinculante 14*. Boletim IBCCRIM, São Paulo, ano 24, nº 288, nov./2016; PRADO, Geraldo. *Prova Penal e sistema de controles epistêmicos: a quebra da cadeia de custódia das provas obtidas por meios ocultos*. São Paulo: Editora Marcial Pons, 2014, p. 41.

[650] EDINGER, Carlos. *Cadeia De Custódia, Rastreabilidade Probatória*. Revista Brasileira de Ciências Criminais, vol. 120, mai.-jun./2016, p. 254-255.

prova ou ausência de demonstração segura de sua autenticidade poderia comprometer o resultado condenatório[651].

Com a reforma legislativa operada pela Lei n.º 13.964/2019, foram introduzidos no Código de Processo Penal os artigos 158-A a 158-F, com redação inspirada na Portaria n.º 82, de 16 de julho de 2014, da Secretaria Nacional de Segurança Pública do Ministério da Justiça e no artigo 254 do *Código de Procedimiento Penal* colombiano[652].

Assim, a cadeia de custódia tem início com a efetiva preservação do local do crime ou com procedimentos policiais ou periciais nos quais seja detectada a existência de vestígio (artigo 158-A, § 1º, do Código de Processo Penal) e se encerrará com o descarte do vestígio (artigo 158-B, inciso X, do mesmo Diploma Legal), mesmo se já apresentado o laudo pericial e prestados os esclarecimentos necessários pelos peritos.

De maneira descritiva e em caráter protocolar, o artigo 158-B do Código de Processo Penal cuidou de estabelecer que a cadeia de custódia compreende o rastreamento dos vestígios nas etapas do *reconhecimento* (artigo 158-B, inciso I), *isolamento* (artigo 158-B, inciso II), *fixação* (artigo 158-B, inciso III), *coleta* (artigo 158-B, inciso IV), *acondicionamento* (artigo 158-B, inciso V), *transporte* (artigo 158-B, inciso VI), *recebimento* (artigo 158-B, inciso VII), *processamento* (artigo 158-B, inciso VIII), *armazenamento* (artigo 158-B, inciso IX) e *descarte* (artigo 158-B, inciso X).

De igual sorte, nos artigos 158-C, 158-D, 158-E e 158-F o legislador estabeleceu a forma pela qual deverá ser implementada a coleta dos vestígios, o recipiente para acondicionamento da prova, bem como disciplinou como deveriam ser implementadas as centrais de custódia destinadas à guarda e controle dos vestígios, além de seu acesso e a forma de registro.

---

[651] BADARÓ, Gustavo Henrique Righi Ivahy. *A cadeia de custódia e sua relevância para a prova penal* Op. cit. p. 526-527.

[652] Artículo 254. Aplicación. Con el fin de demostrar la autenticidad de los elementos materiales probatorios y evidencia física, la cadena de custodia se aplicará teniendo en cuenta los siguientes factores: identidad, estado original, condiciones de recolección, preservación, embalaje y envío; lugares y fechas de permanencia y los cambios que cada custodio haya realizado. Igualmente se registrará el nombre y la identificación de todas las personas que hayan estado em contacto con esos elementos. La cadena de custodia se iniciará en el lugar donde se descubran, recauden o encuentren los elementos materiales probatorios y evidencia física, y finaliza por orden de autoridad competente. Parágrafo. El Fiscal General de la Nación reglamentará lo relacionado con el diseño, aplicación y control del sistema de cadena de custodia, de acuerdo con los avances científicos, técnicos y artísticos.

Embora louvável a iniciativa legislativa de estabelecer as etapas da cadeia de custódia e reconhecer a importância do instituto, especialmente nos delitos que demandam a produção de prova pericial, é certo que a implementação efetiva das etapas e, principalmente, da central de custódia nos Institutos de Criminalística demandará dotação orçamentária aos Estados, sob pena de tornar letra morta as inovações legislativas trazidas[653].

Não bastasse, uma questão relevante passou ao largo da reforma implementada: as consequências da violação da cadeia de custódia, o que será visto oportunamente.

7.3. A cadeia de custódia da prova digital

Como visto, a cadeia de custódia consiste na sequência de proteção e guarda de elementos materiais encontrados durante uma atividade investigativa, a fim de se assegurar a idoneidade do conteúdo e a manutenção de suas características originais, além de se estabelecer a autenticidade da prova[654].

Nesta perspectiva, é indiscutível que a cadeia de custódia goza de distinta importância no tratamento das provas obtidas no contexto digital, especialmente em razão de suas características já anteriormente tratadas[655], notadamente a imaterialidade, volatilidade, fragilidade, intrusividade, suscetibilidade de clonagem e imprescindibilidade de intermediação de equipamento para acesso ao conteúdo.

Como bem destaca CASEY: *“*

> chain of custody and integrity documentation are important for demonstrating the authenticity of digital evidence. Proper chain of custody demonstrates that digital evidence was acquired from a specific system and/or location, and that it was continuously controlled since it was collected. Thus, proper chain of custody documentation enables the court to link the digital evidence to the crime. Incomplete documentation can

---

[653] DEZEM, Guilherme Madeira. *Curso de processo penal*. Op. cit. p. 695

[654] ESPINDULA, Alberi, *Perícia criminal e cível: uma visão geral para peritos e usuários da perícia.* 4ª Ed. Campinas: Editora Millenium, 2013.

[655] Vide tópico 2.1.

> result in confusion over where the digital evidence was obtained and can raise doubts about the trustworthiness of the digital evidence (CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers and the internet*. 3th Edition, Maryland: Ed. Elsevier, 2011, p. 60)[656].

É relevante assentar que o Código de Processo Penal deixou de estabelecer, de maneira expressa, um regramento particular de cadeia de custódia para a prova digital. Entretanto, embora fosse desejável uma disciplina expressa sobre o tema, há de se atentar para a advertência de DANIELE, para quem a adoção de uma legislação que cristalize os métodos próprios correria o risco da obsolescência quase imediata, diante da constante evolução e superação da tecnologia da informação[657].

Especificamente com relação à prova digital, ganha projeção o estudo da "computer forensic"[658], expressão cunhada para se definir a utilização de técnicas confiáveis, seguras e relevantes para busca, autenticação e exame dos dados amealhados em dispositivos eletrônicos.

---

[656] Na mesma linha, Fábio Bechara aponta que "(...) tais cuidados são de extrema importância considerando o fim da fronteira entre o ambiente físico e o digital, dada a migração do ambiente off-line para o ambiente online. Hoje, a maioria das evidências é coletada em ambientes digitais, como servidores, computadores e outros dispositivos eletrônicos. Os dispositivos de armazenamento digital, em geral, são voláteis, frágeis e se não manuseados corretamente, podem acarretar na destruição ou deturpação das evidências do ilícito (...)" (BECHARA, Fábio Ramazzini. *Evidências Digitais e Confiabilidade do Conteúdo*. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/evidencias-digitais-e-a-confiabilidade-do-conteudo-16072019. Acesso em: 20 de dezembro de 2020).

[657] Para Marcello Daniele, "(...) un primo antidoto è rappresentato dall'impiego delle metodologie di individuazione e di apprensione delle prove digitali in assoluto ritenute migliori dalla tecnica informatica. Sotto questo profilo, l'ideale sarebbe che il legislatore potesse prestabilire uma specifica tecnica di acquisizione dalle prove digitali, da osservare scrupolosamente a pena di inutilizzabilità ogni volta in cui un reato lasciasse tracce in un sistema informatico. Il metodo prescelto diventerebbe la 'regola d'oro' della formazione delle prove digitali, come l'esame incrociato lo è per l'assunzione delle prove dichiarative. Al momento, però, purtroppo questa strada non e` percorribile. L'informatica è una scienza relativamente giovane, e non si può dire che ad oggi esista un método di raccolta delle prove digitali in grado di imporsi su tutti gli altri. Gli esperti in materia suggeriscono perlopiù un approccio pragmatico: la scelta della técnica da impiegare dipende dalla situazione che si presenta in concreto agli investigatori (52). Una normativa che cristallizzasse un metodo piuttosto che un altro sarebbe a rischio di immediata obsolescenza, in quanto fisserebbe regole che potrebbero essere velocemente superate dell'evoluzione (...)" (DANIELE, Marcello. *La prova digitale nel processo penale*. Rivista di diritto processuale. Padova, p. 283 s., 201, p. 293)

[658] O termo "computer forensics", embora utilizado inicialmente quando as fontes digitais primárias eram computadores, já é considerada inapropriada para se reconhecer a coleta de novos elementos digitais em outras fontes digitais distintas dos computadores (CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers and the internet.* Op. cit. p. p. 37-38). Sobre o tema, recomenda-se ainda: LUPARIA, Luca; ZICCARDI, Giovanni. *Investigazione penale e tecnologia informatica: L'accertamento del reato tra progresso scientifico e garanzie fondamentali*. Milano: Editora Giuffrè, 2007, p. 31-46.

Em razão das características próprias da prova digital, especialmente sua fragilidade e a possibilidade de a evidência vir a ser adulterada, modificada ou excluída, ainda que não intencionalmente[659], a admissibilidade da cadeia de custódia deverá assegurar que a prova digital[660] seja:

a) autêntica, exigindo-se a comprovação de que tenha provido do suporte eletrônico indicado e que os dados permaneceram inalterados desde sua coleção, o que poderá se comprovar mediante a utilização de metadados relacionados aos dados a serem extraídos[661];

b) completa, de forma a evitar a elucubração de suspeitas alternativas, permitindo-se a análise, pelas partes, de toda a fonte de prova da qual se extraiu a evidência, assegurando-se seu contraditório de forma a evitar que apenas o material que interessar a cada uma delas seja introduzido, acriticamente, no processo[662];

c) confiável, que visa assegurar a legítima expectativa de confiança das partes na prova digital coletada, o que demanda a minuciosa identificação das etapas da cadeia de custódia, com a correta individualização dos *hardwares* e *softwares* utilizados, bem como o manejo das evidências por profissionais capacitados que, diante de sua *expertise*, evitem a adulteração da prova digital;

d) crível, a fim de que a prova digital seja compreensível às partes e ao julgador, de forma clara, permitindo-se sua interpretação sem que venha a perder seu rigor metodológico.

É certo que algumas evidências de cunho digital possuem padrões de autenticação que permitem certificar a veracidade de um documento e sua intangibilidade. *Ad exemplum*, a certidão de antecedentes federais solicitada diretamente no sítio eletrônico

---

659 VACCA, John. R. *Computer Forensics: Computer Crime Scene Investigation*. Second Edition, Charles River Media, p. 240.
660 PINHEIRO, Patrícia Peck. *Direito Digital*. 3ª ed. São Paulo: Saraiva, 2009, p. 411.
661 CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers and the internet.* 3th Edition, Ed. Elsevier, 2011, p. 60.
662 LOPES JR., Aury. *Direito Processual Penal.* Op. cit, p. 457.

da Polícia Federal é suscetível de validação mediante códigos de autenticação próprios[663], o que permite atestar a autenticidade e integridade do conteúdo emitido.

Entretanto, outros elementos de prova, notadamente os dados armazenados em aparelhos celulares que vierem a ser obtidos, não dispõem de padrões de autenticação instantâneos e, com isso, podem ser mais facilmente manipulados[664]. De igual sorte, por se tratar de evidente meio de investigação de prova, a busca é realizada normalmente em fase investigativa, sem a possibilidade da realização do contraditório prévio, o que exige um maior rigor na observância de toda a trajetória da prova, desde sua coleção até seu descarte[665].

Ainda que as provas digitais gozem de disciplina própria em razão de suas características já mencionadas, a sua cadeia de custódia não difere substancialmente das etapas a serem percorridas para os demais tipos tradicionais de provas[666], com algumas especificidades próprias, normalmente de cunho tecnológico, que já vem sendo objeto de atenção por legislações processuais internacionais[667].

---

[663] https://www.gov.br/pf/pt-br/assuntos/antecedentes-criminais. Acesso em: 20 de dezembro de 2020.

[664] CALDEIRA, Rodrigo de Andrade Figaro. *Cadeia de Custódia: arts. 158-A a 158-F, do CPP*. In: AKERMAN, William; DUTRA, Bruna Martins Amorim (Orgs.) Pacote Anticrime. Análise crítica à luz da Constituição Federal. São Paulo: Editora RT, 2020, p. 216.

[665] AZEVEDO, Yuri; VASCONCELOS, Caroline Regina Oliveira. *Ensaios sobre a cadeia de custódia das provas no processo penal brasileiro.* Florianópolis: Editora Empório do Direito, 2017, p. 127.

[666] FRIEDEN e MURRAY reconhecem que "(...) it is important to remember that there is nothing 'magical' about the admission of electronic evidence. The prevalence of electronic evidence has required no substantial changes to the Federal Rules of Evidence. In analyzing the admissibility of such evidence, it is often best to treat it as originating from the most similar, non-electronic source as thoughtful application of traditional evidentiary principles will nearly always lead to the correct result. Thus, while electronic evidence may present some unique challenges to admissibility and complicate matters of establishing authenticity and foundation, it does not require the proponent to discard his knowledge of traditional evidentiary principles or learn anything truly new (…)" (FRIEDEN, Jonathan D.; MURRAY, Leigh M. *The Admissibility of Electronic Evidence Under the Federal Rules of Evidence*, XVII Richmond Journal of Law and Technology, Vol. XVII, Issue 2, p. 2). No mesmo sentido: MENDES, Carlos Hélder Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software*, p. 138.

[667] À guisa de exemplo do artigo 247, 1-*bis*, do *Codice de Procedura Penale Italiano*[667], alterado como forma de se amoldar as disposições normativas italianas às previsões da Convenção de Budapeste para o *cybercrime*: "(...) Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorchè protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione (...)"

7.3.1 As etapas da cadeia de custódia para obtenção dos dados armazenados em aparelhos celulares

A cadeia de custódia da prova digital, em geral, deve abranger etapas de *recolha, autenticação, exame, análise* e *relatório*[668] da prova, atentando-se ainda para as diretrizes contidas na normativa ABNT/ISO 27037:2013, estabelecida pela Associação Brasileira de Normas Técnicas (ABNT), que objetiva padronizar o tratamento das evidências digitais a fim de preservar sua integridade.

A partir da nova disciplina trazida pelo Código de Processo Penal, buscar-se-á estabelecer, de maneira breve e sem adensamentos em especificidades técnicas próprias[669], as etapas a serem observadas para se assegurar a integridade e idoneidade dos dados armazenados em aparelho celular ou *smartphone*, desde seu *reconhecimento* até seu *descarte*.

As primeiras etapas da cadeia de custódia se referem ao *reconhecimento* (artigo 158-B, inciso I, do CPP), *isolamento* (artigo 158-B, inciso II, do CPP) e *fixação* (artigo 158-B, inciso III, do CPP).

Assim, tão logo identificado um dispositivo eletrônico (*v.g.*, um *smartphone* ou um aparelho celular convencional) que seja de interesse investigativo, especialmente durante uma apreensão determinada por ordem judicial prévia ou nas hipóteses do artigo 6º, inciso III, do Código de Processo Penal, deverá a autoridade promover o *isolamento* e a *fixação* do objeto, evitando-se que terceiros tenham contato com o objeto, descrevendo-o detalhadamente e ilustrando as circunstâncias de sua localização com fotografias, imagens ou *croquis* que permitam identificar a sua posição na área dos exames[670].

---

[668] MENDES, Carlos Hélder Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software,* p. 154-155.

[669] As etapas para o cumprimento da cadeia de custódia das provas armazenadas em aparelhos celulares são bem individualizadas na obra de Luca Luparia e Giovanni Ziccardi: LUPARIA, Luca; ZICCARDI, Giovanni. *Investigazione penale e tecnologia informatica: L'accertamento del reato tra progresso scientifico e garanzie fondamentali.* Op. cit., p. 80-83.

[670] Idêntica observação é feita pelo Electronic Crime Scene Investigation, *Second Edition,* elaborado pelo U.S. Department of Justice (National Institute of Justice), que recomenda que o *first responder* realize os seguintes procedimentos: "(...) immediately secure all electronic devices, including personal or portable devices; Ensure that no unauthorized person has access to any electronic devices at the crime scene. Refuse offers of help or technical assistance from any unauthorized persons. Remove all persons from the crime scene or the immediate

O investigador deve-se atentar, também, para a possibilidade de que o dispositivo eletrônico possua evidências de DNA ou impressões digitais que, eventualmente, possam possuir interesse investigativo.

Ainda na etapa do *isolamento*, deve-se observar que os aparelhos celulares modernos, via de regra, possuem conexão com a *internet* por *Wi-Fi* ou rede de dados, o que exige uma cautela adicional diante da possibilidade de, remotamente, novos dados serem introduzidos e sobrepostos sobre outros existentes ou, ainda, modificados ou deletados, prejudicando-se a integridade da evidência pretendida[671].

Caso o aparelho celular esteja desligado, é recomendado que este permaneça nesta condição, evitando-se que, caso seja ligado, venha a ser remotamente alterado[672]. Entretanto, caso o *smartphone* esteja ligado, o investigador deverá avaliar a possibilidade de desconectá-lo da rede de *internet*[673], novamente com o intuito de se prevenir a alteração remota de dados por intermédio de conexões sem fio.

Este isolamento do aparelho do contato externo poderá se dar mediante[674]: *a)* acionamento do *modo avião* (*offline)*, nos aparelhos que dispõem desta funcionalidade, rompendo qualquer contato externo com o suporte eletrônico; *b)*

---

area from which evidence is to be collected. Ensure that the condition of any electronic device is not altered. Leave a computer or electronic device off if it is already turned off. Components such as keyboard, mouse, removable storage media, and other items may hold latent evidence such as fingerprints, DNA, or other physical evidence that should be preserved. First responders should take the appropriate steps to ensure that physical evidence is not compromised during documentation (…)" (p. 15-16). Disponível em <https://www.ncjrs.gov/pdffiles1/nij/219941.pdf>. Acesso em: 20 de dezembro de 2020.

[671] CASEY, Eoghan; TURNBULL, Benjamin. *Digital Evidence on Mobile Devices*. In: Digital Evidence and Computer Crime, 3 Ed. Elsevier, 2011, p. 13 e 16.

[672] No mesmo sentido a *Resolución* nº 234/2016, do *Ministerio de Seguridad de la Nación* Argentina, em seu artigo 2.5, C (Disponível em: <http://www.informaticalegal.com.ar/2016/06/07/resolucion-2342016-del-ministerio-de-seguridad-protocolo-general-de-actuacion-para-las-fuerzas-policiales-y-de-seguridad-en-la-investigacion-y-proceso-de-recoleccion-de-pruebas-en-ciberdelitos/>. Acesso em: 20 de dezembro de 2020).

[673] Para AYERS, BROTHERS e JANSEN, "(…) isolating a mobile device from all radio networks (e.g. WiFi, Cellular and Bluetooth) is important to keep new traffic, such as SMS messages, from overwriting existing data. Besides the risk of overwriting potential evidence, the question may arise whether data received on the mobile device after seizure is within the scope of the original authority granted. Vulnerabilities may exist that may exploit a weaknesses related to software vulnerabilities from the web browser and OS, SMS, MMS, third-party applications and WiFi networks. The possibility of such vulnerabilities being exploited may permit the argument that data may have been modified during the forensic examination (…)" (AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. *Guideline on Mobile Device Forensics*, In: *National Institute of Standards and Technology of U. S. Department of Commerce*, May 2014 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf. Acesso em: 20 de dezembro de 2020, p. 29).

[674] VECCHIA, Evandro Dalla. *Perícia Digital: Da investigação à análise forense.* Campinas: Editora Millenium, 2ª edição, 2019, p. 286.

desligamento do aparelho celular, com a remoção da bateria (sempre que possível), atentando-se para o fato de que, no momento da nova ligação do objeto, poderá ser necessário ultrapassar um sistema de autenticação de senhas que poderão inviabilizar o acesso aos dados; *c)* alocação do aparelho ligado em uma *Gaiola de Faraday*, que consiste em um instrumento que permite criar uma barreira de isolamento em dispositivos elétricos e eletrônicos, evitando-se a interferência em outros dispositivos próximos a ele[675].

Após o *isolamento* e a *fixação* do dispositivo pretendido, a próxima etapa consiste na *coleta* do *smartphone* (artigo 158-B, inciso IV, do CPP), etapa que desperta atenção por ser complexa e suscetível de impactar substancialmente a cadeia de custódia[676].

Por esta razão, tem-se recomendado[677] que, quando possível, a fase da *coleta* do aparelho seja acompanhada de profissionais técnicos e especializados, justamente por envolver, nos dizeres de MARSHALL[678], a fase da pré-visualização (*previewing) online* e *offline* da fonte da prova digital, com o contato direto do investigador com o objeto informático, a quem caberá analisar o dispositivo para constatar se há dados relevantes para a investigação e, por conseguinte, se há justificativa para apreensão física do suporte eletrônico com a subsequente análise minuciosa do seu conteúdo.

Nesta etapa e durante o próprio exame do suporte eletrônico apreendido, é comum que os investigadores constatem a exigência de etapas de autenticação

---

[675] No caso *Riley vs California*, a Suprema Corte Norte-Americana sustentou que a simples possibilidade de acesso e destruição remota dos dados armazenados em *smartphones* não justifica, por si só, a necessidade do acesso sem autorização judicial*"* (Disponível em: https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf. Acesso em: 20 de dezembro de 2020, p. 13-14). Entretanto, AYERS, BROTHERS e JANSEN advertem que, em pesquisas recentes, apurou-se que estes materiais de isolamento de rádio frequência não conseguem isolar completamente o aparelho apreendido, permitindo-se o recebimento de mensagens de texto e vídeo (AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. *Guideline on Mobile Device Forensics.* Op. cit., p. 31).

[676] COSIC, Jasmin; COSIC, Zoran. *Chain of Custody and Life Cycle of Digital Evidence.* Computer Technology and Application 3 (2012), p. 128.

[677] Márcio Satalino Mesquita registra, com acerto, que a participação deste técnico se limita a auxiliar na busca a ser realizada, já que as técnicas e procedimentos empregados não constituem o exame de corpo de delito, sendo que a perícia nos equipamentos será realizada posteriormente, por peritos oficiais (MESQUITA, Márcio Satalino. *A busca e apreensão na investigação e prova dos crimes cibernéticos.* In: Brasil. Tribunal Regional Federal da 3ª Região. Escola de Magistrados. Investigação e prova nos crimes cibernéticos. São Paulo: EMAG, 2017, p. 203).

[678] MARSHALL, Angus. *Digital forensics: digital evidence in Criminal Investigation.* Wiley-Blackwell, 2008, p. 43, *Apud* MENDES, Carlos Hélder Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software,* p. 155.

decorrente de criptografia ou biometria estabelecidas pelo detentor dos dados, tanto para acesso ao conteúdo do aparelho quanto para aplicativos específicos.

Ao se deparar com um aparelho protegido por senhas numéricas, sequenciais, biométricas ou por outras formas de criptografias, caberá ao investigador solicitar ao titular do aparelho que, de maneira voluntária, forneça as senhas ou códigos necessários para acesso ao dispositivo[679], anotando-os para posterior fornecimento ao perito

[679] É relevante a discussão quanto à possibilidade da adoção de medidas sancionatórias e coercitivas para constranger o detentor a fornecer a senha que guarnece a proteção de seu aparelho celular. O tema demandaria um estudo denso e específico sobre as garantias contra a autoincriminação, o que transcende os limites do presente trabalho científico. Em uma perfunctória análise do tema, destaca-se a existência de vertente doutrinária e jurisprudencial que assenta ser impossível se obrigar o titular do suporte eletrônico a fornecer as senhas e códigos de acesso, em homenagem ao princípio do *nemu tenetur se detegere*, extraídos do artigo 5º, inciso LXIII, da Constituição Federal, artigo 14, n.º 3, alínea *"g"*, do Pacto Internacional sobre Direitos Civis e Políticos e artigo 8º parágrafo 2º, alínea *"g"*, da Convenção Americana sobre Direitos Humanos ("Pacto de San Jose da Costa Rica"). Nesta linha, o Supremo Tribunal Federal (STF) já reconheceu que a garantia da não autoincriminação se estende às provas que demandem a participação ativa do acusado, conforme se verifica de alguns precedentes daquela Corte (STF, HC n.º 80.616/SP, 2ª Turma, Rel. Min. Marco Aurélio Mello, julgado em 18 de setembro de 2001, DJ 12/04/2004; HC n.º 83.096/RJ, Rel. Min. Ellen Gracie, julgado em 8 de agosto de 2003, DJ 22/08/2003; HC n.º 93.916/PA, 1ª Turma, Rel. Min. Carmen Lucia, julgado em 10 de junho de 2008, DJ*e* 26/06/2008. Portanto, sob essa ótica, o detentor da senha não poderia ser coagido, legal ou arbitrariamente, a fornecê-la, cabendo ao órgão investigativo adotar os meios tecnológicos próprios para decodificar a senha e garantir o acesso aos dados armazenados em seu aparelho celular.
Entretanto, parte da doutrina tem reconhecido a necessidade de se restringir a incidência do princípio da não autoincriminação, dentro de uma perspectiva relacionada ao equilíbrio de armas no processo penal. Assim, a garantia constitucional do direito ao silêncio não se estenderia aos elementos de prova que possuam existência independente do investigado. Especificamente no que tange à busca de aparelhos celulares, interpreta-se a necessidade da obtenção da senha como um obstáculo que impediria, propriamente, a apreensão do objeto pretendido, à exemplo da porta de uma residência ou um cofre, o que autorizaria a adoção de medidas de força para vencer o obstáculo e assegurar a apreensão do elemento de prova pretendido. Assentando-se nestas premissas, *Diogo Erthal Alves da Costa* reconhece que a questão deva ser solucionada à luz da proporcionalidade, admitindo-se inclusive a adoção de medidas coercitivas como a incriminação pelo delito de desobediência (artigo 330 do Código Penal), sem prejuízo da decretação da prisão temporária ou da prisão preventiva do investigado que se nega a fornecer a senha, sempre que estiver previamente demonstrada: (a) existência do crime; (b) indícios de vinculação do possuidor do dispositivo com o crime em investigação; (c) que há verossimilhança na alegação de que o dispositivo apreendido pode conter dados relevantes que se relacionam com o delito; (d) que o possuidor tem ciência da senha; (e) não há meio hábil para acessá-las diverso da obtenção da senha. Finalmente, *Diogo Costa* cita precedentes dos Estados Unidos e do Tribunal Europeu de Direitos Humanos (*Murray vs. Reino Unido)* para reconhecer a possibilidade de que, caso a medida de prisão não surta o efeito desejado ou não possa ser aplicada em razão de outras circunstâncias, o magistrado poderá valorar negativamente a obrigação do investigado em fornecer a senha, aplicando-se consequências negativas ao investigado a partir das regras de experiência, sem que isso importe em inversão do ônus da prova (COSTA, Diogo Erthal Alves da Costa. *Nemo tenetur se detegere e dados criptografados: restabelecendo o equilíbrio.* In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro de (Org.). *A prova no enfrentamento à macrocriminalidade*. Salvador: Editora JusPodivm, 2019. cap. 8, p. 209-252). Também discorrendo sobre o tema, DARIO KIST reconhece a inexistência de obrigatoriedade ou dever do acusado em fornecer a senha. Entretanto, o autor admite a possibilidade de por alteração legislativa, se impor ao acusado o dever de fornecer a senha em determinadas condições e para alguns tipos penais específicos, cabendo ao julgador analisar o caso à luz da proporcionalidade (KIST, Dario José. *Prova digital no processo penal.* Op. cit. p. 406-452).
Algumas legislações estrangeiras têm admitido a aplicação de consequências jurídicas, inclusive administrativas e penais, para os casos de recusas do investigado no fornecimento de senhas ou biometrias. Na França, o *Article 434-15-2* do *Códe Penal* prevê, expressamente, a pena de prisão e de multa para aquele que, detendo conhecimento sobre a senha de uma criptografia, deixa de informá-lo às autoridades judiciárias ou de

na fase de *processamento* dos dados. Deverá o investigador se atentar para o fato de que, em algumas plataformas operacionais de aparelhos celulares, a inserção repetida e equivocada de senhas poderá gerar o bloqueio indevido do aparelho ou, ainda, a remoção automática de todos os dados armazenados no dispositivo, prejudicando-se a evidência digital pretendida.

Caso a senha não seja fornecida voluntariamente pelo seu detentor, os investigadores poderão adotar outras medidas capazes de identificar a chave da criptografia que guarnece o acesso ao aparelho ou a um aplicativo específico, verificando se há indicações da senha em materiais anotados durante a busca – tais como cadernos, livros ou agendas – ou, ainda, solicitar aos provedores de serviço para que os forneça[680].

Registre-se que, em dispositivos conectados a servidores e que sejam de difícil apreensão[681], é recomendável a criação de cópia forense da mídia de armazenamento, seja por intermédio de cópia *bit a bit* do dispositivo ("espelhamento") ou, ainda, mediante a criação de uma imagem das informações contidas no dispositivo[682].

O procedimento de cópia integral deve ser realizado, preferencialmente, em modo *off-line,* conectando-se o dispositivo a uma estação de processamento e geração de *images* e a um bloqueador de gravações, evitando-se a introdução ou alteração de dados por um sistema informático[683].

---

execução, mediante requisições desta, sempre que a criptografia foi utilizada para preparação, facilitação ou cometimento de um crime ou de um delito. A questão foi levada à apreciação do *Conseil constitutionnel* da França, sob alegação de que a punição trazida no tipo penal violaria o direito ao silêncio e a garantia da não autoincriminação. Entretanto, a Corte admitiu, em decisão de 29 de março de 2018, que "(...) Le premier alinéa de l'article 434-15-2 du code pénal, dans sa rédaction résultant de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, est conforme à la Constitution (...)". De igual sorte, o *Regulation of Investigatory Powers Act 2000* do Reino Unido estabelece, na Parte III, item n.º 53, a pena de prisão de até 5 (cinco) anos, em casos envolvendo segurança nacional ou pedofilia, ou 2 (dois) anos nas hipóteses residuais, e multa, para o descumprimento de ordem de fornecimento de chave para acesso a dados protegidos por criptografia. Em julgamento ocorrido em 2008, a *Royal Courts of Justice* Britânica admitiu a regularidade da intimação dos proprietários de computadores para que informassem a senha para acesso aos dados contidos no dispositivo, sob pena de desobediência (http://www.bailii.org/ew/cases/EWCA/Crim/2008/2177.html. Acesso em: 20 de dezembro de 2020).

680 AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. *Guideline on Mobile Device Forensics,* Op. cit. p. 24-25.

681 Vide subtópico 4.2.1.

682 BECHARA, Fábio Ramazzini. *Evidências Digitais e Confiabilidade do Conteúdo*. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/evidencias-digitais-e-a-confiabilidade-do-conteudo-16072019>. Acesso em: 20 de dezembro de 2020).

683 MENDES, Carlos Hélder Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software,* p. 156.

Entretanto, com relação aos aparelhos celulares, ainda é comum que sua apreensão seja realizada e as cópias sejam providenciadas em etapa subsequente, durante o *processamento* da evidência, salvo em situações de urgência em que há necessidade de análise imediata dos dados armazenados no suporte eletrônico[684].

Juntamente com a *coleta* do dispositivo informático, deverá o investigador zelar pelo *acondicionamento*) do objeto (artigo 158-B, inciso V, do CPP), ocasião em que deverá cuidar para que o aparelho seja acondicionado e embalado em um pacote com atributos antiestáticos, em formato distinto de plásticos que possam transmitir eletricidade estática ou permitir um acúmulo indevido de condensação ou umidade[685], conforme artigo 158-D do Código de Processo Penal.

Ainda durante a fase do *acondicionamento,* o investigador deverá, para além de identificar a data, hora e nome de quem realizou a coleta e o acondicionamento, discriminar o suporte eletrônico apreendido, indicando o fabricante, marca, modelo do aparelho, cor, operador de telefonia, a existência de danos físicos constatáveis imediatamente, a numeração do IMEI (*International Mobile Equipment Identifier*) e do respectivo SIM-Card (*Subscriber Identity Module Card*), bem como outros dados que permitam a correta individualização do objeto.

Em seguida, o aparelho deverá ser *transportado* (artigo 158-B, inciso VI, do CPP) de forma adequada até o local onde vier a ocorrer seu *recebimento* (artigo 158-B, inciso VII, do CPP), em ambiente com temperatura e condições ideais, preservando-se a integridade do aparelho até a transferência da posse do objeto. Nesta etapa, deverá ser observada a necessidade de documentação completa do ato, com 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.

---

[684] AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. *Guideline on Mobile Device Forensics*. Op. cit. p. 36.

[685] Conforme recomendação oriunda do guia "*Electronic Crime Scene Investigation: An On-the-Scene Reference to First Responders",* do *National Institute of Justice* do *U.S. Department of Justice*, Nov. 2009, p. 21-22. Disponível em www.ojp.usdoj.gov/nij. Acesso em: 20 de dezembro de 2020.

Após o recebimento, inicia-se a fase de *processamento* do objeto (artigo 158-B, inciso VIII, do CPP), em que o setor técnico pericial deverá manipular o vestígio de acordo com a metodologia adequada, realizando-se o laudo pericial correspondente.

Nesta etapa, o perito que ficar incumbido de realizar o *processamento* e a análise dos vestígios deverá adotar cuidados adicionais para preservar a autenticidade e integridade dos dados, mantendo-se o isolamento do aparelho de conexões *wireless*, bem como instalando um *"write-blocking software",* que visa impedir o acréscimo, supressão ou modificação dos dados a serem analisados[686].

Durante a *coleta* dos dados[687], é importante que a bateria do aparelho esteja suficientemente carregada, o que extrai a importância da apreensão do carregador do aparelho celular durante as fases de *coleta* e *acondicionamento.*

Para extração dos dados, recomenda-se a conexão direta, por cabos, entre o aparelho e a estação pericial, evitando-se a utilização de procedimentos *wireless*, à medida que a simples habilitação e conexão *bluetooth* poderá alterar o estado do aparelho[688].

A extração dos dados do aparelho poderá se dar de diversas formas[689], dentre elas: *a) forma manual:* mediante análise individual realizada diretamente no

---

[686] Recomendação extraída do guia "*A Simplified Guide to Digital Evidence",* elaborado pela *National Forensic Science Technology Center* e pelo *U.S. Department of Justice.* Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/dados-da-atuacao/eventos-2/eventos-internacionais/conteudo-banners-1/crimes-ciberneticos/a-simplified-guide-to-digital-evidence>. Acesso em: 20 de dezembro de 2020.

[687] A coleta dos dados é expressão trazida por Evandro Dalla Vecchia para se referir à etapa de extração dos dados, não se confundindo com a "coleta" do vestígio, prevista no artigo 158-B, inciso IV, do Código de Processo Penal (VECCHIA, Evandro Dalla. *Perícia Digital: Da investigação à análise forense.* Op. cit. p. 287).

[688] VECCHIA, Evandro Dalla. *Perícia Digital: Da investigação à análise forense.* Op. cit. p. 288. CASEY e TURNBULL, por sua vez, recomendam a utilização complementar dos métodos de aquisição via cabo e *bluetooth*, haja vista que "(...) in some instances, the information retrievable from a data cable is different from the information extractable via Bluetooth, so it may be beneficial to perform logical extraction in different ways to ensure all possible content has been extracted (…)" (CASEY, Eoghan; TURNBULL, Benjamin. *Digital Evidence on Mobile Devices*. Op. cit. p. 21).

[689] CASEY, E. & TURNBULL, B. *Digital Evidence on Mobile Devices*. Op. cit. p. 19; OWEN, Paul; THOMAS, Paula; MCPHEE, Duncan. *An analysis of the Digital Forensic Examination of Mobile Phones.* 2010. In: Fourth International Conference on Next Generation Mobile Applications, Services and Technologies (Disponível em: <https://www.researchgate.net/publication/221328104_An_Analysis_of_the_Digital_Forensic_Examination_of_Mobile_Phones>. Acesso em: 20 de dezembro de 2020); AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. *Guideline on Mobile Device Forensics.* Op. cit. p. 18-24).

dispositivo, utilizada para a identificação particular de uma informação específica, adotando-se cuidados adicionais para evitar a alteração ou exclusão acidental de dados. Trata-se da forma mais básica de extração de dados e permite o acesso a toda informação disponível na plataforma[690]; *b) forma direta:* mediante acesso físico e direto à memória interna do dispositivo, mediante reconhecimento pelo sistema operacional ou do cartão de memória; *c) forma automática:* mediante a utilização de *software* capaz de ler, captar e sistematizar os dados.

Com a completa extração dos dados, o perito deverá condensar os elementos obtidos e proceder a análise das informações, com a subsequente elaboração de um laudo pericial a ser apresentado[691].

Ainda durante a fase de *processamento*, é relevante que as partes especifiquem ao perito qual o objetivo da diligência, notadamente o conteúdo dos dados que são de interesse para a atividade investigativa desenvolvida.

Em verdade, os aparelhos celulares possuem vasta capacidade de armazenamento de diversa gama de dados, compreendendo mensagens de texto, fotografias, vídeos, áudios, histórico de buscas e acessos a aplicativos, conteúdo de geolocalização, dentre outras. Desta feita, é tarefa árdua ao perito buscar analisar e condensar cada uma das informações e apresentar suas conclusões em laudo pericial e relatório sem, ao menos, ter conhecimento do objetivo da prova pericial.

---

[690] GOODISON, Sean E., DAVIS, Robert C., JACKSON, Brian A. *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*. Op. cit. p. 5-6; CARNEIRO, Márcio Rodrigo de Freitas. *Perícia de informática nos crimes cibernéticos.* In. *Caderno de Estudos de Investigação e prova nos crimes cibernéticos*, da Escola de Magistrados da Justiça Federal da 3ª Região, São Paulo: 1ª edição, 2017, p. 50-51.

[691] Em normatização interna, o Instituto de Criminalística (IC) da Polícia Civil do Estado de São Paulo, por intermédio dos pareceres CJ/SSP 1559/2016 e 2363/2016, tem exigido a prévia autorização judicial para a análise pericial dos dados armazenados no aparelho celular, sob pena da análise ser meramente de constatação física e detalhada do objeto, sem imersão quanto ao seu conteúdo. Como destaca KIST, "(...) tem-se por adequado que, como regra, seja solicitada autorização judicial para o acesso aos dados arquivados (...)", uma vez que "(...) a proteção da intimidade e a reserva da vida privada contra devassas e ingerências indevidas, em especial por agentes públicos, é direito fundamental de envergadura constitucional e que, em situação concreta, deve ser cotejado com o também e igualmente relevante interesse público na elucidação de infrações penais, condição para a correta aplicação da lei penal, o que inclui a necessidade de direcionar a persecução penal contra quem efetivamente é seu autor e, com isso, evitar a punição de inocentes (...)" (KIST, Dario José. *Prova digital no processo penal.* Op. cit. p. 161).

Portanto, com o intuito de se evitar subsequentes complementações do laudo pericial, é importante que, tanto quanto possível, as partes especifiquem ao perito qual o objeto da investigação e o conteúdo a ser analisado na sua atividade técnica[692], tais como, por exemplo, mensagens de texto que aparentemente façam menção a tráfico de entorpecentes, os dados da geolocalização de um aparelho em determinado período, fotografias e vídeos envolvendo pornografia infantil, a agenda de contatos e o rol de ligações efetuadas e recebidas para determinados contatos, etc.

Inegável que a análise forense do conteúdo extraído de um aparelho celular demandará a utilização de procedimentos bastante específicos e que, no mais das vezes, serão desconhecidos pelas partes do processo. Entretanto, considerando que o relatório da análise probatória deverá servir para sustentar ou refutar as hipóteses trazidas pela defesa ou pela acusação, é importante que a linguagem técnico-informática ceda espaço a uma perspectiva acessível aos sujeitos processuais, sem deixar de especificar, detalhada e minuciosamente, cada etapa dos procedimentos adotados para a obtenção dos dados relevantes[693].

---

[692] No guia *Best Practices for Seizing Eletronic Evidence (A Pocket Guide for First Responders), v. 3,* do *United States Secret Services,* há recomendação das informações que devem ser repassadas ao perito forense, além de uma sugestão de questões a serem formuladas e respondidos pelo profissional na conclusão de seu trabalho analítico-pericial (Disponível em http://www.mpf.mp.br/atuacao-tematica/sci/dados-da-atuacao/eventos-2/eventos-internacionais/conteudo-banners-1/crimes-ciberneticos/best-practices-for-seizing-electronic-evidence-v-3-a-pocket-guide-for-first-responders/view. Acesso em: 20 de dezembro de 2020).

[693] MENDES, Carlos Hélder Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software,* p. 160. O Procedimento Operacional Padrão (POP) para provas digitais, elaborado pelo Ministério da Justiça, prevê em seu *item 3.2. Informática Forense*, os tópicos a serem observados quando da elaboração do laudo pericial, a saber: "4.4. Elaboração do laudo. Esta etapa envolve a descrição dos exames efetuados e a apresentação, de forma clara e sucinta, dos procedimentos e métodos utilizados, esclarecendo os temas relevantes para a compreensão dos exames. Tópicos a serem observados: A descrição do material (equipamento, bateria, cartão SIM, cartão de memória removível, etc.) deve conter todos os dados para a sua correta identificação e individualização, tais como marca, modelo, número de série, IMEI (número internacional de identificação do aparelho GSM), ICCID (impresso no cartão SIM), MSI (número de identificação do assinante junto à operadora) e operadora do cartão SIM. Descrever os exames de forma proporcional à sua complexidade, evitando-se assim descrições extensas e complexas para laudos simples, e vice-versa. Especificar os softwares utilizados durante os exames somente quando essencial para a compreensão dos procedimentos adotados ou para futuras verificações dos resultados. Descrever as técnicas periciais propriamente ditas, e não os detalhes da utilização dos aplicativos forenses. Para o caso de existência de mídia anexa ao laudo, explicar que os arquivos ali gravados foram submetidos a uma função de hash para fins de garantia de integridade. Mencionar eventuais alterações (físicas ou lógicas) promovidas no material examinado. As ferramentas forenses de extração de dados geralmente apresentam os dados analisados em forma de relatório. Dependendo do volume e das características das informações extraídas, esse relatório poderá compor o laudo de forma impressa ou seguir em mídia anexa (...)" (*Procedimento Operacional Padrão (POP) Perícia Criminal n.º 3.2. Informática Forense,* do Ministério da Justiça do Brasil, publicado em setembro de 2013, p. 95).

Finalmente, com a elaboração do laudo pericial respectivo, encerra-se a fase do *processamento.* Assim, caberá ao perito promover o *armazenamento* (artigo 158-B, inciso IX, do CPP) do aparelho celular, em condições adequadas para preservação da evidência, seguindo-se ao seu *descarte* (artigo 158-B, inciso X, do CPP) após decisão judicial, com a destruição do objeto ou sua restituição ao legítimo proprietário.

Infere-se, portanto, que a cadeia de custódia da prova digital deve ser documentada por intermédio de relatório[694] que permita verificar a efetiva compreensão da diligência da recolha das *fontes de provas*, notadamente quando, onde e quem teve contato com a evidência digital em cada etapa da investigação[695], como forma de se garantir o cumprimento dos procedimentos forenses que assegurem o afastamento das hipóteses de contaminação por ingerência humana – no manuseio inapropriado de dispositivos informáticos – ou por via digital.

7.4 Consequências da violação da cadeia de custódia

Estabelecidas os regramentos a serem observados para cada etapa da cadeia de custódia, impende avançar sobre as consequências advindas de sua eventual violação ("break on the chain of custody").

Ao que se percebe, as consequências da violação poderão repercutir em dois campos, notadamente o da admissibilidade e o da valoração da prova[696].

Uma primeira vertente doutrinária aponta a inadmissibilidade da prova produzida com violação à cadeia de custódia. Para tanto, sustentam que a consequência inerente ao descumprimento das etapas seja a proibição de qualquer valoração probatória (*inadmissibilidade*), em razão da ilicitude da prova[697] e das que dela decorram,

---

[694] RAMALHO, David Silva. *Métodos Ocultos de Investigação.* Op. cit. p. 258.
[695] GIOVA, Giuliano. *Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems.* IJCSNS International Journal of Computer Science and Network Security, VOL. 11 No. 1, January 2011, p. 1.
[696] Para Badaró, "(...) no caso de violação da cadeia de custódia, em tese, duas soluções seriam possíveis: a primeira, considerar que a prova se torna ilegítima, não podendo ser admitida no processo; a segunda, superar o problema da admissão da prova e resolver o problema do vício da cadeia de custódia dando menor valor ao meio de prova produzido a partir de fontes de prova cuja cadeia de custódia tenha sido violada (...)" (BADARÓ, Gustavo Henrique Righi Ivahy. *A cadeia de custódia e sua relevância para a prova penal* Op. cit. p. 533).
[697] LOPES JR., Aury. *Direito Processual Penal.* Op. cit, p. 459; PRADO, Geraldo. *Prova Penal e sistema de controles epistêmicos: a quebra da cadeia de custódia das provas obtidas por meios ocultos*. Op. cit. p. 92; AZEVEDO, Yuri; VASCONCELOS, Caroline Regina Oliveira. *Ensaios sobre a Cadeia de Custódia das*

conforme artigo 157 do Código de Processo Penal e artigo 5º, inciso LVI, da Constituição Federal, acarretando-se a consequente exclusão física da prova e de toda a ela derivada.

Trata-se de uma interpretação que encontra inspiração no direito anglo-saxão, especialmente considerando que as *Rules* 901 e 902 do *Federal Rules of Evidence* dos Estados Unidos trazem a análise da cadeia de custódia para o campo da admissibilidade[698].

Uma segunda corrente, amparada na reforma legislativa que introduziu os artigos 158-A a 158-F no Código de Processo Penal, sustenta que eventual violação à sistemática adotada poderá acarretar a ilegitimidade da prova, por violação a regras de direito processual, com a consequente aplicação da teoria das nulidades[699].

Já para uma terceira corrente, a violação da cadeia de custódia deve ser apreciada na perspectiva da valoração da prova, de modo que eventual problema de higidez é solucionado no âmbito do peso a ser dado à prova pelo juiz, na formação de seu convencimento. Com efeito, a cadeia de custódia não teria relação com a licitude ou ilicitude da prova, mormente considerando que a cadeia de custódia não é a prova em si, mas sim uma metaprova ("prova sobre prova"), que visa assegurar a autenticidade e integridade da fonte de prova[700].

Provas no Processo Penal Brasileiro. Op. cit., p. 109; JEZLER JÚNIOR, Ivan. *Prova penal digital: tempo, risco e busca telemática.* Op. cit. p. 186; EDINGER, Carlos. *Cadeia De Custódia, Rastreabilidade Probatória*, Op. cit. p. 251; MENEZES, Isabela Aparecida; MENEZES, Isabela Aparecida; BORRI, Luiz Antônio; SOARES, Rafael Júnior. *A quebra da cadeia de custódia da prova e seus desdobramentos no processo penal brasileiro.* Op. cit., p. 293.

[698] DALLAGNOL, Deltan Martinazzo; CÂMARA, Juliana de Azevedo Santa Rosa. *A cadeia de custódia da prova.* Op. cit. p. 553.

[699] Guilherme Dezem aponta que toda violação da cadeia de custódia acarretará a nulidade pela não observância das regras, mas poderá o Estado, por seu órgão acusador, comprovar que não houve prejuízo e, aí, afastar a nulidade na forma do artigo 563 do Código de Processo Penal (DEZEM, Guilherme Madeira. *Curso de processo penal*. Op. cit. p. 696). Registre-se que parte da divergência entre a primeira e a segunda correntes deriva da discussão doutrinária quanto à distinção entre prova ilícita e prova ilegítima, especialmente a parte da redação dada ao artigo 157, *caput*, do Código de Processo Penal, com a reforma da Lei n.º 11.690/2008. O tema já foi discutido no subtópico 5.5.1.

[700] BADARÓ, Gustavo Henrique Righi Ivahy. *A cadeia de custódia e sua relevância para a prova penal* Op. cit. p. 535; DALLAGNOL, Deltan Martinazzo; CÂMARA, Juliana de Azevedo Santa Rosa. *A cadeia de custódia da prova.* Op. cit. p. 552 e 566.

Portanto, especialmente nos casos de omissões ou irregularidades sem maiores gravidades[701] (*v.g.*, o armazenamento do objeto a ser periciado na Delegacia de Polícia, ao invés do Instituto de Criminalística[702]; a ausência de indicação do número do pacote e a concisão do ofício[703]; a ausência de lacre em todos os documentos ou bens apreendidos[704], dentre outros), sem que haja indicativos concretos de que a fonte de prova possa ter sido modificada, adulterada ou substituída, a questão deve ser resolvida no momento da apreciação da prova[705], admitindo-se sua produção e valoração.

Entrementes, nos casos de vícios mais graves que coloquem em dúvida a integridade e autenticidade da prova (*v.g.*, a contaminação da amostra de sangue ou a modificação ou alteração de dados armazenados em um aparelho celular), é evidente que isso enfraquecerá sobremaneira sua valoração.

No campo jurisprudencial, a jurisprudência não é segura no tocante às consequências da violação da cadeia de custódia da prova. Com efeito, no *Habeas Corpus n.º 160.662/RJ,* a Corte reconheceu que o extravio de parte de áudios telefônicos interceptados ao longo de uma investigação acarreta a ilicitude de todo o material derivado da interceptação telefônica.

Sem mencionar expressamente a "cadeia de custódia", a Corte apontou que a perda de parte do material repercute no próprio dever de garantida da paridade de armas, inviabilizando-se o próprio exercício da ampla defesa[706], o que seria um aceno à interpretação de que a violação à cadeia de custódia atingiria a própria admissibilidade da evidência.

---

[701] O Supremo Tribunal Federal (STF), no bojo da Ação Penal n.º 1.030/DF, foi instado a apreciar supostas irregularidades decorrentes de violação da cadeia de custódia. Na ocasião, a Corte reconheceu que meras irregularidades relacionadas à forma de transporte do material colhido e sua manipulação não seriam aptas, por si só, a macular as conclusões extraídas em laudo pericial, especialmente quando analisadas conjuntamente com outras provas (STF, Ação Penal n.º 1.030/DF, 2ª Turma, Rel. Min. Edson Fachin, julgado em 22 de outubro de 2019, DJe 13/02/2020).

[702] STJ, HC n.º 462.087/SP, 5ª Turma, Rel. Min. Ribeiro Dantas, julgado em 17 de outubro de 2019, DJe 29/10/2019.

[703] STJ, HC n.º 574.103/MG, 6ª Turma, Rel. Min. Nefi Cordeiro, julgado em 4 de agosto de 2020, DJe 14/08/2020.

[704] STJ, RHC n.º 59.414/SP, 5ª Turma, Rel. Min. Reynaldo Soares da Fonseca, julgado em 27 de junho de 2017, DJe 03/08/2018.

[705] BADARÓ, Gustavo Henrique Righi Ivahy. *A cadeia de custódia e sua relevância para a prova penal* Op. cit. p. 535.

[706] STJ, *Habeas Corpus* n.º 160.662/RJ, 6ª Turma, Rel. Min. Assusete Magalhães, julgado em 18 de fevereiro de 2014, DJe 17/03/2014.

Entretanto, a decisão vem sendo objeto de críticas[707], cabendo o registro de que o Superior Tribunal de Justiça não mencionou, ao menos expressamente, que a ilicitude teria decorrido de uma quebra ou violação da cadeia de custódia, razão pela qual não seria correto assentar que os resultados das interceptações telefônicas foram considerados ilícitos por violação da cadeia de custódia[708].

Em outra decisão sobre tema, a mesma Corte invocou o princípio do prejuízo para afastar a nulidade sustentada pela defesa, em razão de erro em gravações de mídias decorrentes de interceptação telefônica. Na ocasião, reconheceu-se que não estaria caracterizada a violação à cadeia de custódia, uma vez que o material que não pôde ser captado ou gravado deixou de ser usado por quaisquer das partes, não sendo possível se falar em prejuízo ou nulidade[709].

No julgamento da Ação Penal 684/DF[710], o Superior Tribunal de Justiça aparentemente deslocou a análise da violação à cadeia de custódia para a perspectiva

---

[707] Dallagnol e Câmara afirmam que a perda de parte dos diálogos seria lesiva à "prova" da acusação e à sua força, o que deveria ser avaliado no campo da valoração da prova, e não de sua licitude ou ilicitude. Ademais, apontam que a nulidade não deveria ser declarada por ausência de prejuízo, devendo ser demonstrada a repercussão do defeito do ato processual no exercício do contraditório ou da ampla defesa. Assim, haveria a possibilidade da utilização do material que não fora perdido, aduzindo que a perda de parte dos diálogos colocou a defesa, e não a acusação, em posição vantajosa. Finalmente, os autores reconhecem que, se fosse uma questão de validade e não de peso, e ainda que houvesse efetivo prejuízo, a nulidade das provas desaparecidas não contaminaria as provas existentes (DALLAGNOL, Deltan Martinazzo; CÂMARA, Juliana de Azevedo Santa Rosa. *A cadeia de custódia da prova.* Op. cit. p. 554-560).

[708] BADARÓ, Gustavo Henrique Righi Ivahy. *A cadeia de custódia e sua relevância para a prova penal* Op. cit. p. 532.

[709] STJ, HC n.º 422.642/SP, 5ª Turma, Rel. Min. Reynaldo Soares da Fonseca, julgado em 25 de setembro de 2018, DJe 02/10/2019. Por sua vez, no REsp n.º 1.795.341/RS, o STJ invocou expressamente a "quebra da cadeia de custódia" para sustentar a nulidade da prova diante da falta de acesso à defesa da integralidade da interceptação telefônica, já que a a apresentação de parcela do produto extraído dos áudios, cuja filtragem foi estabelecida sem a presença do defensor, acarreta ofensa ao princípio da paridade de armas e ao direito à prova (STJ, REsp n.º 1.795.341/RS, 6ª Turma, Rel. Min. Nefi Cordeiro, julgado em 7 de maio de 2019, DJe 14/05/2019).

[710] Na referida ação penal, imputou-se ao réu a prática dos crimes de injúria, difamação e calúnia, os quais teriam sido cometidos por intermédio de e-mails enviados à suposta vítima. Com a localização e apreensão do computador por intermédio do qual as mensagens eletrônicas foram enviadas, realizou-se a perícia do disco rígido e, na oportunidade, apurou-se que a máquina estaria infectada com um vírus conhecido por "cavalo de Tróia". Os peritos, no curso da atividade técnica, promoveram a exclusão do arquivo infectado. A defesa sustentou, por sua vez, que o vírus teria permitido o acesso remoto ao computador por pessoa desconhecida, o que teria ocasionado o envio dos e-mails. Entretanto, a análise da tese aventada pela defesa não foi passível de comprovação, diante da impossibilidade de reexame dos arquivos deletados, o que acarretou a absolvição do réu por insuficiência de provas para a condenação. Assim, a Corte decidiu que "a regra básica da perícia criminal é a de que seu objeto seja preservado. Espécie em que os peritos flagrando no computador apreendido um 'vírus' conhecido como 'cavalo de tróia', excluíram-no do material a ser periciado, gerando incerteza acerca de sua potencialidade para invadir o equipamento e transmitir mensagens à revelia do usuário" (STJ, Ação Penal n.º 684/DF, Corte Especial, Rel. Min. Ari Pargendler, julgado em 3 de abril de 2013, DJE 09/04/2013).

valorativa. De igual sorte, na hipótese de interceptação telefônica por intermédio do *WhatsApp Web*[711], as dúvidas acerca da confiabilidade e integridade da prova foram utilizados como fundamentos para se reconhecer a nulidade da decisão judicial que autorizou o espelhamento do *WhatsApp* via "Código QR", especialmente diante da possibilidade de alteração ou exclusão de dados, sem a possibilidade de recuperação para efeitos de prova no processo penal.

Já na perspectiva do Supremo Tribunal Federal (STF), a Corte manteve decisão do Tribunal de Justiça do Paraná que reconheceu não ser razoável ou proporcional que a quebra da cadeia de custódia acarretasse a anulação e desentranhamento da totalidade do material coletado através das interceptações telefônicas, limitando-se à anulação, afastamento e desentranhamento do material probatório coletado contemporaneamente àquele subtraídos dos autos[712].

[711] STJ, RHC n.º 99.735/SC, 6ª Turma, Rel. Min. Laurita Vaz, j. 27/11/2018, DJe 12/12/2018. Sobre o tema, vide subtópico 4.2.3.1.
[712] STF, Agravo Regimental no *Habeas Corpus* n.º 156.157/PR, 1ª Turma, Rel. Min. Alexandre de Moraes, julgamento em 19 de novemnro de 2018, DJe 26/11/2018.

CONCLUSÃO

Ao final do presente trabalho científico e considerando os estudos realizados acerca da proteção constitucional ao sigilo e o acesso a dados armazenados em aparelhos celulares, é possível se levar aos seguintes entendimentos, ainda que de maneira provisória:

1) A privacidade, concebida originariamente dentro de uma perspectiva meramente individualista, foi consagrada como cláusula pétrea no artigo 5º, inciso X, da Constituição Federal, além de ser resguardada por intermédio de outras proteções constitucionalmente asseguradas, notadamente a da inviolabilidade de domicílio (artigo 5º, inciso XI) e ao sigilo da correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas (artigo 5º, inciso XII).

2) Embora seja uma expressão dotada de plúrimas significações, a privacidade pode ser compreendida como o gênero que integra a "intimidade" e a "vida privada", sendo reconhecida como direito fundamental autônomo inerente à própria personalidade, evoluindo-se como marco para a tutela de dados pessoais (Lei n.º 13.709/2018).

3) A privacidade foi ressignificada a partir da maximização das relações intersubjetivas propiciadas a partir do exponencial avanço tecnológico, especialmente com o advento das redes sociais, aliada ao crescente enfraquecimento de sua proteção, em prol de uma tutela da segurança nacional direcionada à produção preventiva e antecipada de informações.

4) O crescimento da tecnologia e a possibilidade de criação de instrumentos de produção, captação e compartilhamento massificado de dados digitais também foi utilizado pela moderna criminalidade, que se valeu destas facilidades para a perpetração de novas e antigas condutas criminosas, especialmente diante de uma sensação de anonimização dos dados cibernéticos.

5) A evolução tecnológica também exigiu a adoção de novas ferramentas de investigação criminal e de meios de produção de provas, que passaram a se

ater à realidade do entorno digital e aos delitos informáticos, mormente considerando que mecanismos de criptografia fizeram com que meios tradicionais de obtenção de prova se tornassem obsoletos.

6) Dentre os recursos que receberam substanciosa achega tecnológica estão os *smartphones*, modernos aparelhos celulares que deixaram de servir apenas como instrumento de comunicação, ganhando natureza multifuncional, com diversificada gama de funcionalidades a serviço do usuário, permitindo o armazenamento massivo de dados relacionados à personalidade de seus titulares e de terceiros que com ele tenham interagido.

7) Embora a crescente projeção tecnológica tenha alterado permanentemente a forma como são interpretadas as relações sociais, muito pouco se evoluiu, legislativa e doutrinariamente, para se fazer frente a esta realidade, o que recomendou um delicado exercício interpretativo na tentativa de se estabelecer parâmetros legais, formais e procedimentais para a obtenção de provas a partir destes modernos recursos tecnológicos, na busca de um ponto de equilíbrio entre a necessidade de uma investigação eficiente e a proteção à privacidade e ao sigilo de dados, enquanto direitos fundamentais da pessoa humana.

8) Os dados armazenados em aparelhos celulares, por conterem representação de fatos ou ideias, são consideradas provas digitais dotadas de características como a imaterialidade, a volatilidade, a fragilidade, a intrusividade, a suscetibilidade de clonagem e a necessidade de intermediação de equipamento para seu acesso.

9) A prova digital é passível de ser produzida sob a forma documental e pericial, mas exigem novas formas, métodos e ferramentas que permitam assegurar a credibilidade e confiabilidade destas provas.

10) A utilização de meios atípicos de produção de provas exige, concomitantemente, a inexistência de afronta a direitos fundamentais e a regras proibitivas de prova, devendo se respeitar o direito de defesa, os valores da dignidade da pessoa humana, além de serem idôneos à produção de um resultado útil ao processo. Outrossim, os referidos meios devem ser veiculados de maneira excepcional e suplementar, sempre que, diante da forma em que o delito tenha se aperfeiçoado ou em razão de suas peculiares características,

a veiculação de outros meios típicos seja inaplicável ou comprovadamente insuficiente para os propósitos técnico-investigativos almejados.

11) O acesso a dados armazenados em aparelhos celulares, enquanto meio de produção de provas sem regulamentação legislativa específica, faz uso da analogia a outros meios de produção de provas (*v.g.*, a busca e apreensão, a interceptação telemática, a requisição a dados em poder de prestadores de serviços de aplicações de *internet*, dentre outros), permitindo-se a formação de uma base regulamentar e legal para sua operacionalização.

12) Uma das formas pelas quais se admite o regular acesso à base de dados consolidada em um aparelho celular é cessão voluntária dos dados, mediante consentimento e colaboração livre e desimpedida de seu titular, o que dispensa a prévia autorização judicial.

13) O consentimento, para que seja válido e eficaz, exigirá que a outorga seja conferida por pessoa dotada de capacidade ativa, notadamente os maiores de 18 (dezoito) anos de idade e no exercício regular de seus direitos e faculdades mentais, além da manifestação do consentimento de forma livre e consciente, com plena liberdade de escolha. Saliente-se que o simples fato de o acusado estar preso ou desassistido de advogado no momento da manifestação de vontade não configuram, necessariamente, óbice ao consentimento livre e desimpedido para o acesso aos dados.

14) Ainda, a validade do consentimento exigirá que o outorgante detenha um mínimo de conhecimento das consequências de seu ato, inclusive sobre a não obrigação de conceder o acesso voluntário a seu conteúdo. Ainda, embora o consentimento deva ser expresso, não há forma preestabelecida para seu exercício, o que poderá ser manifestado por escrito ou qualquer outro meio demonstrativo da manifestação de vontade do titular.

15) Finalmente, o consentimento poderá ser concedido de forma parcial, limitado a determinados dados a serem buscados, não podendo ser interpretado como renúncia genérica à proteção constitucional conferida à privacidade e intimidade.

16) Para além do consentimento prestado pelo próprio titular, é possível que terceiros venham a ceder os dados comunicados e compartilhados, em gravação unilateral de seu conteúdo, além da entrega de dados pelo proprietário do aparelho celular, especialmente quanto ao conteúdo profissional e não pessoal produzido e armazenado pelo usuário do suporte eletrônico.

17) Durante as atividades investigativas encetadas, poderá ser imprescindível a busca ao conteúdo do aparelho celular do acusado independentemente da anuência do seu titular, o que exigirá, no mais das vezes, prévia autorização judicial para veiculação da medida invasiva.

18) Dentre estas hipóteses, destaca-se a possibilidade de acesso remoto ao conteúdo do aparelho, o que dispensa a apreensão física do próprio suporte eletrônico.

19) O acesso remoto aos dados poderá se dar mediante aquisição de dados por servidores remotos e apreensão de arquivos eletrônicos em "*cloud computing*"; por intermédio da requisição de dados em poder de provedores ou de serviços de *internet,* com base na Lei do Marco Civil da *Internet* (Lei n.º 12.965/2014); mediante infiltração clandestina, através da utilização de *malwares* para se permitir a interceptação, busca, monitoramento e apreensão dos dados, inclusive em tempo real, além da geolocalização dos dispositivos; finalmente, através de ações encobertas em meio digital, prevista no ordenamento jurídico brasileiro sob a forma de infiltração de agentes de polícia para investigação de determinados crimes.

20) Considerando os meios de acesso remoto acima nominados, conclui-se que a utilização de *malwares,* conjunto de *softwares* maliciosos que são instalados discreta e clandestinamente, sem o consentimento do usuário, para a captação, interceptação e acesso a dados armazenados em aparelhos celulares, não possui regulamentação legal e sua veiculação constitui afronta a direitos e garantias fundamentais, especialmente por se franquear o acesso facilitado a chaves de criptografia que guarnecem os dados, para além de permitir a inclusão, modificação ou supressão de arquivos, o que comprometeria a integridade da prova produzida.

21) A despeito da possibilidade do acesso remoto, a forma mais comum de busca ao conteúdo do suporte eletrônico ainda se dá mediante apreensão física do aparelho celular.

22) A apreensão física do aparelho celular poderá se dar mediante busca previamente determinada judicialmente, que deverá obedecer aos requisitos legais previstos no artigo 240 e seguintes do Código de Processo Penal, cabendo ao juiz realizar um juízo de ponderação, à luz da proporcionalidade, a partir do conflito de interesses subjacentes.

23) A concessão da ordem judicial prescinde de uma nova autorização específica para o acesso aos dados que ali estão armazenados, já que o aparelho celular, individualmente considerado, constitui mero objeto físico que desperta pouca relevância probatória, já que o interesse da apreensão decorre da necessidade de se acessar os dados que ali estejam armazenados.

24) O mandado de busca e apreensão deverá descrever os suportes eletrônicos que deverão ser apreendidos, bem como, na medida do possível, os dados que interessariam à investigação, a forma de apreensão e extração de seu conteúdo, a fim de se evitar o acesso indiscriminado a dados que não guardem relação com o propósito investigativo que motivou a busca e apreensão.

25) A apreensão do aparelho celular também poderá ocorrer sem a prévia decisão judicial concessiva da medida, especialmente nas hipóteses de uma prisão em flagrante delito ou durante o exercício de atividades investigativas policiais, na forma do artigo 6º, incisos II e III, do Código de Processo Penal.

26) A despeito dos recentes posicionamentos doutrinários, não se verifica a existência de cláusula constitucional de reserva de jurisdição que resguardem o acesso aos dados armazenados em aparelhos celulares, os quais estão sujeitos à proteção conferida no artigo 5º, inciso X, da Constituição Federal. Com efeito, não nos parece possível a "espiritualização do domicílio", para se estender a tutela conferida à inviolabilidade de domicílio (artigo 5º, inciso XI, da CF), nem tampouco a proteção referente ao sigilo das comunicações (artigo 5º, inciso XII, da CF), uma vez que a disciplina visa resguardar o fluxo de dados, e não aqueles estanques e já comunicados.

27) Também não há, de maneira clara e específica, uma cláusula legal de reserva de jurisdição para o acesso aos dados armazenados em aparelhos celulares, uma vez que a disciplina prevista no artigo 7º, inciso III e artigo 10, § 2º, da Lei n.º 12.965/2014, bem como do artigo 3º, inciso V, da Lei n.º 9.472/1997, são direcionados aos prestadores dos serviços públicos ou privados de especial interesse público, que possuem a guarda legal dos dados.

28) Embora não haja cláusula constitucional ou legal de reserva de jurisdição, conclui-se pela imprescindibilidade de autorização judicial para seu acesso, mormente por se tratar de um meio de produção de provas que não possui regulamentação legal, além de ser potencialmente compressor de direitos e garantias fundamentais. Não bastasse, a vastidão de dados estáticos armazenados tem grande aptidão para expor a intimidade e privacidade do seu titular, fazendo-o de maneira mais significativa do que outros meios de obtenção de prova que, por sua vez, exigem requisitos qualificados para sua concessão, além de ordem judicial específica (*v.g.*, a interceptação telefônica, disciplinada pela Lei n.º 9.296/1996).

29) A autorização judicial concessiva do acesso deverá obedecer a um juízo de proporcionalidade, que deverá observar a existência de indícios de autoria ou participação; a adequação da medida para a prova pretendida, especialmente diante da natureza do crime investigado, que deve ser punido com reclusão; a necessidade da prova para a apuração dos fatos e a formação do arcabouço probatório; e a proporcionalidade com relação ao período de abrangência dos dados a serem coletados e fornecidos.

30) A apreensão e o acesso ao aparelho celular, durante busca pessoal realizada em abordagens policiais, comportam distinção quanto ao momento fático: a da busca sem prévia situação flagrancial e quando nenhum fato criminoso é caracterizado; e durante a busca realizada de maneira incidental à prisão em flagrante, previamente identificada.

31) Nas hipóteses em que a busca é realizada sem prévia constatação de situação flagrancial e nenhum fato criminoso é constatado, a apreensão do aparelho celular e o acesso ao seu conteúdo, sem o consentimento de seu titular, constitui medida arbitrária e potencialmente caracterizadora de *fishing expedition*, com caráter

randômico e especulativo, destinado à captura prospectiva de elementos incriminatórios aleatórios.

32) Por sua vez, nas hipóteses em que a busca é realizada de maneira incidental a uma hipótese previamente caracterizada de flagrante delito, tem-se por legítima a apreensão do aparelho, sempre que guardar possível relação com os fatos motivadores da prisão em flagrante. Entretanto, o acesso aos dados deverá exigir, em regra, autorização judicial prévia, especialmente considerando que a situação flagrancial não permite, de *per si*, a realização de buscas desmedidas no conteúdo do aparelho, uma vez que a potencial exposição à intimidade e à privacidade do acusado poderão se revelar desproporcionais às próprias circunstâncias da prisão.

33) Excepcionalmente, admite-se a possibilidade do acesso direto, por policiais, em situações de urgência ou emergência plenamente justificadas, bem como nos casos em que a materialidade delitiva estiver incorporada no aparelho celular, à exemplo dos crimes previstos no artigo 241-A e 241-B da Lei n.º 8.069/1990. Ainda, tem-se por legítima a consulta policial ao IMEI (*International Mobile Equipment Identity*) do aparelho, sempre que houver fundadas razões para se acreditar que o objeto possa ser produto de um crime anterior, bem como o acesso direto aos dados quando o aparelho é encontrado em situação de abandono, sendo a medida necessária para identificação do seu proprietário.

34) O acesso ilegal aos dados armazenados em aparelhos celulares poderá acarretar a ilicitude da prova, salvo nos casos de exceção à inadmissibilidade da prova ilícita, tais como a da fonte independente e descoberta inevitável, já reconhecidas em âmbito jurisprudencial.

35) A realização de um estudo comparado a partir de precedentes da Argentina, Estados Unidos, Canadá, México, Inglaterra e Espanha revelam como o tema vem sendo tratado por outros países e contribuem para a formação de um modelo normativo processual para regulamentação do tema.

36) A cadeia de custódia da prova, enquanto metodologia para se atestar a integridade e confiabilidade da prova, foi incluída expressamente nos artigos 158-A a 158-F do Código de Processo Penal. Com relação à prova digital, a cadeia de custódia

da prova assume especial relevância, visando assegurar sua autenticidade, completude, confiabilidade e credibilidade.

37) As etapas da cadeia de custódia para obtenção dos dados armazenados em aparelhos celulares deverão observar as diretrizes legais, atentando-se para algumas especificidades relacionadas ao isolamento do suporte eletrônico, a extração dos dados do aparelho e a necessidade de as partes especificarem ao perito qual o objeto da investigação e o conteúdo a ser analisado, considerando a vastidão de dados passíveis de extração.

38) Em caso de descumprimento da cadeia de custódia, em que pesem as divergências doutrinárias e jurisprudenciais, entende-se que a repercussão deverá se dar no campo da valoração da prova, mormente em hipóteses de omissões ou irregularidades sem maiores gravidades.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Jacqueline de Souza. *Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação*. Rev. Bras. Polít. Públicas, Brasília, v. 7, nº 3, 2017.

ABREU, Jacqueline de Souza; ANTONIALLI, Dennys M.. *E quando o policial vira hacker?*. Disponível em: <https://www.internetlab.org.br/pt/privacidade-e-vigilancia/e-quando-o-policial-vira-hacker/:. Acesso em: 20 de dezembro de 2020.

_____. *O conto do baú do tesouro: a expansão da vigilância pela evolução e popularização dos celulares no Brasil*. Surveillance in Latin America, v. 5, p. 353, 2017.

_____. *Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais.* São Paulo: InternetLab, 2017.

_____; MASSARO, Heloisa Maria Machado. LUCIANO, Maria. *Acesso de autoridades policiais a celulares em abordagens e flagrantes: retrato e análise da jurisprudência de tribunais estaduais.* In: Revista Brasileira de Ciências Criminais, vol. 154/2019, p. 177-214, abril/2019.

ACILA, Carlos Roberto. *Criminologia e estigmas – um estudo sobre os preconceitos*. 4. ed. São Paulo: Atlas, 2015. p. 23, *Apud*, NETO, Francisco Alves Cangerana. Meios de Obtenção de Prova no Processo Penal, Paraná: Editora Juruá, 2018.

ALBRECHT, Hans-Joerg. *Secret Surveillance. Measures of Secret Investigation in the Criminal Process.* Revista Brasileira de Ciências Criminais, 92, p. 123-153.

ALEXY, Robert. *Teoria dos direitos fundamentais.* 2ª edição, São Paulo: Editora Malheiros, 2015.

ALMEIDA, José Raul Gavião de. *Anotações acerca do direito à privacidade*. In: Jorge Miranda; Marco Antônio Marques da Silva. (Org.). Visão Luso-Brasileira da Dignidade Humana. 1ª edição, São Paulo: Editora Quartier Latin, 2008, v. 1.

AMARAL, Cláudio do Prado. *Inviolabilidade do domicílio e flagrante de crime permanente.* Revista Brasileira de Ciências Criminais, vol. 95, p. 165, São Paulo: Ed. RT, mar. 2012, *Apud* DEZEM, Guilherme Madeira. A espiritualização do domicílio. In: MASSO, Fabiano Del. ABRUSIO, Juliana, FILHO, Marco Aurélio Florêncio (org.). Marco Civil da Internet – Lei n.º 12.965/2014. São Paulo: Editora Revista dos Tribunais, 2014, 2ª tiragem.

ANDRADE, Manoel da Costa. *Métodos ocultos de investigações (plädoyer para uma teoria geral).* In: MONTE, Mário Ferreira et ali (org.). Que futuro para o direito processual penal? Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do código de processo penal português. Coimbra: Editora Coimbra, 2009.

_____. *Sobre as Proibições de Prova em Processo Penal*, Coimbra: Editora Coimbra, 2006.

ANTONIALLI, Dennys Marcelo; BRITO CRUZ, Francisco; VALENTE, Mariana Giorgetti. *Smartphones: treasure chests of the Lava-Jato investigation*. Disponível em: <https://www.internetlab.org.br/en/policy-watch/smartphones-treasure-chests-of-the-lava-jato-investigation/>. Acesso em: 20 de dezembro de 2020.

ANTUNES, Leonardo Leal Peret. *(Re)pensando a busca e apreensão no processo penal*. Rio de Janeiro: Editora Lumen Juris, 2016.

ARANHA, Adalberto José Q. T. de Camargo: *Da prova no processo penal.* 7ª ed., São Paulo: Editora Saraiva, 2006.

ARANTES FILHO, Márcio Geraldo Britto. *A interceptação de comunicação entre pessoas presentes como meio de investigação de prova no processo penal brasileiro.* Dissertação (Mestrado em Direito Processual Penal) - Faculdade de Direito da Universidade de São Paulo, 2011.

ARAÚJO, Márcio Schusterschitz da Silva. *O lixo como fonte de prova no processo penal.* In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro de (Org.). In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro de (Org.). A prova no enfrentamento à macrocriminalidade. Salvador: Editora JusPodivm, 2019.

ARAÚJO, Luiz Alberto David; NUNES JÚNIOR, Vidal Serrano. *Curso de Direito Constitucional*. 10ª edição. São Paulo: Editora Saraiva, 2006.

AVOLIO, Luiz Francisco Torquato. *Provas Ilícitas Interceptações telefônicas e gravações clandestinas*, 7ª ed., São Paulo: Editora Revista dos Tribunais, 2019.

_____; REBELLATO, Luiz Fernando Bugiga. *Provas ilícitas*. In: Contraponto jurídico. Posicionamentos divergentes sobre grandes temas do Direito. São Paulo: Editora RT, 2018.

AZEVEDO, David Teixeira de. *Delação premiada e direito de defesa*. Boletim IBCCRIM, São Paulo, IBCCRIM, v. 22, n. 265, p. 4, 2014.

_____. *O interrogatório do réu e o direito ao silêncio.* Revista dos Tribunais, São Paulo, v. 682, ago. 1992.

AZEVEDO, Yuri; VASCONCELOS, Caroline Regina Oliveira. *Ensaios sobre a cadeia de custódia das provas no processo penal brasileiro.* Florianópolis: Editora Empório do Direito, 2017.

AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. *Guideline on Mobile Device Forensics*, In: National Institute of Standards and Technology of U. S. Department of Commerce, May 2014 (Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf> Acesso em: 20 de dezembro de 2020.

BACHMAIER WINTER, Lorena. *Investigación criminal y protección de la privacidad en la doctrina del Tribunal Europeo de Derechos Humanos*. In: 2º Congresso de Investigação

Criminal. Coordenação: Maria Fernanda Palma, Augusto Silva Dias e Paulo de Sousa Mendes. Lisboa: Almedina, 2010.

BADARÓ, Gustavo Henrique Righi Ivahy. *A cadeia de custódia e sua relevância para a prova penal.* In. SIDI, Ricardo, LOPES, Anderson Bezerra (org.) Temas atuais da investigação preliminar no processo penal. Belo Horizonte: Editora D' Plácido, 2017.

_____. *Direito à prova e os limites lógicos de sua admissão: os conceitos de pertinência e relevância*. In: *Sistema penal e poder punitivo: estudos em homenagem ao prof. Aury Lopes Jr.*, p. 550; 2015; e BADARÓ, Gustavo Henrique Righi Ivahy. *Editorial dossiê "Prova penal: fundamentos epistemológicos e jurídicos"*. In: Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 4, n. 1, p. 43-80, jan.-abr. 2018.

_____. *Direito Processual Penal. Tomo I.* Rio de Janeiro: Editora Elsevier, 2008.

_____. *Interceptação de Comunicações Telefônicas e Telemáticas: limites ante o Avanço da Tecnologia*. In CASARA, Rubens Roberto R.; Lima, Joel Correa de (Org.). Temas para uma Perspectiva Crítica do Direito - Homenagem ao Professor Geraldo Prado. Rio de Janeiro: Editora Lumen Juris, 2010.

_____. *Processo Penal*, 8ª edição, São Paulo: Editora RT, 2020.

_____. *Provas atípicas e provas anômalas: inadmissibilidade da substituição da prova testemunhal pela juntada de declarações escritas de quem poderia ser testemunha.* In: Yarshell, Flávio Luiz; Moraes, Maurício Zanoide (coord.). Estudos em homenagem à professora Ada Pellegrini Grinover. São Paulo: DPJ, 2005.

_____. *Quem está preso pode delatar?* Jota, 23 jun. 2015. Disponível em: <http://jota.uol.com.br/quem-esta-preso-pode-delatar>. Acesso em: 20 de dezembro de 2020.

BADARÓ, Jennifer Falk. *Produção de provas: WhatsApp, Facebook, e-mail.* AASP Boletim, Edição n. º 3096, Dezembro/2019.

BARNES, Susan, *A privacy paradox: Social networking in the United States*, First Monday, volume 11, number 9, September 2006. Disponível em: <http://firstmonday.org/issues/issue11_9/barnes/index.html>. Acesso em: 3 de julho de 2020.

BARRETO, Alesandro Gonçalves; ALMEIDA, Everton Ferreira de. *Perícia em celular: necessidade de autorização judicial?* Revista Direito & TI, Porto Alegre, 04.06.2016. Disponível em: http://direitoeti.com.br/artigos/pericia-em-celular-necessidade-de-autorizacao-judicial. Acesso em: 20 de dezembro de 2020.

BARROSO, Luís Roberto. *Interpretação e aplicação da Constituição: fundamentos de uma dogmática constitucional transformadora*, 4ª Edição, São Paulo: Editora Saraiva, 2001.

_____. *Temas de direito constitucional – tomo III*. Rio de Janeiro: Editora Renovar, 2005.

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. *Comentários à Constituição do Brasil*. São Paulo: Editora Saraiva, v. 2, 1989.

_____. *Comentários à Constituição do Brasil: promulgada em 5 de outubro de 1988.* São Paulo: Editora Saraiva, 1988.

BAUMAN, Zygmunt. *Danos colaterais. Desigualdades sociais numa era global*. Tradução: Carlos Alberto Medeiros, Rio de Janeiro: Editora Zahar, 2013.

_____. *Modernidade Líquida*. Tradução: Plínio Dentzien, Rio de Janeiro: Editora Zahar, 2000.

BECHARA, Fábio Ramazzini. *Evidências Digitais e Confiabilidade do Conteúdo*. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/evidencias-digitais-e-a-confiabilidade-do-conteudo-16072019>. Acesso em: 20 de dezembro de 2020.

BELLOQUE, Juliana Garcia. *Sigilo Bancário: Análise Crítica da LC 102/2001*. São Paulo, Ed. Revista dos Tribunais: 2003.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento.* 2ª edição. Rio de Janeiro: Editora Forense, 2019.

BONFIM, Edilson Mougenot. *Curso de Processo Penal*. São Paulo: Editora Saraiva, 2012.

BORGES DA ROSA, Inocêncio. *Processo penal brasileiro*, Porto Alegre: Editora Globo, 1942.

BORRI, Luiz Antônio. *Delação premiada do investigado/acusado preso cautelarmente: quando o Estado se transfigura em criminoso para extorquir a prova do investigado*. Boletim IBCCRIM, São Paulo, v. 24, n. 285, p. 6-8, ago. 2016.

BOTTINI, Pierpaolo Cruz. *Buscas policiais sem mandado judicial parecem ter se normatizado.* Conjur, 11 de novembro de 2014. Disponível em <https://www.conjur.com.br/2014-nov-11/direito-defesa-buscas-policiais-mandado-parecem-normatizado#_edn7>. Acesso em: 20 de dezembro de 2020.

BOYD, Dana; HARGITTAI, Eszter. *Facebook privacy settings: Who cares?*. 2010, First Monday,15(8)<http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589>. Acesso em 3 de julho de 2020.

BULOS, Uadi Lammêgo. *Constituição Federal Anotada*. São Paulo: Editora Saraiva, 2012.

CALDEIRA, Rodrigo de Andrade Figaro. *Cadeia de Custódia: arts. 158-A a 158-F, do CPP*. In: AKERMAN, William; DUTRA, Bruna Martins Amorim (Org.) Pacote Anticrime. Análise crítica à luz da Constituição Federal. São Paulo: Editora RT, 2020.

CAMARGO, Coriolano Almeida; SANTOS, Cleórbete. *Crimes digitais no ordenamento brasileiro.* Revista de Direito e as Novas Tecnologias, vol. 2/2019, Jan-Mar/2019.

CARMEN, Rolando V. Del. *Criminal procedure Law and Practice*, Wadsworth Publishing; 8 edition, p. 86-88.

CAPEZ, Fernando. *Curso de Processo Penal*. 13ª edição, São Paulo: Editora Saraiva, 2006.

CAPEZ, Rodrigo. *Pressupostos de admissibilidade e requisitos de validade da colaboração premiada: critérios para orientar a proposta e o controle da justiça criminal negocial*. In: *Colaboração Premiada*. Org. Maria Thereza de Assis Moura e Pierpaolo Cruz Bottini, São Paulo: Editora Revista dos Tribunais.

CAPRIOLI, Francesco. *Il 'captatore informatico' come strumento di ricerca della prova in Italia.* Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 3, n. 2, p. 483-510, mai.-ago. 2017.

CARDOZO, José Eduardo Martins. *Prefácio*. In: LEITE. George Salomão; LEMOS, Ronaldo. (Coord.). Marco Civil da Internet. São Paulo: Editora Atlas.

CARVALHO, Manuel da Cunha. *O conceito de servidor em informática e suas implicações jurídicas.* In: Revista de Direito do Consumidor n.º 39/158 – São Paulo: Editora RT.

CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers and the internet.* 3rd Edition, Maryland: Ed. Elsevier, 2011.

_____; TURNBULL, Benjamin. *Digital Evidence on Mobile Devices*. In: Digital Evidence and Computer Crime, 3 Ed. Elsevier, 2011.

CASTELLS, Manuel. *A sociedade em rede: a era da informação: economia, sociedade e cultura*. Tradução Roneide Venancio Majer. 21. edição, São Paulo: Editora Paz e Terra, 2020.

CASTILHOS, Guilherme Machado; POLL, Roberta Eggert. *"E se a sua geladeira pudesse depor contra você no tribunal?": internet das coisas e provas no processo penal brasileiro".* Revista Brasileira de Ciências Criminais, vol. 163/2020, p. 363-391, Jan/2020.

CASTRO, Pedro Machado de Almeida. *Operação Lava Jato e gravações clandestinas.* In. SIDI, Ricardo, LOPES, Anderson Bezerra (org.) Temas atuais da investigação preliminar no processo penal. Belo Horizonte, Editora D' Plácido, 2017.

CASTRO, Luiz Augusto Sartori de. *Busca e apreensão mediante uso de 'malware'.* In: Boletim do Instituto Brasileiro de Ciências Criminais, São Paulo, ano 21, n.º 251, outubro de 2013.

CESCA, Brenno Gimenes; GUARDIA, Gregório Edoardo Raphael Selingardi. *Busca e apreensão: o regime jurídico de Argentina, Inglaterra e Itália.* Revista Liberdades, Edição n.º 24, julho/dezembro de 2017.

CINTRA, Antônio Carlos de Araújo; GRINOVER, Ada Pellegrini; DINAMARCO, Candido Rangel. *Teoria Geral do Processo*. São Paulo: Editora Malheiros, 2001.

COOLEY, Thomas McIntyre. *A treatise on the law of torts*. Chicago: Callaghan, 1880.

CÓRDOBA, Gabriela E. *Nemo tenetur se ipsum accusare: ¿principio de pasividad?* Estudios sobre Justicia Penal: Homenaje al Profesor Julio B. J. Maier, Buenos Aires: Editores del Puerto, 2005.

COSIC, Jasmin; COSIC, Zoran. *Chain of Custody and Life Cycle of Digital Evidence.* Computer Technology and Application 3 (2012).

COSTA, Diogo Erthal Alves da Costa. *Nemo tenetur se detegere e dados criptografados: restabelecendo o equilíbrio.* In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro de (Org.). A prova no enfrentamento à macrocriminalidade. Salvador: Editora JusPodivm, 2019.

COSTA, Helena Regina Lobo da; LEONARDI, Marcel. *Busca e apreensão e acesso remoto a dados em servidores.* In: Revista Brasileira de Ciências Criminais, São Paulo, v. 19, n. 88, p. 203-223, jan.fev/2011.

COSTA, Leonardo Dantas. *Delação Premiada*, Paraná: Editora Juruá, 2017.

COSTA ANDRADE, Manoel. *Sobre as Proibições de Prova em Processo Penal*, Coimbra: Editora Coimbra, 1992.

COSTA JÚNIOR, Paulo José da. *O direito de estar só: tutela penal da intimidade*. 2ª edição, São Paulo, RT, 1995.

COUTINHO, Gustavo Leuzinger. *A Era dos 'Smartphones: Um estudo exploratório sobre o uso dos 'smartphones' no Brasil.* Monografia. Universidade de Brasília (UNB), dezembro de 2014.

CUNHA, Rogério Sanches; PINTO, Ronaldo Batista. *Código de Processo Penal e Lei de Execução Penal Comentados.* 2ª ed. São Paulo: Editora Juspodivm, 2018.

CUNHA JÚNIOR, Dirley da. *Curso de Direito Constitucional.* 5ª edição, Salvador: Editora Juspodivm, 2011.

DALLAGNOL, Deltan Martinazzo; CÂMARA, Juliana de Azevedo Santa Rosa. *A cadeia de custódia da prova.* In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro de (Org.). A prova no enfrentamento à macrocriminalidade. Salvador: Editora JusPodivm, 2019.

DANIELE, Marcelo. *La prova digitale nel processo penale.* Rivista di Diritto Processuale Anno LXVI (Seconda Serie) – n. 2, Marzo – Aprile, 2011.

DELGADO MARTÍN, Joaquín. *La prueba electrónica em el proceso penal.* Diario La Ley, n.º 8167, Sección Doctrina, 10 Oct. 2013, Año XXXIV, Editorial La Ley.

DELMANTO, Roberto e DELMANTO JÚNIOR, Roberto. *A permissão constitucional e a nova lei de interceptação telefônica*, em Boletim *IBCCrim* n. 47, p. 2.

DEZEM, Guilherme Madeira. *A espiritualização do domicílio.* In: MASSO, Fabiano Del. ABRUSIO, Juliana, FILHO, Marco Aurélio Florêncio (org.). *Marco Civil da Internet – Lei n.º 12.965/2014.* São Paulo: Editora Revista dos Tribunais, 2014, 2ª tiragem.

_____. *Curso de processo penal*. 6ª edição, São Paulo: Editora Revista dos Tribunais, 2020.

_____. *Da prova penal: tipo processual, provas típicas e atípicas (Atualizado de acordo com as Lei 11.689/08, 11.690/08 e 11.719/08).* Campinas: Ed. Millenium, 2008.

DIAS FILHO, Claudemir Rodrigues. *Cadeia de custódia: do local de crime ao trânsito em julgado; do vestígio à evidência*. In: MOURA, Maria Thereza Rocha de Assis; NUCCI, Guilherme de Souza (org.). Doutrinas Essenciais - Processo Penal. v. 3. São Paulo: Editora RT, 2012.

DINAMARCO, Cândido Rangel. *Instituições de Direito Processual Civil.* São Paulo: Editora Malheiros, 2001, vol. III.

DINIZ, Maria Helena. *Código Civil Anotado.* 15ª edição, São Paulo: Editora Saraiva, 2010.

DI PAOLO, Gabriella. *Tecnologie del controllo e prova penale: l'esperienza statunitense e spunti per la comparazione*. Padova: Editora Cedam, 2008.

DOENES, William S. *Search and Seizure: The Physical Trespass Doctrine and the Adaption of the Fourth Amendment to Modern Technology*, 2 Tulsa L. J. 180 (2013), Disponível em: https://digitalcommons.law.utulsa.edu/cgi/viewcontent.cgi?article=1038&context=tlr. Acesso em: 20 de dezembro de 2020.

DOMINGOS, Fernanda Teixeira Souza. *As provas digitais nos delitos de pornografia infantil na Internet*. In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro de (Org.). A prova no enfrentamento à macrocriminalidade. Salvador: Editora JusPodivm, 2019.

_____. RÖDER, Priscila Costa Schreiner. *Obtenção de provas digitais e jurisdição na Internet.* In. *Caderno de Estudos de Investigação e prova nos crimes cibernéticos*, da Escola de Magistrados da Justiça Federal da 3ª Região, São Paulo: 1ª edição, 2017.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* 2ª ed. São Paulo: Editora RT, 2019.

D'URSO, Luiz Flávio Borges. *Delação premiada – Proibição para quem está preso. Migalhas,* 28 de julho de 2015, Disponível em: <https://www.migalhas.com.br/depeso/224179/delacao-premiada-proibicao-para-quem-esta-preso>. Acesso em: 20 de dezembro de 2020.

DUPUY, Daniela. *Desafíos procesales en la investigación de delitos informáticos.* Reunión preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal (AIDP) Grupo argentino, Facultad de Derecho, UBA, marzo de 2014.

EDINGER, Carlos. *Cadeia De Custódia, Rastreabilidade Probatória*. Revista Brasileira de Ciências Criminais, vol. 120, mai.-jun./2016.

EIBE, Manuel José Arias. *Funcionalismo penal moderado o teleológico-valorativo Versus Funcionalismo Normativo o Radical*. Doxa: Cuadernos de Filosofia del Derecho, Alicante, n. 29, p. 439-453, 2006.

ESPINDULA, Alberi, *Perícia criminal e cível: uma visão geral para peritos e usuários da perícia.* 4ª Ed. Campinas: Editora Millenium, 2013.

FAYET, Fábio Agne; CARVALHO, Andersson Vieira. *WhatsApp, sigilo de dados e prova ilícita: para dizer o óbvio.* Revista Brasileira de Ciências Criminais, vol. 140/2018, p. 297-322, fevereiro/2018.

FERNANDES, Antônio Scarance. *A lei de interceptação telefônica.* In: Justiça Penal, n. 4, coord. de Jaques de C. Penteado, São Paulo: Editora RT, 1997.

_____. *Equilíbrio entre a eficiência e o garantismo*. Revista Brasileira de Ciências Criminais n.º 70/229, jan-fev/2008.

_____. *O sigilo financeiro e a prova criminal*. In "*Direito Penal, Processo Penal e Direitos Fundamentais. Uma visão Luso-brasileira*", p.457/477, 2006.

_____. *Processo penal constitucional.* 6ª edição. rev. atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2010.

_____. *Teoria geral do procedimento e o procedimento no processo penal*. São Paulo: Editora RT, 2005.

_____. *Tipicidade e sucedâneos de prova*. In: FERNANDES, Antônio Scarance; GAVIÃO DE ALMEIDA, José Raul; ZANOIDE DE MORAES, Maurício (coord.). *Provas no Processo Penal: estudo comparado*. São Paulo: Editora Saraiva, 2011.

FERRAJOLI, Luigi. *Derecho y razón: Teoría del garantismo penal.* Madrid: Editora Trotta, 2014.

FERRAZ JÚNIOR, Tércio Sampaio. *Comunicação de dados e proteção ao sigilo.* In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas. Lei Geral de Proteção de Dados (Lei n.º 13.709/2018): a caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Editora RT, 2020.

_____. *Sigilo bancário, a Constituição Federal e a Lei Complementar n. 105/2001, de dados: o direito à privacidade e os limites à função fiscalizadora do Estado*. In: Direito Constitucional: liberdade de fumar, privacidade, estado, direitos humanos e outros temas. Sampaio Ferraz Junior, Barueri: Editora Manole, 2007.

_____. *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado*. Revista da Faculdade de Direito, Universidade de São Paulo, São Paulo, v. 88, p. 440, jan. 1993. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67231/69841>.

_____. *Sigilo de dados, o direito à privacidade e os limites do poder do Estado: 25 anos depois.* In: ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (eds.). *Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate*. Vol. I. São Paulo. Internet Lab, 2018.

FERREIRA FILHO, Manoel Gonçalves. *Comentários à Constituição Brasileira de 1988.* São Paulo: Editora Saraiva, 1990, v. 1.

FERRER BELTRÁN, Jordi. *La valoración racional de la prueba*. Madrid: Marcial Pons, 2007

FIGUEIREDO DIAS, Jorge. *Direito processual penal.* Coimbra: Editora Coimbra, 2004.

FILIOL, Eric. *Computer Viruses: from theory to application*. Paris: Springer, 2005, p. 86. *Apud:* VACIAGO, Giuseppe; RAMALHO, David Silva. Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings, Digital Evidence and Electronic Signature, Law Review, 13 (2016).

FISCHER, Douglas; OLIVEIRA, Eugênio Pacelli de. C*omentários ao Código de Processo Penal e sua Jurisprudência*. Rio de Janeiro: Editora Lumen Juris. 2010.

FRANCO, Alberto Silva; LIRA, Rafael; FELIX, Yuri. *Crimes hediondos*. 7ª edição, São Paulo: Editora Revista dos Tribunais, 2011.

FRIEDEN, Jonathan D.; MURRAY, Leigh M. *The Admissibility of Electronic Evidence Under the Federal Rules of Evidence,* XVII Richmond Journal of Law and Technology, Vol. XVII, Issue 2.

GASCÓN ABELLÁN, MARINA, *Los hechos en el Derecho. Bases argumentales de la prueba,* 1ª edic., Madrid: Editora Marcial Pons, 1999.

GARIBALDO, Gustavo E. L. *Las modernas tecnologias de control y de investigación del delito: su incidência em el derecho penal y los princípios constitucionales.* 1ª Ed. Buenos Aires: Editora Ad-Hoc, 2010, p. 103, *apud* MENDES, Carlos Hélder Furtado. Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software. São Paulo: Editora Juspodivm, 2020.

GIOVA, Giuliano. *Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems.* IJCSNS International Journal of Computer Science and Network Security, VOL. 11 No. 1, January 2011, p. 1

GLANCY, Doroth. *The invention of the right to privacy.* Arizona Law Review, v. 21, n. 1, p. 2 (1979).

GLOECKNER, Ricardo Jacobsen. EILBERG, Daniela Dora. *Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos.* In: Revista Brasileira de Ciências Criminais, vol. 156/2019, Jun/2019.

GOLDSCHMIDT, James. *Problemas Jurídicos y Políticos del Proceso Penal*. Barcelona: Editora Bosch, 1935.

GOMES, Marcus Alan de Melo. *Breve crítica ao afastamento dos sigilos financeiro, bancário e fiscal na Lei nº 12.850/2013*. In: AMBOS, Kai; ROMERO, Eneas (Org.). Crime organizado: análise da Lei 12.850/2013. 1ª edição, São Paulo: Editora Marcial Pons, 2017.

GOMES, Luiz Flávio; CERVINI, Raúl. *Crime organizado: enfoques criminológicos, jurídico (Lei 9.034/1995) e político-criminal*. São Paulo: Editora RT, 1995.

GOMES FILHO, Antônio Magalhães. *A Motivação das Decisões Penais*, 1ª edição, São Paulo: Editora Revista dos Tribunais, 2001.

_____. *Da busca e apreensão*. In: GOMES FILHO, Antônio Magalhães; TORON, Alberto Zacharias; e BADARÓ, Gustavo Henrique (coord.). *Código de Processo penal comentado*. São Paulo: Editora Thomson Reuters Brasil, 2018.

_____, *Direito à prova no processo penal*, São Paulo: Editora RT, 1997.

_____. *Notas sobre a terminologia da prova (reflexos no processo penal brasileiro)*. In YARSHELL, Flávio Luiz; MORAES, Maurício Zanoide de (coord.). Estudos em homenagem à professora Ada Pellegrini Grinover. São Paulo: DPJ, 2005.

_____. *Provas. Lei 11.690, de 09.06.2008*. In. ASSIS MOURA, Maria Thereza Rocha de (Coord.). As reformas no processo penal. As novas leis de 2008 e os projetos de reforma. São Paulo: Editora Revista dos Tribunais, 2008.

_____; BADARÓ, Gustavo. *Prova e sucedâneos da prova no processo penal brasileiro*. Revista Brasileira de Ciências Criminais, São Paulo, v. 15, n. 65, p. 175-208, mar./abr., 2007.

GOMES DA SILVA, Paulo Thadeu. *Direitos Fundamentais. Contribuição para uma teoria geral.* São Paulo: Editora Atlas, 2010.

GONÇALVES, Carlos Roberto. *Direito civil brasileiro*, volume 1: parte geral, 10ª edição, São Paulo: Editora Saraiva, 2012.

GONZÁLEZ-CUÉLLAR SERRANO, Nicolás. *Garantías constitucionales de la persecución penal em el entorno digital.* In: GÓMEZ COLOMER, Juan Luis. Prueba y proceso penal (Análisis especial de la prueba prohibida em el sistema español y em el derecho comparado). Valencia: Tirant Le Blanch, 2008.

GOODISON, Sean E., DAVIS, Robert C., JACKSON, Brian A. *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*. Santa Monica, CA: RAND Corporation, 2015, Disponível em <https://www.rand.org/pubs/research_reports/RR890.html>. Acesso em 20 de dezembro de 2020.

GRANDIS, Rodrigo de. *Prisão não invalida a delação premiada.* Jota, 5 de agosto de 2015, Disponível em: <http://jota.uol.com.br/quem-esta-preso-pode-delatar>. Acesso em: 20 de dezembro de 2020.

GRASSI, Roberto Joacir. *Busca e apreensão (Processo Penal).* Enciclopédia Saraiva do Direito. São Paulo: Saraiva, 305, 1978., v. 12, p. 306, *apud* PITOMBO, Cleunice Valentim Bastos. *Da Busca e da Apreensão no Processo Penal*. São Paulo: Editora Revista dos Tribunais, 1999.

GRAY, David. *The Fourth Amendment in an Age of Surveillance.* Cambridge: Cambridge University Press, 2017.

GRECO FILHO, Vicente. *Interceptação telefônica (considerações sobre a lei nº 9.296 de 24 de julho de 1996)*. São Paulo: Editora Saraiva, 1996.

GRINOVER, Ada Pellegrini; FERNANDES, Antônio Scarance; GOMES FILHO, Antônio Magalhães. *As nulidades no processo penal*. 7.ed. São Paulo: Editora RT, 2001

_____. *O regime brasileiro das interceptações telefônicas.* Revista de Direito Administrativo. Rio de Janeiro, 207, jan/mar., 1997.

_____. *Liberdades públicas e processo penal – as interceptações telefônicas.* 2ª edição, São Paulo: Editora Saraiva, 1982.

_____. *Lineamentos gerais do novo processo penal na América Latina.* Revista de Processo. São Paulo, v. 15, n. 58, p. 134, 1990, *apud* FERNANDES, Antônio Scarance. *Equilíbrio entre a eficiência e o garantismo*. Revista Brasileira de Ciências Criminais n.º 70/229, jan-fev/2008.

GUARDIA, Gregório Edoardo Raphael Selingardi. *Comunicações Eletrônicas e dados digitais no processo penal*. Tese (Mestrado em Direito Processo Penal) – Faculdade de Direito, Universidade de São Paulo, 2016.

HUTCHINS, Renée McDonald, *Tied Up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L. Rev. 409, 444, 2007.

JESUS, Francisco Marcolino. *Os Meios de Obtenção da Prova em Processo Penal*, 2.ª edição, Coimbra: Editora Almedina, 2015.

JEZLER JÚNIOR, Ivan. *Prova penal digital: tempo, risco e busca telemática.* Florianópolis: Editora Tirant lo Blanch, 2019.

KERR, Orin S. *An Equilibrium-Adjustment Theory of the Fourth Amendment.* 125 Harvard Law Review 476. 2011.

_____. *Applying the Fourth Amendment to the Internet: A General Approach*. Vol. 62: 1005 Stanford Law Review, 2010.

_____. *Digital Evidence and The New Criminal Procedure. Digital Evidence and the New Criminal Procedure.* 105 Columbia Law Review 279 (2005). Disponível em https://ssrn.com/abstract=594101. Acesso em 20 de dezembro de 2020.

_____. *Fernandez v. California and the problem of third-party consent*. 2013, Disponível em: <https://www.scotusblog.com/2013/11/fernandez-v-california-and-the-problem-of-third-party-consent/> . Acesso em: 20 de dezembro de 2020

_____. *Fourth Amendment Seizures of Computer Data*. 119 Yale Law Journal 700 (2010).

KIST, Dario José. *Prova digital no processo penal.* Leme: Editora JHMizuno, 2019.

KNIJNIK, Danilo. *A trilogia Olmstead-Katz-Kyllo: o art. 5º da Constituição Federal do século XXI.* Revista Escola da Magistratura do TRF da 4ª Região, ano 2, número 4. Porto Alegre/RS, 2016.

LANGER, Maximo. *From Legal Transplants to Legal Translations: The Globalization of Plea Bargaining and the Americanization Thesis in Criminal Procedure*. In Harvard International Law Journal. v. 45. n. 01, 2004.

LASH, Scott. *Crítica de la información*. Buenos Aires: Editora Amorrortu, 2005.

LEMOS, Bruno Espiñeira; CALDEIRA, Felipe Machado. *Delação premiada de acusado preso*. In: LEMOS, Bruno Espiñeira; CALDEIRA, Felipe Machado (Org.). Delação premiada: estudos em homenagem ao ministro Marco Aurélio de Mello. Belo Horizonte: Editora D´Plácido, 2016.

LEONARDI, Marcel. *Responsabilidade Civil dos Provedores de Serviços de Internet*. São Paulo: Editora Juarez de Oliveira, 2005.

_____. *Tutela e Privacidade na Internet*. São Paulo: Editora Saraiva, 2012.

LIMA, Renato Brasileiro. *Manual de Processo Penal.* São Paulo: Editora Juspodivm, 2020.

LOMBARDO, Luigi, *Profili delle prove civile atipiche*, Rivista trimestrale di diritto e procedura civile, Milano, A. LXIII, n.º 4, Diciembre 2009.

LOPES, Anderson Bezerra. *Os conhecimentos fortuitos de prova no direito processual penal.* Dissertação (Mestrado em Direito Processual Penal) - Faculdade de Direito da Universidade de São Paulo, 2013.

LOPES JR., Aury. *Direito Processual Penal.* São Paulo: Saraiva, 2020.

LÓPEZ, Juan José Gonzalez. *Los datos de tráfico de las comunicaciones electrónicas em el proceso penal.* Madrid: La Ley, 2007.

LUPARIA, Luca; ZICCARDI, Giovanni. *Investigazione penale e tecnologia informatica: L'accertamento del reato tra progresso scientifico e garanzie fondamentali.* Milano: Editora Giuffrè, 2007.

MAIER, Julio B. J. *Derecho Procesal Penal. Tomo I: Fundamentos*. 3ª edição, Buenos Aires: Editores del Puerto, 2004.

MARANHÃO, Juliano. *O acesso ao WhatsApp pela operação Lava Jato*. Disponível em <http://jota.info/artigos/o-acesso-ao-whatsapp-pela-operacao-lava-jato-05122016>. Acesso em 20 de dezembro de 2020.

_____. *O que é dado não é comunicado?* In: ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. I. São Paulo. Internet Lab, 2018.

MACHADO, André Augusto Mendes; KEHDI, André Pires de Andrade. *Sigilo das comunicações e de dados.* In: FERNANDES, Antônio Scarance; ALMEIDA, José Raul

Gavião de; MORAES, Maurício Zanoide de. *Sigilo no processo penal: eficiência e garantismo.* São Paulo: Editora RT, 2008.

MACHADO, Vitor Paczek; JEZLER JUNIOR, Ivan. *A prova eletrônica-digital e a cadeia de custódia das provas: uma (re)leitura da Súmula Vinculante 14*. Boletim IBCCRIM, São Paulo, ano 24, nº 288, nov./2016.

MAGALHÃES, Vlamir Costa. *Ilicitude probatória em processo penal e regra de exclusão (exclusionary rule): comentários sobre a legitimidade do acesso a aparelhos eletrônicos apreendidos em situação flagrancial*. Direito Federal: Revista da AJUFE. São Paulo, v. 31, n. 97, jan./jun. 2019.

MARÍN, Fernando Rodríguez. *Los delitos de escuchas ilegales y el derecho a la intimidad. Anuario de Derecho Penal y Ciencias Penales,* Madrid, t. XLIII, Fasc/Mes 1, 1990.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. *Prova*. 2ª edição, São Paulo: Editora RT, 2011.

MARQUES, José Frederico. *Elementos de Direito Processual Penal.* 3ª Atualização, vol. II, Campinas: Millenium Editora, 2009.

MARQUES, Pedro Campanholo. *Busca e apreensão: juízo de admissibilidade.* Florianópolis: Editora Tirant Lo Blanch, 2019.

MARTINS, Leonardo (org.) *Cinquenta anos de Jurisprudência do Tribunal Constitucional Federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de Direito Constitucional*. 13ª Edição, São Paulo: Editora Saraiva, 2018.

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. Volume 1. São Paulo: Editora Saraiva, 2015.

MENDES, Carlos Hélder Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software.* São Paulo: Editora Juspodivm, 2020.

MENDES, Laura Schertel Ferreira. *Habeas data e autodeterminação informativa: os dois lados da mesma moeda*. Direitos Fundamentais & Justiça, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018.

_____. *Uso de softwares espiões pela polícia: prática legal?*, disponível em: www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espioes-pela-policia-pratica-legal-04062015. Acesso em: 20 de dezembro de 2020.

MENDONÇA, Andrey Borges de. *Os benefícios possíveis na colaboração premiada: entre a legalidade e a autonomia da vontade*. In: MOURA, Maria Thereza de Assis; BOTTINI, Pierpaolo Cruz (Coord.). Colaboração premiada. São Paulo: Editora Revista dos Tribunais, 2017.

_____. *Prova documental no processo penal: aspectos relevantes e controvertidos.* In: SALGADO, Daniel Resende. KIRCHER, Luis Felipe Schneider. QUEIROZ, Ronaldo Pinheiro. *Altos Estudos sobre a prova no processo penal*. São Paulo: Ed. Juspodium, 2020.

MENEZES, Isabela Aparecida; BORRI, Luiz Antônio; SOARES, Rafael Júnior. *A quebra da cadeia de custódia da prova e seus desdobramentos no processo penal brasileiro.* Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 4, n. 1, jan.-abr. 2018.

MESQUITA, Paulo Dá. *Processo Penal, Prova e Sistema Judiciário*, Coimbra: Editora Coimbra (Wolters Kluwer), 2010.

MESQUITA, Márcio Satalino. *A busca e apreensão na investigação e prova dos crimes cibernéticos.* In: Brasil. Tribunal Regional Federal da 3ª Região. Escola de Magistrados. Investigação e prova nos crimes cibernéticos. São Paulo: EMAG, 2017.

MONCAU, Luiz; LEMOS, Ronaldo; BOTTINO, Thiago. *Projeto de Lei de Cibercrimes: há outra alternativa para a internet brasileira?* Revista de Direito Administrativo – RDA, Belo Horizonte, ano 2008, n. 249, set.-dez. 2008.

MONTEIRO, Renato Leite. *Da Proteção aos Registros, aos dados pessoais e às comunicações privadas*. In: MASSO, Fabiano del et al. (Coord.). Marco Civil da Internet. São Paulo: Revista dos Tribunais, 2014.

MONTEIRO, Washington de Barros. *Curso de Direito Civil – Parte Geral.* 39ª Edição, São Paulo: Editora Saraiva, 2003.

MOORE, Jennifer L.; LANGTON, Jonathan; POCHRON, Joseph. *The cost of privacy: Riley v. California's impact on cell phone searches,* JDFSL, vol. 9, number 3.

MORAES, Alexandre de. *Direito Constitucional.* 28ª edição, São Paulo: Editora Atlas, 2012.

MORAES, Maurício Zanoide de. *Presunção de inocência no processo penal brasileiro: análise de sua estrutura normativa para elaboração legislativa e para a decisão judicial.* Rio de Janeiro: Editora Lumen Juris, 2012.

MOREIRA, Rômulo de Andrade. *A nova lei que permite a infiltração de agentes na investigação criminal.* In: SIDI, Ricardo, LOPES, Anderson Bezerra (org.) Temas atuais da investigação preliminar no processo penal. Belo Horizonte: Editora D' Plácido.

MORO, Sérgio Fernando. *Direito fundamental contra o crime*. In: CLÈVE, Clèmerson Merlin. Direito Constitucional brasileiro: teoria da Constituição e direitos fundamentais. São Paulo: Revista dos Tribunais, 2014.

MOURA, Maria Thereza Rocha de Assis. *Interceptação Telefônica e Telemática na Jurisprudência Brasileira.* In: AMBOS, Kai; ROMERO, Eneas (org.). Crime Organizado: Análise da Lei n.º 12.850/2013. São Paulo: Editora Marcial Pons, 2017.

_____; BARBOSA, Daniel Marchionatti. *Dados digitais: interceptação, busca e apreensão e requisição.* In: LUCON, Paulo Henrique dos Santos; WOLKART, Erik

Navarro. LAUX, Francisco de Mesquita; RAVAGNANI, Giovani dos Santos. *Direito, processo e tecnologia.* São Paulo: Editora RT, 2020.

NERY JUNIOR, Nelson; NERY, Rosa Maria de Andrade. *Constituição Federal comentada e legislação constitucional.* 2ª edição, São Paulo: Editora RT, 2009.

NIETZSCHE, Friedrich. *Ecce homo: como alguém se torna o que é*. Traduzido por Artur Morão. Covilhã: Editora Lusosofia, 2008. Disponível em: <http://www.lusosofia.net/textos/nietzsche_friedrich_ecce_homo.pdf>. Acesso em: 3 de julho de 2020.

OWEN, Paul; THOMAS, Paula; MCPHEE, Duncan. *An analysis of the Digital Forensic Examination of Mobile Phones.* 2010. In: Fourth International Conference on Next Generation Mobile Applications, Services and Technologies (Disponível em: <https://www.researchgate.net/publication/221328104_An_Analysis_of_the_Digital_Forensic_Examination_of_Mobile_Phones>. Acesso em: 20 de dezembro de 2020.

PACELLI, Eugenio. *Curso de processo penal*. 19. ed. rev. atual. São Paulo: Editora Atlas, 2015.

PANNAIN, Remo. *Manuale di diritto penale: parte generale*. Torino: 1967, p. 649. *Apud* COSTA, Álvaro Mayrink. Direito penal: parte geral. v. 1., tomo II. 6ª ed. Rio de Janeiro: Editora Forense, 1998.

PASCHOAL, Jorge Coutinho. *Caso Riley v. California (Suprema Corte dos Estados Unidos da América) – o acesso aos dados registrados em aparelhos de telefonia móvel e o resguardo da intimidade*. Revista Fórum de Ciências Criminais (RFCC), v. 4, 2015.

PÉREZ ESTRADA, Miren J. *La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información.* Revista Brasileira de Direito Processual Penal, vol. 5, n. 3, set./dez. 2019.

PINHEIRO, Patrícia Peck. *Direito Digital*. 3ª ed. São Paulo: Saraiva, 2009.

PINTO PALACIOS, Fernando. PUJOL CAPILLA, Purificación. *La prueba en la era digital.* 1ª Edicion. Madrid: Editora Wolters Kluwer, 2017.

PITOMBO, Cleunice Valentim Bastos. *Da Busca e da Apreensão no Processo Penal*. São Paulo: Editora Revista dos Tribunais, 1999.

PITOMBO, Sérgio Marcos de Moraes. *Do sequestro no processo penal brasileiro.* São Paulo: Editora Bushatsky, 1993.

_____. *Sigilo nas comunicações. Aspecto processual penal.* Boletim IBCCrim, São Paulo, n. 49, p. 7-8. dez. 1996.

POSNER, Richard. A. *Not a Suicide Pact.* New York: Oxford University Press, 2006.

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

_____. *Ainda sobre a quebra da cadeia de custódia das provas*, Boletim IBCCRIM, São Paulo, ano 22, n.º 262, setembro de 2014.

_____. *Limite às interceptações telefônicas e a jurisprudência do Superior Tribunal de Justiça*. 2ª edição, Rio de Janeiro: Editora Lumen Juris, 2006.

_____. *Prova Penal e sistema de controles epistêmicos: a quebra da cadeia de custódia das provas obtidas por meios ocultos*. São Paulo: Editora Marcial Pons, 2014

QUEIJO, Maria Elizabeth. *O direito de não produzir prova contra si mesmo*. São Paulo: Editora Saraiva, 2003.

QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Pedigone. *Tércio Sampaio Ferraz Júnior e sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do estado: o que permanece e o que deve ser reconsiderado*. Internet & sociedade. N.1., volume 1, fevereiro de 2020. Disponível em <https://revista.internetlab.org.br/tercio-sampaio-ferraz-junior-e-sigilo-de-dados-o-direito-a-privacidade-e-os-limites-a-funcao-fiscalizadora-do-

estado-o-que-permanece-e-o-que-deve-ser-reconsiderado/>. Acesso em 20 de dezembro de 2020).

QUINTIERI, Victor Minervino; MOURA, Humberto Fernandes de. *As (i)legalidades no processo penal: breve reflexão a respeito do 'WhatsApp' a partir da lei 9.296/1996 – um estudo de caso.* In: FREITAS FILHO, Roberto; VELOSO FILHO, José Carlos (org.). Cadernos jurídicos temáticos. Direito do Consumidor e Direito Penal. Brasília: UNICEUB, 2016.

QUITO, Carina. *As quebras de sigilo telemático no processo penal.* In: LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro. LAUX, Francisco de Mesquita; RAVAGNANI, Giovani dos Santos. Direito, processo e tecnologia. São Paulo: Editora RT.

RAMALHO, David Silva. *Métodos Ocultos de Investigação*. Coimbra: Editora Almedina, 2017.

RAMOS, Armando Dias. *A prova digital em processo penal: o correio eletrônico*. Lisboa: Editora Chiado, 2014.

RANGEL, Paulo. *Breves considerações sobre a Lei n.º 9.296/1996: interceptação telefônica.* Revista Brasileira de Ciência Criminais, São Paulo, v. 7, n. 26, p.143-151, abr./jun. 1999.

RASSAT, Michèle-Laure. *Procédure pénale*, 3e édition, Paris: Editora Ellipses, 2017.

RESTA, Giorgio. *Revoca del consenso ed interesse al tratamento nella legge sulla protezione dei dati personali,* In: Rivista Critica del Diritto Privado, 200, p. 307, *apud* DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 2ª ed. São Paulo: Editora. RT, 2019.

RICHARDS, Neil M. *The Dangers of Surveillance,* 126 Harvard Law Review, 2013.

RIGAUX, François. *La protection de la vie privée et des autres biens de la personnalité*. Bruylant: Bruxelles, 1990, p. 588-589, n.º 532.

RICCI, Gian Franco. *Le Prove atipiche.* Milano: Editora Giuffrè, 1999.

RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. (Org.) MORAES, Maia Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RODRIGUES, Benjamim Silva. *Das Escutas Telefónicas à Obtenção de Prova (Em Ambiente) Digital: a monitorização dos fluxos informais e comunicacionais*, Tomo II, Coimbra: Editora Coimbra, 2009.

_____. *Da prova penal: Tomo II – Bruscamente...a(s) face(s) oculta(s) dos métodos ocultos de investigação criminal.* Lisboa: Editora Rei dos Livros, 2010.

ROMERO COLOMA, Aurelio. *Estudios de la prueba procesal,* Madrid; Editora Colex, 1986.

ROVIRA DEL CANTO, Enrique. *Delincuencia informática y fraudes informáticos.* Granada: Editora Comares, 2002.

ROXIN, Claus. *Derecho Procesal Penal.* Buenos Aires: Editores del Puerto, 2003.

SAAD, Marta Cristina Cury. *Defesa no inquérito policial.* Revista de Direito de Polícia Judiciária, Brasília, ano 2, n. 4, p. 67, jul-dez de 2018

_____. *O direito de defesa no inquérito policial*. São Paulo: Editora Revista dos Tribunais, 2004.

SALT, Marcos G. *Tecnología informática: um nuevo desafio para el Derecho Procesal Penal?* 1ª ed. Bueno Aires: Ad-hoc, 2017, p. 7, *apud* MENDES, Carlos Hélder Furtado. Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software, São Paulo: Editora Juspodivm, 2020.

SALTZBURG, Stephen A, SCHLUETER, David A. *Federal Criminal Procedure Litigation Manual,* Huntington, New York: Editora Juris, 2015.

SAMPAIO, José Adércio Leite. *Direito à intimidade e à vida privada*. Belo Horizonte: Editora Del Rey, 1998.

SANNINI NETO, Francisco. *Dados de telefone celular apreendido podem ser vasculhados em investigação criminal*. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 21, n. 4762, 15 de julho de 2016. Disponível em: <https://jus.com.br/artigos/40053/investigacao-criminal-e-os-dados-obtidos-de-aparelhos-de-celular-apreendidos>. Acesso em: 20 de dezembro de 2020.

SARAIVA, Wellington Cabral. *Obtenção de prova decorrente de agente infiltrado.* In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro de (Org.). A prova no enfrentamento à macrocriminalidade. Salvador: Editora JusPodivm, 2019.

SCHULHOFER, Stephen J. *More Essential Than Ever. The Fourth Amendment in the Twenty-first Century.* Oxford University Press, 2012.

SCHÜNEMANN, Bernd. *La Reforma del Proceso Penal*. Madrid: Editora Dykinson, 2005.

SHOEBOTHAM, Leslie A. *The Strife of Riley: The Search-Incident Consequences of Making an Easy Case Simple.* Loyola University New Orleans College of Law, 75 La. L. Rev. 29 (2014).

SIDI, Ricardo. *A interceptação de e-mails e a apreensão física de e-mails armazenados*. Revista Fórum de Ciências Criminais – RFCC, Belo Horizonte, ano 2, n. 4, p. 101-121, jul./dez. 2015.

SILVA, José Afonso da. *Comentário contextual à Constituição*. São Paulo: Editora Malheiros, 2006.

_____. *Curso de Direito Constitucional Positivo*. 29. edição, São Paulo: Editora Malheiros, 2007.

SILVA, Viviane Ghizoni da; MELO E SILVA, Philipe Benoni; MORAIS DA ROSA, Alexandre. *Fishing Expedition e Encontro Fortuito na Busca e Apreensão*. Florianópolis: Editora Emais, 2019.

SILVA, Gabriela Buarque Pereira; MOURA, Tâmara. *Prisão em flagrante e acesso a dados de celular: deságios entre a privacidade e a investigação criminal.* In: ARAS, Vladimir Barros; MENDONÇA, Andrey Borges de; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira da; COSTA, Marcos Antônio da Silva. Proteção de dados pessoais e investigação criminal. Associação Nacional do Procuradores da República, 3ª Câmara de Coordenação e Revisão. Brasília: ANPR, 2020.

SILVA JÚNIOR, Walter Nunes. *Curso de direito processual penal: teoria (constitucional) do processo penal.* Rio de Janeiro: Editora Renovar, 2008, *apud* LIMA, Renato Brasileiro. Manual de Processo Penal. São Paulo: Editora Juspodivm, 2020.

SIMAS SANTOS, Manoel. LEAL HENRIQUE, Manuel. *Código de Processo Penal Anotado*, 3.ª edição, 2008, volume I, pág. 832, *apud* Supremo Tribunal de Justiça, Processo n.º 149/07.9 JELSB.E1.S1, 3ª Secção, Rel. Raul Borges, julgado em 14 de julho de 2010.

SOARES, Gustavo Torres. *Investigação criminal e inovações técnicas e tecnológicas: perspectivas e limites.* Tese (Doutorado em Direito Processual Penal) - Faculdade de Direito da Universidade de São Paulo, 2014.

SOARES, Paulo Vinícius de Carvalho. *A Diluição das Esferas de Privacidade e de Intimidade diante da Era dos Dados.* In: LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro. LAUX, Francisco de Mesquita; RAVAGNANI, Giovani dos Santos. Direito, processo e tecnologia. São Paulo: Editora RT, 2020.

SOUSA, Marllon. *Busca Pessoal v. Stop and Frisk: um breve exame sobre a abordagem policial de rua no Brasil e nos EUA*. Revista Brasileira de Ciências Criminais, vol. 151/2019, jan./2019, p. 317-343.

SOUZA, Gilson Sidney Amancio de. *Princípio da indenidade ou da Higidez da Prova.* In: HAMMERSCHMIDT, Denise (Org.). Código de Processo Penal Comentado. Curitiba: Editora Juruá, 2020.

SOUZA, Rodrigo Telles de. *A exigência de autorização judicial para acesso ao conteúdo de telefone móvel apreendido: uma ampliação da garantia à inviolabilidade domiciliar incompatível com o sistema jurídico brasileiro.* In: SALGADO, Daniel Resende. KIRCHER, Luis Felipe Schneider. QUEIROZ, Ronaldo Pinheiro. Altos Estudos sobre a prova no processo penal. São Paulo: Ed. Juspodium, 2020.

STARR, Adriana Galvão. *A dificuldade de acesso ao conteúdo das mensagens ilícitas trocadas via WhatsApp para uso em procedimento de investigação e ação penal.* In. Caderno de Estudos de Investigação e prova nos crimes cibernéticos, da Escola de Magistrados da Justiça Federal da 3ª Região, São Paulo: 1ª edição, 2017.

STEINMETZ, R. WEHRLE, K. *Peer-to-Peer Systems and Applications. Lecture Notes in Computer Science*, vol. 3485. Springer, Berlin: Heidelberg.

STRECK, Lênio. *Sigilo de correspondência e comunicações*. Comentário ao art. 5º, XII, da CF. In: CANOTILHO, J.J.; MENDES, Gilmar; SARLET, Ingo; STRECK, Lênio (Coord.). Comentários à Constituição do Brasil. São Paulo: Saraiva/Almedina, 2013.

STUNTZ, William J. *Secret Service: Against Privacy and Transparency.* The New Republic, April 17, 2006.

SYDOW, Spencer Toth. *Crimes informáticos e suas vítimas*. São Paulo: Editora Saraiva, 2015.

TADDICKEN, Monika. "*The 'Privacy Paradox'in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure*". Journal of Computer-Mediated Communication, 19 (2014) 248–273. Disponível em: < https://academic.oup.com/jcmc/article/19/2/248/4067550>. Acesso em 3 de julho de 2020.

TARUFFO, Michele. *La prova dei fatti giuridici*. Milano: Editora Giuffrè, 1992.

TAVARES, Letícia Antunes; ALVAREZ, Bruna Acosta. *Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil*. In: ONODERA, Marcus Vinicius Kiyoshi; FILLIPO, Thiago Baldani Gomes de. (Org.). Brasil e EUA: Temas de Direito Comparado. 1ª edição. São Paulo: Escola Paulista da Magistratura, 2017.

TEBET, Diogo. *Inadmissibilidade da gravação telefônica e ambiental clandestina: da necessária revisão da jurisprudência do Supremo Tribunal Federal* In. SIDI, Ricardo, LOPES, Anderson Bezerra (org.) Temas atuais da investigação preliminar no processo penal. Belo Horizonte, Editora. D' Plácido, 2017.

TEIXEIRA, Tarcísio. *Curso de direito e processo eletrônico: doutrina, jurisprudência e prática*. 3ª edição. São Paulo: Editora Saraiva, 2015.

THAMAY, Rennan; TAMER, Mauricio. *Provas no direito digital. Conceito da prova digital, procedimentos e provas digitais em espécie.* São Paulo: Editora RT, 2020, p. 33

THEOHARIDOU, Marianthi; MYLONAS, Alexios; GRITZALIS, Dimitris. *A Risk Assessment Method for Smartphones. 27th Information Security and Privacy Conference (SEC)*, Jun 2012, Heraklion, Crete, Greece.

TOKSON, Matthew. *Knowledge and Fourth Amendment Privacy*. Vol. 111, n.1, Northwestern University Law Review.

TONINI, Paolo. *Manuale di Procedura Penale,* Undicesima edizione, Milano: Editora Giuffè, 2010.

TONINI, Paolo. CONTI, Carlotta. *Il diritto delle prove penali*. 1ª *edizione aggiornata,* Milano: Editora Giuffrè, 2011.

TORNAGHI, Hélio. *Curso de processo penal*. 7ª. Ed. São Paulo: Editora Saraiva, 1990.

TOURINHO FILHO, Fernando da Costa. *Processo Penal.* 33ª edição. São Paulo: Editora Saraiva, 2011.

TUCCI, Rogério Lauria. *Direitos e garantias individuais no processo penal brasileiro*. São Paulo: Editora Saraiva, 1993.

VACCA, John. R. *Computer Forensics: Computer Crime Scene Investigation.* Second Edition, Charles River Media.

VACIAGO, Giuseppe; RAMALHO, David Silva. *Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings,* Digital Evidence and Electronic Signature, Law Review, 13 (2016).

VALIENTE, Luis M. PIAY, Tomás Farto. *El proceso penal español: jurisprudencia sistematizada.* Madrid: Editora La Ley, 2007.

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

VECCHIA, Evandro Dalla. *Perícia Digital: Da investigação à análise forense.* Campinas: Editora Millenium, 2ª edição, 2019.

VIANNA, Túlio Lima. *Transparência pública, opacidade privada: o Direito como instrumento de limitação do poder na sociedade de controle.* Tese (Doutorado em Direito) – Faculdade de Direito da Universidade Federal do Paraná, Curitiba, 2006.

VIANNA, Túlio Lima; MACHADO, Felipe. *Crimes informáticos*. Belo Horizonte: Editora Fórum, 2013.

VIEIRA, Renato Stanziola. *Dados cadastrais na Lei n.º 12.850/2013.* In: AMBOS, Kai; ROMERO, Eneas (Org.). Crime organizado: análise da Lei 12.850/2013. 1ª Ed, São Paulo: Editora Marcial Pons, 2017.

WANDERLEY, Gisela Aguiar. *Privacidade e Cidadania: os limites jurídicos da atividade investigativa e a legalidade do acesso policial a aparelhos celulares*, disponível em <https://www.internetlab.org.br/wpcontent/uploads/2019/08/InternetLabCongressoII_simples.pdf>. Acesso em: 20 de dezembro de 2020.

WARREN, Samuel Dennis; BRANDEIS, Louis Dembitz. *The Right to Privacy*, Harvard Law Review, Vol. IV, n. º 5, 1890.

WINN, Peter. *Katz and the Origins of the "Reasonable Expectation of Privacy"* Test. 40 McGeorge L. Rev. (2016). Disponível em https://scholarlycommons.pacific.edu/mlr/vol40/iss1/1. Acesso em: 20 de dezembro de 2020.

ZANINI, Leonardo Estevam de Assis. *O surgimento e o desenvolvimento do right of privacy nos Estados Unidos*. Revista Brasileira de Direito Civil. Vol. 3, Jan/Março 2015.

ZAWOAD, Shams; HASAN, Ragib. *Digital forensics in the cloud*. CrossTalk. The Journal of Defense Software Engineering, September/October 2013.

ZICCARDI, Giovanni. *Informatica giuridica. 2: Privacy, sicurezza informatica, computer forensics e investigazioni digitali.* Milano: Editora Giuffrè, 2008.

ZILLI, Marcos Alexandre Coelho. *A iniciativa instrutória do juiz no processo penal.* São Paulo: RT, 2003.

_____. *A prisão em flagrante e o acesso de dados em dispositivos móveis. Nem utopia, nem distopia. Apenas a racionalidade.* In: ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. I. São Paulo. InternetLab, 2018.

_____. *O Pomar e as Pragas*. Boletim do IBCCrim, n.º 188, julho/2008.

_____. *Resquícios Inquisitórios na Lei 9.034/1998*. *In*: Revista Brasileira de Ciências Criminais. Bimestral, ano 12 n° 46, jan-fev 2004.